International Journal of Future Generation Communication and Networking
Vol. 13, No. 3, (2020), pp. 286 – 294

Protecting Personal Health Record System Using Ciphertext Attributes based Encryption

Mrs M. Nithya RamaKrishna[1], T Jahnavi[2]
[1]Assistant Professor,5years Experience, [2]M.TechScholor
Department of Computer Science and Engineering,
QIS College of Engineering & Technology, Ongole, Andhra Pradesh

Abstract

Since cloud computing has been assuming an inexorably significant job in real life; the privacy protection in numerous fields has been given increasingly more consideration, particularly, in the field of Personal Health Record (PHR). The traditional ciphertext-policy attribute based encryption (CP-ABE) gives the fine-grained get to control policy for scrambled PHR information, however the entrance policy is likewise sent alongside ciphertext unequivocally. In any case, the entrance policy will uncover the users privacy since it contains an excessive amount of sensitive data of the legitimate information users. Henceforth it is critical to ensure users' privacy by concealing access strategies. In the vast majority of the past plans, despite the fact that the entrance policy is covered up, they face two down to earth issues: (1) these plans don't bolster huge attribute universe, so their common sense in PHR is significantly constrained, 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 proficient decryption, where both the size of open parameters and the expense of decryption are steady. In addition, we additionally show the proposed conspire accomplishes full security in the standard model under static suppositions by utilizing the dual system encryption technique.

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

Introduction

As a developing innovation as of late, cloud computing gives a fast and proficient approach to share data assets, and mountain number of individual's access data through the network. For instance, in the personal system health record system, a patient doesn't need to convey different paper renditions of the test structures to make a determination as per the traditional way, however he/she can store, recover and share the health record just by transferring his very own health record to the PHR system. A patient has the full control to his/her own PHR record and approves who can access these health data, for example, companions, family or healthcare suppliers. So as to accomplish accurate access control of PHR, data proprietors desperately need a sort of encryption conspire that can realize fine-grained access control.

Hidden ciphertext policy attribute-based encryption conspire gives a decent method to tackle the issue, where it accomplishes privacy protection by hiding access control policy. Be that as it may, In the past systems [2], [3], [7], the access control policy is frequently sent alongside ciphertext unequivocally, which makes it simple uncover the users' privacy, since certain attributes in access structure

ISSN: 2233-7857 IJFGCN

convey urgent identity data of the legitimate users. In PHR, an access policy defined by a patient may contain some sensitive attributes, for example, cardiologist, focal clinic and so on [8]. Thusly, for an unapproved client, regardless of whether he can't decode effectively, he can likewise construe from the access policy in clear content structure which the encryptor experiences some malady. The principal hidden ciphertext-policy attribute-based encryption (HCP-ABE) was presented in [16], where the access structure was implanted in the ciphertext and not sent legitimately. Thusly, some other hidden CP-ABE plans were additionally progressively proposed in [17], [19]. Be that as it may, access structures in these plans just help AND doors or AND entryways on positive, negative and special case.

These lead to two downsides. To start with, the size of public parameters increments directly with the quantity of attributes, and furthermore, the expense of the decryption is significantly expanded. Because of the above downsides, some low-overhead plans are presented in [13], [14] and the regular technique received by these plans is to present a decryption test by adding some excess parts to aciphertext before the decryption stage. In spite of the fact that the above plans improve the productivity of decryption, the length of ciphertext is likewise altogether expanded and this will end up being a bottleneck confining better. Furthermore, these plans are incredibly defenseless against decisional Diffie-Hellman test (DDH-test) attack [9], [20].

Lately, with the fast advancement of web and cloud computing, a mountain number of Intelligent Medical Systems have been planned. Be that as it may, in the past instruments based attribute encryption, access control strategies are regularly sent alongside ciphertext, which makes it simple to uncover the sensitive data of users in the system. Particularly, in PHR, the particular attribute esteems in an access policy convey substantially more sensitive data, for example, the patients beat recurrence, his family ancestry of genetic ailments, the consequence of the patient's research facility test report and so on. So as to manage the above issues, our commitments principally incorporate the following three sections.

Access structure: Each attribute in this paper contains two sections, attribute name file and its attribute esteem. And each attribute has numerous candidate esteems. Each decrytor just realizes the attribute name file of his own and his attribute esteem. Besides, the estimations of the attributes in the access policy defined by the encryptor are hidden, and they are not sent with the ciphertext. Just the access grid and the defined capacity ρ are sent to the decryption alongside the ciphertext. In addition, the proposed plan can handle any access control policy that can be communicated as a straight mystery sharing plan.

Fast decryption: Obviously, it is difficult for a client to know whether his attribute set fulfills the access policy defined by the encryptor, if the access policy related with a ciphertext is completely hidden. Hence, a decryption needs to do a ton of figurings to decide if he is legitimate or not. In this paper, we present an effective development of Hidden Ciphertext Policy Attribute-Based Encryption Supports Fast Decryption, where, the quantity of bilinear pairing assessments is diminished to a consistent in decryption stage.

ISSN: 2233-7857 IJFGCN

Data verifiability: In many past plans, there are typically two functional issues have the right to be thought of. One is the size of the public parameters increments directly with the size of the universe. And the other is the approved client can't decide if the message he got through decryption is substantial or not, on the grounds that there is no evident connect to the message. Nonetheless, in the proposed conspire, the size of public parameters is consistent, so the attribute universe in this plan can be exponentially huge and it likewise underpins approval of unscrambled messages, which can additionally improve the unwavering quality of decryption. Moreover, we likewise demonstrate the full security of the proposed plot in the standard model under static suspicions by utilizing the dual system encryption technique [1].

Related work

B. Waters, We present another strategy for demonstrating security of encryption systems utilizing what we call Dual System Encryption. Our procedures bring about completely secure Identity-Based Encryption (IBE) and Hierarchical Identity-Based Encryption (HIBE) systems under the basic and set up decisional Bilinear Diffie-Hellman and decisional Linear presumptions. Our IBE system has ciphertexts, private keys, and public parameters each comprising of a consistent number of gathering components. These outcomes are the first HIBE system and the first IBE system with short parameters under basic presumptions. In a Dual System Encryption system both ciphertexts and private keys can take on one of two undefined structures. A private key or ciphertext will be typical in the event that they are produced separately from the system's key age or encryption calculation. These keys and ciphertexts will act as one expects in an IBE system. Likewise, we define semi-practical keys and ciphertexts. A semi-utilitarian private key will have the option to decode all regularly produced ciphertexts; be that as it may, decryption will come up short in the event that one endeavors to unscramble a semi-practical ciphertext with a semi-useful private key. Comparably, semi-practical ciphertexts will be decryptable just by typical private keys.

M. Qutaibah, S. Abdullatif, and C.T. Viet, We address the issue of ciphertext-policy attribute-based encryption with fine access control, a cryptographic crude which has many solid application situations, for example, Pay-TV, e-Health, Cloud Storage and so on. In this setting we enhance past LSSS based procedures by expanding on past work of Hohenberger and Waters at PKC'13 and proposing a development that accomplishes ciphertext size direct in the base between the size of the Boolean access equation and the quantity of its provisos. Our development additionally bolsters fast decryption. We additionally propose two intriguing expansions: the first targets lessening stockpiling and calculation at the client side and is helpful with regards to lightweight gadgets or gadgets utilizing a cloud administrator. The second proposes the utilization of numerous specialists to moderate key escrow by the power.

B. Waters, We present another system for realizing Ciphertext-Policy Attribute Encryption (CP-ABE) under cement and non-intuitive cryptographic presumptions in the standard model. Our answers allow any encryptor to indicate access control

ISSN: 2233-7857 IJFGCN

regarding any access recipe over the attributes in the system. In our most proficient system, ciphertext size, encryption, and decryption time scales directly with the intricacy of the access recipe. The main past work to accomplish these parameters was restricted to a proof in the nonexclusive gathering model. We present three developments inside our structure. Our first system is demonstrated specifically secure under a presumption that we call the decisional Parallel Bilinear Diffie-Hellman Exponent(PBDHE) supposition which can be seen as a speculation of the BDHE suspicion. Our next two developments give execution tradeoffs to accomplish provable security individually under the (more fragile) decisional Bilinear-Diffie-Hellman Exponent and decisional Bilinear Diffie-Hellman presumptions.

J. Lai, R.H. Deng, and Y. Li, Introduced the idea of attribute-based encryption (ABE). ABE empowers public key based one-to-numerous encryption and is imagined as a promising cryptographic crude for realizing versatile and fine-grained access control systems. There are two sorts of ABE plans [1], key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE) plans. This paper, our anxiety is on the last mentioned.

A. Sahai and B. Waters, We present another kind of Identity-Based Encryption (IBE) scheme that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE we see an identity as set of elucidating attributes. A Fuzzy IBE scheme allows for a private key for an identity, ω, to decode a ciphertext encoded with an identity, ω ′, if and just if the personalities ω and ω ′ are near one another as estimated by the "set cover" separation metric. A Fuzzy IBE scheme can be applied to empower encryption utilizing biometric contributions as characters; the mistake resilience property of a Fuzzy IBE scheme is accurately what allows for the utilization of biometric personalities, which naturally will have some commotion each time they are inspected. Also, we show that Fuzzy-IBE can be utilized for a kind of use that we term "attribute-based encryption". In this paper we present two developments of Fuzzy IBE schemes. Our developments can be seen as an Identity-Based Encryption of a message under a few attributes that form a (fuzzy) identity. Our IBE schemes are both blunder open minded and secure against intrigue attacks. Furthermore, our fundamental development doesn't utilize random prophets. We demonstrate the security of our schemes under the Selective-ID security model.

J. Bethencourt, A. Sahai, and B. Waters, In a few dispersed systems a client should possibly have the option to access data if a client forces a specific arrangement of certifications or attributes. Right now, the main strategy for upholding such arrangements is to utilize a believed server to store the data and intervene access control. In any case, in the event that any server putting away the data is undermined, at that point the classification of the data will be undermined. In this paper we present a system for realizing complex access control on encoded data that we call ciphertext-policy attribute-based encryption. By utilizing our strategies encoded data can be kept secret regardless of whether the capacity server is untrusted; in addition, our techniques are secure against plot attacks. Past attribute-based encryption systems utilized attributes to depict the scrambled data and incorporated approaches with client's keys; while in our system attributes are utilized to portray a client's qualifications, and a gathering encoding data decides a

ISSN: 2233-7857 IJFGCN

policy for who can decode. In this manner, our techniques are adroitly nearer to traditional access control strategies, for example, role-based access control (RBAC). What's more, we give an implementation of our system and give execution estimations.

Implementation methodology

The first CP-ABE scheme was presented in [7], where ciphertexts were related with access structure defined by data proprietors and the key are related with sets of attributes about users. Therefore, there are a ton of CPABE schemes were likewise progressively proposed in [15], [17], [18], however these schemes just help AND entryways. To realize the access structure increasingly expressive, Waters proposed an access structure based a linear secret sharing scheme(LSSS), and it is likewise a provably secure scheme under the standard model [3]. So as to additionally secure users' privacy, the principal the CP-ABE scheme with hidden access structure was proposed by Yoneyama et al. [16]. In their work, access control policy isn't sent alongside ciphertext unequivocally, as such, no unapproved client can get helpful data about the access structure. Some different schemes with a similar presentation have been proposed by different scientists, which are called Anonymous Attribute-Based Encryption.

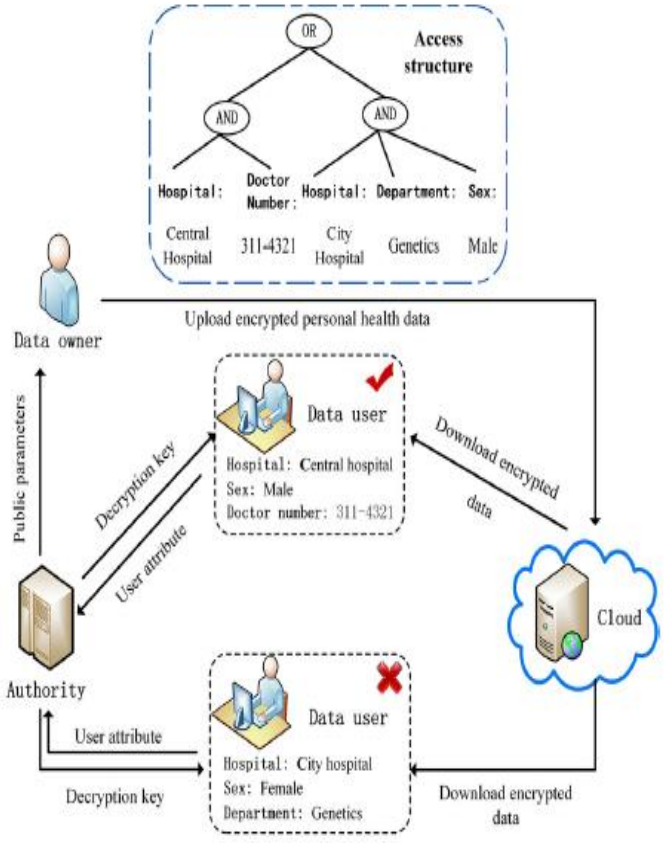

Figure1: PHR cloud storage.

In these schemes, just arrangements of the client satisfying the access policy were installed in the ciphertext, and then the client can effectively decode the

ciphertext. Afterward, creators in presented another exceptionally powerful mysterious CP-ABE scheme, and its security evidence was given under the Decisional Modified Bilinear Diffie-Hellman assumption (MBDH) [20].However, their work just gives a general examination and needs point by point security confirmation. Some different works were proposed in [9], [14] to make further enhancements for unknown CP-ABE scheme. Shockingly, every one of them need to confront high-overhead of decryption, which may cause them to lose their practicability.

Hidden Ciphertext Policy ABE

A hidden CP-ABE scheme comprises of the following four calculations.

Setup (1λ) → (PK, MSK): It is a randomized calculation that takes a security parameter λ as information and yields the public parameters PK and master key MSK.

KeyGen(PK, MSK, S) → SK: The key age calculation takes the public parameters PK, the master key MSK and the users attributes set S as info. It yields the users private key SK related with S.

Encrypt (PK, M, (A, ρ, T)) → CT: The encryption calculation takes the public parameters PK, a plaintext message M, and an access structure (A, ρ , T) as info, and yields aciphertext CT , where T is a lot of attribute esteems in the access structure and not sent alongside the ciphertext CT.

Decode (PK, SK, CT) → M: It takes the public parameters PK, a secret key SK related with the attributes set S = (IS, LS),and a ciphertext CT encrypted under access structure (A,ρ) as information, and yields the message M or an extraordinary image $\perp$ signifies that a client neglected to unscramble the ciphertext CT.

Security Proof

Semi-functional ciphertext and secret key

Our security evidence utilizes the methodology as same as Lai's [5], which is called dual system encryption. From the start, we define two semi-functional structures: Semi-Functional Ciphertexts SFC and Semi-Functional Keys SFK. Both typical ciphertexts and semi-functional ciphertexts can be decoded by the ordinary private keys, yet it is infeasible for a semi-functional private key to unscramble a semi-functional ciphertext. We made it understood specifically that SFC and SFK won't be utilized in the real system, and they just utilized in our evidence.

Performance Analysis

In this area, we will give a few examinations of our scheme with past related works [5], [8], [9] as far as security and performance. In Table 1, we give thorough correlations with some significant highlights, including the size of public keys, private keys and ciphertexts, decryption overhead, bunch request, and the

articulation and status of access policy. Here we can see that the size of keys in our scheme is the equivalent with different works, yet the ciphertext size of proposed scheme is littler than them.

What's more, just the proposed scheme and the work in [8] bolster huge universe developments. Additionally, contrasted and the above work, just our scheme can realize steady pairing activity in the decryption stage, which can incredibly improve the decryption effectiveness.

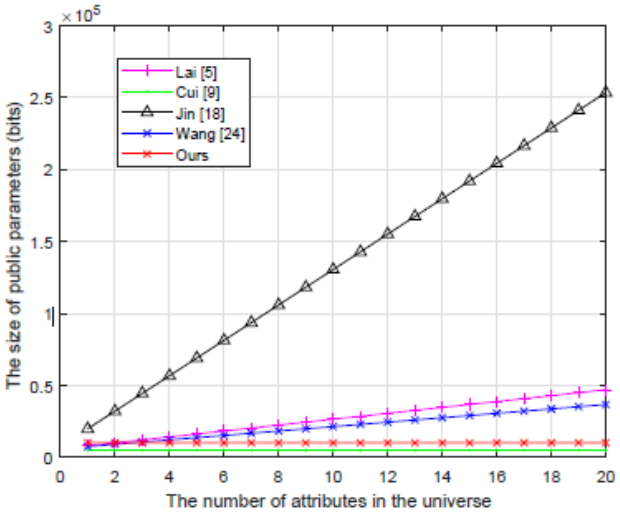

Figure2: The storage cost of the public parameters

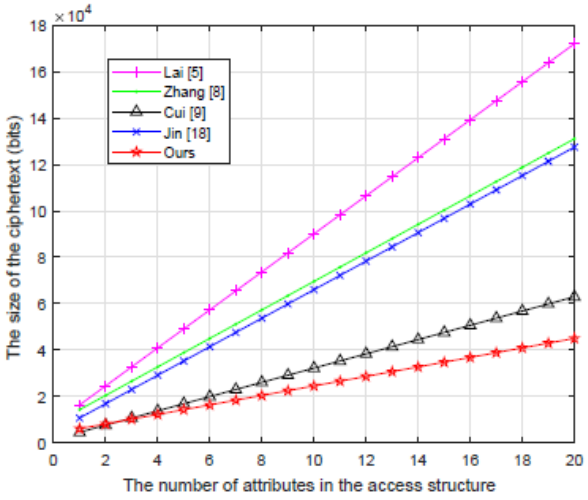

Figure3: The storage cost of the ciphertext

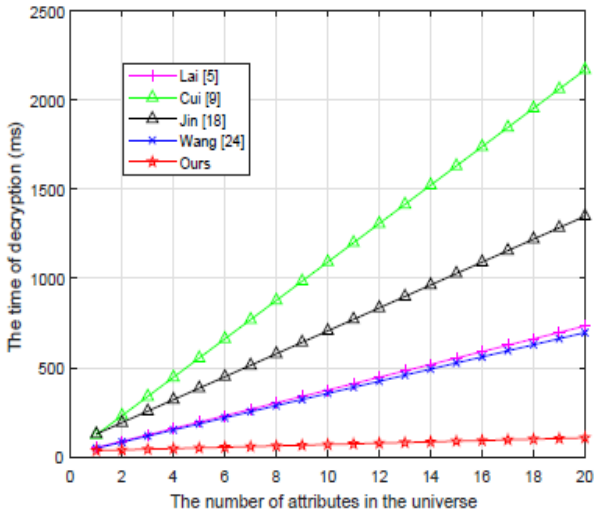

Figure4: The decryption overhead for data users

Conclusion

In this paper, we present another technique called linear secret sharing with numerous qualities, which can incredibly improve the statement of access policy. Besides, each attribute is partitioned into two sections, in particular the attribute name and its worth. In this manner, the most clear bit of leeway of the proposed scheme is that sensitive attribute esteems can be hidden. And it can ensure users' privacy well in PHR. In the proposed scheme, the size of public parameters is steady and the expense of the decryption is just two pairing tasks, which additionally make it progressively down to earth. In the long run, we demonstrate the full security of the proposed scheme in the standard model under static assumptions by utilizing the dual system encryption technique. The proposed scheme just accomplishes halfway hiding policy. It is a fascinating issue that accomplishes completely hiding policy with fast encryption, which is left as a future work.

References

[1] 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. 619–636.

[2] 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. 230–240.

[3] 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.

[4] 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.

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

[6] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Advancesin Cryptology—EUROCRYPT (Lecture Notes in Computer Science), vol.3494, R. Cramer, Eds. Berlin, Germany: Springer, May 2005, pp. 457–473.

[7] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute based encryption,” in Proc. IEEE Symp. Secur. Privacy (SP), May 2007, pp. 321–334.

[8] Y. Zhang, D. Zheng, and R.H. Deng, "Security and privacy in smarthealth: Efficient policy-hiding attribute-based access control," IEEE Internet Things J., vol. 5, no. 3, pp. 2130–2145, Jun. 2018.
[9] H. Cui, R.H. Deng, G. Wu, and J. Lai, "An Efficient and Expressive Ciphertext-Policy Attribute-Based Encryption Scheme with Partially Hidden Access Structures," in Provable Security—PROVSEC (LectureNotes in Computer Science), vol. 10005, L. Chen, Eds. Berlin, Germany: Springer, Nov. 2016, pp.19–38.
[10] C.Y. Umesh, "Ciphertext-policy attribute-based encryption with hiding access structure," in IEEE Inter.Adv. Comput. Conf. (IACC), Jul 2015, pp.6–10.
[11] 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. 1343–1356, May. 2013.
[12] 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. 5735, P.Samarati, Eds. Berlin, Germany: Springer, Sep. 2009, pp.347–362.
[13] 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. 3339–3352, Jul. 2016.
[14] 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.
[15] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A Ciphertext-Policy Attribute-Based Encryption Scheme with Constant CiphertextLength," in Infor. Secur.Prac., Experience—ISPEC (Lecture Notes inComputer Science), vol. 5451, F. Bao, H. Li, Eds. Berlin, Germany:Springer, Sep. 2009, pp.13–23.
[16] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-Based Encryptionwith Partially Hidden Encryptor-Specified Access Structures," in AppliedCryptography and Network Security—ACNS (Lecture Notes in ComputerScience), vol. 5037, S.M. Bellovin, R. Gennaro, Eds. Berlin, Germany:Springer, Sep. 2009, pp.13–23.
[17] T.V. Phoung, G. Yang, andW. Susilo, "Hidden Ciphertext Policy Attribute-Based Encryption Under Standard Assumptions," IEEE Trans. InformationForen. Security, vol. 11, no. 1, pp. 35–45, Sep. 2015.
[18] C. Jin, X. Feng, and Q. Shen, "Fully Secure Hidden Ciphertext PolicyAttribute-Based Encryption with Short Ciphertext Size," in Proc. Inter.Conf., Commun. Netw. Secur. (ICCNS), Nov. 2016, pp. 91–98.
[19] Q.Wang, L. Peng, H. Xiong, and J. Sun, "Ciphertext-policy attribute-basedencryption with delegated equality test in cloud computing," IEEE AccessJ., vol. 6, pp. 760–771, Nov. 2017.