Research Paper

Volume : 2 | Issue : 10 | October 2013 • ISSN No 2277 - 8179

Secure Sharing of Personal Health Records using Multi Authority Attribute based Encryption in Cloud Computing

Engineering

KEYWORDS : Personal Health Records, Cloud Computing, Data Privacy, Fine-grained access control, Multi-authority Attribute Based Encryption

Soumya Parvatikar	Department of Computer Engineering, Bharati Vidyapeeth's College of Engineering for Women, Pune University, Pune-411003, India.
Puja Prakash	Department of Computer Engineering, Bharati Vidyapeeth's College of Engineering for Women, Pune University, Pune-411003, India.
Richa Prakash	Department of Computer Engineering, Bharati Vidyapeeth's College of Engineering for Women, Pune University, Pune-411003, India.
Pragati Dhawale	Department of Computer Engineering, Bharati Vidyapeeth's College of Engineering for Women, Pune University, Pune-411003, India.
S. B. Jadhav	Department of Computer Engineering, Bharati Vidyapeeth's College of Engineering for Women, Pune University, Pune-411003, India.

ABSTRACT

Personal health record (PHR) is often seen as a patient-centric model of health information exchange. However there has been privacy concerns when information is outsourced to be stored at a third party. Also when patient is given full control of his own PHR, he proves to be inefficient in maintaining the information. Yet, issues such as risks of privacy exposure, Scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. Thus, in this paper, we propose a novel framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability and efficiency of our proposed scheme.

Introduction

In recent years, Personal Health Record (PHR) is emerged as a patient-centric model of health Information exchange. It enables the patient to create and control their medical data which may be placed in a single place such as data center. Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to third-party service providers, for example, Microsoft Health Vault, Google Health. While it is exciting to have convenient PHR data privacy risks which could impede its wide adoption. The main concern is about whether the patients could actually control the sharing of their sensitive personal health information (PHI), especially when they are stored on a third-party server which people may not fully trust. On the one hand, although there exists health care Regulations such as HIPAA which is recently amended to incorporate business associates, cloud Providers are usually not covered entities. On the other hand, due to the high value of the sensitive Personal Health Information (PHI), the third-party storage servers are often the targets of various malicious behaviors which may lead to exposure of the PHI. As a famous incident, a Department of Veterans Affairs database containing sensitive PHI of 26.5 million military veterans, including their social security numbers and health problems was stolen by an employee who took the data home without authorization". To ensure privacy control over their own PHRs, it is essential to have Fine-grained data access control mechanisms that work with semi-trusted servers. Hence we move to a new encryption pattern namely Attribute Based Encryption (ABE). In ABE, it is the attributes of the users or the data that selects the access policies, which enables a patient to selectively share their PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users. As a result, the number of attributes involved determines the complexities in encryption, key generation and decryption. The Multi Authority Attribute Based Encryption (MAABE) scheme is used to provide multiple authority based access control mechanism.

RELATED WORK

This paper is mostly related to work in cryptographically enforced access control for outsourced data and attribute based encryption. To improve upon the scalability of the above solutions, one-to-many encryption methods such as ABE can be used. A fundamental property of ABE is preventing against user collusion. In addition, the encryptor is not required to know the \ACL.

Attribute Based Encryption

It is a well-known challenging problem to revoke users/attributes efficiently and on-demand in ABE. Traditionally this is often done by the authority broadcasting periodic key updates to unrevoked users frequently, which does not achieve complete backward/forward security and is less efficient.

PROPOSED FRAMEWORK

Data Encryption Before Insert Into Cloud

A PHR service allows a patient to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient.

A feasible and promising approach would be to en-crypt the data before outsourcing. Basically, the PHR owner herself should decide how to encrypt her ales and to allow which set of users to obtain access to each file. A PHR file should only be available to the users who are given the corresponding decryption key, while remain confidential to the rest of users. Furthermore, the patient shall always retain the right to not only grant, but also revoke access privileges when they feel it is necessary.

Grouping of personal and Public Users (Personal and Public Domains)

Each patient is owner of his/her PHR. During registration he/she can gives his/her friend or relative email id that can access his/her data. Patient and email id of friends or relative are present in personal domain while during registration we are assign doctor, nurse to that patient that authorities are present in pub-

lic domain.

Deal with Break-glass Access
For certain parts of the PHR data, medical staffs need to have temporary access complete data of patients. The medical staffs will need some temporary authorization (e.g., emergency key) to decrypt those all data. Under our framework, this can be naturally achieved by letting each patient delegate her emergency key to an emergency department (ED).

Algorithms Used
- RSA(Rivest,Shamir and Adelman)
- AES(Advanced Encryption Standard)
- DES(Data Encryption Standard)

Advantages
- Complete data access in emergency condition.
- Data Security.
- Data Reliability

MATHEMATICAL MODEL
Encryption
- Input: Attribute Value (Attr).
- Get Byte [](B1) of that Attr.
- Generate Public Key(Pk).
- Perform Encryption on B1.
- Convert B1 into string(EAttr).

Decryption
- Input: Encrypted attribute value(EAttr)
- Convert EAttr into byte [](B2).
- Generate Private Key.
- Perform Decryption on B2.
- Convert B2 into string(DAttr).

Secret Key
- Input : Private Key (see Decryption-3) and No. of Authority (NAuth) =10.
- Get Length of private key : Length = PrivateKey.Length.
- To become private key multiple of NAuth (i.e. 10) pad it by zero (0).
- M = Length / NAuth
- Each authority having 'M' no. of bytes.
  For Each Byte value from 'M'.
  For (int I = 0 ; I < M.Length ; i++)
  {
  Square = M[i] * M[i] ;
  Hexvalue = Hex (Square) ;
  Hexvalue = Hexvalue + "&"
  Fullhexvalue = Fullhexvalue + Hexvalue;
  }
  Add this Hex value into database as a secret key.

Attribute Key Generation
- List = List of Attribute assign to the user(Authorities).
  Foreach (string Attribute in List){
  Foreach (char ch in Attribute)
  {
  Value = Value + ch;
  }
  }
  In the Value we get ASCII value of that character.
  ASCII values save into database.

CONCLUSION
The Personal Health Records are maintained in a data server under the cloud environment. A novel framework of secure sharing of personal health records has been proposed in this paper. Public and Personal access models are designed with security and privacy enabled mechanism. The framework addresses the unique challenges brought by multiple PHR owners and users, in that the complexity of key management is greatly reduced. The attribute-based encryption model is enhanced to support operations with MAABE.

Acknowledgment
We express our sincere thanks to our project guide Prof. S. B. JADHAV who always being with presence & constant, constructive criticism to made project successful. I would also like to thank all the staff of COMPUTER DEPARTMENT for their valuable guidance, suggestion and support through the project work, who has given co-operation for the project with personal attention. We again take it as great privilege to express our heartfelt thanks to our principal and Head of Department for their valuable suggestion for developing project at every state. Above all we express our deepest gratitude to all of them for their kind-hearted support which helped us a lot during project development. They offered us plenty of opportunities while working with them, rendered us in valuable help & helped us linking practical knowledge with theoretical one taught to us in our college. At the last we are thankful to our friends, colleagues for the inspirational help for they gave us through a project work.

REFERENCE

[1] Ming Li, Shucheng Yu, and Wenjing Lou, "Scalable and Secure | Sharing of Personal Health Records in Cloud Computing using Attribute based Encryption", IEEE Transactions On Parallel And Distributed Systems 2012. | [2] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes," 2009. | [3] S. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," ser. CCSW '10, 2010, pp. 47–52. | [4] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in IEEE INFOCOM'10, 2010. | [5] "Privacy-preserving personal health record system using attribute-based encryption," Master's thesis, WORCESTER POLYTECHNIC INSTITUTE, 2011. | [6] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing," in ICDCS '11, Jun. 2011. |