Effective key management privacy for accessing health data with auditability in cloud service

Packialatha A
Department of Information Technology, Jeppiaar Engineering College, Chennai, Tamilnadu, India
***Corresponding author: E-Mail:packiafluffy@gmail.com**

ABSTRACT

In cloud storage, E-health data can be stored .so that we accessing e-health data from anywhere at any time all around the world. This data will be conserved by third party, such as data owner. Determining the privacy issues in shortening the adoption of electronic health care system and success of cloud service models, we propose to develop privacy into health care system with auditability. Our system proposals significant features as well as effective key management privacy conserving storage and recovery of data and auditability for maltreating health data. Specially, we propose to combine key management for unlinkability, for hiding both such and access patterns securable indexing method is used based on redundancy and finally we integrated the concept of searchable Symmetric Encryption together with auditability to avoid possible misbehaving activities in both normal and emergency cases.

KEY WORDS: Cloud Computing, E-Health Data, Searchable Symmetric Encryption, Privacy.

1. INTRODUCTION

Storing data in the cloud has turn into an approach. An increasing number of clients stores their important data in remote servers in the cloud, without maintaining even a copy in the local computers. In recent years, e-health care system has emerged as a patient-centric sculpt of health information reinstate. A healthcare service allows a patient to create, manage, and control their health data in one place through the web, which has made the storage retrieval and distribution of the medical information more competent. But many healthcare services are outsourced to or provided by third-party service providers due to the high cost of building and maintaining specialized data centres.

As a famous incident, a Department of Veterans association's record containing receptive PHI of 26.5 million martial veterans, including their social security records and health struggle was stolen by an employee who took the data home without any approval. In order to protect the health data stored on a server, we adopt searchable symmetric encryption (SSE) as the main encryption primitive. SSE permits data owners to store the encrypted documents on remote server, patterned as honest-but-keen party, and provides a way in a concurrent manner to search over the encrypted documents. More outstandingly, neither outsourcing nor keyword searching operation would result in several information outflow to any parties other than the data owner, hence attaining a wide ranging assurance of privacy. In this paper, a new type of encryption technology (SSE) is propose for secure sharing of E-health in cloud computing environments, under the data-owner settings.

To address the key management challenges, the customers are separated in the system into two types of domains, namely *public* and *personal domains*. In the public domain, the multi-authority SSE is used to improve the security and avoid key escrow problem.

In this paper a new mechanism is proposed for key distribution and encryption so that e-health data owners can specify fine-grained access policies during encryption of files. In the domain, owners directly access privileges for personal users and encrypt a E-health data. Furthermore, we enhance SSE by putting forward an efficient and on-demand index and trapdoor keyword searching scheme, and show its refuge under standard security suppositions. In this approach, patients have complete privacy control over their E-Health data. The rest of the paper is organized as follows. Section II discusses some related work in security methods for E-health data. Section III presents the overview of Frame work for E-Health data. Section IV describes about the particulars of future Framework. Section V gives the conclusion.

Related Work: A number of works have been done to enforce the security problem on the area of health data in Cloud Computing Environment. This section lists some of these works .Some untimely works on seclusion protection for e-health data concentrate on the design including the demo of the significance of privacy in e-health systems, the authentication based on existing wireless infrastructure, the role based approach for access restrictions. Mostly, identity-based encryption has been used for enforcing simple cryptographic access control. There is also a huge body of research works on preservation of authentications accessing data and allocation of rights in e-health systems. Preservation of privacy in health data storage is studied by Sun *et al.*[1], where patients to encrypt their own physical condition records and store it on a third-party server. This work and Searchable Symmetric Encryption (SSE) schemes are most relevant to this paper.

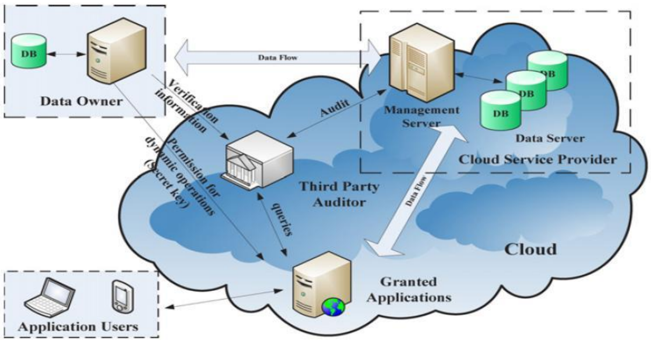
The proposed health data storage in cloud intimates the challenges that have not been solved in the previous works. The retrieving and storing mechanisms in for emergency access rely on something the patient trusts whose availability cannot be guaranteed every time. Likewise, the storage privacy proposed in is pathetic form of privacy because it does not hide search and accessing patterns. The previous research works failed to address the challenges in privacy of data, we aim to overcome in this paper. Finally, we also remark that there are other cryptographic techniques for preserving privacy access of health data stored in a cloud environment. The proposed scheme also has salient properties of user access privilege confidentiality and user secret key liability. Widespread analysis shows that our proposed scheme is highly efficient and provably secures under existing security models.

Health data Framework: This section describes about the patient-centric secure data sharing frame work for cloud based Ehealth systems.

Problem Definition: The authenticity of the attributes cannot be verified which a very practical problem is and highly challenging in the proposed health data problems, where the set of attributes is well-defined for each role (e.g., physician, electronic medical technician, and assurance provider) that will access the data. However, it does not provide any mechanism for audit-ability, i.e., to record and prove that an authorized party has accessed certain data. Without audit-ability, it is not possible to identify the source of breach if authorized parties illegally distribute the health data.

System and Threat Models

System model: The key units implicated in our system are portrayed below



Audit system architecture for cloud computing.

Figure.1.Audit system architecture for cloud computing

Users gathers health data from EMT[who performs emergency treatment] by sending queries about their diseases. Cloud ihe infrastructure owned by cloud providers like amazon and google which advances more storage and high computing power. Every user informations are stored in the cloud by trusted party data-owner. Cloud are at all time online and accessible of health data by users are made very easy. this can be suitable for any situations. With the help of auditors we can easily drag maltreaters. auditor plays a key role here.

Threat Model: Cloud is fully trusted by user to perform health data computations. they are assumed to be honest-but-keen, in that it wont prune or change any user informations but it will challenge to concile oue privacy. EMT allowed access rights to the data which are related to the treatment. They also effort to compensate our privacy issues by accessing his/her datas are not authorised to. Auditors are available to find out unauthorised users and EMT ,this makes the system further more securable.

Requirements: To achieve *patient-centric*‖ ehealth data sharing, a core requirement is that each patient can control who are authorized to access to their own e-health data documents. The security and performance requirements are as follows:

a)Data confidentiality: Unauthorized users (including the server) who do not possess enough attributes gratifying the way in policy or do not have proper key right of entry privileges should be prevented from decrypting a e-health data document, even under user collusion. Fine-grained access control should be imposed, means many users are authorized to read different sets of documents.

b) Scalability and Efficiency: The ehealth care system should support users from both the personal and public domains. then the set of users from the public domain may be large in size and volatile, the system should be vastly scalable, in terms of complexity in key management, computation power and storage. The data Owner's efforts in managing users and keys should be minimized to enjoy usability.

c) Anonymity: The storage and retrieval process can't be associated with any particular user, i.e., the process should be anonymous

d)Unlinkability:Multiple data files should not be linked by unauthorised parties to the user profile. It indicates the file identifiers should seems to be random and leak no beneficial information

e) Search pattern privacy: Determines the searches were for the identical keyword or not, and the accessing scheme. This requirement is the perplxing and no other existing efficient SSE can satisfy it. Stronger privacy which is needed for applications like health data is represented by SSE.

f) Auditability: In emergency accessing of data, the users may be unable to allow data access or without the perfect reason to choose if the data requester is a genuine EMT. We require authorization to be fine and authorized parties right to use activities to leave a cryptographic evidence

Proposed Framework: Our accessing health data with privacy and auditability in cloud service system contains two components: searchable symmetric encryption and auditable access control. Upon getting the health facts from users, the private cloud processes and stores it on public cloud such that privacy in storing and retrieving of data can be guaranteed. Cloud engages in the bootstrapping of data accessing and auditability with user so that on behalf of user it can later act to carry out access control and auditing on authorized parties.

Technique Used

Searchable symmetric encryption [SSE]: Searchable symmetric encryption (SSE) allows a party to farm out the storage of its data to an extra party (a server) in a safe manner, while upholding the capability to selectively search over it. The participants in a single-user SSE scheme include a client that wants to store a private document collection D = (D1…..,Dn) on an candid but-inquisitive server in such a way that (1) the server will not learn any useful information about the group; and that the server process can be given the ability to search through the collection and return the appropriate (encrypted) documents to the client.

Definition: An index-based SSE scheme over a dictionary Δ is a collection of 5 polynomial equation- time algorithms SSE = (Gen, Enc, Trpdr, Search, Dec) such that,

Steps:

KeyGen (1^k): is a probabilistic key generation algorithm that is sprint by the user to setup the scheme. It takes input as a security factor k, and secret key K as a output.

Encryption (K,D): is a probabilistic algorithm run by the user to encrypt the collected documents. takes input a secret key K and a document collection D = ($D1……,D_n$), and outputs a secure index I and a sequence of ciphertexts c = ($c1……,C_n$).

Trapdoor (K,w): is a deterministic algorithm run by the user to generate a trapdoor for a given keyword. It gets as input a furtive key K and a keyword w, and trapdoor t as an output.S.

Search (I, t): is a deterministic algorithm sprint by the server to look for the documents in D that contain a keyword w. It takes as key an encrypted index I for a data group D and a trapdoor t and outputs a set X of (lexicographically-ordered) document identifiers.

Decryption (K, c_i): is a deterministic algorithm run by the client to recover a document. It gets as input a secret input K and a ciphertext c_i, and outputs a document D_i.

Algorithm

Step1: Registering the user details and identity tokens are generated to the users who are registered only.
Step2: The user take his/her medical data build the secure indexing and trapdoor keyword.
Step3: The specific data will be forward to data owner for encryption process.
Step4: Data owners store the documents in the cloud storage services in the encrypted format based on keywords.
Step5: Generation of distinctive secret key in for every document.
Step6: Cloud stores the data of the data owner in encrypted format.
Step7: User can accessing their data and verify the encrypted file in cloud services using keyword.
Step8: User send request to the EMT to get a solution in online communication.
Step9: EMT will send request to data owner to get the data access on cloud.
Step10: Suggestions provided to the user.
Step11: Authorised users and EMT are checked and auditing report is generated to them.

Levels:

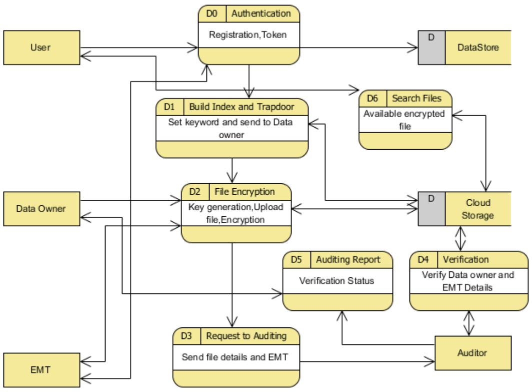
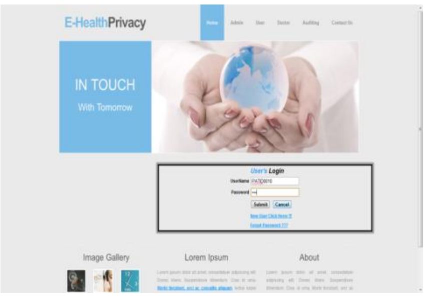


Figure.2.Flowsheet showing the pattern of work flow

Ehealth data Encryption and Access: Patient upload a file by creating securable index and trapdoor keywords.After receiving the file, data owner generate the keys for the uploaded file. Using these key generation, files has been encrypted and stored in a cloud in a well-organised manner. Trapdoor keyword has been used for downloading the encrypted files that stored in cloud and index keyword has been used for decryption purpose.Hence storage and retrival of datas are effectively done. Doctor and patient (User) will be interact on emergency case. User send request to the EMT to get a solution in online communication. EMT will send request to data owner to get the data access on cloud. Verification will take place for EMT to view the user data. the auditor perceives and recognizes the propositions before examining, collects evidence, estimates the same and on this basis formulates his judgement which is communicated through his report. Data Owner directs the auditing request to auditor along with the signatures and details of the file. Then auditor will request for generated proof from cloud storage service in order to do auditing process. Finally data owner will get the audit report. The scalability and efficiency of our solution in terms of storage, communication and computation costs can be evaluated. And can be comparing with previous schemes in terms of size of ciphertext, user secret key, public key/information.

Sample input and output:



UserName: PATID010

Figure.3.User login page

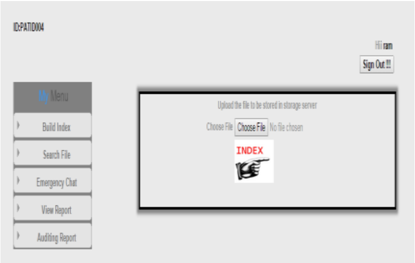
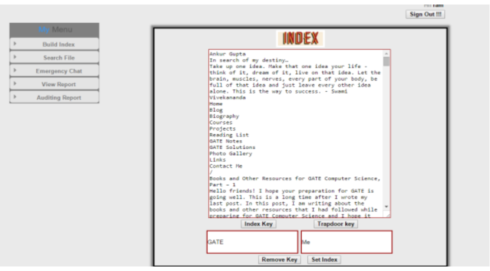


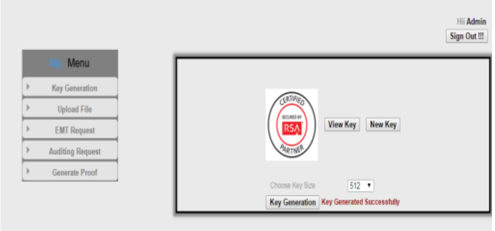
Figure.4.Index page



```
Ankur Gupta
In search of my destiny…
Take up one idea. Make that one idea your life -
think of it, dream of it, live on that idea. Let the
brain, muscles, nerves, every part of your body, be
full of that idea and just leave every other idea
alone. This is the way to success. - Swami
Vivekananda
Home
Blog
Biography
Courses
Projects
Reading List
GATE Notes
GATE Solutions
Photo Gallery
Links
Contact Me
/
Books and Other Resources for GATE Computer Science,
Part - 1
Hello friends! I hope your preparation for GATE is
going well. This is a long time after I wrote my
last post. In this post, I am writing about the
books and other resources that I had followed while
preparing for GATE Computer Science and I hope it
```

Index Key: GATE
Trapdoor key: Me

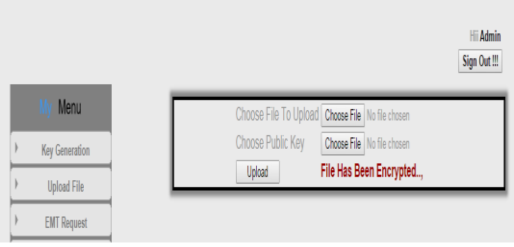
Figure.5.Index keyword build screen



Choose Key Size: 512

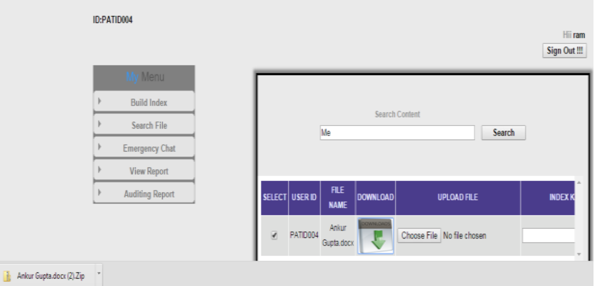
Key Generated Successfully

Figure.6.Key generation screen



File Has Been Encrypted..

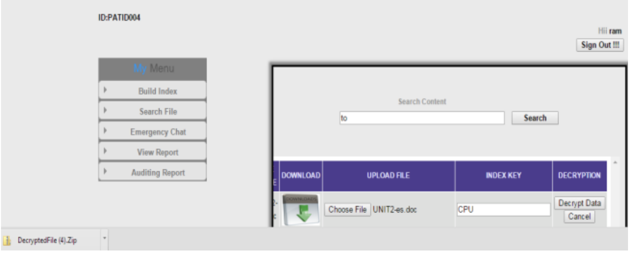
Figure.7.User report encryption



Search Content: Me

SELECT	USER ID	FILE NAME	DOWNLOAD	UPLOAD FILE	INDEX K
☑	PATID004	Ankur Gupta.docx		Choose File No file chosen	

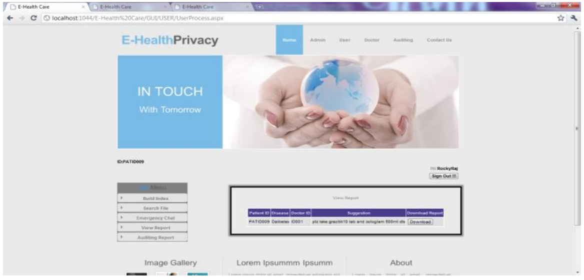
Figure.8. Search Encrypted Trapdoor Keyword



Search Content: to

DOWNLOAD	UPLOAD FILE	INDEX KEY	DECRYPTION
	Choose File UNIT2-es.doc	CPU	Decrypt Data Cancel

Figure.9. Index Keyword for Decryption



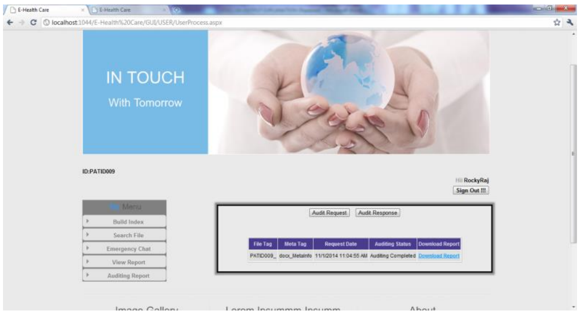
ID:PATID009

Hi RockyRaj

View Report

Patient ID	Disease	Doctor ID	Suggestion	Download Report
PATID009	Daibetes	ID001	plz take grazitk10 tab and cologlam 500ml dis	Download

Figure.10.User Report



ID:PATID009

Hi RockyRaj

File Tag	Meta Tag	Request Date	Auditing Status	Download Report
PATID009_	docx_MetaInfo	11/1/2014 11:04:55 AM	Auditing Completed	Download Report

Figure.11. Received Auditing Report

2. CONCLUSION

The cloud-assisted health networking is inspired by the power, flexibility, convenience, and cost effectiveness of the cloud-based data/computation out sourcing paradigm. Patients shall have complete control of their own privacy through encrypting their files to allow fine-grained access. SSE is used to encrypt the ehealth data, so that patients can agree to right of entry not only by private users, but also various users from public domains with different professional roles, qualifications and affiliations. We also investigated techniques that provide access control (in both normal and emergency cases) and audit-ability of the authorized parties to prevent misbehavior access.

REFERENCES

Sun J, Zhu X, Zhang, and Y. Fang, HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare, in *Proc.* IEEE Int. Conf. Distrib. Comput. Syst., 2011, 373–382.

Mont MC, Bramhall P, and Harrison K, 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.

Boneh D and Franklin M, Identity-based encryption from the Weil pairing. Extended abstract in CRYPTO 2001, SIAM J. Comput., 32(3), 2003, 586–615.

At risk of exposure – in the push for electronic medical records, concern is growing about how well privacy can be safeguarded, 2006.

L¨ohr H, Sadeghi, and Winandy M, Securing the e-health cloud, in Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI '10, 2010, 220–229.

Buyya R, Yeo CS, Venugopal S, Broberg J, and Brandic I, Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility,‖ Future Generation Computer Systems, 25(6), 2009, 599 – 616.

Chang YC and Mitzenmacher M, Privacy preserving keyword searches on remote encrypted data, in Proc. 3rd Int. Conf. Appl. Cryptogr. Netw.Security, 2005, 442–455.

Song D, Wagner D, and Perrig A, Practical techniques for searching on encrypted data, in Proc. IEEE Symp. Security Privacy, 2000, 44–55.

U.S. Department of Health & Human Service, Breaches Affecting 500 or Individuals, 2001.

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

Mont MC, Bramhall P, and Harrison K, 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.