Enhanced Secure Data sharing in Cloud Computing

Priyanka M[1], Revathi P[2], Samundeeshwari M[3]
[1, 2] Dept of Science and Engineering
[3]Assistant Professor, Dept of Science and Engineering
[1, 2, 3]Kingston Engineering College , Vellore-59

Abstract- *Data sharing is a commodious and economic service supplied by cloud computing. Data contents conceal also arises from it since the data is outsourced to some cloud servers. To preserve the essential and sensitive information, various techniques are used to enhance access control on the shared data. By using, Light Weight operations And Ciphertext-policy attribute-based encryption (CP-ABE),it makes the application more flexible, reliable and secure . Traditional CP-ABE focuses on discreetness merely, while the user's personal conceal protection is an important issue at present. CP-ABE with hidden access policy guarantees users data confidentiality and prevents the users privacy as well. However, most of the existing system are inefficacious in communication overhead and computation cost. Moreover, most of those works take no consideration about authority verification or the problem of conceal leakage in authority verification phase. To tackle the problems mentioned above, a conceal preserving CP-ABE scheme with efficient authority verification is introduced in this paper. Additionally, the secret keys of it accomplish constant size. Meanwhile, the proposed scheme accomplish the selective security under the decisional n-BDHE problem and decisional linear assumption. The computational results confirm the advantages of the presented scheme.*

Keywords- Light Weight Operation, Data Sharing, Revocation Data Conceal , Integrity.

I. INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of software and hardware resources made available on the Internet as managed thirdparty services. These services typically provide access to advanced software applications and high-end networks of server computers.

II. LITERATURE SURVEY

1) The Work done by P. P.Kumar, P. S.Kumar, and P. J. A. Alphonse " Attribute based encryption in cloud computing: A survey, gap analysis, and future directions"

Cloud computing facilitates to store and access the data remotely over the internet. However, storing the data in the unreliable cloud server leads the conceal and access control issues in the cloud. The traditional encryption schemes such as symmetric and asymmetric schemes are not suitable to provide the access control due to lack of flexibility and fine-grained access control. One of the prominent cryptographic technique to provide conceal and fine-grained access control in cloud computing is Attribute Based Encryption. In this paper, we comprehensively survey the various existing key policy and ciphertext policy attribute based encryption schemes

[2]The Work done by: A. Sahai and B. Waters"Fuzzy identity-based encryption"

We introduce a new type of Identity-Based Encryption (IBE) scheme that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE we view an identity as set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for an identity, ω, to decrypt a ciphertext encrypted with an identity, ω 0 , if and only if the identities ω and ω 0 are close to each other as measured by the "set overlap" distance metric. A Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each period they are sampled. Additionally, we show that Fuzzy-Identity Based Encryption can be used for a type of application that we term "attribute-based encryption". In this paper we present two constructions of Fuzzy IBE schemes. Our constructions can be viewed as an Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity. Our IBE schemes are both error-tolerant and secure against collusion attacks. Additionally, our basic construction does not use random oracles. We prove the security of our schemes under the Selective-ID security model.

[3]The Work done byK. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi "A cipher text policy attribute-based encryption scheme with constant cipher text length"

An Attribute-Based Encryption (ABE) is an encryption scheme, where users with some attributes can decrypt ciphertexts associated with these attributes. However, the length of the ciphertext depends on the number of attributes in previous ABE schemes. In this paper, we propose a new Ciphertext-Policy Attribute-Based Encryption (CP-ABE) with constant ciphertext length. Moreover, the number of pairing computations is also constant.

III. EXISTING SYSTEM

A framework of HP-CP-ABE with efficient and secure authority identification is proposed, which guarantees the data confidentiality and does not protects the user personal conceal as well. we design an authority identification method, which can help the user verify whether he/she is an authorized one and decrypts successfully. The proposed scheme accomplish constant private key size, which is independent of user's attribute number. It reduces the cost of transmission and storage

3.1 DISADVANTAGE

- Existing scheme only supports "AND" policy and relies on a weak security model.
- High computational process of Encryption and Decryption.
- Lacks User revocation (Data Users must be revoked to stop his access to shared data when he leaves the organization).
- It accomplishs constant private key size, which is independent of user's attribute number.
- It reduces the cost of transmission and storage

IV. PROPOSED SYSTEM

The Proposed system overcomes the difficulties in existing scheme by ensuring Data Conceal (Prevent user information without leakage), guarantees Data Confidentiality and reduce high computational process.

We design an algorithm called LDSS-HP-CP-ABE based on Attribute-Based Encryption (ABE) method to offer efficient access control over authority center. The modules used are data user, data owner , key generation ,cloud server. To accomplish security, we used user revocation in the data sharing scheme. We guarantee conceal preserving of sensitive data in sharing process and access authorization control for data requesters. The data is permute into equal number of blocks and N x N matrix will be generated on the basis of these blocks. Based on no. of blocks, pool of threads will be generated. Run the threads in multi core system to generate encrypted data in short amount of period. We accomplish lightweight computation operations on data owner and data requester side.

4.1 ADVANTAGES OF PROPOSED SYSTEM

The data sharing scheme is designed to accomplish

- Data conceal preservation (prevents user conceal leakage and guarantees there security).
- Data security
- We accomplish light weight computation operations on data owner and data requester side, So it increases the efficiency of the program.
- Reduces high computational process of Encryption and Decryption.
- Low maintenance cost.
- Protect the data and ensure the violation of third party(threads).

4.2 SYSTEM ARCHITECTURE

System Model:

There are four entities in a HP-CP-ABE system: A CS, an authority center (AC), DO, and data users (DU) as shown in Fig. 1

1) AC: In the HP-CP-ABE, it should be fully reliable and
accepts the registration of all DU. Then it will generate
public keys and secret keys for each DU.

2) DO: DO specifies access policies and encrypts data. Then he/she uploads the encrypted data to the CS.

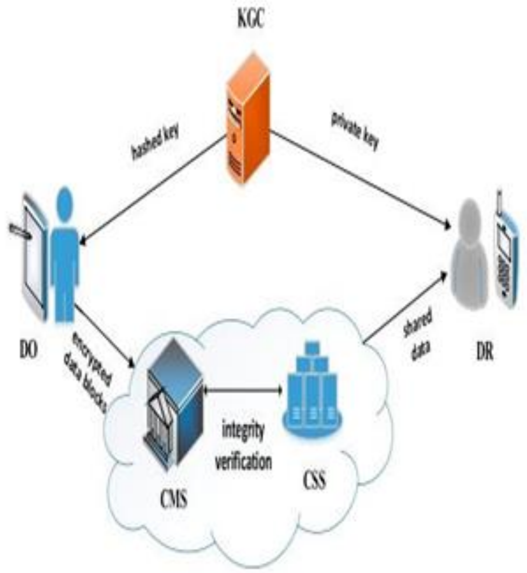


FIGURE 1. ARCHITECTURE DIAGRAM

3) CS: CS may not be genuine in the system. It is in charge of storing encrypted data.

4) DU: DU can request secret keys associated with their at tributes from AC and access to encrypted data from CS. If DU can pass the authentication, which means their attributes match the policy, then DU can recover the encrypted contents. Note that in this situation, the access policies are hidden when DO encrypt data, thus no one can get any information from the ciphertext.

2. Framework:

A HP-CP-ABE is stated as follows.

1) Setup(κ, U) → (PK, MK): Let κ, U indicate the security parameter and universe of attribute. This algorithm takes as input κ,U and outputs the public keys PK and the master key MK.

2) KeyGen(PK, MK, L) → SKL: Stated PK MK, and a subset L ⊂ U, this algorithm generates the corresponding private key SKL.

3) Encrypt(PK,M,W) → CT: Stated PK, data M, and the policy W, this algorithm outputs the encrypted content CT.

4) Decrypt(PK, SK,CT) → M or ⊥: Stated PK, CT, if DU's attribute satisfies W, this algorithm outputs the plain text M.

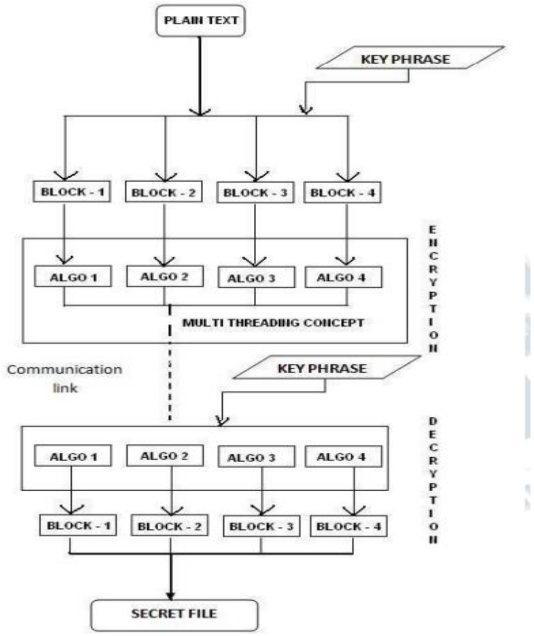
Light Weight Operations

The data is converted into equal number of blocks and N x N matrix will be changed on the premises of these blocks. Based on no. of blocks, pool of threads will be generated. Run the threads in multi core system to generate Encrypted data in short span of period

Revocation(Uid) → (DRTable).

DR can be revoked after leaving the organization. After revocation of DR, DSS eliminate DR's information from DR Table and DR cannot download the shared file later.

Revocation is the act of annulment or recall . It is the the recalling of a grant or privilege, or the making void of some deed previously existing. A temporary revocation of a grant or privilege is called a suspension.



V. IMPLEMENTATION

5.1 DIFFERENT MODULES

The system model consists of four modules named Key Generator Center (KGC), Data Owner (DO), Cloud Servers (CS) and Data Requester (DR) as illustrated in Fig. 1.

Key generation centre (KGC)

It is amenable for generating public parameters and issuing private key for other entities and master key for the system.

Data owner (DO)

It is amenable to generate and encrypt the shared data using secret key and access structures then divide encrypted data into severalblocks.

Cloud servers (CS)

Cloud servers comes inCloud Manage Servers (CMS) and Cloud Storage Servers (CSS). CSS is amenable for storing shared data, block tags and Software applicationand communication costs of mobile terminals of DO and DR, CMS is employed to manipulate complex computations including generating algebraic signatures of blocks, authorizing data integrity of shared data and computing the intermediate data for encryption and decryption. CMS is based on their roles

Data Requester (DR):

It is amenable to download and decrypt the shared data for utilization. In the scheme, only the authorized DR is able to download shared data from CSS and decrypt the data. In our secure data sharing scheme for mobile terminal devices, DO has large sensitive data to share with legalized DR. Before sharing, DO encrypts the data with his private key and outsources the data to CSS. If a DR wants to examine the data, he must register his identity to KGC and acquire his private key for decryption. To accomplish authorized access, only legitimate DRs with correct attributes can download and utilize the shared data. To ensure cloud data intact and decrease computation burden of requesters, CMS helps DR to verify the integrity of data before sharing. Only when data is undamaged, DR downloads and decrypts shared data with his private key.

VI. ALGORITHM

STEP 1. (Key Generation):

1) The group manager randomly selects $\beta i \in Zp*$, which will act as the private key of *TPMi* . He then evaluates $g\beta i$.

2) The group manager randomly selects $k1 \in Zp*$and sends it to the group members and the cloud.

3) The group manager randomly selects $\alpha j \in Zp*$, calculates $g\alpha j$, and computes *pkTPMi* as the public key of *TPMi*: $pkTPMi = (g\beta i, g\alpha 1\beta i, g\alpha 2\beta i , . . . , g\alpha j\beta i)$

4) The group manager selects the interconnection function *f*, the interconnection function sequence *f i* and the sending windows of the input and output, and then sends them to the cloud.

STEP 2. (Data Blind):

1) Group members use the secret seed $k1$ to evaluate the blind factor $\alpha i = \zeta k1$ (*i, name*), which in turn evaluates the blind data *mij*, i.e., $m0ij = mij + \alpha i$

2) A group member sends a request to upload the data to the group manager, evaluates the hash value *hash*(*idi*,*j*), and sends *idi*,*j*,*m*to the group manager through the secure channel. A new event is then generated by the group member. The *hash*(*idi*,*j*) will broadcasted within the group and will be used as a transaction record for the new event. After receiving the request, the group manager verifies *hash*(*idi*,*j*) according to the same hash algorithm and receives *m*0*ij* after the verification is passed.

STEP 3. (Authorize):

1) The group manager evaluate the output port *TPMi* in
the virtual TPM pool corresponding to the input port *ui* (the
requesting group member) according to the TPM manage
ment strategy.

2) The group manager generates the authorization message
for *TPMi* as follows.

(*IDgroup*||*ui* ||*1 ti*),where *IDgroup* is the identity of the group manager, *1 ti* is the period when the group manager processes the request, and *1 t*is the period authorized by the group manager for the TPM.

3) The group manager evaluates the value *H*1 according to the authorization message as follows.

$$H1 = H1((IDgroup||ui\ ||1\ ti), 1t$$

04) The group manager then sends the authorization message (3) to the cloud, and sends αj,βi,*m*, and *H*1 to *TPMi.*

STEP 4. (Authentication label Generation):

1) After receiving the blind data block *mj*, *TPMi* uses private key βi to generate authentication label is the modified blind block, then $05 = (H2(5) \cdot$ Q $sj{=}1\ (g\alpha j)m05j)\beta i$. Then, *TPMi* send the data fifile of the corresponding *TPMi* and the authorization message (3) of the corresponding group manager, the cloud fifirst evaluates the output port *TPMi*. If *TPMi* just sends the message at *1 ti* , then the cloud calculates *H*1((*IDgroup*||*ui* ||*1 ti*), *1t*) and determines whether the value is

consistent with the value *H*1((*IDgroup*||*ui* ||*1 ti*), *1t*0from *TPMi* . If they are stable, STEP 5 is executed; otherwise the implementation is refused.

STEP 5. (Authentication label Check):

The cloud verifies the correctness of label *σ*is received and stored; otherwise it is rejected.

STEP 6. (Data Recovery):

The cloud evaluates *αi* = *ζk*1 (*i*, *name*) based on *k*1, and then computes the real data *mij* using the following equation: (*gαjβi*)−*αi* = (*H*2(*i*) · Y *sj*=1 (*gαj*)*mij*)*βi* (8)
Finally, the cloud stores the real data blocks *mij* = (*mi*1, *mi*2,. .. ,*mis*) and their corresponding real authenticator labels *σi*.

STEP 7. (Challenge):

When the group manager wants to initiate a challenge to the cloud, he randomly selects *1 t* as the authorization period to *TPMi* , where *1 t* corresponds to the *ui* of sending window on the input side. The group manager then sends an audit authorization command to the *TPMi* through *ui* at *1 t*, and sends *IDgroup*||*ui* ||*1 t*as the audit authorization information to the cloud.
After receiving the authorization command from the group manager, the *TPMi* implements the audit process.

1) *TPMi* randomly selects *c* blocks from all blocks of the shared data and indicates the indexs of the selected blocks as *L*.

2) *TPMi* generates two random numbers *o,r* ∈*Zp*∗, and evaluates *X* = g*o* and R=g*r*.

3) *TPMi* evaluates {*Xαj*}1≤*j*≤*s*.

4) *TPMi* outputs the challenge information:

CM = {*L*, *R*,{*Xαj*

Then, *TPMi* sends *CM* to the cloud.

STEP 8. (Proof Generation):

After receiving the challenge information *CM*, the cloud fifirst evaluates the output port *TPMi* according to *IDgroup*||*ui* ||*1 t*. The cloud then uses the method in STEP 4 to verify the authorization message *IDgroup*||*ui* ||*1 t*. The cloud then generates the proof of possessing shared data as follows:

1) The index set *L* of the selected blocks is divided into subsets *L*1, . . . , *Ld* , where *Li* is the subset of the selected blocks that are signed by *TPMi*.

2) For each subset *Li* , the cloud server evaluates

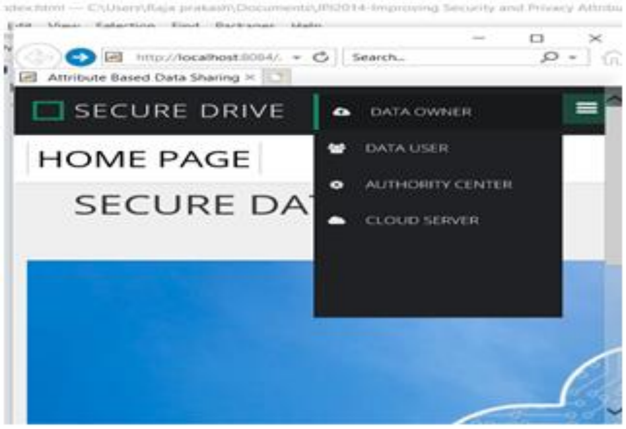
3) The cloud server evaluates*πi* . Then it returns *prf* as a response to the challenge message from the *TPMi* , i.e.,
prf = {{*wi*}1≤*i*≤*d* , *π*}

STEP 9. (Proof Check):

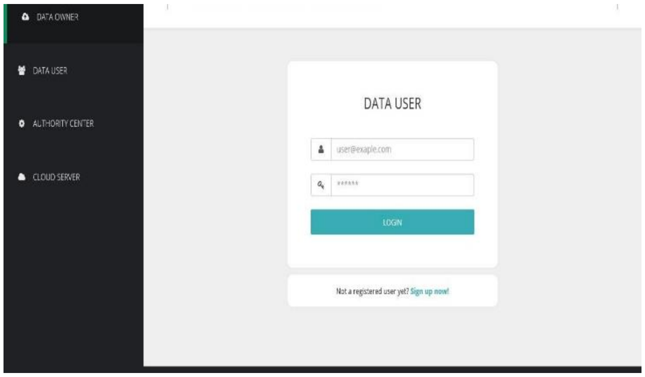
Based on the received *prf* and the challenge message *CM*, *TPMi* verififies the integrity of the shared data by checking
If the equation is true, then *TPMi* outputs *True*; otherwise *False* is returned. In other words, if the selected block in the challenge has been tampered with, the cloud service provider cannot generate valid evidence, and the cloud service provider will not be able to pass the audit process from the *TPMi*.

VII. EXPERIMENT ANALYSIS

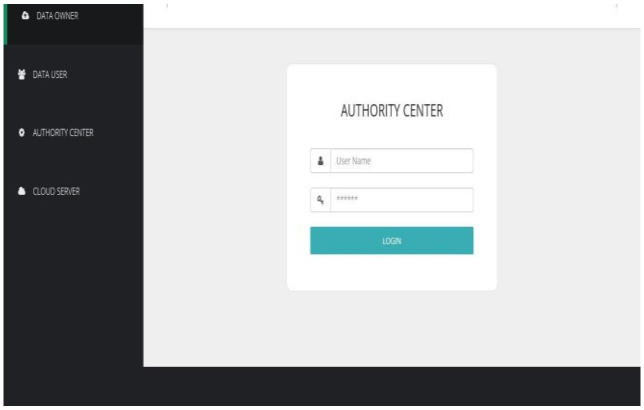
In order to demonstrate the performance advantages of the proposed scheme, we give some comparisons of it with . The experiments are performed on a 64-bit PC with Intel Core i5- 6400 CPU (2.70GHz) and 8 GB of RAM. The comparisons of the parameters’ size show. This article has been acquired for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination. comparisons of the running period cost. From Fig. 4, we can know that secret key size in our strategy is constant, while it increases linearly with the number of attributes . From it is obvious that the ciphertext size of our strategy is much shorter than the other two schemes. it is shown that the preferred scheme takes less period in KeyGen phase and encryption phase than the other two schemes. It show that decryption phaseand Encryption test phase in our scheme take much less period than the other two schemes. In conclusion, our scheme is much more efficient than schemes in in terms of performance.



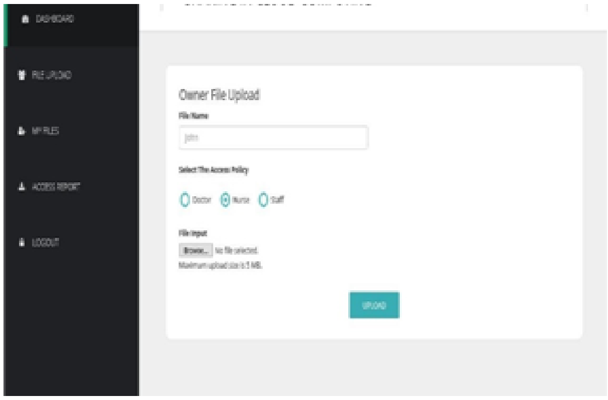
HOMEPAGE



LOGIN PAGE FOR DATA USER



SIGNUP PAGE FOR AUTHORITY CENTRE



Owner File Upload

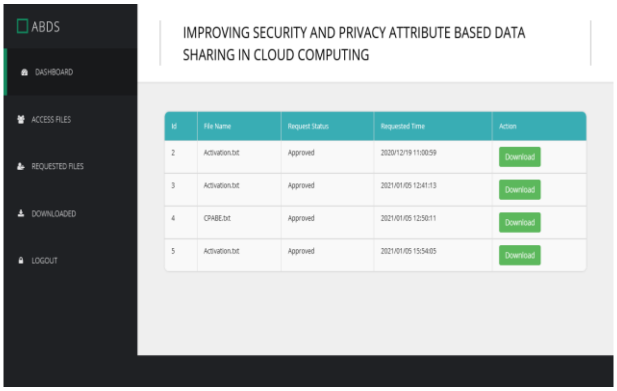
File Name: john

Select The Access Policy: ○ Doctor ● Nurse ○ Staff

File input: No file selected.

Maximum upload size is 5 MB.

SETTING UP THE ACCESS POLICY



IMPROVING SECURITY AND PRIVACY ATTRIBUTE BASED DATA SHARING IN CLOUD COMPUTING

Id	File Name	Request Status	Requested Time	Action
2	Activation.txt	Approved	2020/12/19 11:00:59	Download
3	Activation.txt	Approved	2021/01/05 12:41:13	Download
4	CPABE.txt	Approved	2021/01/05 12:50:11	Download
5	Activation.txt	Approved	2021/01/05 15:54:05	Download

DOWNLOADING THE ENCRYPTED FILE

VII. CONCLUSION

We proposed a conceal preserving CP-ABE scheme in the standard model. The presented scheme has many advantages over the existing schemes, such as constant size private keys and short ciphertexts. And in decryption, it only needs four twinning process. This article has been accepted for incorporation in a future issue of this journal. Content is final as presented, with the exception of pagination. The proposed scheme accomplish enhanced security and anonymity in a prime order group. In the standard model, we show the security of the proposed scheme is reduced to the decisional n-BDHE and the DL assumptions. Additionally, the proposed scheme supports authority verification with no data conceal leakage.

In this paper, we propose an secure and efficient data sharing scheme for mobile devices. The scheme ensures security and authorized access of shared sensitive data. Furtherly, the scheme efficient obtains integrity verification before DR shares the data to avoid incorrect computation. Finally, the scheme accomplish lightweight operations of terminals on both DO and DR sides.In this paper, we propose an efficient and secure data sharing scheme for mobile devices. This ensures security and authorized access of shared sensitive verification before DR shares the data to avoid incorrect computation. Finally, the scheme accomplish lightweight operations of terminals on both DO and DR sides.This policy and relies on a weak security model. How to construct a enhanced secure HP-CP-ABE scheme with more flexible and relaible access policy is left for the future works.

VIII. ACKNOWLEDGEMENT

The authors would like to thank **Mrs.M.SAMUNDEESHWARI** for her suggestions and excellent guidance throughout the project period.

REFERENCES

[1] Farahat IS, Tolba AS (2018) A secure real-period internet of medical smart things (IOMST). Comput Electrical Eng 72:455–467

[2] Rahmani AM, Gia TN, Negash KB (2018) Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. Futur Gener Comput Syst 78:641–658

[3] Zhang Y, Qiu M, Tsai C, Hassan M, Alamri A (2017) Health-CPS: healthcare cyber-physical system assisted by cloud and big data. IEEE Syst J 11:88–95

[4] Ghazvini A, Shukur Z (2013) Security challenges and success factors of electronic healthcare system. Proc Technol 11:212–219

[5] Guan Z, Lv Z, Du X et al (2019) Achieving data utility-conceal tradeoff in internet of medical things: a machine learning approach. Futur Gener Comput Syst 98:60–68

[6] Elhoseny M, Abdelaziz A (2018) A hybrid model of internet of things and cloud computing to manage big data in health services applications. Futur Gener Comput Syst 86:1383–1394

[7] Han K, Li Q, Deng Z (2016) Security and efficiency data sharing scheme for cloud storage. Chaos Solitons Fractals 86:107–116

[8] Zhang L, Zhang H, Jia Y (2020) Blockchain-based two-party fair contract signing scheme. Inf Sci 535:142–155

[9] Lu X, Cheng X (2020) A secure and lightweight data sharing scheme for internet of medical things

[10] J. Lai, X. Zhou, R. H. Deng, Y. Li, and K. Chen, “Expressive CP-ABE with partially hidden access structures,” in *Proc. 7th ACM Symp. Inf. Comput. Commun. Secur.*, May 2012, pp. 18–19.

[11] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, effificient, and provably secure realization,” in *Proc. 14th Int. Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography*, Mar. 2011, pp 53–70.

[12] Y. S. Rao and R. Dutta, “Recipient anonymous ciphertext-policy attribute based encryption,” in *Proc. 9th Int. Conf. Inf. Sys. Secur.*, Dec. 2013, pp. 329–344.

[13] L. Zhang, Q. Wu, Y. Mu, and J. Zhang, “Conceal-preserving and secure sharing of PHR in the cloud,” *J. Med. Syst.*, vol. 40, pp. 1–13, 2016.

[14] M. Abdalla, D. Catalano, and D. Fiore,“Verififiable random functions: Relations to identity-based key encapsulation and new constructions,” *J. Cryptol.*, vol. 27, pp. 544–593, 2014.

[15] C. Huang, K. Yan, S. Wei, G. Zhang, and D. H. Lee, “Effificient anonymous attribute-based encryption with access policy hidden for cloud computing,” in *Proc. IEEE Int. Conf. Progress Inform. Comput.*, Dec. 2017, pp. 266–270.

[16] Y. Zhang, X. Chen, J. Li, D. Wong, and H. Li “Anonymous attribute-based encryption supporting effificient decryption test,” in *Proc. 8th ACM Symp. Inf. Comput. Commun. Secur.*, May 2013, pp. 511–516.

[17] J. Li, H. Wang, Y. Zhang, and J. Shen, “Ciphertext-policy attribute-based encryption with hidden access policy and testing,” *KSII Trans. Internet Inf. Syst.*, vol. 10, no. 7, pp. 3339–3352, Jul. 2016.

[18] H. Cui, R. H. Deng, G. Wu, and J. Lai, “An effificient and expressive Ciphertext-policy attribute-based encryption scheme with partially hidden access structures,” in *Proc. 10th Int. Conf. Prov. Secur.*, Nov. 2016, pp. 19–38.

[19] [19] F. Khan, H. Li, L. Zhang, and J. Shen, “An expressive hidden access policy CP-ABE,” in *Proc. IEEE 2nd Int. Conf. Data Sci. Cyberspace*, Jun. 2017, pp. 26–29.

[20] Y. Zhang, Z. Dong, and R. H. Deng, “Security and conceal in smart health: Effificient policy-hiding attribute-based access control,” *IEEE Int. Things J.*, vol. 5, no. 3, pp. 2130–2145, Jun. 2018.

[21] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, “Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption,” in *Proc. 29th Annu. Int. Conf. Theory Appl. Cryptographic Techn.*, 2010, pp. 62–91.

[22] T. Okamoto and K. Takashima, “Adaptively attribute-hiding (hierarchical) inner product encryption,” in *Proc. 31st Annu. Int. Conf. Theory Appl. Cryptographic Techn.*, May 2012, pp. 591–608.

[23] T. V. X. Phuong, G. Yang, and W. Susilo, “Hidden ciphertext policy attribute-based encryption under standard assumptions,” *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 1, pp. 35–45, Jan. 2015.

[24] X. Boyen and B. Waters, “Anonymous hierarchical identity-based encryption (without random ora