A PROTECTING DATA SHARING AND TRUSTED SEARCHABLE STRUCTURE FOR ONLINE HEALTHCARE SYSTEM IN CLOUD

Spurthi K [1] ,Dr. Kishore Kumar K[2] , Mr. G Naga Kumar Kakarla[3]

[1]*Assistant Professor, Dept of CSE, Siddhartha Institute of Technology & Sciences, Narapally, Hyderabad, 500088, India.*

[2]*Associate Professor Dept of CSE, Siddhartha Institute of Technology & Sciences, Narapally, Hyderabad, 500088, India.*

[3]*Associate Professor, Computer Science and Engineering Gokaraju Lailavathi Womens Engineering College Hyderabad, 500049*

ABSTRAT

In the electronic healthcare system, an increasing number of patients enjoy high-quality medical services by sharing encrypted personal health records (PHRs) with doctors or medical research institutions. However, one important issue is that encrypted personal health records prevent effective information searching, resulting in decreased data usage. Another problem is that the medical treatment process requires the doctor to be online all the time, which may not be within the reach of all doctors (for example, absence in certain circumstances). In this paper, we design a new, secure and practical proxy search cryptosystem, which allows healthcare providers to realize remote PHR monitoring and investigation safely and efficiently. With our DSAS system, (1) patient healthcare records collected by devices are encrypted before being uploaded to the cloud server, ensuring the privacy and confidentiality of personal health records; (2) only physicians or accredited research institutions have access to personal health records; (3) Alice (the responsible doctor) can delegate and benefit from medical research to Bob (the responsible doctor) or a designated research institution through the cloud server, thus reducing the information exposure to the cloud server. We formalize the definition of security and explain the security of our scheme. Finally, the performance evaluation shows the efficiency of our scheme.

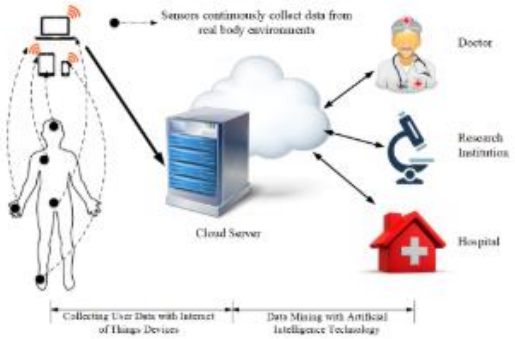
Keywords: Proxy re-encryption, proxy invisibility, searchable encryption, mobile healthcare sensor networks.

I INTRODUCTION

Nowadays, with the rapid development of artificial intelligence and the advancement of sensors and wearable devices, electronic healthcare sensor network has reached the maturity stage for commercial-scale adoption and deployment. The network of electronic healthcare sensors acting as a mobile platform greatly benefits patients by getting high-quality and effective medical treatment. As shown in Figure 1, patient devices collect a large amount of personal medical records through sensors, allowing doctors to diagnose and meet patients' needs more effectively through the use of these histories. This information also allows researchers and medical analysts to perform analyzes to gain better insights into diseases and devise better treatments. However, this data may be stored in the cloud provided by third-party service providers [10] which may lead to potential security issues such as data leakage. This is because neither patients nor doctors can control the information by simply outsourcing the data. This means that the privacy and confidentiality of this external data must be protected in such an environment. For example, some medical organizations collect and store a large number of personal health records on cloud servers and report the use of this data to the Centers for Disease Control and Prevention (CDC). To facilitate disease prevention and control, CDC doctors can study this data using data mining technology. However, in the process of collecting case information from medical institutions and implementing traditional data mining technology, the CDC may inevitably reveal sensitive patient data. How to store, manage,

and retrieve personal health records securely and efficiently are a major challenge.

The electronic healthcare system requires greater assurances of security and privacy for practices regarding data and access to it. To prevent information leakage from stored personal health records, all personal health records stored in the cloud should be encrypted [11], [14], [15] .Although encryption ensures data confidentiality and can be used to address data privacy issues and prevent attacks from malicious users and cloud servers, it also has disadvantages in use. To



Finger no: 1. Mobile healthcare system.

For example, traditional encryption techniques make it difficult to query this encrypted data because plain text-based information retrieval methods are useless. Because of this traditional limitation, most research uses a searchable encryption (SE) scheme to mitigate these concerns. Using searchable encryption technology, patients in the electronic healthcare system first encode the potential keyword as an index and then upload it to the cloud server along with their encrypted personal health records. Then, the doctor or licensed research institution can perform an encrypted search for a keyword by sending a trapdoor generated using a specific keyword to the cloud server. Using a trapdoor, the cloud server can perform a keyword search in the encrypted index and retrieve the corresponding records. In general, a searchable encryption system allows a cloud server to search encrypted data on behalf of users without knowledge of keywords or plain text. Using searchable encryption technology, CDC doctors can retrieve information through encrypted personal health records and perform medical treatments. However, such a system also means that doctors must be available at all times. If the doctor is not connected, medical treatment will not be possible. Proxy reencryption (PRE) [4], [5], has been proposed to solve the above problem by allowing a trusted agent to securely transfer one doctor's ciphertext to another so that the doctor can authorize the correct medical treatment. For the other doctor in his absence. For example, suppose there are two doctors, Alice and Bob. Every patient who has Alice's public key can encrypt Alice's medical records. Suppose Alice is on vacation and wants to delegate the decryption right to Bob. Using the PRE technique, Alice generates a re-encryption key based on her private key and Bob's public key, so that the agent can, using the re-encryption key, re-encrypt ciphertext using Alice's public key into the ciphertext of the same message. Under Bob's public key. However, there are two problems with the current PRE approach. First, the proxy is very powerful: using the re-encryption key, the proxy can convert all of Alice's ciphertexts regardless of what keyword the ciphertext contains. Second, inherent in the two-way property, it is impossible to provide collusion resistance when the dishonest proxy colludes with the delegate to export the delegate's private key, which poses a serious security problem for the system as you can now impersonate the delegate. Therefore, it is necessary to restrict the power of the proxy server. A searchable conditional proxy re-encryption (CPRE) scheme can be implemented to overcome the above problem. In a CPRE system, the delegate generates the re-encryption key with a condition that aims to identify the ciphertext that satisfies the condition. Unfortunately, most existing CPRE schemes cannot

guarantee the privacy of the case, which also contains sensitive information. On the other hand, if a malicious user can distinguish between the re-encrypted ciphertext and the original ciphertext, the security risks increase, such as the malicious user knowing that Alice is currently unavailable. Therefore, the new conditional proxy encryption must be invisible to the proxy, as the malicious user cannot distinguish between the original ciphertext and the re-encrypted ciphertext. In brief, existing solutions apply several approaches (e.g., searchable encryption, new proxy encryption, new conditional proxy encryption) and share personal health records with doctors or medical research institutions to protect data privacy. However, retrieving information through encrypted personal health records remains a challenge, especially when dealing with big data at a granular level.

II EXISTING SYSTEM

With the rapid advancement of cloud computing, more and more patients are willing to transfer their personal health records to cloud servers to benefit from the convenient services provided. These personal health records are often stored in encrypted form in the cloud to protect the security of user data and private information. However, when the user tries to access files that contain some interesting keywords, data encryption comes in the way of effective data usage. To protect sensitive healthcare files in cloud storage and enable cloud servers to search encrypted data under patient control, Yang et al. . Provide a secure, searchable, and privacy-preserving system based on searchable encryption. Bonnet et al. Introduced the idea of public key encryption using keyword search (PEKS) and provided the first application of PEKS to an electronic healthcare system operating in a public key environment. Later, the idea of consistency was proposed and the PEKS concept was reviewed by Abdullah et al. Electronic healthcare system has more expressive search schemes and search schemes are proposed to improve data storage and retrieval in a multi-user environment in order to store a large number of personal health records from multiple users. In addition to searchable encryption, Blaze et al. The proposed proxy re-encryption (PRE) technique has also been used in electronic healthcare system to store and exchange medical data. Recently, new proxy encryption has been widely used to enable transfer of ciphertext to cloud storage services, making it a very promising option for cloud computing. A one-way approach was developed in 2005 by Ateniese et al. Which also showed how to prevent the agent from working with delegates to reveal the delegate's secret key. Green and his colleagues presented a non-transferable proxy encryption method that addresses both the tyranny of PKG and key security issues. Fang et al. Introduced a new fuzzy conditional agent cipher, along with a concrete construct based on the “overlap set” distance metric. To allow the data owner to grant permission to the healthcare analyst to access his or her data, PRE was implemented in a healthcare mobile social network.

III LITERATURE SURVEY

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

Public key encryption using keyword search (PEKS), introduced by Bonnet et al. In Eurocrypt'04, users are allowed to search for encrypted documents on an untrusted server without revealing any information. This idea is very useful in many applications and has attracted a lot of attention from the crypto research community. However, one limitation of all existing PEKS schemes is that they cannot resist a Keyword Guessing Attack (KGA) launched by a malicious server. In this paper, we propose a new PEKS framework called Double Server Public Key Encryption with Keyword Search (DS-PEKS). This new

framework can resist all attacks, including KGA attacks from two untrusted attacks.

2 Searchable symmetric encryption: Improved Definitions and Efficient Constructions Searchable Symmetric Encryption (SSE) allows one party to outsource the storage of its data to another party privately, while maintaining the ability to perform selective searches on it. This problem has been the focus of active research and several definitions and security architectures have been proposed. In this article we begin by reviewing current concepts of security and propose new and more robust definitions of security. We then present two constructs that we feel confident based on our new definitions. Interestingly, in addition to meeting greater safety guarantees, our facilities are more efficient than all previous constructions. Furthermore, previous work on SSE only considered the setting in which only the data owner can submit search queries. We consider the normal extent to which an arbitrary group of parties other than the owner can submit search queries. We formally define ESS in this multi-user environment and provide an efficient architecture.

IV PROPOSED SYSTEM

In all directions: One-way intermediate re-encoding is more common than multi-directional intermediate re-encoding; However, the delegate may give consent to a third party, which will increase the security exposure. Therefore, the unidirectionality of the esalud system is a very important property. _ Hidden agent: In a protected e-health setting, if a malicious agent can identify a ciphertext that has been recoded from a unique ciphertext, this will create a security risk; For example, the malicious client knows that the delegate is not malicious. is accessible at this time. Therefore, the e-healthcare framework must make the middleman undetectable. Condition Hiding: The condition of the conditional proxy re-encryption system often contains private data. The system will suffer greatly if the condition is detected. Obviously, assuming the intermediary state is hidden, the intermediary server will obtain less sensitive data, making the e-healthcare framework more secure. Consensus and Dissent: When a dishonest agent conspires with the delegate to export the delegate's private key, which could be disastrous for an electronic healthcare system, it is impossible to resist collusion due to the inherent nature of trusted ownership. Because these authorized actions are usually performed on a proxy server that is assumed to be untrusted for security reasons and is operated by a third-party service provider. As a result, a secure electronic healthcare system that provides resistance to collusion is essential.

SYSTEM ARCHITECTURE:

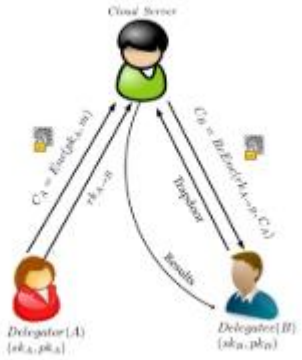


FIGURE 2. System model.

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 ⊥ indicating an error.

B. DSAS CONSTRUCTION

Let G and GT be groups of order p, and let e : G × G → GT be the bilinear map. Our conditional proxy re-encryption with keyword search system works as follows.

• **Setup(1λ):** Given a security parameter λ, the setup algorithm chooses G and GT to be groups of order p with the bilinear map e : G × G → GT and chooses a strongly unforgeable one-time signature Sig = (G, S, V). It picks random generators g, f , h, u, v ∈ G. Also, two hash functions H1 : {0, 1} ∗ → G and H2 : {0, 1} ∗ → Z ∗ p are selected randomly. The public parameters param are given by

param = (G, GT , e, g, f , h, u, v, Sig, H1, H2)

• **KeyGen(1λ):** On input 1λ , user i chooses random xi, yi ∈ Z ∗ p and sets Xi = f xi and Yi = h yi . The public key and private key of user i are

pki = (Xi, Yi), ski = (xi, yi)

• **Enc(pk, m,w):** To encrypt a message m ∈ GT under the public key pki , the data owner selects a one-time signature key pair (ssk,svk) ← G(λ), picks random s,r ∈ Z ∗ p , and sets h {C1 = Y r i ,C2 = f 1 r ,C3 = f s r ,C4 = X s i · f −s·H2(IDi) , C5 = e(h, H1(w))r ,C6 = (u svk · v) s }

C7 = m · e(f , h) −s i

where IDi is identity of user i. Then, the data owner generates a one-time signature σ = S(ssk, (C6,C7)), outputs the ciphertext as

CTi = (svk,C1,C2,C3,C4,C5,C6,C7, σ)

ReKeyGen(ski, pkj,w): Given a user i's private key ski , a user j's public key pkj and condition w, user i sets re-encryption key rkw i→j = (rk1,rk2,rk3) as rk1 = Y 1 xi−H2 (IDi) j , rk2 = H1(w) 1 yi , rk3 = e(H1(w), h) 1 xi−H2 (IDi)

ReEnc(rkw i→j ,CTi): Given the re-encryption key rkw i→j = (rk1,rk2,rk3) and a ciphertext CTi =(svk,C1,C2,C3,C4,C5,C6,C7, σ), the cloud server first checks whether the condition hold by running Test. If the outputs is ⊥ then terminate; Otherwise, the cloud server picks random t ∈ Z ∗ p and computes {C 0 1 = rkt 1 ,C 0 2 = (Xi · f −H2(IDi)) 1 t ,C 0 3 = C 1 t 4 , C 0 4 = C4,C 0 5 = rkt 3 ,C 0 6 = C6,C 0 7 = C7i}

The re-encrypted ciphertext for user j is

CTj = (svk,C 0 1 ,C 0 2 ,C 0 3 ,C 0 4 ,C 0 5 ,C 0 6 ,C 0 7 , σ)

• **Trapdoor(sk,w):** On input a user i's private key ski and a keyword w, output the keyword w's trapdoor as tw = H1(w) 1 yi

• **Test(CT , tw):** Given the trapdoor tw and ciphertext CTi , the cloud server checks the the validity of the ciphertext by testing the following relations. – V(svk, σ,(C6,C7)) = 1 –

e(C2,C1 · C6) = e(f , Yi) · e(u svk · v,C3) If the check is fails, output ⊥. Otherwise do the test step: If e(tw,C1) = C5, then output ‘‘1’’; otherwise output ‘‘0’’.

• **Dec(sk,CT):** On input of a user i’s private key ski and ciphertext CTi = (svk,C1,C2,C3,C4,C5,C6,C7, σ), user i first checks the validity of the ciphertext. If the check fails, then output ⊥. Otherwise, user i output a message by computing m = C7 · e(C1,C3) 1 yi

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 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

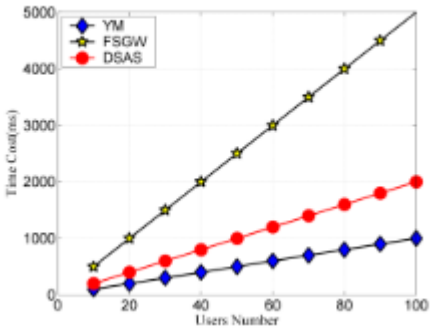


Fig no 3: Performance of KeyGen.

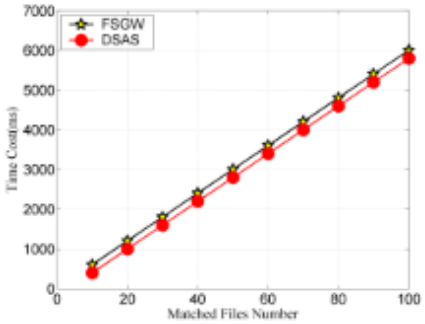


Fig no 4: Performance of decrypt.

CONCLUSION

We present an invisible condition-hiding proxy encryption system supporting keyword search that can be applied to secure data sharing and authorization in e-healthcare systems. Using our new system, the doctor, Alice (the delegate), can create a conditional license for the doctor, Bob (the delegate), by specifying the re-encryption key. Using the re-encrypted key, the cloud server can perform ciphertext transformation so that Bob can access the original personal health records encrypted with Alice's public key, enabling secure authorization. The cloud server can search encrypted personal health records on behalf of the doctor without obtaining information about the keyword or underlying condition. Specifically, we achieve the property of an invisible agent in the system. We have also gained a collusion-proof feature in the system, where the private key of the delegate (Alice) remains secure until a rogue cloud server colludes with the delegate (Bob). We have proven the security through rigorous testing and performance analysis that

confirms that our proposed DSAS scheme is efficient and practical.

REFERANCES

[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.