E-Healthcare System DSAS: A Secure Data Sharing and Authorised Searchable Framework

SHAIK SHAHANAJ [1], T SURESH [2]

[1] PG Scholar, Dept of CSE, Gokula Krishna College of Engineering, Sullurpeta, AP, India.

[2] Associate Professor, Dept of CSE, Gokula Krishna College of Engineering, Sullurpeta, AP, India.

ABSTRACT

By sharing encrypted personal healthcare records (PHRs) with doctors or medical research institutions, an increasing number of patients in the e-healthcare system receive high-quality medical services. However, one of the most significant issues is that encrypted PHRs make it impossible to efficiently search for information, which reduces data usage. Another issue is that the process of getting a medical treatment requires the doctor to be online all the time, which may not be possible for all doctors to afford (for example, being absent in certain situations). Medical service providers will be able to carry out remote PHR monitoring and research in an effective and safe manner thanks to the new secure and practical proxy searchable re-encryption scheme we develop in this paper. (1) Patients' healthcare records collected by devices are encrypted prior to uploading to the cloud server, ensuring privacy and confidentiality of PHRs, as part of our scheme, DSAS. 2) The PHRs can only be accessed by authorized doctors or research institutions; 3) Through the cloud server, Alice, the doctor in charge, can delegate medical research and utilization to Bob, the doctor in agent, or a specific research institution, thereby minimizing information exposure to the cloud server. We demonstrate our scheme's security and formalize the definition of security. Finally, our plan's effectiveness is demonstrated by performance evaluation.

1. INTRODUCTION

These days, with the quick improvement of man-made consciousness and the progression of wearable gadgets and sensors, e-medical services sensor network has arrived at a phase of development for reception and sending at a business scale. Patients greatly benefit from the e-healthcare sensor network as a mobile platform for receiving high-quality and efficient medical care. Patients' devices, as depicted in Fig. 1, collect a significant amount of personal healthcare records through sensor devices. By utilizing this data, doctors are able to more effectively diagnose and address the needs of patients. Additionally, this kind of data makes it possible for analysts and researchers in the medical field to use analytics to better understand diseases and develop more effective treatments. However, these data may be stored on cloud storage that is provided by third-party service providers [10, 16], [34], which raises the possibility of data leakage and other security concerns. This is because once the data is outsourced, neither the patients nor the doctors have control over the information. As a result, the confidentiality and privacy of these outsourced data ought to be safeguarded in such an environment. For instance, a number of medical facilities authorize the use of large amounts of PHRs by the Centers for Disease Control and Prevention (CDC) and store them on cloud servers. Doctors at the CDC are allowed to use data mining technology to study these data in order to make disease prevention and control easier. Be that as it may, during the time spent gathering case data from clinical foundations and the execution of customary information mining innovation, the CDC may definitely uncover touchy information of patients. It is extremely difficult to store, manage, and retrieve PHRs securely and effectively.

For practices, the e-healthcare system necessitates greater data and access security and privacy guarantees. All PHRs stored in the cloud should be encrypted in order to prevent information leakage [11], [14], [15], [26], [27], [42]_[44]. Despite the fact that encryption guarantees information classification and can be utilized to address worries of information protection and dodges the assaults from malignant clients and cloud servers, it additionally brings bother of use. For example, traditional encryption procedures render it dif_-faction to inquiry these encoded information [28] in light of the futile data recovery techniques in view of plaintext. Because of this restriction of customary, a large portion of the explores utilizes accessible encryption (SE) cryptosystem to ease such worries. Patients in the e-healthcare system use searchable encryption technology to first encrypt the potential keyword as an index before uploading it, along with the encrypted PHRs, to the cloud server. The authorized doctor or research institution can then use encrypted keyword search by sending the cloud server a trapdoor that was made with a particular keyword. The cloud server can use the trapdoor to perform keyword searches on the encrypted index and retrieve the records that correspond to those searches. In general, a searchable encryption cryptosystem makes it possible for a cloud server to search encrypted data on behalf of users without having to learn about keywords or plaintext.

With accessible encryption innovation, specialists in CDC can perform data recovery over scrambled PHRs and complete clinical treatment. However, such a system also implies that doctors must always be available. Treatment would be impossible if the doctor were not available. Intermediary re-encryption (PRE) [4], [5], [36] was proposed to tackle the above issue by permitting a confided in intermediary to safely change figure message having a place with one specialist to another so a specialist can designate the clinical treatment right to the next specialist in his missing. Take, for instance, the two physicians Alice and Bob. With Alice's public key, each patient can encrypt their healthcare records for Alice. Let's say Alice wants to delegate the decryption authority to Bob while she is away on vacation. With PRE innovation, Alice creates an encryption key in light of his confidential key and Bounce's public key, so that with the re-encryption key, the intermediary can re-encode a code message scrambled under Alice's public key into a code message of a similar message under Weave's public key. Nonetheless, there are two issues with the current PRE approach. To begin, the proxy has too much power: The proxy can transform all Alice cipher texts using the re-encryption key, regardless of the cipher text's keyword. Second, because of the bidirectional property, it is impossible to provide collusion-resistance in the event that a dishonest proxy conspires with the delegate to export the delegator's private key. This poses a serious security risk to the system because the delegate now has the ability to impersonate the delegator. As a result, it is necessary to limit the proxy server's capabilities.

2. LITERATURE SURVEY

1) A new general framework for secure public key encryption with keyword search

Public Key Encryption with Keyword Search (PEKS), introduced by Boneh et al. in Eurocrypt’04, allows users to search encrypted documents on an untrusted server without revealing any information. This notion is very useful in many applications and has attracted a lot of attention by the cryptographic research community. However, one limitation of all the existing PEKS schemes is that they cannot resist the Keyword Guessing Attack (KGA) launched by a malicious server. In this paper, we propose a new PEKS framework named Dual- Server Public Key Encryption with Keyword Search (DS-PEKS). This new framework can withstand all the attacks, including the KGA from the two untrusted

2) Searchable symmetric encryption: Improved definitions and efficient constructions

Searchable symmetric encryption (SSE) allows a party to outsource the storage of his data to another party in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research and several security definitions and constructions have been proposed. In this paper we begin by reviewing existing notions of security and propose new and stronger security definitions. We then present two constructions that we show secure under our new definitions. Interestingly, in addition to satisfying stronger security guarantees, our constructions are more efficient than all previous constructions.

Further, prior work on SSE only considered the setting where only the owner of the data is capable of submitting search queries. We consider the natural extension where an arbitrary group of parties other than the owner can submit search queries. We formally define SSE in this multi-user setting, and present an efficient construction

3. PROPOSED SYSTEM

In All Directions: Uni-directional intermediary re-encryption is more prevalent than multi-directional intermediary re encryption, in any case, the delegatee may pass consents to an outsider, which will build the exposure of security. As a result, the e-healthcare system's unidirectionality is a very important characteristic.

_ Invisible proxy: In the protected e-medical care framework, on the off chance that a malevolent client can recognize a re-scrambled ciphertext from a unique ciphertext, it will build the security hazard, for example, the malignant client knows the delegator isnot accessible at this moment. Thus, e-medical care framework should give intermediary undetectable.

Condition concealment: The condition of the conditional proxy re-encryption scheme frequently contains private data. The system will suffer greatly if the condition is revealed. Clearly, assuming that the intermediary condition is covered up, the intermediary server will get less delicate data, which makes the e-medical care framework safer.Consensus and Opposition: When a dishonest proxy conspires with the delegatee to export the delegator's private key, which would be disastrous for the e-healthcare system, it is impossible to provide collusion-resistance because of the inherent nature of trustworthy property. because these authorized works are typically carried out on a proxy server that is presumed to be untrusted for security reasons and is operated by a third-party service provider. As a result, a secure e-healthcare system that provides collusion resistance is essential**.**

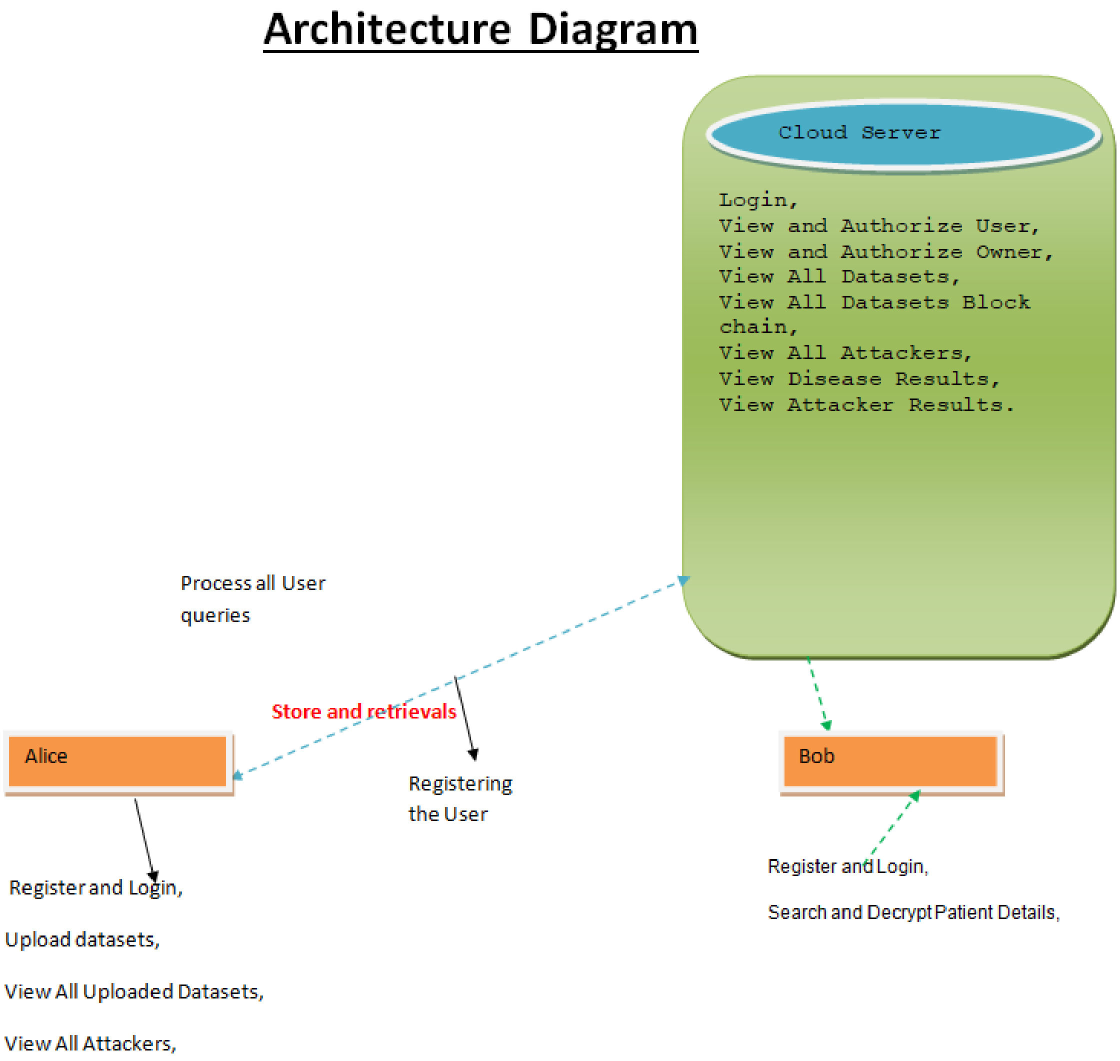


Fig 1:Architecture

3.1 IMPLEMENTATION

Cloud Server

In this module, the Admin has to login by using valid user name and password. After login successful he can do some operations such as Login, View and Authorize User, View and Authorize Owner, View All Datasets, View All Datasets Block chain, View All Attackers, View Disease Results, View Attacker Results.

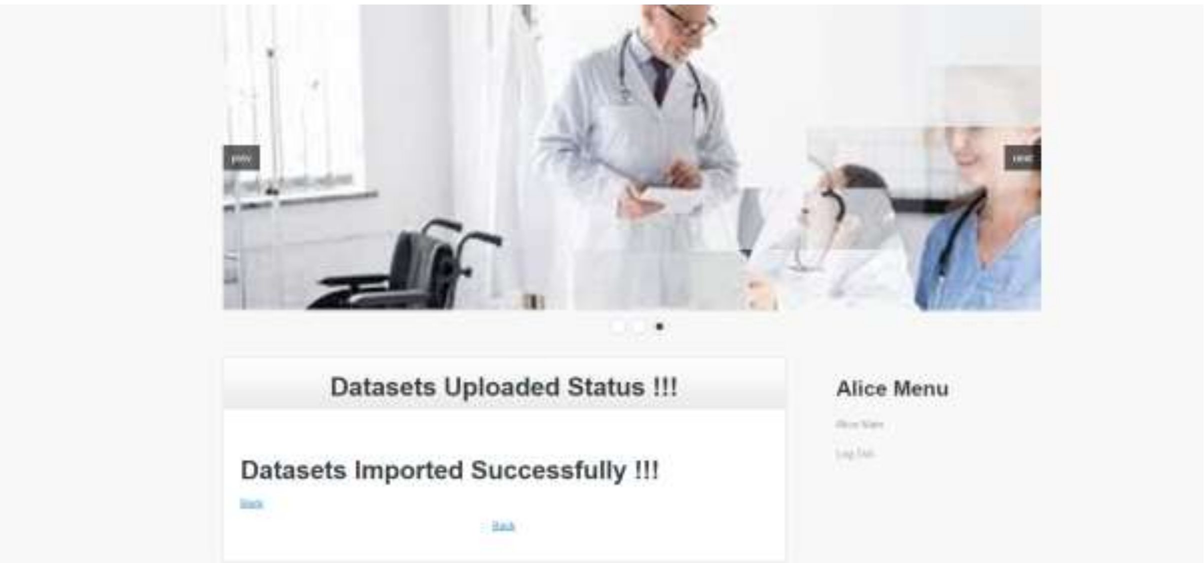
Bob

In this module, there are n numbers of users are present. User should register with group option before doing some operations. After registration successful he has to wait for admin to authorize him and after admin authorized him. He can login by using authorized user name and password. Login successful he will do some operations like Register and Login, Search and Decrypt Patient Details

Alice

In this module, there are n numbers of users are present. Transport Company user should register with group option before doing some operations. After registration successful he has to wait for admin to authorize him and after admin authorized him. He can login by using authorized user name and password. Login successful he will do some operations like Register and Login, Upload datasets, View All Uploaded Datasets, View All Attackers,

4. RESULTS AND DISCUSSION



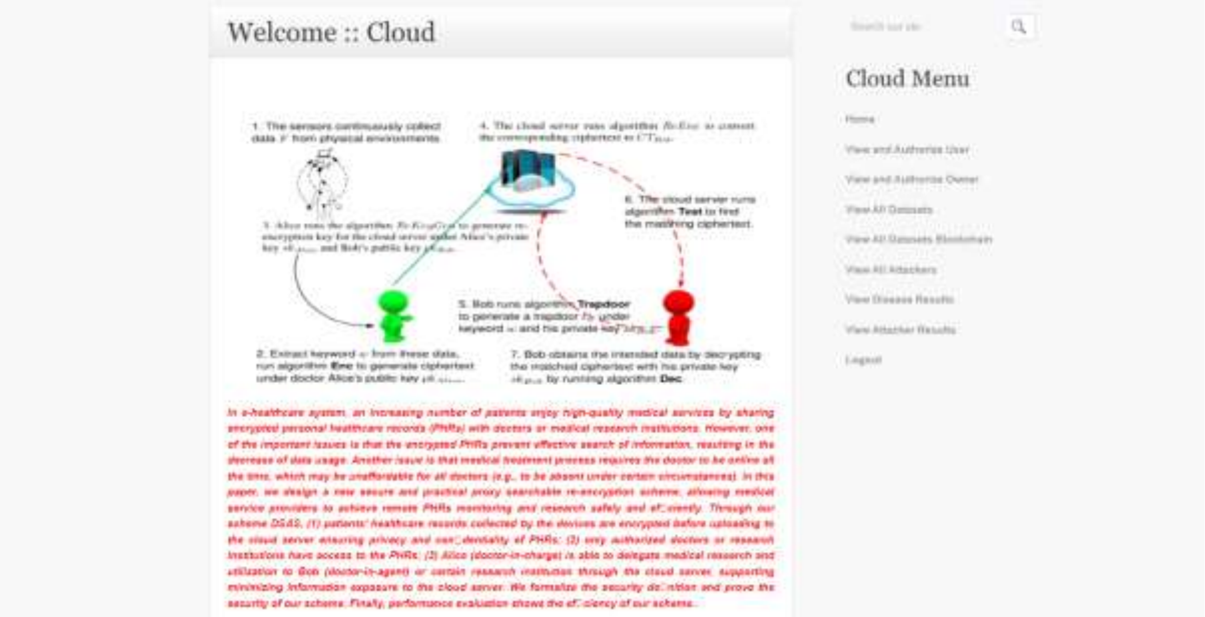
Datasets Uploaded Status !!!

Datasets Imported Successfully !!!

Back

Back

Fig 2:Dataset Uploaded Successfully


Welcome :: Cloud

1. The sensors continuously collect data from physical environments.

2. Extract keyword from these data, run algorithm **Enc** to generate ciphertext under doctor Alice's public key.

3. Alice runs the algorithm Re-KeyGen to generate re-encryption key for the cloud server under Alice's private key and Bob's public key.

4. The cloud server runs algorithm Re-Enc to convert the corresponding ciphertext to CT_{Bob}.

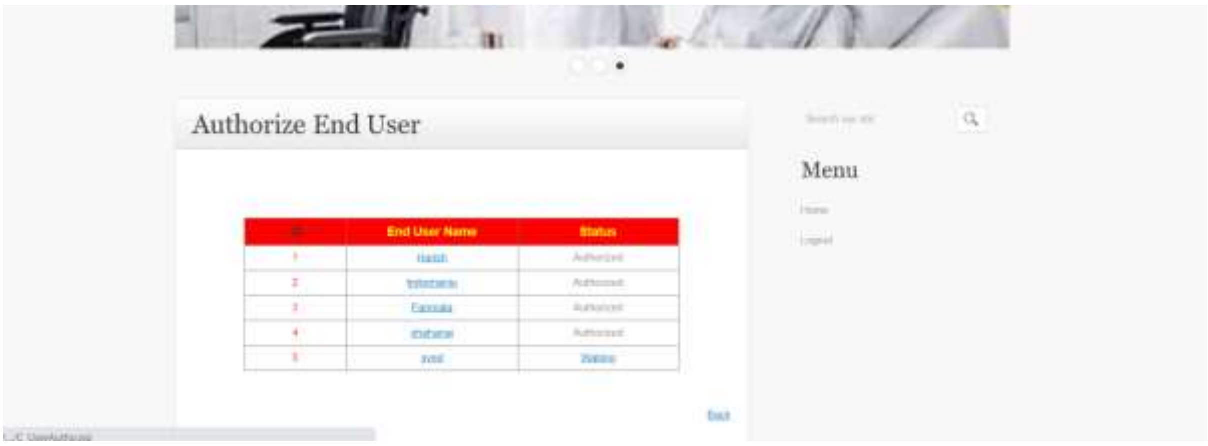
5. Bob runs algorithm **Trapdoor** to generate a trapdoor under keyword and his private key.

6. The cloud server runs algorithm **Test** to find the matching ciphertext.

7. Bob obtains the intended data by decrypting the matched ciphertext with his private key by running algorithm **Dec**.

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 ef□ciently. Through our scheme DSAS, (1) patients' healthcare records collected by the devices are encrypted before uploading to the cloud server ensuring privacy and con□dentiality 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 de□nition and prove the security of our scheme. Finally, performance evaluation shows the ef□ciency of our scheme.

Fig 3:Cloud Main Page



Authorize End User

[illegible]	End User Name	Status
1	Harish	Authorized
2	[illegible]	Authorized
3	[illegible]	Authorized
4	[illegible]	Authorized
5	[illegible]	Waiting

Fig 4:Authorise User

5. CONCLUSION

In this paper, we introduced an intermediary imperceptible condition-concealing intermediary re-encryption plot which upholds watchword search that can be applied to getting information sharing and designation in e-medical services frameworks. By specifying a re-encryption key, a doctor named Alice (the delegator) can use our new system to create a conditional authorization for a doctor named Bob (the delegate). The cloud server can perform cipher text transformation with the re-encryption key so that Bob can access the PHRs that were originally encrypted using Alice's public key and enable secure delegation. The doctor's encrypted PHRs can be searched by the cloud server without the doctor knowing anything about the keyword or the hidden condition. In particular, we were successful in achieving the system-invisible proxy property. In addition, we have obtained the system's property of collusion-resistance, which ensures that a delegator's (Alice) private key remains secure even when a dishonest cloud server conspires with Bob. The performance analysis confirms that our proposed scheme, DSAS, is effective and practical, and we have demonstrated security through rigorous proof.

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 exten-
sions,'' 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 re-encryption 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 certi_cateless 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 re-encryption," *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, ``Certi_cateless 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, ``Certi_cateless 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.