Lightweight Shareable Mobile Health Care System using Cloud

Uma E. S[1] Sana Nasar M[2]
[1]Assistant. Professor [2]PG Scholar
[1,2]Department of Computer Science and Engineering
[1,2]Cochin College of Engineering and Technology, India

Abstract— Mobile health care system has emerged as a new patient central model that permits real-time collection of patient information, aggregation of those information and encrypt them, and then the encrypted information is uploaded to the cloud for storage and access by health care employees and researchers. However, efficient and scalable sharing of encrypted information has been a challenging drawback. This approach propose a light-weight sharable secure mobile health care system within which patient information are encrypted end-to-end from a patients mobile device to information users. It allows efficient fine-grained access management of encrypted information, supports tracing of traitors who sell their search and access privileges for financial gain, chatbox for doctor-patient interaction and allows on-demand user revocation. It is light-weight within the sense that it drops most of the serious cryptographic computations to the cloud whereas the light-weight operations are performed solely at the end user devices. It additionally conduct in depth experiments in order access the systems performance.

Keywords: Access Control, Encryption, Traceability, User Revocation, Mobile Health System

I. INTRODUCTION

MOBILE health (mHealth) comprises of mobile devices and wireless communication technology to gather clinical health knowledge and deliver them to aid providers. The emergence of wireless body sensor network (WBSN) accelerates the event of mHealth. Implantable or wearable medical sensors are placed on patients to watch and collect the physiological symptoms. These medical knowledge are collective at a mobile device (such as a smart phone) and transmitted to the cloud via wireless networks for remote storage and access. The two major advantages that brought by mHealth are improved patient care and improved data access. Im- proved patient care implies that mobile health might notice telemedicine since the patients conditions can be calculated remotely rather than face-to-face in the hospital. Improved knowledge access implies that the healthcare providers will access important electronic health record (EHR) at the pur- pose of care or at a remote location employing a mobile terminal to produce in time during medical treatment.

Attribute based encryption (ABE) is a good mechanism to supply fine-grained access management on encrypted data, within which secret keys of users and ciphertexts are dependent upon attributes. In ciphertext-policy ABE, which we'll adopt, an access policy is related to a ciphertext and a users secret key's related to a collection of attributes. The ciphertext will be decrypted as long as the set of attributes related to the users secret key satisfies the policy. additionally to fine-grained access management, effective keyword search over encrypted EHRs is a very helpful feature in observe.

The high worth of EHRs may encourage sure rogue healthcare employees, referred to as traitors, to sell their secret keys for financial gains. Hence, it's imperative that the identity of a key owner who maliciously sells his/her secret key within the black market be traceable in mHealth systems. Moreover, a mHealth system ought to be ready to revoke approved users access privileges once the users misconduct or once their secret keys are being compromised. Most existing ABE based data encryption systems need massive scale periodic key update or ciphertext update to accomplish user revocation, which incur an excessive amount of operational overhead for mHealth systems.

II. RELATED WORKS

Goyal[1] developed a far richer style of attribute-based encryption cryptosystem and demonstrate its applications. In this system every ciphertext is labeled by the encryptor with a group of descriptive attributes. Every private key is related to an access structure that specifies which type of ciphertexts the key will decrypt. It have a tendency to decision such a theme a Key-Policy Attribute-Based encryption (KPABE), since the access structure is laid out in the private key, whereas the ciphertexts are merely labeled with a group of descriptive attributes.

In this work[2] presents another Attribute-Based encryp- tion scheme where private keys will represent any access formula over attributes, together with non-monotone ones. Above all, this approach will handle any access structure which will be represented by a boolean formula involving AND, OR, NOT, and threshold operations.

[3]proposes a privacy-preserving DCP-ABE (PPDCP- ABE) scheme wherever the central authority isn't required and every authority will work alone without any cooperation. As a notable feature, every authority will dynamically be part of or leave the system, specifically different authorities ought not to modify their secret keys and reinitialize the system once an authority joins or leaves the system. Each authority monitors a group of attributes and issues secret keys to users accordingly. To resist the collusion attacks, a users secret keys are tied to his GID. Especially, a user will acquire secret keys for his attributes from multiple authorities without them knowing any data regarding his GID and attributes. Therefore, the proposed PPDCP-ABE scheme will give stronger privacy protection compared to the previous PPMAABE schemes wherever solely the GID is protected.

The main aim of framework[4] is to give secure patient- centric PHR access and efficient key management at the same time. The key plan is to divide the system into multiple secu- rity domains (namely, public domains and personal domains) consistent with the various users knowledge access needs. The PUDs contains users who create access supported their skilled roles, like doctors, nurses, and medical researchers. In practice, a PUD are often

mapped to an independent sector within the society, like the health care, government, or insurance sector. For every PSD, its users are personally related to a data owner (such as members of the family or shut friends), and that they create accesses to PHRs supported access rights assigned by the owner.

Attribute-based encryption (ABE) is a new vision for public key encryption that enables users to encrypt and decrypt messages based on user attributes. [5]proposed a new paradigm for ABE that largely eliminates this type of overhead for users. To precisely outline and demonstrate the benefits of this approach, new security definitions for both CPA and replayable CCA security with outsourcing, several new constructions, an implementation of our algorithms and elaborated performance measurements. In a typical con- figuration, the user saves considerably on each bandwidth and decryption time, while not increasing the number of transmissions.

The approach[6] has a new requirement of ABE with outsourced decryption: verifiability. Informally, verifiability guarantees that a user can efficiently check whether the transformation is done properly. This offer the formal model of ABE with verifiable outsourced decryption and propose a concrete scheme. It proves that the new scheme is both secure and verifiable, without relying on random oracles. Finally, we show an implementation of our scheme and results of performance measurements, that indicates a significant reduction on computing resources obligatory on users.

In[7] it first formalize a security model of ABE with verifiable outsourced decryption by introducing a verification key in the output of the encryption algorithm. Then, this presents an approach to convert any ABE scheme with outsourced decryption into an ABE scheme with verifiable outsourced decryption. The new approach is simple, general and almost optimum. Compared with the first outsourced ABE, this verifiable outsourced ABE neither will increase the users and the cloud servers computation costs except some non-dominant operations (e.g., hash computations), nor expands the ciphertext size except adding a hash price (which is smaller than than 20 byte for 80-bit security level). It shows a concrete construction primarily based on Green et al.s ciphertext policy ABE scheme with outsourced decryption, and supply a detailed performance analysis to demonstrate the benefits of our approach.

[8] provides generic constructions of CPA-secure and RCCA-secure ABE with verifiable outsourced decryption from CPA-secure ABE with outsourced decryption, respec- tively. At a high level, both of our generic constructions have a decrypt-then-verify flavor. That is, when receiving a partially-decrypted ciphertext remodeled by a proxy, the information receiver initial decrypts it using some simple operations and so verifies the correctness of the outsourced decryption.

In[9] a new CP-ABE system that supports traceability of malicious users who leaked their decryption privileges. This Traceable CP-ABE doesn't weaken the quality or efficiency when compared with the most efficient non-traceable CP- ABE systems presently accessible for high quality. Above all, every decryption key in our system will be traced to its owner, the ciphertext policy will be any monotone access structures, the decryption key size grows linearly with the number of corresponding attributes, and therefore the ciphertext size grows linearly with the scale of corresponding access structure. Also, the system will be shown to be adaptively secure within the standard model. It also propose an extended version for this Traceable CP-ABE system. In this extension, there are two authorities, one for generating tracing data, and therefore the different one for issuing decryption keys to users, whereas no single authority is able to independently generate decryption keys.

The approach[10] describes cryptographic schemes for the problem of looking out on encrypted data and give proofs of security for the resulting cryptosystems. These techniques have variety of crucial benefits. They are provably secure: they supply obvious secrecy for encryption, in the sense that the untrusted server cannot learn anything regarding the plaintext once solely given the ciphertext; they provide query isolation for searches, meaning that the untrusted server cannot learn anything additional regarding the plaintext than the search result; they provide controlled searching, so the untrusted server cannot look for an arbitrary word without the users authorization; they additionally support hidden queries, so the user might ask the untrusted server to look for a secret word without revealing the word to the server.

The approach[11] proposes first DSSE theme that achieves the simplest of each words, DSSE scheme leaks considerably less data than the other previous DSSE construction and supports each updates and searches in sublinear time within the worst case, maintaining at the same time an information structure of only linear size. Finally provide an implementa- tion of the construction, showing its practical efficiency.

[12] secure k-nearest neighbor to propose a secure dy- namic searchable symmetric encryption scheme. It can do two necessary security features, that is, forward privacy and backward privacy that are very difficult in Dynamic Search- able symmetric encryption (DSSE) space. Additionally, it judge the performance of this method compared with dif- ferent DSSE schemes. The comparison results demonstrate the efficiency of this approach in terms of the storage, search and update complexity.

In[13], it enhance the security model of the public key encryption with keyword search to properly incorporate the ability of an adversary. Additionally it also construct a public key encryption scheme with keyword search secure within the enhanced security model.

[14]started by reviewing existing notions of security and propose new and stronger security definitions. It includes two constructions that show secure under our new defini- tions. Apparently, in addition to satisfying stronger security guarantees, these constructions are more efficient than all previous constructions. Further, previous work on SSE only considered the setting wherever solely the owner of the information is capable of submitting search queries. This take into account the natural extension where an arbitrary cluster of parties alternative than the owner will submit search queries. This formally define SSE in this multi-user setting, and present an efficient construction.

This work[15], proposes a searchable attribute- based proxy re-encryption system. While compared to

existing systems only supporting either searchable attribute-based functionality or attribute-based proxy re-encryption, the new primitive supports both skills and provides versatile keyword update service. Specifically, the system allows a data owner to efficiently share his knowledge to a such that cluster of users matching a sharing policy and in the meantime, the information can maintain its searchable property but additionally the corresponding search keyword(s) is updated after the information sharing. The new mechanism is applicable to several real-world applications.

[16]specializes in a different however more difficult scenario where the outsourced dataset will be contributed from multiple owners and are searchable by multiple users. Im- pressed by attribute-based encryption (ABE), proposes the primary attribute-based keyword search method with efficient user revocation (ABKS-UR) that allows scalable fine-grained search authorization. It permits multiple owners to encrypt and source their information to the cloud server independently. Users will generate their own search capabilities while not looking forward to an invariably online trustworthy authority.

In this method[17] proposes a unique primitive named hidden policy ciphertext-policy attribute-based encryption with keyword search (HP-CPABKS). With the primitive, information user is unable to look on encrypted data and learn any information regarding access structure if his/her attribute credentials cannot satisfy the access control policy specified by the data owner. It present a rigorous selective security analysis of the proposed HP-CPABKS method, that at the same time keeps the identity of the keywords and also the access structures. Finally, the performance analysis verifies that our proposed theme is efficient and practical.

[18]introduced the notion of Public-key authenticated en- cryption with Keyword Search (PAEKS) to resolve the problem, in which the information sender not solely encrypts a keyword, however additionally authenticates it, so that a verifier would be convinced that the encrypted keyword will also be generated by the sender. It proposes a concrete and ef- ficient construction of PAEKS, and proves its security based on simple and static assumptions within the random oracle model under the given security models. Encryption of data maintains the confidentiality, however this makes keyword search troublesome. To resolve this issue, selected server based public key encryption with keyword search (dPEKS) method is employed. In dPEKS theme, to get the encrypted information, the client computes a trapdoor associated with a relevant keyword, and sends it to the cloud server, which then offers the ciphertext to the client provided that the trapdoor is verified. Hence, the client gets the information from the ciphertext. However, an adversary won't get any information on the data or the keywords. A certificateless dPEKS (CL- dPEKS) schemeis proposed in [19]. It provides identity to the ciphertext and trapdoor, and resilience to off-line keyword guessing attack. The computational Diffie-Hellman (CDH) problem and bilinear Diffie- Hellman (BDH) problem keep this approach secure.

Most of the SE schemes are created using the bilinear map. However, both discrete logarithms and factorization are tried to be solved by quantum computer in a polynomial time. Thus, those schemes don't seem to be secure in quantum age. Moreover, majority SE schemes are restricted in actual or fuzzy keyword search. They'll not support the semantically keyword equivalent judgement. So as to resolve those issues, in[20] proposes a completely new data retrieval approach for multiple users supported the lattice based mechanism. The contribution of this paper is summarized in 3 aspects: lattice assumption primarily based scheme to resist quantum attack, semantically keyword search to modify synonym query and broadcast encryption based mechanism to support multiple user system while not sharing secret key. This approach may be a candidate for secure multimedia cloud even in quantum- era since the LWE problem is secure against quantum attack.

III. Conclusion

LiST is a light-weight secure data sharing solution with traceability for mHealth systems. LiST seamlessly integrates variety of key security functions, such as fine-grained access control of encrypted data, keyword search over encrypted data, traitor tracing, and user revocation into a coherent system design. Considering that mobile devices in mobile health are resource constrained, operations in data owners and data users devices in LiST are kept at light-weight. It has evident security. The qualitative analysis showed that LiST is superior to most of the prevailing systems. Extensive experiments on its performance (on both laptop and mobile device) demonstrated that LiST is incredibly promising for practical applications.

References

[1] Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryp- tion for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications secu- rity. Acm, 2006, pp. 89–98.
[2] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 195–203.
[3] J. Han, W. Susilo, Y. Mu, J. Zhou, and M. H. A. Au, "Improving privacy and security in decentralized ciphertext-policy attribute-based encryption," IEEE transactions on information forensics and security, vol. 10, no. 3, pp. 665–678, 2015.
[4] 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 encryption," IEEE transactions on parallel and distributed systems, vol. 24, no. 1, pp. 131–143, 2013.
[5] M. Green, S. Hohenberger, B. Waters et al., "Outsourcing the decryp- tion of abe ciphertexts." in USENIX Security Symposium, vol. 2011, no. 3, 2011.
[6] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Transactions on informa- tion forensics and security, vol. 8, no. 8, pp. 1343–1354, 2013.
[7] B. Qin, R. H. Deng, S. Liu, and S. Ma, "Attribute-based encryption with efficient verifiable outsourced decryption," IEEE Transactions on Information

Forensics and Security, vol. 10, no. 7, pp. 1384–1393, 2015.
[8] X. Mao, J. Lai, Q. Mei, K. Chen, and J. Weng, "Generic and efficient constructions of attribute-based encryption with verifiable outsourced decryption," IEEE Transactions on Dependable and Secure Computing, no. 1, pp. 1–1, 2016.
[9] Z. Liu, Z. Cao, and D. S. Wong, "White-box traceable ciphertext- policy attribute-based encryption supporting any monotone access structures," IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 76–88, 2013.
[10] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000, pp. 44–55.
[11] E. Stefanov, C. Papamanthou, and E. Shi, "Practical dynamic search- able encryption with small leakage." in NDSS, vol. 71, 2014, pp. 72– 75.
[12] Y. Yang, H. Li, W. Liu, H. Yao, and M. Wen, "Secure dynamic searchable symmetric encryption with constant document update cost," in Global Communications Conference (GLOBECOM), 2014 IEEE. IEEE, 2014, pp. 775–780.
[13] H. S. Rhee, J. H. Park, W. Susilo, and D. H. Lee, "Improved searchable public key encryption with designated tester," in Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. ACM, 2009, pp. 376–379.
[14] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable sym- metric encryption: improved definitions and efficient constructions," Journal of Computer Security, vol. 19, no. 5, pp. 895–934, 2011.
[15] K. Liang and W. Susilo, "Searchable attribute-based mechanism with efficient data sharing for secure cloud storage," IEEE Transactions on Information Forensics and Security, vol. 10, no. 9, pp. 1981–1992, 2015.
[16] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, "Protecting your right: verifiable attribute-based keyword search with fine-grained owner- enforced search authorization in the cloud," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 4, pp. 1187–1198, 2016.
[17] S. Qiu, J. Liu, Y. Shi, and R. Zhang, "Hidden policy ciphertext- policy attribute-based encryption with keyword search against keyword guessing attack ŁŁŁ," Science China Information Sciences, vol. 60, no. 5, p. 052105, 2017.
[18] Q. Huang and H. Li, "An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks," Information Sciences, vol. 403, pp. 1–14, 2017.
[19] R. Amin, "Design of a certificateless designated server based search- able public key encryption scheme," in Mathematics and Computing: Third International Conference, ICMC 2017, Haldia, India, January 17-21, 2017, Proceedings, vol. 655. Springer, 2017, p. 3.
[20] Y. Yang, X. Zheng, V. Chang, S. Ye, and C. Tang, "Lattice assumption based fuzzy information retrieval scheme support multi-user for secure multimedia cloud," Multimedia Tools and Applications, pp. 1–15, 2017.

