Materials Today: Proceedings xxx (xxxx) xxx

Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

Security on mobile cloud computing using cipher text policy and attribute based encryption scheme

Madireddy Swetha [a,*], M. Latha [b]

[a] Department Of Computer Science & Engineering, Vels Institute of Science, Technology and Advanced Studies, Tamil Nadu, India
[b] Vels Institute of Science, Technology & Advance Studies, Tamil Nadu, India

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Mobile Cloud Computing
Attribute-Based Encryption
CP-ABE

ABSTRACT

Mobile Cloud Computing (MCC) is a new paradigm that has been emerged by the advances in the Cloud Computing for Mobile devices to access Cloud services. The data security challenges against the data thefting, deleting, corrupting, or exploiting are existed as the data storage and access to/from the cloud has been most popular. In order to handle these data security issues in the cloud and to provide protection for the data, some innovative encryption methods have been developed. One of such encryption methods is Attribute-Based Encryption (ABE) that has a more control on the data in cloud as which is accessed by whom. Since from the recent years, many of academic researchers have paying a widespread of attention on using advanced cryptographic techniques to securely store, process, also share data over the untrusted cloud environment. One of the promising cryptographic techniques which can solve the open challenge of regulating the fine-grained access control of important data over the distributed cloud is the Cipher text Policy – Attribute Based Encryption (CP-ABE). Therefore, a survey of work is presented in this paper on different CP-ABE methods for the secure mobile cloud computing architecture. This paper presents some works that are focused on secure data storing, accessing and sharing using CP-ABE methods over the untrusted cloud environments. All the works that are studied are analyzed and compared with each other in the results to find the best out of it.

1. Introduction

The persistent access can be empowered by the distributed computing for the information resources. The information management systems such as remote information storage, calculation of outsourced label, etc. can provide cloud servers over distribute computing environment. Then such cloud servers are used along with the CP-ABE methods and Verifiable Delegation (VD) approaches in order to ensure the data protection and the undisputed status of the appointment [1].Fig. 1.Fig. 2.Fig. 3.Fig. 4.Table 1.

Two types of attribute-based encryptions are there in which first one is the Key Policy-Attribute Based Encryption (KP-ABE) and second one is the Cipher text based-ABE (CP-ABE). The key dealer determines the access control model to be taken in the middle of KP-ABE framework instead of enciphering which limits that framework usage and incentive in sensible applications [2]. The cipher text in this CP-ABE scheme identified within actuality related to maintaining access structure. Then the all attributes are gathered to label every unopened secret key. The user can get an access to encrypted data file if and only if the privilege of his/her cipher text matches with the privilege of access control model's predefined cipher text. Obviously, this method is theoretically closer to the previous access control models.

On the other hand, the access control model for universal framework is the most ingrained type of category criteria in the middle of an ABE framework which the devices express a predetermined program [3]. Some of the previous methods addressed for the secure mobile cloud computing environment are surveyed and three of the works are presented in this paper. At last all the works are analyzed and compared in the result which may help the researchers who are doing works under finding the reliable security framework for the mobile cloud computing environment.

2. A brief review of Cp-Abe

The private data to be shared to all data users is the wish of data owner. Suppose the cloud is utilized to save the data [4]. The data owner gives access to all data users to access the data rather than giving permission to individual data users. All the data users can

* Corresponding author.
E-mail address: swetha.mudupu@gmail.com (M. Swetha).

https://doi.org/10.1016/j.matpr.2021.06.462
2214-7853/

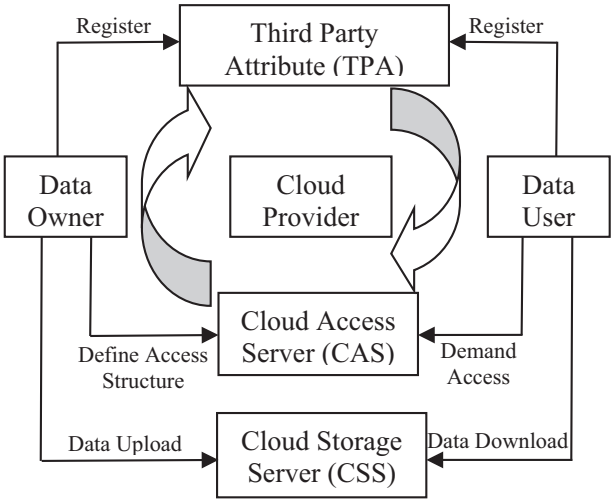

Fig. 1. Rs Cpabe Model.

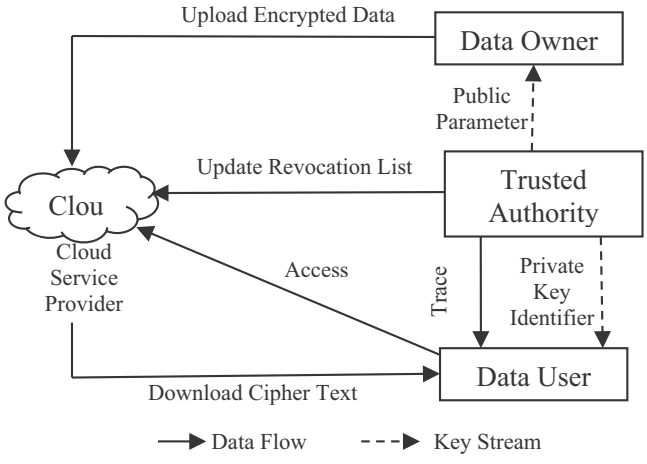

Fig. 2. System Model Of Updatable Cp-Abe Scheme.

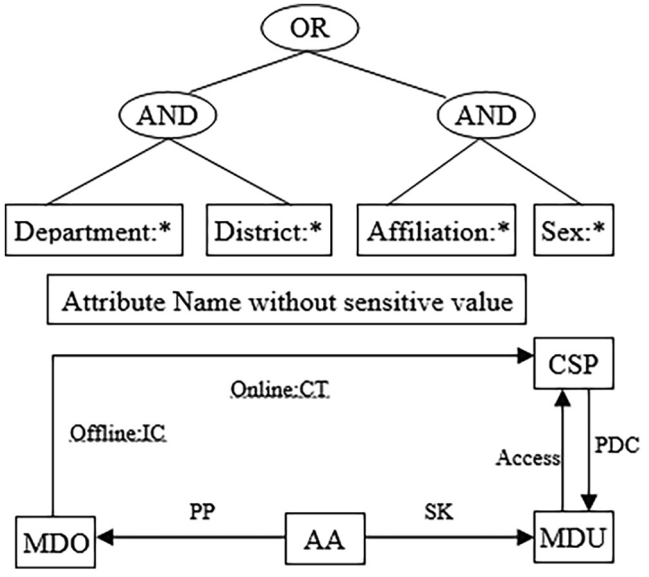

Fig. 3. system model of ppcmm.

only access data when they have proper attributes to access data of others or else cannot access the data. An Access Policy is applied by DO for this private data. If the attributes of the users and access policy are matched then data can be accessed by the end user. With following steps the CP-ABE encounter this need. They are A) The owner of the data summing up the data in a single Cipher text and the access policy B) The cipher text is decrypted by the data user by utilizing their secret key when the user have correct attributes. The CP-ABE implementation is based on 4 algorithms such as (A) Setup (B) Generation of Key, (C) Encryption, (D) Decryption ((E) Global set-up).

AU stands for Attribute Universe which is having all users' population. Based on the set of attributes in the AU the access set called A is configured by DO (Data Owner) for data named as M in CP-ABE [9]. Through a PK means Public Key the M named as message and its A called access set both are encrypted by the DO. A private key called SK is assigned by a Data User called DU. The SK is subset of the AU and associated with his attribute list. For the Master Key the AA is generated both SK and PK. Using SK the DU can decrypt the message and access it when SK have the correct attributes for that message.

(A) Setup: A security parameter is given to the setup algorithm as input. The master secret key of system MK and PK public key are returned by setup. Data owner utilizes the PK for encryption. To generate secret keys MK is utilized by AA and SK is utilized for DU. The key authority is only one knows the MK. Output is Setup: $\{\lambda\} \rightarrow \{MK, PK\}$.

(B) Encrypt: PK is the input to this encryption algorithm. M is the plain text and A is used as access structure. The output of this algorithm is cipher text named as CT. Output is Enc: $\{PK, MK, A\} \rightarrow$ CT.

(C) Generation of Key: 'w' is allocated as bunch of attributes which are given as input to this algorithm. These are associated with the secret master key MK and user. Secret key SK is the output of this algorithm. Output is Key Gen: $\{MK, w\} \rightarrow SK$.

(D) Decrypt: For attribute set a secret key SK and the cipher text CT are takes as inputs to this algorithm. It gives return the message M when the user attribute is matched with the access structure of cipher text CT. Output is Decryption: {Secret Key, Cipher Test} → Message.

2.1. CP-ABE in computing architecture of mobile cloud

CP-ABE Challenges in MCC: Up to now discussed about the algorithms which are contained by the CP-ABE. Now it is good to discuss about the problem which are encountered in CP-ABE. Mainly 3 challenges are faced by data user. They are computation cost of cipher text (DO), the communication cost of cipher text (DO) and finally computation cost of secret Key (DU) [10].

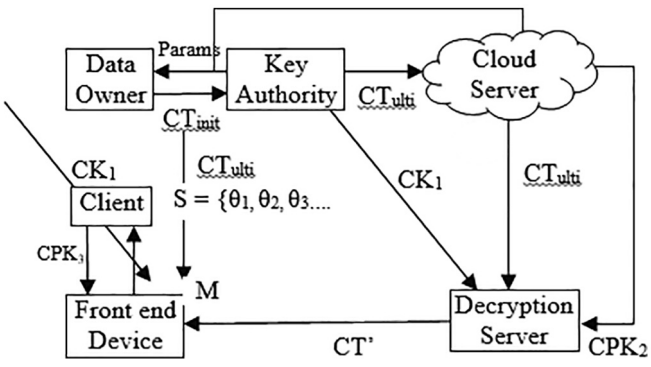

Fig. 4. Ckm-Cp-Abe Model For Cloud Data Sharing.

Table 1
Comparison Of Performance Analysis.

Paper	[5]	[6]	[7]	[8]
Revocation	√	√	X	√
Privacy policy	–	√	√	–
Key Update	X	√	X	√
Security	more	more	more	Less
Computation Cost	Low	high	Very low	high

Architecture features: To remove the problem called resource-constrained mobile devices different schemes are researched and architectures are developed. Different schemes of architectural features are explained in below list. Note that some of these schemes can utilize more than one feature.

2.2. Architecture features

(1) Encryption in the Cloud: In this feature the encryption of ABE is given to Cloud server from mobile device [11].

(2) Decryption in the Cloud: In this feature the decryption of ABE is given to Cloud server from mobile device.

(3) Pre-encryption: In this feature to distribute computation costs the encryption of ABE is converted into pre-encryption.

(4) Pre-decryption: ABE decryption scheme in this feature converted into pre-decryption first and decryption secondly in order to address the computation cost challenges [12].

(5) Finite size cipher texts: In this feature the access policy is defined through constant-size cipher texts to limit the extensive attribute lists computation impact.

(6) Constant-size secret keys: In this feature through secret keys with constant-size and restricting the impact of extensive attribute computation is sets of individuals.

(7) Multiple Authority extension: In multiple attribute authorities the CPABE scheme is operated in this feature and supports "universal attribute set" which is a large scale [13].

(8) Online-Offline feature: In this feature the encryption of ABE and decryption of ABE are fully dependent on Cloud services. It has an ability of performing local high difficulty computation when internet is not connected to this mobile device. That means mobile is in charging [1415].

3. Survey on Cp-Abe schemes

3.1. RS-CP attribute based encryption scheme

A scalable, flexible and fine-grained access control method is developed and implemented with Cipher text Policy-Attribute Based Encryption (CP-ABE) like an effective cryptographic technique. But the computation cost, overhead of data owner and revocation are some of the challenges faced by the existed CP-ABE based techniques. Such challenges can be addressed in the paper [5] by proposing a Revocable Sliced-Cipher text Policy ABE (RS-CP ABE) in which splitting algorithm is applied. In this paper, symmetric encryption is executed on huge size of dataset with the Advanced Encryption Standard (AES) while the asymmetric encryption is executed on a finite length of key with CP-ABE. If the only one slice revocation is a case, then the re-encryption is carried out. Then the performance and security evaluations are exposed and proved their model. A fine-grained access control method which overcome afore mentioned limitations is ensured with this RS-CP ABE technique by employing it into the cloud computing environment. Figure (1) shows the system model of this RS-CP ABE model which comprised of four major parts as follows:

DO: DO is Data Owner. Publishing the data and defining the structure to access it are the responsibilities of a DO. The accessing of data in unauthorized way and even in authorized way also controlled accordingly by applying the access structure policy to the proper data. Therefore, a digital envelop is created in this model by suggesting this DO in this system model with all the aforementioned activities for providing security to the data against network attacks.

TPA: TPA is a Third-Party Authority. A truthful authority is offered by this. The honest responses for various performed requests are correctly provided with this TPA. In configuring and generation of secret key it acts as an essential one.

CP: CP (Cloud Provider) is contains two interactive devices as follows:

CAS: CAS (Cloud Access Server) is a server dedicated to the access control. It executes the re-encryption technique on a single slice randomly selected among 'n' slices that are divided from data file in order to reduce the utilization of resources and provide the more security levels to the data which is the main function of this CAS. Data integrity is also ensured by execution of XOR operation followed by computation of hash key for various slices. At last, such re-encrypted slice with encrypted data is send to the cloud server and then the respective URL (Uniform Resource allocator) can be received as a response.

CSS: CSS (Cloud Storage Server) is a device in which data is stored. In general, it is a hardware component.

DU: In order to execute some operations on data file like read and write, this DU (Data user) entities the request. According to the attributes of user DO predefine such privileges. A directory is used to register every DU and group of attributes are utilized to describe such DUs. Accessing the cloud environment stored with the encrypted data is the main intention of Him/her. This encrypted data file is decrypted by the DU exactly when the solicited file's attributes list that are predefined in the access structure associated with the attributes of Him/her are matched.

3.2. Traceability and revocation updatable CP-ABE scheme

The fine-grained access control model that is suitable to the complex commercial applications over the encrypted data is offered by CP-ABE. There may be a challenging problem occurred by the malicious users or attackers misuse their secret key which can't be traced because of the rights to multiple users in one-to-many encryption method for sharing the similar decryption privileges. The revocation of a malicious user from system is necessary if he intercepted an attack in order to further increase the security level.

Therefore, a new white box traceable and traitor vocation updatable CP-ABE method is proposed in the paper [6] to deal with such above mentioned challenges. This scheme used a fixed point and unique identifier to achieve the traceability and revocation respectively. Traceability is achieved by embedding the fixed point in secret key of users whereas traceability is achieved by assigning the identifier to every user. Furthermore, message is encrypted by using the secret exponent which was separated into two components. The access policy is assigned with the one element and other one is assigned to revocation list. The updatable cipher text process thus significantly simplified since it was just required to update some part of cipher text components if there is change in revocation list. The method proposed in this paper has more efficient in achieving a proper revocation and updating cipher text in comparison with the other existed methods. Figure (2) shows this CP-ABE system model framework for made more clear illustration of system. It has four parts that are discussed below.

TA: This TA called Trusted Authority is completely trusted one. The master secret key along with the public parameters are defined

by this TA for the entire system. Furthermore, it performed the responsibilities of secret key generation, malicious users or attacker tracing and traitor revocations. The public revocation list and identity table are also maintained by this TA in this structure.

DO: DO or Data Owner is the user who shared his/her data to a user group. Then the responsibilities of DO are specifying the access structure, data encrypting and the cipher text outsourcing to cloud.

DU: The cipher text outsourced in the cloud is accessed by this DU (Data User). However, DU can only be recover the messages successfully if he/she has authorized set of attributes and is not present in revocation list.

CSP: This CSP (Cloud Service Provider) an honest but curious service provider. That means every authorized request will execute honestly but the information from the process and their results are taken as much as possible. The outsourced cipher text in the cloud is updated if change occurred in revocation list.

3.3. Privacy-Preserving access control using CP-ABE

In order to design a cloud assisted system for the sharing of mobile multimedia information, the primitive method that has been adopting most widely is the Cipher text-policy ABE (CP-ABE) because of its ability to allow the encrypt or in defining the access policy in prior to the message encryption. The access policy in the majority of researches uses the cipher text to send in the form of plaintext. The privacy of users against the other users who can know the cipher text or even against the unauthorized user to decrypt the data can be exposed by such of plaintext form. Moreover, the CP-ABE includes encrypt and decrypt operations which cannot be frequently carried out in the limited resource mobile devices. This problem may result in reduction of mobile device user's interest for the sharing of their multimedia information through such devices [7].

In this method, attribute name as well as value are used to describe every attribute. Here, the access policy exposed just the attribute names only and the cipher text is embedded with the attribute values. Offline and Online are the two encryption phases that are divided. The intermediate components of cipher text are first prepared in offline phase of encryption by the data owner. Then the legal cipher text resulting from the reception of an access policies encryption requirements and multimedia information can be formed quickly in the online phase by the data owner. The decryption computation overhead and matching test's computation overhead are finally offloaded into the cloud server with the decryption outsourcing approach employment. This paper described that the PPCMM method in a standard model has showed an adaptively more secure from the security proof. This also indicated that there is a great reduction in the computation cost for online encryption phase also for user decryption by analyzing the performance of the PCMM.

The system model of PPCMM is shown in figure (3) which includes four different bodies. Multimedia Data Owner (MDO), Attribute Authority (AA), Multimedia Data User (MDU) and Cloud Service Provider (CSP) are such four types of bodies.

MDO: The multimedia information that is to be shared through CSP is present in this MDO. There is a requirement of defining access policy which describes the attribute using the attribute name with their subsequent attribute value in prior to the encryption and uploading of multimedia information in to CSP. The intermediate components of cipher text can also prepared by this MDO for the battery power saving in prior to the execution of online encryption phase which operation was carried out with existing multimedia file information on a particular access policy.

AA: The system model is initialized by this AA and he is responsible in issuing public parameters and keys generation for MDU based on the attributes.

MDU: private keys are obtained by the MDU from AA. He also tried to access CSP for the multimedia data that has been encrypted. If the name and the values of attributes matched with those of names and values in the current access policy, then only accessing is success. For doing such matching test operation in addition to perform partial decryption task, CSP is used.

CSP: The ABE cipher text corresponding to the encrypted multimedia information is stored. In addition, with partial decryption, matching test computational outsourcing service is also provided by the CSP.

3.4. Collaborative key management protocol in cipher text policy Attribute-Based encryption

A CP-ABE (CKM-CP-ABE) scheme is proposed in the paper [8].

The representation of the CKM-CP-ABE system model for cloud data sharing is shown in figure (4). In cloud data sharing, it contains mainly 5 steps.

1) CL: In this step by using the front-end devices user nothing but client named as CL wants to approach data in cloud storage. Now a day's mostly the mobiles are the front-end devices used for cloud services. The plain text in the cloud to be accessed by the CL when the user attributes are matched with the cipher text access policy. Assuming that some mobiles are performance-restrained so that the client may threatens from key exposure.

2) KA: In this system KA means key authority is main component. Main calculation parts are covered by the KA like key update, key generation, etc. In this system KA is curious to know the plain text value but it will not tamper with it. So KS can be assumed as semi-trusted.

3) CS: In this system total storage management is under CS (Cloud Server) responsibility. Any data transfer is under control of cloud server. Cloud server may semi-trusted.

4) DS: DS is denoted as Decryption server which can provide more dominant computing capabilities. It takes the control of most operations and isolates them but not all operations in decryption. Let us say decryption server is semi-trusted. Since DS was suitable to CKM-CP-ABE scheme such access channel is not secured to guarantee data security.

5) DO: The DO is named as data owner. Data owner is the first user who uploads the data in server. Data owners are the original owners of data who have the access attributes, but others require permission to access the plain text.

Hoping that all steps involved in this system are not combined with each other to theft the data. If it happens then the proposed system will not helpful and waste. In this system key authority is utilized to authenticate the all attributes. In its system KA and CS are worked together to generate the set of elements represent the all issued attributes in public parameters. Let public parameters denoted as *params*. When the data is uploaded by the data owner it encrypted first by utilizing the *params* and forwarded to for the initial CT called CT_{init} and uploaded to key authority. It is re-encrypted by the key authority for ultimate CT denoted as CT_{ulti} and is saved in cloud server. To continuously and secretly produce 3 various elements of the PK management protocol was helped based on client's attribute set $S = \{\theta_1, \theta_2, \theta_3 \cdots .\}$. They are CPK_1, CPK_2 and CPK_3 are hold on by key authority, cloud server or client. When the user try to get the data from server then the decryption server takes CPK_1 and CPK_2 to change into the CT from CT_{ulti} from CTM eventually. The client takes the plaintext CPK_3. In this CKM-CP-ABE system from the ultimate cipher text only the plaintext is gained using all 3 PK elements. It means to decrypt CT user need to be in touch with cloud server and key authority.

4. Result analysis

In this result analysis section, all the results and performance evaluation of four papers that are surveyed in this paper are studied and then a comparison among those schemes can be carried out and a tabular form is given to show the comparison analysis. Here, in paper [5] the CP-ABE scheme is implemented in mobile cloud computing environment which provide a fine-grained access control. It uses a splitting algorithm with re-encryption in revocation scheme and key is updated when there is a change in revocation list. This CP-ABE scheme has a robustness against various attacks thus provide high security and it also provides low computation cost and high performance. Then the paper [6] used updated CP-ABE scheme with which three functionalities are achieved such are traceability of white-box, revoking of traitor and updating the cipher text. The secrecy forward characteristic has also achieved by this scheme which makes it most suitable one for the realistic and complex business application.

The PPCMM is implemented in the paper [7] in which the privacy policy is addressed simultaneously with the efficient encryption and decryption techniques. This scheme has a very low computation cost because of the efficient decryption outsourcing technique which helps in realizing matching test and reduced the final decryption for the users. The security analysis in this paper demonstrated that this scheme achieved more secured, effective and practical outcome. Finally, the paper [8] used a CP-ABE scheme with collaborative key management protocol which enhanced the key management efficiency and security over a mobile cloud data sharing environment. In this, private key update algorithm is constructed by introducing set of attributes for fine-grained access control and instant revoking of attributes. Table (1) depicts the comparison of performance analysis of different works surveyed in this paper.

5. Conclusion

In general, one of the most widely used schemes to deal with the security challenges of data in the cloud environment is CP-ABE. This method has provided a finite level of scalability and flexibility to eliminate the requirement of data owners for managing every single request. Therefore, for this a fine-grained access control model is maintained by each data owner and they issue the access to the user if he/she had proper attributes. In this paper four papers that addressed this CP-ABE scheme in providing fine grained access control are surveyed. The main aim of this survey is to obtain the knowledge on such scheme and how they overcome the challenges occurred in mobile cloud environment. The performance analysis and result analysis of studied works are analyzed and then a comparison was performed. This survey can in future helpful for the researchers to work on their research under implementing a reliable mobile cloud computing system with high security.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] K Xue, J Hong and Y Xue, "TAFC: time and attribute factors combined access control for time-sensitive data in public cloud", IEEE Transaction on Service Computers, pp: 13, 158–171, 2020.
[2] C. Ma, Z. Yan, C.W. Chen, Scalable access control for privacy-aware media sharing, IEEE Transaction on Multi. Pp 21 (1) (2019) 173–183.
[3] Li J, Chen N and Y. Zhang, "Extended file hierarchy access control scheme with attribute-based encryption in cloud computing", IEEE Transaction on, Emerging Topologies of Computer Epublic, March, 2019.
[4] W. Li, B.M. Liu, D. Liu, R.P. Liu, P. Wang, S. Luo, W. Ni, Unified fine-grained access control for personal health records in cloud computing, IEEE Journal of Biomedical on Health PP 23 (3) (2019) 1278–1289.
[5] L.A. Saidane, C. Ghazel, M. Bouchaala, Revocable Sliced CipherText Policy Attribute Based Encryption Scheme in Cloud Computing, 15th Inter. Wirel. Comm. & Mobile Comput. Confe. (IWCMC) (2019).
[6] Baocang Wang, Zhenhua Liu, Yan Liu and Jing Xu, "Updatable Ciphertext-Policy Attribute-Based Encryption Scheme With Traceability and Revocability", IEEE Access, May 22, 2019
[7] Q.i. Li, Y. Tian, Y. Zhang, L. Shen, J. Guo, Qi Li, Yinghui Zhang Jingjing Guo and Youliang Tian, "Efficient privacy-preserving access control of mobile multimedia data in cloud computing", IEEE, Access 7 (2019) 131534–131542.
[8] Z. Sun, H. Hong, G. Lin, A Collaborative Key Management Protocol in Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing, IEEE Access (2017), https://doi.org/10.1109/ACCESS.2017.2707126.
[9] J. Meng, B. Wu, H. Wen, Y. Jiang and Y. Xie, "A Modified Hierarchical Attribute-based Encryption Access Control Method for Mobile Cloud Computing," IEEE Trans. Cloud Comput., pp. 1-1, 2017.
[10] Y. Xiang, W. Teng, T. Zhang, G. Yang and D. Wang, "Attribute-based Access Control with Constant-size Ciphertext in Cloud Computing," IEEE Trans. Cloud Comput., pp. 1-1, 2016.
[11] Jiguo Li, Xiaonan Lin, Yichen Zhang, and Jinguang Han. Ksfoabe: Outsourced attribute-based encryption with keyword search function for cloud storage. IEEE Transactions on Services Computing, pages 1–1, 2016.
[12] Jie Xu, Qiaoyan Wen, Wenmin Li, and Zhengping Jin, "Circuit CiphertextPolicy Attribute-Based Hybrid Encryption with Verifiable Delegation in Cloud Computing", IEEE Trans. Parall. & Distrib. Syst., Volume: 27, Number: 1, January, 2016
[13] Ambrosin, M. et al(2016) On the Feasibility of Attribute-Based Encryption on Internet of Things Devices. 2016 IEEE Micro Volume:36 Issue:6
[14] T. Jung, X.-Y. Li, Z. Wan, M. Wan, Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption, IEEE Trans. Information Foren. & Secur. 10 (1) (2015) 190–199.
[15] Jianting Ning, Xiaolei Dong, Zhenfu Cao, Lifei Wei, Xiaodong Lin, Lifei Wei and Xiaolei Dong, "White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes", IEEE Trans. Infor. Fore. & Secur. 10 (6) (2015) 1274–1288.