EHR System Implementation for Securing e-Health Record in Public Cloud

Prajwal H Jagdale, Prachi R Salve, Deepak R Khatik, Soumitra N Kamble
Computer Engineering ,DY Patil School of Engineering Ambi, Talegaon Pune

Abstract: *The health care has resulted during a price-effective and convenient exchange of personal Health Records (PHRs) among several collaborating entities of the e-Health systems. Still, storing the confidential health information to cloud servers is vulnerable to revelation or stealing and Demand the event of methodologies that confirm the privacy of the PHRs. There for we Have Proposed How to our PHR is secure using AES Algorithm, also stored PHR on the Cloud and Share this personal health record to other users as a confidential of the PHR. The patients store the encrypted PHRs on the un-trusted cloud servers and selectively grant access to differing types of users on whole totally different components of the PHRs. Also store record on Semi trusted Proxy server in the Re-Encryption Format with using the public and Private key pairs and provide the re-encryptions keys The AES Algorithm is secure against Hackers or Attackers and Add Security for the PHR Records in Sharing to Medical Workers, during this paper, to strength en the system security and meet the necessity of specific applications, we add functionalities of user revocation, secret key delegation and cipher text update to the primary ABE, and propose a revocable-storage hierarchical attribute-based encryption (RS-HABE)scheme, because the core building of building a framework for secure sharing of EHR publicly cloud. The proposed RS-HABE scheme features of forward security (a revoked user can't access previously encrypted data) and backward security (a revoked user also cannot access subsequently encrypted data) simultaneously, and is proved to be selectively secure under a complexity assumption in bilinear groups, without random oracles*

Keywords: Personal Health records, fine-grained access control, attribute-based encryption, secret key delegation, forward and backward security, Access control, cloud computing

Introduction:

The rapid development of technologies on cloud computing and big data has brought great changes in the medical field. Specifically, the emergence and wide use of electronic health records (EHR) enable medical workers(such as doctors and nurses) to conveniently and quickly access each patient’s medical history through the internet. Compared with the traditional management manner of medical data, EHR greatly improve the treatment efficiency, which is especially important in medical emergencies. Additionally, the digitization of personal health information results in tremendous amounts of medical data, from which some invaluable information that cannot be obtained by sending individual medical data can be disclosed by employing the data mining technology, such as flu forecast and pathology disclosure. Due to the serious challenges introduced by the storage, access and management of a large collection of EHR data, various EHR based healthcare services are popularly outsourced to external cloud computing service providers, such as Microsoft Health Vault and IBM Watson Health. Although EHR can benefit patients and medical workers by providing high-quality of medical diagnosis and services, the EHR owner has to be faced with the serious risk of HER data exposure, since he/she completely loses the control of the data when it is outsourced to cloud servers. These security and privacy issues will impede the wide adoption of EHR based heath care services. While there have been many legislations focusing on the preservation of personal health information in countries around the world, this can not present malicious cybercriminals from attacking those HER cloud servers for the high value of EHR data. For example, it was reported that a database containing sensitive EHR of half a million children, including the names of these children and their parents, social security numbers, phone numbers, addresses and health issues, was popularly sold on the dark web. Therefore, to make patients actively share their HER data in the context of public cloud, it is absolutely necessary to place patient-centric access control mechanisms over their EHR data in semi-trusted cloud servers. In this paper, we further study the problem of secure sharing of outsourced EHR data with ABE. We mainly focus on addressing the problems of user revocation, cipher text update and secret key delegation, which are not well studied or omitted in existing schemes. To this end, we first develop the original cipher text-policy ABE by adding essential functionalities, and further combine it with symmetric encryption scheme to build a more practical attribute-based access scheme for secure sharing of EHR data in public cloud.

.

Literature Survey:

1. Secure Identity-based Data Sharing and Profile Matching for Mobile Healthcare Social Networks in Cloud Computing

Author Name: Qinlong Huang, Wei Yue, Yue He, Yixian Yang

Description: Cloud computing and social networks are changing the way of healthcare by pro viding real-time data sharing during a cost-effective manner. during this paper, we introduce a secure data sharing and profile matching scheme for MHSN in cloud computing. The patients can outsource their encrypted health records to cloud storage with identity-based broadcast encryption (IBBE) technique, and share them with a gaggle of doctors during a secure and efficient manner. We then present an attribute-based conditional data re-encryption construction, which allows the doctors who satisfy the pre-defined conditions within the cipher text to authorize the cloud platform to convert a cipher text into a replacement cipher text of an identity-based encryption scheme for specialist without leaking any sensitive information. Further, we offer a profile matching mechanism in MHSN supported identity-based encryption with equality test, that helps patients to find friends during a privacy-preserving way, and achieve flexible authorization on the encrypted health records with resisting the keywords guessing attack. TPA perform auditing on patients PHR. Moreover, this mechanism reduces the computation cost on patient side. the safety analysis and experimental evaluation show that our scheme is practical for shielding the info security and privacy in MHSN

2. Secure and fine-grained access control on e-healthcare records in mobile cloud Computing

Author Name: Y. Liu, Y. Zhang, J. Ling and Z. Liu

Description: In the era of Internet of things, wearable devices are often wont to monitor residents' health and upload collected health data to cloud servers for sharing, which facilitates the development of e-healthcare record (EHR) systems. However, before ending wide applications, EHR systems need to tackle privacy and efficiency challenges. For one thing, the confidentiality of EHRs is one among most vital issues concerned by patients. for an additional , wearable devices in mobile cloud computing are often resource-constrained to some extent. during this paper, author describe a fine grained EHR access control scheme which is proven secure within the standard model under the decisional parallel bilinear Deffei-Hellman exponent assumption. In the proposed scheme, an EHR owner can generate offline cipher texts before knowing HER data and access policies, which performs a majority of computation tasks. Furthermore, the online phase can rapidly assemble the final cipher texts when EHR data and access policies become known. This EHR access control scheme allows access policies encoded in linear secret sharing schemes. Extensive performance comparisons and simulation results indicate that the solution is extremely suitable for mobile cloud computing.

3. Lightweight Sharable and Traceable Secure Mobile Health System

Author Name: Y. Yang, X. Liu, R. Deng and Y. Li

Description: Mobile health (m-Health) has emerged as a replacement patient centric model which al lows real-time collection of patient data via wearable sensors, aggregation and encryption of these data at mobile devices, then uploading the encrypted data to the cloud for storage and access by healthcare staff and researchers. However, efficient and scalable sharing of encrypted data has been a really challenging problem. during this paper, author describe a Lightweight Sharable and Traceable (LiST) secure mobile health system during which patient data are encrypted end-to-end from a patient's mobile device to data users. LiST enables efficient keyword search and fine grained access control of encrypted data, supports tracing of traitors who sell their search and access privileges for monetary gain, and allows on-demand user revocation. LiST is lightweight within the sense that it offloads most of the heavy crypto graphic computations to the cloud while only lightweight operations are performed at the top user devices. Here formally define the safety of LiST and prove that it's secure without random oracle

4. Break-glass access control system for healthcare Internet-of-Things'

Author Name: Y. Yang, X. Liu and R. Deng

Description: Healthcare Internet-of-things (IoT) has been proposed as a promising means to greatly improve the efficiency and quality of patient care. Medical devices in healthcare IoT measure patients' vital signs and aggregate these data into medical files which are uploaded to the cloud for storage and accessed by healthcare workers. to guard patients' privacy, encryption is generally wont to enforce access control of medical files by authorized parties while preventing unauthorized access. In healthcare, it's crucial to enable timely access of patient files in emergency situations. during this paper, author describe a light-weight break-glass access control (LiBAC) system that supports two ways for accessing encrypted medical files attribute-based access and break-glass access. In normal situations, a medical worker with an attribute set satisfying the access policy of a medical file can decrypt and access the info. In emergent situations, the break-glass access mechanism bypasses the access policy of the medical file to permit timely access to the info by emergency medical aid or rescue workers. LiBAC is lightweight since only a few calculations are executed by devices within the healthcare IoT network, and therefore the storage and transmission overheads are low.

5. Cost-effective secure E-health cloud system using identity based cryptographic techniques

Author: X. Wang, J. Ma, F. Xhafa, M. Zhang and X. Luo

Description: Nowadays E-health cloud systems are more and more widely employed. However the security of those systems needs more consideration for the sensitive health information of patients. Some protocols on the way to secure the e-health cloud system are proposed, but many of them use the normal PKI infrastructure to implement cryptographic mechanisms, which is cumbersome for they require every user having and remembering its own public/private keys. Identity based encryption (IBE) may be a cryptographic primitive which uses the identity information of the user (e.g., email address) because the public key. Hence the general public key's implicitly authenticated and therefore the certificate management is simplified. Proxy re-encryption is another cryptographic primitive which aims at transforming a cipher text under the delegator A into another cipher text which may be decrypted by the delegate B. during this paper, authors describe several identity related cryptographic techniques for securing E-health system, which include new IBE schemes, new identity based proxy re-encryption (IBPRE) schemes. Here also prove these schemes' security and provides the performance analysis, the results show that IBPRE scheme is particularly highly efficient for re-encryption, which may be wont to achieve cost-effective cloud usage.

EXISTING SYSTEM:

In existing system data security issues are the main obstacles to the appliance of MHSN. As we all know, health information like treatment and drug information is taken into account to be sensitive . If these data are outsourced to the CSP, the patients cannot directly control the software or hardware platform for storing data. Without careful consideration, patients may suffer serious medical information leakage from the cloud. for instance , many EHRs are compromised in recent years. Hence, it's significant that the EHRs should be stored in an encrypted form. Albeit the CSP is un trusted or compromised, the info maintains security and privacy. Simultaneously, the encrypted records should be shared and accessed during a reasonable way.

Disadvantages:

1. The patients cannot directly control the software or hardware platform for storing data.

System Architecture Diagram:

2. The patients may suffer serious medical information leakage from the cloud.

Proposed System:

Attribute authority: The attribute authority is a third party assumed to be totally trusted. by delegating the assignment of generating secret keys and update keys of users located at other levels, the workload of the attribute authority greatly decreases.

Medical worker: A medical worker might be a nurse , a doctor or a relevant administrator. Depending on their own permissions, each medical worker possibly has different attributes, which are located at different levels. is medical worker is allowed to access the EHR data by decrypting the cipher text

Cloud Service Provider: EHR owners upload their encrypted data to the corresponding servers, the provider may attempt to recover the plaintext of the encrypted EHR data.

EHR owner: EHR owner is an entity of holding the corresponding EHR data, which usually contains sensitive information about the holder, such as medical history and home address. EHR owner would only like to share his/her HER data with intended medical workers in a secure way. Cloud server managed by the service provider. This makes that only those medical workers with attributes satisfying the defined access structure can access the HER data with their decryption keys.

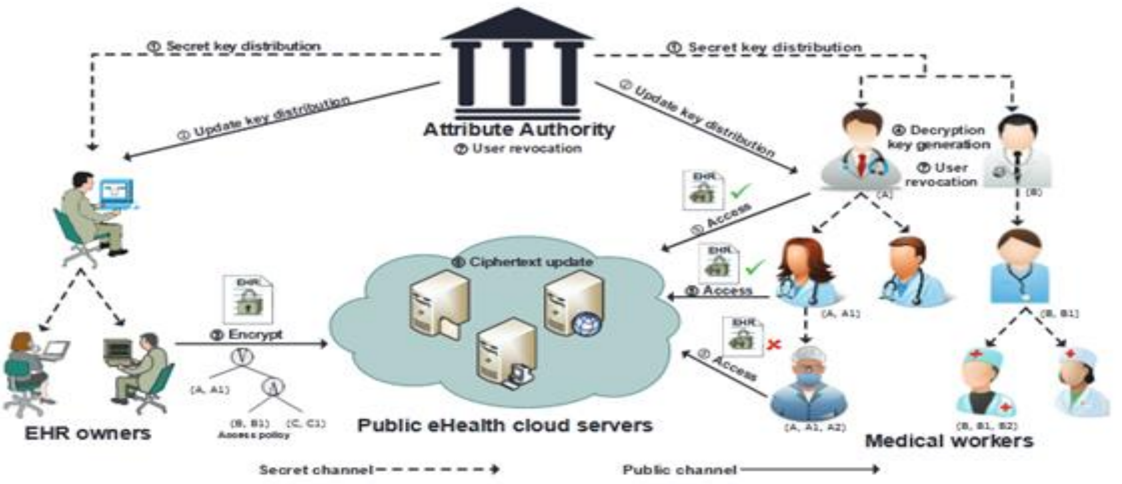

Figure 1: System Architecture Diagram

Conclusion:

In this paper, to overcome several practical security issues(i.e., secret key delegation, user revocation and ciphertext update) that occur when utilizing CP-ABE to secure sharing of EHR data in public cloud, we introduce a new crypto graphic primitive named RS-HABE, based on which we further present an access framework for secure sharing of EHR data. Furthermore, we put forward a concrete construction of RS-HABE to instantiate the framework. The proposed RS-HABE scheme can guarantee the forward and backward security of the encrypted EHR data, meanwhile, delegates each user to generate secret keys for his/her own children. We prove the selective security of the proposal in the standard model, and provide the theoretical analysis to show its advantages in terms of functionality and security. We implement the proposed RS-HABE scheme and evaluate its practical performance. On the whole, the proposed RS-HABE scheme is more desirable for securing EHR sharing in the public cloud.

Reference:

[1]A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Advances in Cryptology–EUROCRYPT 2005.Springer, 2005, pp.457–473.

[2]M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, “Scalable and secure sharing of personal health records in cloud computing using attribute-based eencryption,” IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131–143, 2013.

[3]R. Lu, X. Lin, and X. Shen, “Spoc: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency,” IEEE Transactions on Parallel and Distributed Systems, vol. 24,no. 3, pp. 614–624, 2013.

[4]J. Liu, X. Huang, and J. K. Liu, “Secure sharing of personal health records in cloud computing: cipher text-policy attribute-based sign encryption,” Future Generation Computer Systems, vol. 52,pp. 67–76, 2015

.

[5]M. H. Au, T. H. Yuen, J. K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L. Jiang, “A general framework for secure sharing of personal health records in cloud system,” Journal of Computer and System Sciences, 2017.

[6]A. Sahai, H. Seyalioglu, and B. Waters, “Dynamic credentials and ciphertext delegation for attribute-based encryption,” in Advances in Cryptology–CRYPTO 2012. Springer, 2012, pp. 199–217.

[7]J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, “Charm: a framework for rapidly prototyping crypto systems,” Journal of

Cryptographic Engineering, vol. 3, no. 2, pp. 111–128, 2013.

[8] J. Be then court, A. Sahai, and B. Waters, "Ciphertext policy attribute-based encryption," in IEEE Symposium on Security and Privacy 2007. IEEE, 2007, pp.

[9] D. He, N. Kumar, H. Shen, and J.-H. Lee, "One-to-many authentication for access control in mobile pay-tv systems," Science China Information Sciences, vol. 59, no. 5, p. 052108, 2016.

[13] D. Wang, D. He, P. Wang, and C.-H. Chu, "Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment" IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 4, pp. 428–442, 2015.

[14] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations" IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 9, pp. 2386–2396,2014.

[15] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, "New publicly verifiable databases with efficient updates," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 5, pp. 546–556, 2015.

[16] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, "Verifiable computation over large database with incremental updates," IEEE transactions on Computers, vol. 65, no. 10, pp. 3184–3195, 2016.