Empowering E-Healthcare: A Robust Secure Data Sharing and Authorization Framework

AUTHORS:

DR. DEEPAK A. VIDHATE,

Prof and Head, Information Technology, Dr. Vithalrao Vikhe Patil College of Engineering, Ahmednagar

PROF. MRS.P.S. DOLARE,

Prof, Information Technology, Dr. Vithalrao Vikhe Patil College of Engineering, Ahmednagar

HARSH RAJA, HAMZA SAYED, VISHAL RATHOD, PARAG PALASKAR, DANISH TAMBOLI,

Department of Engg, Information Technology, Dr. Vithalrao Vikhe Patil College of Engineering, Ahmednagar

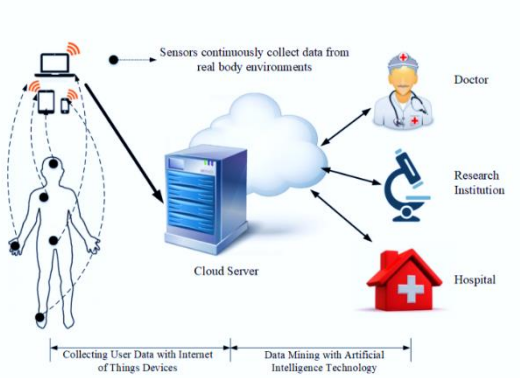
ABSTRACT:

In e-healthcare system, an increasing number of patients enjoy high-quality medical services by sharing encrypted personal healthcare records (PHRs) with doctors or medical research institutions. However, one of the important issues is that the encrypted PHRs prevent effective search of information, resulting in the decrease of data usage. Another issue is that medical treatment process requires the doctor to be online all the time, which may be unaffordable for all doctors (e.g., to be absent under certain circumstances). In this paper, we design a new secure and practical proxy searchable re-encryption scheme, allowing medical service providers to achieve remote PHRs monitoring and research safely and efficiently. Through our scheme DSAS, (1) patients' healthcare records collected by the devices are encrypted before uploading to the cloud server ensuring privacy and confidentiality of PHRs; (2) only authorized doctors or research institutions have access to the PHRs; (3) Alice (doctor-in-charge) is able to delegate medical research and utilization to Bob (doctor-in-agent) or certain research institution through the cloud server, supporting minimizing information exposure to the cloud server. We formalize the security definition and prove the security of our scheme. Finally, performance evaluation shows the efficiency of our scheme.

Keywords: *Proxy re-encryption, proxy invisibility, searchable encryption, mobile healthcare sensor networks.*

INTRODUCTION

Nowadays, with the rapid development of artificial intelligence and the advancement of wearable devices and sensors, e-healthcare sensor network has reached a stage of maturity for adoption and deployment at a commercial scale. Ehealthcare sensor network serving as a mobile platform profoundly benefit patients to obtain medical treatment of high quality and efficiency. As shown in Fig.1, patients' devices collect a large amount of personal healthcare records through sensor devices, which enable doctors to more effectively diagnose and attend to the need of the patients through utilizing these data. Such information also enables medical researchers and analysts to perform analytics to gain better insights on illnesses and



devise better treatments. Nevertheless, these data may be stored on cloud storage provided by third-party service providers [10], [16], [34], which introduce potential security issues such as data leakage. This is because neither the patients nor the doctors have control of the information The associate editor coordinating the review of this manuscript and approving it for publication was Diana Gratiela Berbecaru. once the data is outsourced. This means the privacy and confidentiality of these outsourced data should be protected in such an environment. For instance, some medical institutions collect and store a large amount of PHRs on cloud servers and authorize the usage of these data to the Center for Disease Control and Prevention (CDC). To facilitate disease prevention and control, doctors in CDC are allowed to study these data with data mining technology. However, in the process of collecting case information from medical institutions and the implementation of traditional data mining technology, the CDC may inevitably expose sensitive data of patients. How to store manage and retrieve the PHRs securely and efficiently is a great challenge.

A. RELATED WORK

With the rapid development of cloud computing, more and more patients are willing to move their PHRs to the cloud server to enjoy convenient service [25], [30], [35]. To protect data security and personal information privacy, these PHRs are usually stored with encrypted form in the cloud. However, data encryption hinders effective data utilization when the user tries to retrieve files containing some interesting keywords. Yasnoff [48] proposed a e-healthcare storage framework to eliminate the potential for loss of an entire centralized dataset from a single intrusion while maintaining reasonable search performance. A reliable, searchable and privacy-preserving e-healthcare system was proposed by Yang et al. [45] based on searchable encryption [9], [18], [23], [40], [51] to protect sensitive healthcare files on cloud storage and enable cloud server to search on the encrypted data under the control of patients. The notion of public-key encryption with keyword search (PEKS) was proposed by Boneh et al. [8], who also gave the first PEKS construction for e-healthcare system in the public key environment. Later, Abdalla et al. [1] revisited the concept of PEKS and proposed the consistency notion. Baek et al. [3] extended PEKS which removes secure channels between a user and the cloud server, which make the patients communicate with doctors with a secure way. More expressive searchable schemes for e-healthcaer system are proposed in [24], [29], [33], and zhang2017searchable. To store a huge number of PHRs from multi users, schemes [24], [47] are proposed to optimize data storage and retrieval in the multi user setting. Except for searchable encryption, proxy re-encryption (PRE) technology proposed by Blaze et al. [7] was also employed to store and share medical data in e-healthcare system. Proxy re-encryption is a highly promising solution for cloud computing, which has been widely applied to provide ciphertext transformation in cloud storage services recently. There has been significant progress in PRE over the recent years because of the property called conditional transformation, greatly enriching the commercial applications of PRE. In 2005, Ateniese et al. [2] proposed a unidirectional scheme and demonstrated how to prevent the proxy from colluding with delegatees in order to expose the delegator's private key. In 2006, Green and Ateniese [17] extended the above notion to identity-based proxy re-encryption, and proposed a new CCA secure scheme. Seo et al. [31] proposed the first proxy-invisible CPRE scheme that is secure against CCA secure in the standard model. He et al. [19] proposed a non-transferable proxy re-encryption scheme that solves the PKG despotism problem and key escrow problem. Fang et al. [12], [13] introduced fuzzy conditional proxy re-encryption and proposed a concrete construction based on the "set overlap" distance metric. In [20], PRE was deployed in mobile healthcare social network for a data owner to authorized a healthcare analyzer to access the owner's data. While the underlying purpose is similar, this proposal is more robust using CPRE and examines delegation of duty from a doctor to another, and further provides proxy-invisibility and condition-hiding properties.

Proxy re-encryption with keyword search (PRES), which is proposed by Shao et al. [32], can allow the patients to delegate his search and decrypt capability to doctor or research institution. In the e-healthcare system, suppose doctor Alice (delegator) wants to delegate the search capability to doctor Bob (delegatee), by employing the PRES scheme propose by Shao et al. [32], 1) Bob can decrypt the ciphertexts delegated from Alice using his own private key; 2) given a trapdoor from Bob, the mail gateway can test whether the ciphertext delegated from Alice contains some special keyword. However, we notice that with the re-encryption key, the proxy can transform all ciphertext of Alice no matter which keyword the ciphertext have. In this case, without Alice's delegation, Bob can still read all the message of Alice, this can be make serious security risks to the e-healthcare system. To address this issue, Weng et al. [38], [39] introduced the concept of conditional proxy re-encryption, where the re-encryption key is linked with a condition so that the delegatee can only decrypt ciphertext which satisfying the special condition. After that, a series of CPRE schemes have been proposed [12], [37], [41]. In most CPRE schemes, the condition is specified in the re-encryption key, and thus that the proxy can obtain the condition information such as "HIV". However, in the e-healthcare system, the condition can also contain some sensitive information [46]. Therefore, it is necessary to build a CPRE construction without leaking the condition information. TABLE 1. Functionality summary. Unfortunately, all the above systems do not simultaneously support both encrypted keyword search and condition-hiding in practice, which limits the commercial applications of proxy re-encryption in the e-healthcare system. We propose a proxy-invisible condition-hiding proxy re-encryption scheme with keyword search to address the issues of inefficiency and condition privacy in the e-healthcare system.

B. MOTIVATION AND CONTRIBUTION

Table 1 gives the summary of the related works in terms of uni-directional, proxy-invisible, condition-hiding, collusionresistance, keyword search.

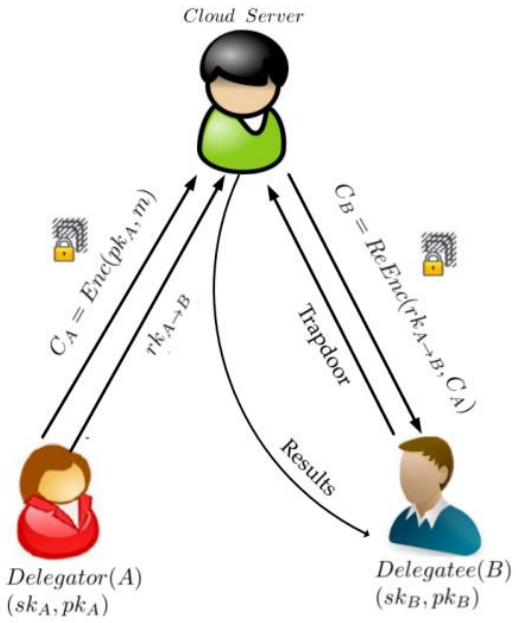
- *Uni-Directional: Uni-directional proxy re-encryption is more superior than multi-directional proxy reencryption, otherwise, the delegatee may pass permissions to a third party, which will*

increase the disclosure of privacy. Hence, unidirectionality is a very important characteristic for e-healthcare system.

• Proxy-Invisible: In the secure e-healthcare system, if a malicious user can distinguish a re-encrypted ciphertext from an original ciphertext, it will increase the security risk such as the malicious user knows the delegator is not available right now. Hence, e-healthcare system must provide proxy-invisible.

• Condition-Hiding: In the conditional proxy re-encryption scheme, the condition often contains some private information. If the condition is exposed, it will cause a great loss to the system. Obviously, if the proxy condition is hidden, the proxy server will get less sensitive information, which makes the e-healthcare system more secure.

• Collusion-Resistance: Inherent from trustworthy property, it is impossible to provide collusion-resistance when the dishonest proxy colludes with the delegatee to export the delegator's private key, which would be a disaster to the e-heathcare system. As these authorized work are usually operated on the proxy server (assumed to be a third-party service provider), which for security reason is assumed to be untrusted. Hence, it is necessary to provide collusion-resistance in a secure e-healthcare system.



System model

• Keyword Search: Encrypting is considered to be a simple and efficient solution to guarantee data confidentiality, but it also makes search over encrypted data extremely difficult. Searchable encryption technology realizes the search operation of encrypted data without decryption, and solves the problem that users cannot control remotely because of data encryption. Hence, searchable is necessary in the e-healthcare system.

As can be seen from Table 1 by giving a comparison among existing shcemes, no scheme can realize secure and reliable ciphertext retrieval functions in the e-healthcare system. In a e-healthcare system, the wearable devices continuously collecting medical data from real body environment. The massive sensitive data leads to a great security and efficiency challenge to the current e-healthcare system due to lack of efficient information retrieve mechanism and poor fine-grained access control. In this paper, we aim to design an efficient, searchable and privacy-preserving e-healthcare system. The overall system consists of three main entities as shown in System Model.

In summary, users (e.g., patients, doctors, research institutions) enjoy an efficient, searchable, privacy protection service in our e-healthcare system. The main results are as follows:

1. Data privacy: patients' data collected by the sensor devices are encrypted before they are uploaded to the cloud storage server. This ensures privacy and confidentiality of data since the cloud server will not be able to learn any information from the encrypted PHRs.

2. Conditional authorization: In the event where the doctorin-charge (Alice) is unavailable, our scheme enables the delegation of the task to another doctor (Bob) through a cloud server, without the need to decrypt the PHRs thus minimizing information exposure to the cloud server.

3. Condition-hiding: Our scheme not only guarantees patients's PHRs privacy through encrypted data but also preserves the privacy of the condition embedded in the re-encryption key.

4. Proxy invisibility: In our scheme, the authorized doctor (Bob) or a malicious user cannot distinguish which ciphertext is sent to delegate and which ciphertext is re-encrypted by the cloud delegated by Alice.

5. Collusion resistance: In our scheme, even a dishonest proxy colludes with Bob, Alice's private key can still be secure.

II. SYSTEM ARCHITECTURE AND CONSTRUCTION

In this section, we first introduce the algorithms definition and system architecture, and then propose the construction of our conditional proxy re-encryption with keyword search system, which is proxy-invisible, condition-hiding and CCAsecure.

A. DEFINITION

A conditional proxy re-encryption with keyword search system consists of the following polynomial time algorithms:

• Setup (1λ) → param: Given a security parameter λ, outputs public parameters param to be used by all parties.

• Keygen (1λ) → (pk, sk): Given a security parameter λ, the key generation algorithm outputs a public/private key pair (pk, sk).

• Enc (pk, m, w) → CT: Given a public key pk, a keyword w, and a message m, the encryption algorithm outputs a ciphertext CT of m corresponding to keyword w.

• ReKeyGen (ski, pkj,w) → rkw i→j : Given a user i's private key ski , a user j's public key pkj and condition w, the re-encryption key generation algorithm outputs a re-encryption key rkw i→j .

• ReEnc(rkw i→j ,CTi) → CTj : Given the re-encryption key rkw i→j and a ciphertext CTi corresponding public key pki , the re-encryption algorithm outputs another ciphertext CTj corresponding public key pkj or the special character ⊥ indicating an error. • Trapdoor(sk,w) → tw: Given a user's private key sk and a keyword w, the trapdoor algorithm outputs a trapdoor tw of keyword w corresponding to the user.

• Test(CT , tw) → 0 or 1: Given ciphertext CT , and a trapdoor tw, the test algorithm outputs 1 if a given ciphertext CT contains the keyword w specified by the trapdoor tw or 0 otherwise.

• Dec(sk,CT) → m: Given a user's private key sk and a ciphertext CT , the decryption algorithm outputs the corresponding message m or the special character ⊥ indicatin

B. SYSTEM ARCHITECTURE

In this paper, we design a new cloud storage framework for e-healthcare system which provides efficient and privacy-preserving information retrieve service and meet the above requirements. The e-healthcare system generally consists of the following phases:

• Setup phase: In this phase, patients' sensors choose a security parameter 1λ , run algorithms Setup and KeyGen to generate and store parameters param, public key and private key (pk,sk) for all patients in the real world to collect PHRs.

• Data collection and encryption phase: The sensors continuously collect PHRs F from physical environments, then extract keyword w from these data, run algorithm Enc to generate medical information under doctor Alice's public key pkAlice. Finally, upload all ciphertext CTAlice to the cloud server.

• Data conversion phase: Alice is able to delegate search and decrypt operation to Bob through the cloud server with the following steps if Alice is unavailable. First, Alice runs algorithm ReKeyGen to generate re-encryption key for the cloud server under Alice's private key skAlice and Bob's public key pkBob. Second, given re-encryption key, the cloud server runs algorithm ReEnc to convert the corresponding ciphertext. Finally, stores the converted ciphertext CTBob. To achieve conditional authorization, algorithm ReKeyGen requires Alice's private key as part of the input. Therefore, anyone (without Alice's private key) given Bob's public key could not launch conditional authorization.

• Data retrival phase: Bob is able to search and decrypt the converted ciphertext with the following steps. First, Bob runs algorithm Trapdoor to generate a trapdoor tw under keyword w and his private key skBob. Second, given the trapdoor tw and ciphertext CTBob, the cloud server runs algorithm Test to find the matching ciphertext. Finally, Bob obtains the intended data by decrypting the matched ciphertext with his private key skBob by running algorithm Dec.

Fig. 3 shows the flow chart of the above system. The black arrow in the figure represents the process of data collection:

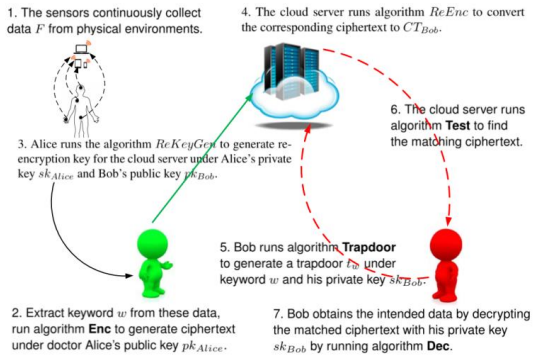


FIGURE 3. Data process, storage, and retrieval in e-healthcare system

patients' data collected by the sensor devices are encrypted before they are uploaded to the cloud storage server. This ensures privacy and confidentiality of data since the cloud server will not be able to learn any information from the encrypted personal health records (PHRs). The red arrows in figure represent the process of secure data query: Only the authorized doctor have access to the PHRs.

In the event where the doctor-in-charge is unavailable, our scheme enables the delegation of task to another doctor through a cloud server, without the need to decrypt the PHRs thus minimizing information exposure to the cloud server, which shown with green arrow in the figure.

IV. SECURITY DEFINITION AND PROOF

In this section, we give the security definition and the concrete proof of the proposed DSAS scheme.

A. SYSTEM THREAT MODEL

We assume cloud server is always online with sufficient storage and computing capacity. Also, we assume that doctor Alice is online most of the time. In some cases, when Alice is not online, he authorizes access to the PHRs to doctor Bob or other medical institutions by distributing a re-encryption key through a secure channel between cloud server and himself.

However, the possible attacks on our system are as follows:

1. The could server is "honest-but-curious", which follows many related work on e-healthcare cloud computing system, which means the cloud server "honestly" follows the designated protocol, but "curiously" infers additional privacy information of the encrypted PHRs content or the search query.

2. Unlike FSGW [12], SCLL [32], WHYLW [37] and YM [46], the cloud server in our system may collude with authorized doctors to export the delegator's private key to access data beyond their access privileges.

B. SYSTEM SECURITY MODEL

We define security for our system in the sense of semanticsecurity. We need to ensure that a ciphertext CT does not reveal any information about the keyword w unless the keyword trapdoor tw is available. We define security against an active attacker who is able to obtain trapdoors tw for any w of his choice, even under such attack, the attacker should not be able to distinguish encryption of a keyword w0 from encryption of a keyword w1 for which he did not obtain the trapdoor. Formally, we define security against an active adversary.

V. PERFORMANCE ANALYSIS

In this section, we evaluate the performance of our DSAS system based on both real experiments and simulation.

A. EXPERIMENTAL SETTING

By adopting the Type A curves within the Paring Based Cryptography (PBC) library [22], we perform our proposed scheme on a laptop with 1.8-GHz Intel Core processor i5- 8250U (Window 10 operation system, and a RAM of 8 GB) to act as the cloud server. This simulation environment is used to perform algorithms ReEnc and Test, which require a great computational and storage capability. In contrast, the users or sensor devices in our system require low computational capability, to perform algorithms KeyGen, Enc, ReKeyGen, Trapdoor and Dec, we deploy two Raspberry Pi sensor nodes (ARM Cortex-A53 1.2GHz 64-bit quad-core ARMv8 CPU) to form a wireless linked Industrial Internet of Things (IIoT). The nodes communicate with each other by ZigBee protocol. The sensor nodes communicate with the cloud server through one-hop or multihop manner. In the experiment, Let $|G|$ denote a bit length of an element of G, $|GT|$ denote a bit length of an element of GT . Since only schemes FSGW [12] and YM [46] are about conditional searchable proxy reencryption, hence, we only compare our scheme with these two schemes, and the simulation results are exhibited in Fig. 4 to Fig. 11.

B. EXPERIMENTAL EVALUATION

In key generation phase, the system constructs public-private key pairs for each user with only 2 exponential operations.

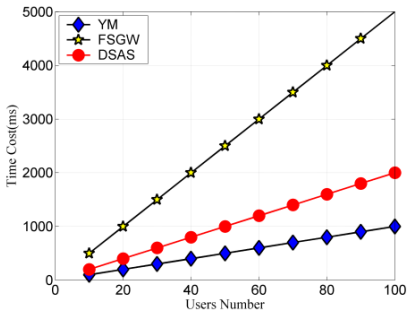


FIGURE 4. Performance of KeyGen.

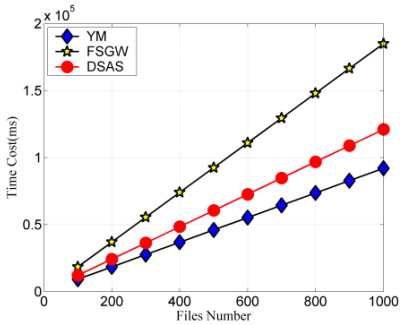


FIGURE 5. Performance of encrypt.

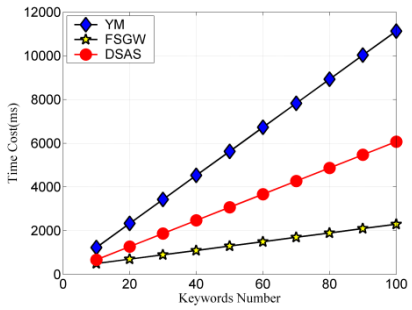


FIGURE 6. Performance of index encrypt.

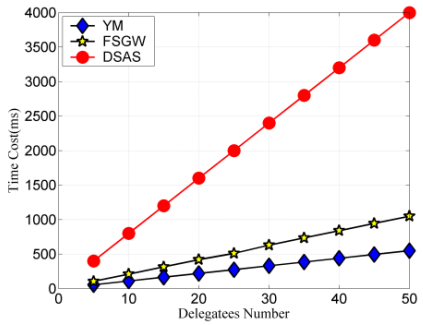


FIGURE 7. Performance of ReKeyGen.

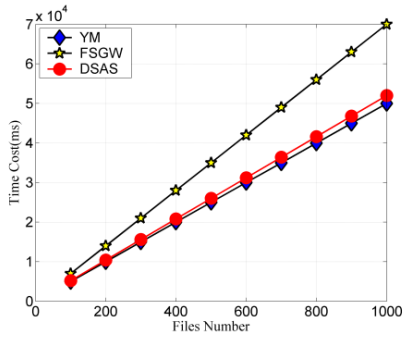


FIGURE 8. Performance of ReEnc.

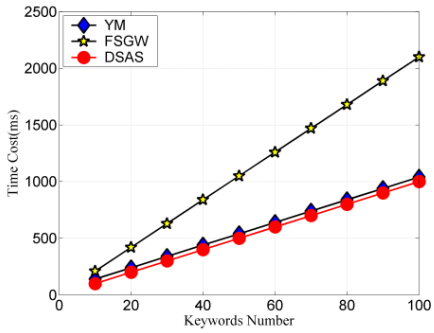


FIGURE 9. Performance of trapdoor.

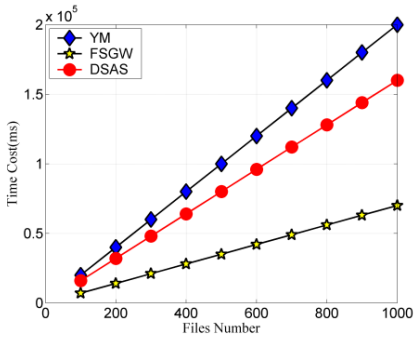


FIGURE 10. Performance of search.

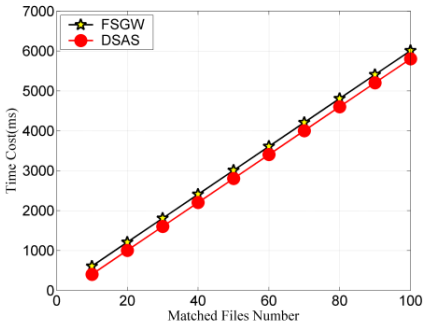


FIGURE 11. Performance of decrypt.

in DSAS. Cost in FSGW [12] and YM [46] are 4 exponential operations and 1 exponential operation respectively. The computational cost of key generation in all schemes for each user is constant, which have significantly efficiency for lightweight devices in e-healthcare system as shown from Fig. 4, the computation cost increases linearly with the growth of users.

On receiving public-private key pairs, sensors for data collection encrypt the collected PHRs with doctor Alice's public key before uploading them to the cloud server. First, the sensors continuously collect PHRs F from physical environment, then extract keyword w from these data. Second, run algorithm Enc to generate searchable index healthcare ciphertext under doctor Alice's public key pkAlice. Finally, upload all ciphertext CTAlice to the cloud server. There are 5|G|+2|GT| cost for each file in DSAS, and 3|G|+2|GT | and 3|G| + 1|GT | in FSGW [12] and YM [46] respectively. The computational cost of ciphertext generation in all schemes for each file is constant. Clearly from Fig. 5 and Fig. 6, the computation cost increases linearly with the growth of files. On receiving the ciphertext, Alice is able to delegate search and decrypt operation to Bob through a cloud server if Alice is unavailable. The computational cost for re-encryption key generation is exhibited in Fig. 7. Cost in FSGW [12] and YM [46] are 4|G| and 2|G| respectively. DSAS requires 1|G| + 2|GT | for each re-encryption key, however, because DSAS considers embeds the trapdoor into re-encryption key, in which way can hidden the proxy condition. Obliviously,

DSAS sacrifices some computing efficiency, thus obtaining better security. Given re-encryption key, the cloud server runs algorithm ReEnc to convert the corresponding ciphertext to CTBob under Bob's public key with only 4 exponential operations in DSAS. Cost in FSGW [12] and YM [46] are 3 exponential operations and 6 exponential operation respectively. Next is about the encrypted keyword search, given trapdoor generated by Bob, the cloud server runs algorithm Test to perform information retrieve over encrypted PHRs. Cost of DSAS is only 3 pairing operations and cost in FSGW [12] and YM [46] are 2 pairing operations and 2 exponential operations and 3 pairing operations and 2 exponential operations respectively. As shown in Fig. 8 and Fig. 10, DSAS and YM [46] have more advantages on re-encryption and encrypted keyword search over FSGW [12]. Bob is able to search the converted ciphertext by running algorithm Trapdoor to generate a trapdoor tw under keyword w and his private key skBob. Cost in YM [46] and DSAS are 1 exponential operation and 4 exponential operations in FSGW [12]. Given the trapdoor tw and ciphertext CTBob, the cloud server runs algorithm Test to find the matching ciphertext. Finally, Bob obtains the intended data by decrypting the matched ciphertext with his private key skBob by running algorithm Dec. Because YM [46] has no capability for decryption, it is not considered in our comparison. As shown in Fig. 9 and Fig. 11, DSAS is as efficient in decryption as FSGW [12]. In summary, compared with FSGW, DSAS requires a little bit high cost in KeyGen and Encrypt; compared with YM, DSAS requires a little bit high cost in Index Encrypt. However, these results are acceptable since these costs are one-time, that is, users only need to take the corresponding costs when joining the system and uploading the e-healthcare records. In order to protect the privacy of conditions, we explore the embedding technology of trapdoor in searchable encryption, which make the performance of ReKeyGen unsatisfactory, which is what we need to improve in the future. Last but not least, our proposed scheme DSAS enjoys a good efficiency in encrypted information retrieve and ciphertext decryption requirement which show that our scheme DSAS is suitable for the e-healthcare system.

VI. CONCLUSION

In this paper, we presented a proxy-invisible condition-hiding proxy re-encryption scheme which supports keyword search that can be applied to securing data sharing and delegation in e-healthcare systems. With our new system, a doctor, Alice (delegator), may construct a conditional authorization for a doctor, Bob (delegatee), by specifying a re-encryption key. With the re-encryption key, the cloud server can perform ciphertext transformation so that Bob is able to access the PHRs original encrypted under Alice's public key, thus enabling secure delegation. The cloud server can operate search over encrypted PHRs on behalf of the doctor without learning information about the keyword or the underlying condition. Specifically, we achieved the property of proxy-invisible in the system. We have also obtained the property of collusion-resistance in the system, where a delegator's (Alice) private key is still secure even a dishonest cloud server colludes with the delegatee (Bob). We have demonstrated security through a rigorous proof, and the performance analysis confirms that our proposed scheme DSAS is efficient and practical.

REFERENCES

[1] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions," in Proc. Annu. Int. Cryptol. Conf. Berlin, Germany: Springer, 2005, pp. 205–222.

[2] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy reencryption schemes with applications to secure distributed storage," ACM Trans. Inf. Syst. Secur., vol. 9, no. 1, pp. 1–30, 2006.

[3] J. Baek, R. Safavi-Naini, and W. Susilo, "Public key encryption with keyword search revisited," in Proc. Int. Conf. Comput. Sci. Appl. (ICCSA), 2008, pp. 1249–1259. [4] T. Bhatia, A. K. Verma, and G. Sharma, "Towards a secure incremental proxy re-encryption for e-healthcare data sharing in mobile cloud computing," Concurrency Comput., Pract. Exper., vol. 32, no. 5, p. e5520, Mar. 2020.

[5] T. Bhatia, A. K. Verma, and G. Sharma, "Secure sharing of mobile personal healthcare records using certificateless proxy re-encryption in cloud," Trans. Emerg. Telecommun. Technol., vol. 29, no. 6, p. e3309, Jun. 2018.

[6] I. F. Blake, G. Seroussi, and N. Smart, "Advances in Elliptic Curve Cryptography (London Mathematical Society Lecture Note Series (317)), vol. 19. Cambridge, U.K.: Cambridge Univ. Press, no. 20, 2005, p. 666.

[7] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Advances in Cryptology-EUROCRYPT. Berlin, Germany: Springer, 1998, pp. 127–144.

[8] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. Int. Conf. Theory Appl. Cryptograph. Techn. Berlin, Germany: Springer, 2004, pp. 506–522.

[9] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Proc. Theory Cryptogr. Conf. Berlin, Germany: Springer, 2007, pp. 535–554.

[10] H. Fang, X. Wang, and L. Hanzo, "Learning-aided physical layer authentication as an intelligent process," IEEE Trans. Commun., vol. 67, no. 3, pp. 2260–2273, Mar. 2019.

[11] H. Fang, L. Xu, and X. Wang, "Coordinated multiple-relays based physical-layer security

improvement: A single-leader multiple-followers Stackelberg game scheme," IEEE Trans. Inf. Forensics Security, vol. 13, no. 1, pp. 197–209, Jan. 2018.

[12] L. Fang, W. Susilo, C. Ge, and J. Wang, "Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search," Theor. Comput. Sci., vol. 462, pp. 39–58, Nov. 2012.

[13] L. Fang, J. Wang, C. Ge, and Y. Ren, "Fuzzy conditional proxy reencryption," Sci. China Inf. Sci., vol. 56, no. 5, pp. 1–13, May 2013.

[14] J. Feng, L. T. Yang, R. Zhang, W. Qiang, and J. Chen, "Privacy preserving high-order bi-Lanczos in cloud-fog computing for industrial applications," IEEE Trans. Ind. Informat., early access, May 28, 2020, doi: 10.1109/TII.2020.2998086.

[15] J. Feng, L. T. Yang, Q. Zhu, and K.-K.-R. Choo, "Privacy-preserving tensor decomposition over encrypted data in a federated cloud environment," IEEE Trans. Dependable Secure Comput., vol. 17, no. 4, pp. 857–868, Jul. 2020.

[16] J.-S. Fu, Y. Liu, H.-C. Chao, B. K. Bhargava, and Z.-J. Zhang, "Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing," IEEE Trans. Ind. Informat., vol. 14, no. 10, pp. 4519–4528, Oct. 2018.

[17] M. Green and G. Ateniese, "Identity-based proxy re-encryption," in Applied Cryptography and Network Security. Berlin, Germany: Springer, 2007, pp. 288–306.

[18] D. He, M. Ma, S. Zeadally, N. Kumar, and K. Liang, "Certificateless public key authenticated encryption with keyword search for industrial Internet of Things," IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3618–3627, Aug. 2018.

[19] Y. J. He, T. W. Chim, L. C. K. Hui, and S.-M. Yiu, "Non-transferable proxy re-encryption scheme for data dissemination control," IACR Cryptol. ePrint Arch., vol. 2010, p. 192, Jan. 2010.

[20] Q. Huang, L. Wang, and Y. Yang, "Secure and privacy-preserving data sharing and collaboration in mobile healthcare social networks of smart cities," Secur. Commun. Netw., vol. 2017, pp. 1–12, Aug. 2017.

[21] Q. Huang, Y. Yang, and J. Fu, "PRECISE: Identity-based private data sharing with conditional proxy re-encryption in online social networks," Future Gener. Comput. Syst., vol. 86, pp. 1523–1533, Sep. 2018.

[22] B. Lynn. (2006). PBC Library. [Online]. Available: http://crypto. stanford.edu/pbc

[23] M. Ma, D. He, D. Kumar, K.-K. R. Choo, and J. Chen, "Certificateless searchable public key encryption scheme for industrial Internet of Things," IEEE Trans. Ind. Informat., vol. 14, no. 2, pp. 759–767, May 2017.

[24] Y. Miao, J. Ma, X. Liu, F. Wei, Z. Liu, and X. A. Wang, "m2-ABKS: Attribute-based multi-keyword search over encrypted personal health records in multi-owner setting,"J. Med. Syst., vol. 40, no. 11, p. 246, Nov. 2016.

[25] M. Naz, F. A. Al-zahrani, R. Khalid, N. Javaid, A. M. Qamar, M. K. Afzal, and M. Shafiq, "A secure data sharing platform using blockchain and interplanetary file system," Sustainability, vol. 11, no. 24, p. 7054, 2019.

[26] J. Ning, Z. Cao, X. Dong, K. Liang, H. Ma, and L. Wei, "Auditable σ time outsourced attribute-based encryption for access control in cloud computting," IEEE Trans. Inf. Forensics Security, vol. 13, no. 1, pp. 94–105, May 2018.

[27] J. Ning, Z. Cao, X. Dong, and L. Wei, "White-box traceable CP-ABE for cloud storage service: How to catch people leaking their access credentials effectively," IEEE Trans. Dependable Secure Comput., vol. 15, no. 5, pp. 883–897, Sep./Oct. 2018.

[28] J. Ning, X. Dong, Z. Cao, L. Wei, and X. Lin, "White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes," IEEE Trans. Inf. Forensics Security, vol. 10, no. 6, pp. 1274–1288, Jun. 2015.

[29] S. Niu, L. Chen, J. Wang, and F. Yu, "Electronic health record sharing scheme with searchable attribute-based encryption on blockchain," IEEE Access, vol. 8, pp. 7195–7204, 2020.

[30] P. Xu, S. He, W. Wang, W. Susilo, and H. Jin, "Lightweight searchable public-key encryption for cloud-assisted wireless sensor networks," IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3712–3723, Aug. 2018.

[31] J. W. Seo, D. H. Yum, and P. J. Lee, "Proxy-invisible CCA-secure typebased proxy re-encryption without random oracles," Theor. Comput. Sci., vol. 491, pp. 83–93, Jun. 2013.

[32] J. Shao, Z. Cao, X. Liang, and H. Lin, "Proxy re-encryption with keyword search," Inf. Sci., vol. 180, no. 13, pp. 2576–2587, 2010.

[33] S. Tahir, S. Ruj, Y. Rahulamathavan, M. Rajarajan, and C. Glackin, "A new secure and lightweight searchable encryption scheme over encrypted cloud data," IEEE Trans. Emerg. Topics Comput., vol. 7, no. 4, pp. 530–544, Oct. 2019.

[34] H. Wang, X. Dong, Z. Cao, D. Li, and N. Cao, "Secure key-aggregation authorized searchable encryption," Sci. China Inf. Sci., vol. 62, no. 3, p. 39111, Mar. 2019.

[35] H. Wang, J. Ning, X. Huang, G. Wei, G. S. Poh, and X. Liu, "Secure fine-grained encrypted keyword search for e-healthcare cloud," IEEE Trans. Dependable Secure Comput., vol. 18, no. 3, pp. 1307–1319, May/Jun. 2019.

[36] Q. Wang, W. Li, and Z. Qin, "Proxy re-encryption in access control framework of

information-centric networks," IEEE Access, vol. 7, pp. 48417–48429, 2019.

[37] X. A. Wang, X. Huang, X. Yang, L. Liu, and X. Wu, "Further observation on proxy re-encryption with keyword search," J. Syst. Softw., vol. 85, no. 3, pp. 643–654, 2012.

[38] J. Weng, R. H. Deng, X. Ding, C.-K. Chu, and J. Lai, "Conditional proxy re-encryption secure against chosen-ciphertext attack," in Proc. 4th Int. Symp. Inf., Comput., Commun. Secur. (ASIACCS), 2009, pp. 322–332.

[39] J. Weng, Y. Yang, Q. Tang, R. H. Deng, and F. Bao, "Efficient conditional proxy re-encryption with chosen-ciphertext security," in Proc. Int. Conf. Inf. Secur. Berlin, Germany: Springer, 2009, pp. 151–166.

[40] L. Xu, C. Xu, J. K. Liu, C. Zuo, and P. Zhang, "Building a dynamic searchable encrypted medical database for multi-client," Inf. Sci., vol. 527, pp. 394–405, Jul. 2020.