RESEARCH ARTICLE OPEN ACCESS

A Lightweight Policy Update Scheme for Outsourced Personal Health Records Sharing

Mrs. B. Vijaya, MCA, M.Tech [1], N. Sai Kalpana [2]

[1] Asst. Professor, Department of Master of Computer Applications
[2] Student, Department of Master of Computer Applications
[1], [2] Chadalawada Ramanamma Engineering College (Autonomous)

ABSTRACT

Personal health record is maintain in the centralize server to maintain patient's personal and diagnosis information. Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. The security schemes are used to protect personal data from public access. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. In the greater part of the past plans, in spite of the fact that the entrance policy is hidden, they face two functional issues: (1) these plans don't bolster huge attribute universe, so their reasonableness in PHR is significantly restricted, and (2) the expense of decryption is particularly high since the entrance policy is installed in ciphertext. To address these issues, we build a CP-ABE plot with effective decryption, where both the size of open parameters and the expense of decryption are steady. It needs to keep multiple encrypted copies of the same key that incurs high computational costs. So, there is a need for a suitable access control mechanism that should support effective policies.

Keywords: Personal Health Record (PHR), Attribute-Based Encryption, Hidden Policy, Fast Decryption.

I. INTRODUCTION

Cloud Computing has become a necessary piece of our day to day life. We can see the utilizations of cloud utilized all over the place, it is possible that it could be web applications or portable applications, IOT Applications or Data-based applications, the cloud has become a typical term in the IT Industry. Indeed, even a layman is likewise utilizing the cloud with or without the information on cloud. As per a report introduced by Statista entrance, the quantity of cloud-based customers has expanded from 2.4 billion of every 2013 to 3.6 billion in the year 2018. The world's all out populace is 7.6 billion individuals, and on the off chance that you see the past insights from Statista entryway, half of the total populace is legitimately or by implication getting to/expending the Cloud Services [1]. When such countless individuals use cloud benefits by putting away what's more, getting to information, you can envision the sort of issues like Storages [2], Processing Speed, Security, Privacy, etc..,.

By one way or another, Cloud Service suppliers have handled the issues referenced above, however Security remains the most vital concern which makes the engineers or IT experts reconsider before utilizing the cloud administrations and due to the prominence and accessibility of cloud computing [3] presently numerous associations redistribute their information to the remote server to forestall monetary weight and offer comprehensively, cloud specialist co-ops are right now problematic in light of the numerous security challenges. Cloud as the computing or preparing of remote assets or administrations and these administrations are IaaS, PaaS, SaaS, etc.

Cloud can send in four different ways, for example, private, open, mixture and network cloud. Each client interfaces with the Web and uses the IT framework to meet their day by day needs as the interest for the Internet increments [4]. Indeed, even help conveyed as programming, stage, database, stockpiling administrations, and so forth cloud offers "Pay more only as costs arise" to the client, greatest advantages can accomplish by utilizing these administrations at a lower cost.

Security issues in cloud computing

In Addition to Benefits for utilizing cloud computing programming what's more, support, there are a couple of wellbeing issues in computing.
They involve:

1. Lock-in: It's the issue of versatility and Inter-operability. Lock-in trouble could be to get merchants and information. Information [5] Lock-in: Information Saved at one cloud site can't promptly evacuate if an individual needs to adjust a cloud provider. It could ascribe to the nonattendance of institutionalized Programming interface. This prompts an

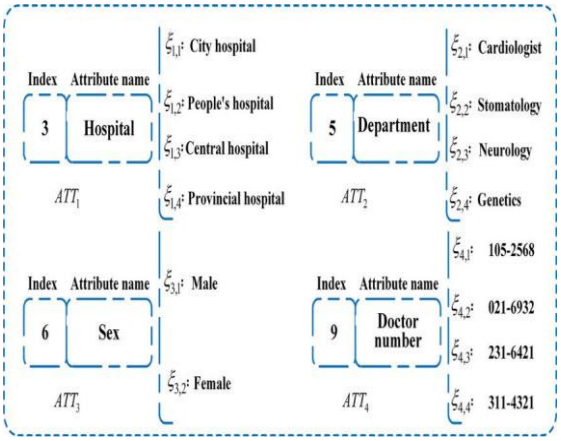

FIGURE 1. Instances of attribute classifications in PHR.

issue of data lock-in. Cloud provider gives administrations concerning APIs. Programming interface made for a single provider of cloud probably won't be useful for another provider's cloud. On the off chance that a difference in provider is fundamental, at that point APIs additionally should be modified, bringing about halfway redevelopment of this program. This issue named as dealer lock-in.

2. Administration Availability: To get cloud customer, administration should be available consistently. Each time a client requests cloud help, the provider and buyer need to enlist SLA (Administration Level Agreement). This characterizes the stipulations and details for cloud facilitating support. Furthermore, it has a level of time support is accessible [6]. A cloud client envisions a top accessible help with negligible or no personal time. A cloud provider and its relating supplier is picked dependent on administration openness and friends necessities.

3. Bottleneck: Data transport bottleneck and backing disturbance are a couple of the issues caused on account of data transfer capacity limitation [7].

4. Data protection: For a Variety of organizations, worries about wellbeing, protection [8], consistence, and power over their data are difficulties in moving towards grasping a cloud model.

The main hidden ciphertext-policy attribute-based encryption (HCP-ABE) was presented in [16], where the entrance structure was installed in the ciphertext and not sent legitimately. In this way, some other hidden CP-ABE plans were additionally progressively proposed in [17]–[19]. Be that as it may, get to structures in these plans just help AND doors or AND entryways on positive, negative and trump card. These lead to two downsides. In spite of the fact that the above plans improve the effectiveness of decryption [9], the length of ciphertext is additionally altogether expanded and this will end up being a bottleneck confining better. Furthermore, these plans are very defenseless against decisional Diffie-Hellman test (DDH-test) assault.

II. RELATED WORK

Since Attribute-Based Encryption was first proposed by Waters [6], it has been viewed as the most encouraging methodology for fine-grained get to control in the field of distributed computing. With the

persistent enhancements of ABE, presently, there are predominantly two fundamental kinds of ABE plans, Key Policy ABE (KP-ABE) [12], and Ciphertext Policy ABE (CP-ABE) [7], [10], [11], [13]. In the KP-ABE plot, keys are related with get to structure and ciphertexts are related with a lot of attributes. The main KP-ABE conspire was proposed by Goyal et al. [14]. Be that as it may, right now, believed authority completely decides the mix of attributes related with the ciphertext, in light of the fact that the entrance control related with the key is produced by the middle for each real decryption client. At that point Sahai et al. proposed another KP-ABE conspire, in which the decryption keys of clients' could communicate any entrance equations over attributes, including non-monotone ones.

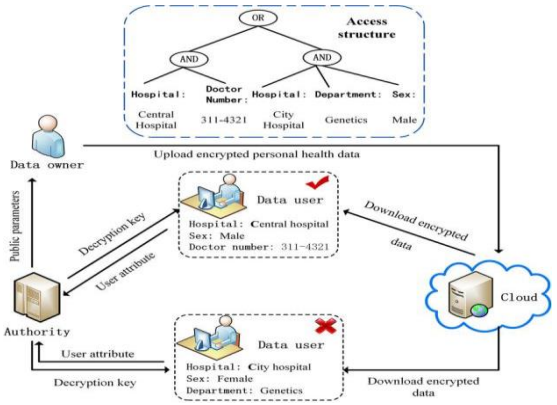

FIGURE 2. Case of PHR distributed storage.

The first CP-ABE conspire was presented in [7], where ciphertexts were related with get to structure characterized by information proprietors and the key is related with sets of attributes about clients. Along these lines, there are a great deal of CP-ABE plans were likewise progressively proposed in [15], [17], [18], [21], however these plans just help AND entryways. To understand the entrance structure progressively expressive, Waters proposed an entrance structure-based a direct mystery sharing plan (LSSS), and it is likewise a provably secure plan under the standard model [23]. So as to additionally ensure clients' protection, the first CP-ABE plot with hidden access structure was proposed by Yoneyama et al. [16]. In their work, get to control policy isn't sent alongside ciphertext unequivocally, at the end of the day, no unapproved client can acquire helpful data about the entrance structure. Some different plans with a similar exhibition have been proposed by different analysts, which are called Anonymous Attribute-Based Encryption [22]. In these plans, just arrangements of the client fulfilling the entrance policy were implanted in the ciphertext; at that point the client can effectively decode the ciphertext [20]. Afterward, the creators presented another profoundly powerful unknown CP-ABE plan, and its security verification was given under the Decisional Modified Bilinear Diffie-Hellman suspicion (MBDH) [20]. Notwithstanding, their work just gives a general investigation and needs itemized security verification. Some different works were proposed in [9], [14], to make further enhancements for the mysterious CP-ABE conspire. Sadly, every one of them needs to confront the high-overhead of decryption, which may cause them to lose their practicability.

A. Storing a PHR

The PHR data storing process begins with creating the PHR data as shown in Figure 3. Once a new record is created, the message digest is calculated to support the data integrity checking in the system. The message digest will be calculated as md = H(m) by using the hashing algorithm (SHA-2).

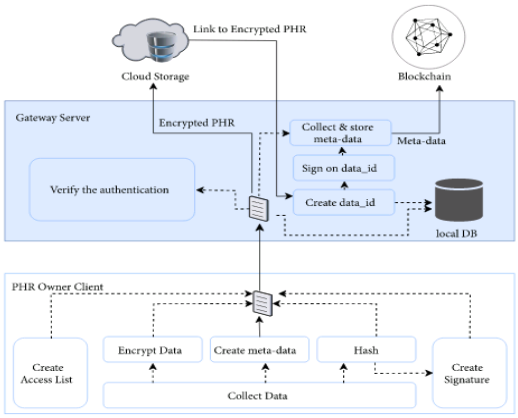

Figure 3 The process for storing a new PHR.

B. Retrieving a PHR

To retrieve the PHR data, the user can get the information of the requested PHR data via the metadata from the private blockchain as shown in Figure 4. The user verifies the PHR data using the owner signature and the signature of the gateway server. If the PHR data is correct, the user appends the timestamp to the data-id and signs on it. Then, the user sends the resulting signed data-id to the gateway server in order to request the actual PHR data.

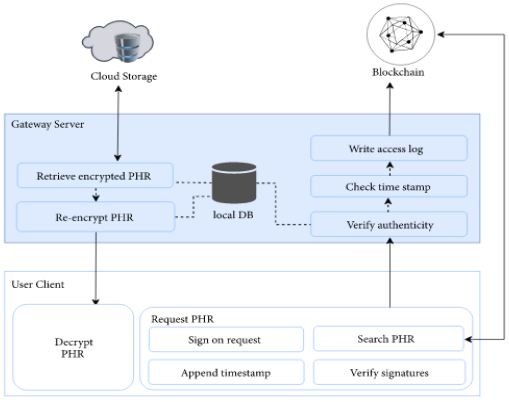

Figure 4 The process for retrieving a PHR.

The gateway server checks the user authenticity using the user signature. Next the gateway server checks the time stamp on the request and validates the request life time. If the user is authorized, the gateway server stores the request on the private blockchain for auditing purpose. Then, the gateway server retrieves the information related to the data from the local storage using the data-id, and the requested encrypted PHR data is retrieved from the cloud storage.

C. Revoking a User

The case of revoking a user is also considered in our PHR model. The cloud storage is provided to store the actual encrypted PHR data. All users query the encrypted PHR through the gateway server. The gateway server verifies each request in terms of the authority of the requester according to the predefined access list generated by the PHR owner. After successfully verifying the request, the gateway server stores the transaction log information on the blockchain and reencrypts the PHR for the authorized users with the corresponding reencryption key. As a result, the PHR owner can revoke any access to his/her PHR data by updating the access list and maintaining the ownership on the PHR. Section provides more information on how our model can resist the collusion attack. The time-consuming encryption process does not need to be performed as long as nobody performs the auditable access of the data. If gateway server violates the assumption that the gateway server follows the procedure defined in this work (semitrusted), it can be audited on blockchain. If

some suspicious action of the revoked user is found on blockchain, the PHR owner must update his/her data and encrypt the data again. Thus, the encryption process will be necessary for totally untrusted gateway server.

D. Access Control Protocol

Under our proposed model, the access control protocol by the way of proxy reencryption reduces the requirement of the gateway server. As such, the gateway server can be viewed as a semitrusted entity in our proposed model. The actual PHR data is securely encrypted with the PHR owner public key, and the ciphertext can be accessed by a group of authorized users according to the access. The access to the actual PHR data can be easily revoked by updating the access list. The delegated user can also add new PHR data and create the corresponding metadata on behalf of the PHR owner. The access control list is stored in the local database of the gateway server. However, the corresponding secret keys are protected because the secret key belongs to the PHR owner. The reencryption keys used by the gateway server can only be generated by the PHR owner. Moreover, the reencryption keys only allow the gateway server to reencrypt the original ciphertext for the authorized user. Thus, the gateway server cannot gain access to the actual PHR data, because the actual PHR data will never be decrypted at the gateway server.

III. PROPOSAL WORK

HIDDEN CIPHERTEXT POLICY ATTRIBUTE-BASED ENCRYPTION

A hidden CP-ABE conspire comprises of the accompanying four calculations.

Arrangement (1 !) (P K; M SK): It is a randomized calculation that accepts a security parameter as info and yields the open parameters P K and ace key M SK.

KeyGen (P K; M SK; S)! SK: The key age calculation takes the open parameters P K, the ace key M SK and the client's attributes set S as information. It yields the client's private key SK related with S.

Scramble (P K; M; (A; ; T))! CT : The encryption al-gorithm takes the open parameters P K, a plaintext message M, and an entrance structure (A; ; T) as information, and yields a ciphertext CT , where T is a lot of attribute esteems in the entrance structure and not sent alongside the ciphertext CT .

Decode (P K; SK; CT!) M: It takes the open parameters P K, a mystery key SK related with the attributes set S= (IS; LS), and a ciphertext CT encoded under access structure (A;) as info, and yields the message M or an exceptional image? Means that a client neglected to unscramble the ciphertext CT .

SECURITY MODEL

Right now, give the security model for our plan. This particular security model is depicted by a security game between an enemy and a challenger B. The game continues as follows.

Arrangement: The challenger B runs this calculation (1) to yield the open parameters P K and the ace key M SK. At that point, the open parameters are sent to the enemy A .

Stage 1: The enemy A submits sets of attributes S1; S2; :::; SQ to the challenger B for the mystery key, where, Q is a polynomial limited number. The challenger creates mystery key SKSi relating to the arrangement of attribute Si by running the calculation (P K; M SK; Si!) SKSi . Challenge: The enemy A submits two test messages M0, M1 (jM0j = jM1j) and two access structures (A; T0), (A; T1) to the challenger B, with the limitation that none of them can be fulfilled by any of the questioned attribute sets in stage 1. Accordingly, the challenger B flips an irregular coin b 2 f0; 1g, sets CTTb is the ciphertext of Mb under the entrance policy (A; Tb), and sends the ciphertext CTTb to the enemy.

Stage 2: Phase 1 is rehashed. Be that as it may, none of the arrangements of attributes SQ+1; SQ+2; :::; Sq fulfilling the entrance policy relating to the challenger. Conjecture the foe A yields a speculation bit b0 2 f0; 1g and dominates the match if b = b0.

The benefit of the enemy A right now characterized as {P r[b = b0] 12}, where the likelihood is assumed control over the arbitrary bits utilized by the foe An and the challenger B.

IV. SECURITY AND PRIVACY ANALYSIS

In this section, the security and privacy of the proposed model are evaluated. Some security properties of the proposed model are also discussed. The privacy of the PHR owner can be achieved by controlling who will be allowed to access the PHR under what conditions. The security of the PHR data can be achieved by securing the PHR data from unauthorized disclosure, alteration, or deletion [24]. The security and privacy analysis are performed according to two assumptions as follows.

Assumption 1. Assume that g is the generator of a cyclic group of order q and cannot be computed from with a no negligible probability.
Assumption 2. The servers that are used in this model are semi trusted so that the servers follow the procedure defined in this work but the severs are curious to know the data.
Case 1. The proposed PHR model is secure against a security attack such as tampering data by an adversary.

Threat model: The PHR system contains the medical data such as diagnosis results or medical records, and the adversary aims to either modifying some data or replace the original data with the new one.

Argument: The uploaded PHR data is actually encrypted and stored on a cloud server. The link to the encrypted PHR is known only by the gateway server. The adversary cannot modify the real encrypted PHR data. Even if the adversary can modify or replace the encrypted PHR data, the message digest on the blockchain will be able to detect such actions. If the adversary wants to modify the metadata on the blockchain, an extensive work is required to construct a new main chain. This situation is nearly impossible because the blockchain characteristic ensures that the stored data will be very difficult to modify or delete once confirmed.

Case 2. The proposed PHR model is secure against a security attack such as collusion between the gateway server and the adversary.

Threat model: The reencryption keys are included in the access list which is stored at the gateway server, and the gateway server can perform a reencryption process. The adversary and the gateway server may collusively try to obtain the PHR data or reencryption the PHR data for the adversary.

Argument: Although the access control list is locally stored at the gateway server, the information on the access control list does not include the corresponding secret key. As a result, the gateway server cannot gain an access to the encrypted PHR data. Since, the secret key is in the care of the PHR owner, the reencryption keys used by the gateway server can only be generated by the PHR owner. The gateway server cannot create a reencryption key for the adversary from its existing reencryption.

V. PERFORMANCE ANALYSIS

In this phase, we can deliver some comparisons of our scheme with previous associated works ([5], [8], [9], [18], [24]) in phrases Of protection and overall performance. In table 1, we offer comprehensive comparisons for a few vital capabilities, including the scale of public keys, private keys and cipher texts, decryption overhead, organization order, and the expression and status of get admission to policy. From table 1, we will see that the scale of Keys in our scheme is the same with other works, but the Ciphertext length of proposed scheme is smaller than them. Similarly, simplest the proposed scheme and the paintings in [8] Aid massive universe buildings. What is more, in comparison With the above work, only our scheme can comprehend consistent Pairing operation inside the decryption segment that can substantially improve the decryption efficiency. In table 1, p denotes the

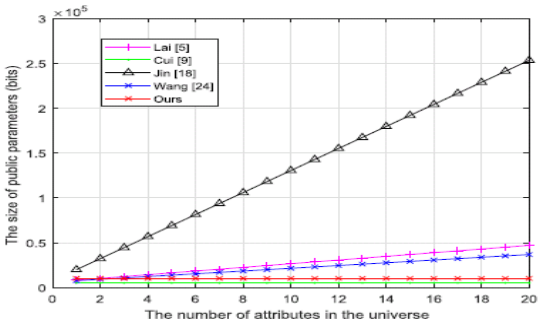

FIGURE 5. The storage cost of the public parameters.

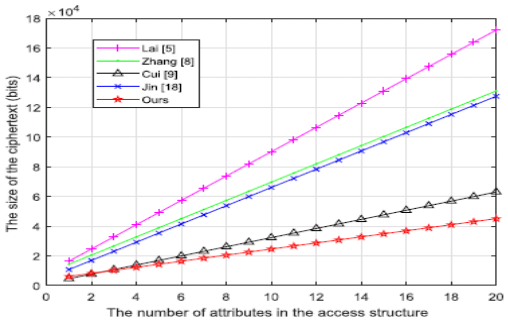

FIGURE 6. The storage cost of the ciphertext.

Pairing operation. l and n are the scale of get right of entry to matrix and The class of attributes inside the universes respectively. I is A fixed fulfilling the get admission to structure defined by using an encryptor. Jgj and jgt j denote the number of bits for the representation Of elements of g and gt . Observe that the dimensions of an element in Group gpi , g and gt is set to 512 bits.

Fig.5, 6 and fig.7 give comparisons of the performance Benefit of the proposed scheme with the above. The simulation is completed on A windows gadget with 3.40 ghz Intel(r) core(tm) i3-3240 cpu and 4 gb rom. from the Fig.5, 6 and fig.7, it is obvious that the proposed scheme is Better than others in desk 1 in phrases of the dimensions of public Parameters, cipher texts and decryption overhead.

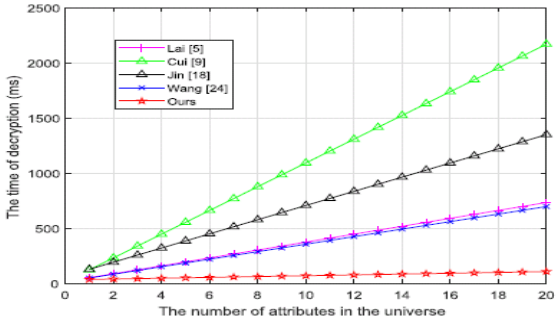

FIGURE 7. The decryption overhead for data users.

VI. CONCLUSION

Right now, present another strategy called straight mystery offering to different qualities, which can extraordinarily improve the declaration of access policy. In addition, each attribute is isolated into two sections, to be specific the attribute name and its worth. Thusly, the most clear bit of leeway of the proposed conspire is that touchy attribute esteems can be hidden. What's more, it can secure clients' protection well in PHR. In the proposed conspire, the size of open parameters is steady and the expense of the decryption is just two blending activities, which likewise make it progressively reasonable. In the end, we demonstrate the full security of the proposed conspire in the standard model under

static suppositions by utilizing the double framework encryption technique. The proposed plot just accomplishes incompletely concealing policy. It is an intriguing issue that accomplishes a completely concealing policy with fast encryption, which is left as future work.

VII. REFERENCES

[1] Chen, D., Chen, L., Fan, X., He, L., Pan, S., & Hu, R. (2014). Securing patient-centric personal health records sharing system in cloud computing. China Communications, 11(13), 121-1.

[2] Zhang, L., Hu, G., Mu, Y., & Rezaeibagha, F. (2019). Hidden ciphertext policy attribute-based encryption with fast decryption for personal health record system. IEEE Access, 7, 302-313.

[3] Barua, M., Liang, X., Lu, R., & Shen, X. (2011, April). Peace: An efficient and secure patient-centric access control scheme for ehealth care system. In 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 970-975). IEEE.

[4] Aboelfotoh, M. H., Martin, P., & Hassanein, H. S. (2014, October). A mobile-based architecture for integrating personal health record data. In 2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom) (pp. 9-4). IEEE.

[5] Barua, M., Liang, X., Lu, R., & Shen, X. (2011). ESPAC: Enabling Security and Patient-centric Access Control for eHealth in cloud computing. International Journal of Security and Networks, 6(2-3), 67-76.

[6] Tao, X., Lin, C., Zhou, Q., Wang, Y., Liang, K., & Li, Y. (2019). Secure and efficient access of personal health record: a group-oriented ciphertext-policy attribute-based encryption. Journal of the Chinese Institute of Engineers, (1), 80-86.

[7] B. Waters, "Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions," in Advances in Cryptology—CRYPTO (Lecture Notes in Computer Science), vol. 5677, S. Halevi, Eds. Berlin, Germany: Springer, Aug. 2009, pp. 619–6.

[8] M. Qutaibah, S. Abdullatif, and C.T. Viet, "A Ciphertext-Policy Attribute-based Encryption Scheme With Optimized Ciphertext Size And Fast Decryption," in Proc. 2017 ACM Asia Conf. Comput, Commun. Secur. (ASIA CCS), Apr. 2017, pp. 2–2.

[9] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography—PKC(Lecture Notes in Computer Science), vol. 6571. Berlin, Germany:Springer, Mar. 2011, pp. 53–70.

[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput, Commun. Secur. (CCS), Nov. 2006, pp. 89–98.

[11] J. Lai, R.H. Deng, and Y. Li, "Expressive CP-ABE with partially hidden access structures," in Proc. 7th ACM Sym. Infor., Comput, Commun. Secur., May. 2012, pp. 18–19.

[12] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE Symp. Secur. Privacy (SP), May 2007, pp. 1– 4.

[13] Y. Zhang, D. Zheng, and R.H. Deng, "Security and privacy in smart health: Efficient policy-hiding attribute-based access control," IEEE Inter-net Things J., vol. 5, no. 3, pp. 21–21, Jun. 2018

[14] H. Cui, R.H. Deng, G. Wu, and J. Lai, "An Efficient and Expres-sive Ciphertext-Policy Attribute-Based Encryption Scheme with Partially Hidden Access Structures," in Provable Security—PROVSEC (Lecture Notes in Computer Science), vol. 10005, L. Chen, Eds. Berlin, Germany: Springer, Nov. 2016, pp.19–.

[15] C.Y. Umesh, "Ciphertext-policy attribute-based encryption with hiding access structure," in IEEE Inter.Adv.Comput. Conf. (IACC), Jul 2015, pp. 6–10.

[16] L. Zhang and Y. Hu, "New Constructions of Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Computing,"

KSII Transactions Internet J., vol. 7, no. 5, pp. 13–16, May. 2013.

[17] J. Li, K. Ren, B. Zhou, and Z. Wan, "Privacy-Aware Attribute-Based Encryption with User Accountability," in Information Security—PROCEEDINGS (Lecture Notes in Computer Science), vol. 57, P. Samarati, Eds. Berlin, Germany: Springer, Sep. 2009, pp.7–2.

[18] J. Li, H. Wang, Y. Zhang, and J. Shen, "Ciphertext-Policy Attribute-Based Encryption with Hidden Access Policy and Testing," KSII Transactions Internet J., vol. 10, no. 7, pp. –52, Jul. 2016.

[19] Y. Zhang, X. Chen, J. Li, and D. Wong, "Anonymous attribute-based encryption supporting efficient decryption test," in Proc. 8th ACM Sym. Infor, Comput. Commun. Secur. (SIGSAC), May. 2013, pp. 511–516.

[20] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A Ciphertext-

[21] Policy Attribute-Based Encryption Scheme with Constant Ciphertex-t Length," in Infor. Secur.Prac., Experience—ISPEC (Lecture Notes in Computer Science), vol. 51, F. Bao, H. Li, Eds. Berlin, Germany: Springer, Sep. 2009, pp.13–23.

[22] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-Based Encryption with Partially Hidden Encryptor-Specified Access Structures," in Applied Cryptography and Network Security—ACNS (Lecture Notes in Computer Science), vol. 50, S.M. Bellovin, R. Gennaro, Eds. Berlin, Germany: Springer, Sep. 2009, pp.13–23.

[23] T.V. Phoung, G. Yang, and W. Susilo, "Hidden Ciphertext Policy Attribute-Based Encryption Under Standard Assumptions," IEEE Trans. Informa-tion Foren. Security, vol. 11, no. 1, pp. –, Sep. 2015.

[24]C. Jin, X. Feng, and Q. Shen, "Fully Secure Hidden Ciphertext Policy Attribute-Based Encryption with Short Ciphertext Size," in Proc. Inter. Conf., Commun. Netw. Secur. (ICCNS), Nov. 2016, pp. 91–98.