IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

To Ensure Data Security and Efficient Data Access Control for Cloud Storage using Immediate Revocable Timestamp MA-ABE Scheme

Prof. Srinath G M, Anusha A, Bhargavi B G, Deeksha M V, Enturi Vyshnavi
Department of Computer Science and Engineering
S.J.C Institute of Technology, Chickballapur, India

Abstract: The achievement for the fine-grained entry control over data and for its guarantee of data security. Multi authority Attribute based encryption schemes not suitable for the devices with resource constrained, due to it is based on expensive bilinear pairing. The major limitation of Multi-authority-ABE scheme is attribute cancellation that is revocation of attributes. Using the elliptic curves cryptography and Diffie Hellman Problem to propose an "To Ensure Data Security and Efficient Data Access Control for Cloud data Storage Using Immediate Revocable Timestamp Multi-authority-ABE scheme". The analysis of security represents that the proposed scheme satisfies similar under adaptive chosen plaintext-attack by using Diffie-Hellman problem. Compared with the other schemes present, the proposed scheme is more economical in computational cost and storage. The timestamp is used in multi authority attributed encryption and the data user can able to view the file within the particular period of time.

Keywords: Revocable, multi-authority attribute-based encryption, timestamp, cloud data storage, elliptic-curve cryptography, Plaintext-attack

I. INTRODUCTION

Cloud computing is the need handiness of computer system resources, as in cloud data storage and computing power. here clouds data is functionally distributed over multiple locations, such as datacentre. Cloud computing is depending on resources sharing to get consistency and typically uses a pay as you go model, helps in reducing acquisition expense and also gets the unpredict expense of operating for users.

The characteristics of cloud computing are: Rapid Flexibility and scalability,Automation, Security, pay as you go, Measured service, Budget friendly, Based network access, CN demand self-service, easy maintenance, resource pooling.

Cloud Data Security: Using timestamp the security is given for the file. Cloud data security refers to the technologies, programs, services and security controls that protect any type of data in the cloud computing platform from the loss, leakage or abuse through breaches, exfiltration and unauthorized views.

A robust cloud computing data security ensures the security and privacy of data across networks as well as within applications, containers, workloads and other clouds environments controlling data views for all users, devices and software, furnishing complete visibility into all data on the network.

The numerous single-authority attribute-based encryption scheme have been put forward. It requires only one trusted attribute authority administers the attributes and distributes secret keys of attributes to the data users. This mechanism may not meet the practical requirements in cloud data storage, when data consumers' attributes are distributed by multiple different attribute authorities. For example, when a data owner intends to share the data to the data user holding the attribute ''Professor'' from a university and the attribute ''Engineer'' from a research institution, obviously Single-authority-ABE scheme cannot be applied to this scenario. To deal with this problem, numerous researchers turn to multi-authority attribute-based encryption, so that secret keys of attributes are issued to data consumers with the corresponding privileges for different attribute authorities respectively. This paper involves the construction of an efficient Revocable MA-ABE scheme for cloud data storage.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

II. RELATED WORK

In [1] the existing Multi authority attribute-based encryption schemes are unfitting for the devices with insufficient resources, because it is based on the expensive bilinear pairing. The major objection of Multi authority-ABE scheme is revocation of attribute. Numerous solutions in this respect are ineffectual enough. Elliptic curves cryptography is proposed an efficient revocable MA-ABE scheme for storage in cloud.

In [2] the forward protect and efficient expand computation algorithm on sharing of data scheme for privacy computing. the existing schemes only outsource decryption computation to the storage of cloud, consumers still have heavy weight in encryption of data. For reducing the computing weight of consumers, most encryption and decryption computations are deployed to the cloud service provider. It proposes a efficient consumer and revocation of attribute. Finally, the analysis of security and outcome shows that this scheme is secure and efficient compared with other existing schemes

In [3] it constructs a new multi-authority CP-ABE scheme over large attribute universe with decentralization of authorities that supports white-box traceability along with policy update and outsourcing decryption. The proposed system is built on prime order groups and supports monotonic view structures. These features improve efficiency and articulateness of the system and implemented the proposed cryptosystem in charm cryptographic framework and it analysed its performance this is production with a diverse set of test cases.

In [4] an attribute-based keyword search scheme, as a cryptographic primitive which explores the notion of public key encryption with keyword search into the context of attribute-based encryption, can enable the data owner shares the data to a group of consumers and satisfying the views policy and meanwhile, it maintains the confidentiality and searchable properties of the sensitive data. our scheme is secure and efficient compared with existing schemes

In [5] the proposed system such as novel pairing-free data belief the control scheme based on ciphertext policy attribute-based encryption using elliptic curve cryptography and abbreviated as PF-CP-ABE. This replaces the complex bilinear pairing with simple scalar form of multiplication on elliptic curves, by this it reduces the overall computation overhead.

In [6] the practical attribute-based encryption scheme is proposed and solves preceding issues at the same time. To support the flexible number of attributes, this scheme achieves large universe and multiple attribute authorities. The security and performance of this proposed scheme are discussed and extensive experiments are followed to demonstrate its practicability and effectiveness.

In [8] there will be concrete attack to the existing ABE scheme with attribute revocation. It defines the definition and the security of the model, where the model collusion attack is executed by the existing consumers cooperating with the revoked consumers. Later it represents the user collision avoidance CPABE scheme with the efficient revocation of attributes for the cloud system.

III. PROBLEM STATEMENT

Multi authority attribute-based encryption schemes are not suitable for the devices with resources constraint, since these kinds of schemes are all mostly based on the expensive bilinear pairing and the major challenge of this scheme is attribute revocation. So far, the many solutions in this are not sufficient. In the MA-ABE revocation of attributes takes time and there is no immediate revocation, so that precious data will be in the hands of unauthorized users and the multi authority attribute-based encryption using timestamp for the attributes to achieve the immediate revocation for data confidentiality. The attribute revocation for multiple data consumers may share the same attribute and each data consumer may possess multiple different attributes, result in that revocation for anyone attribute.

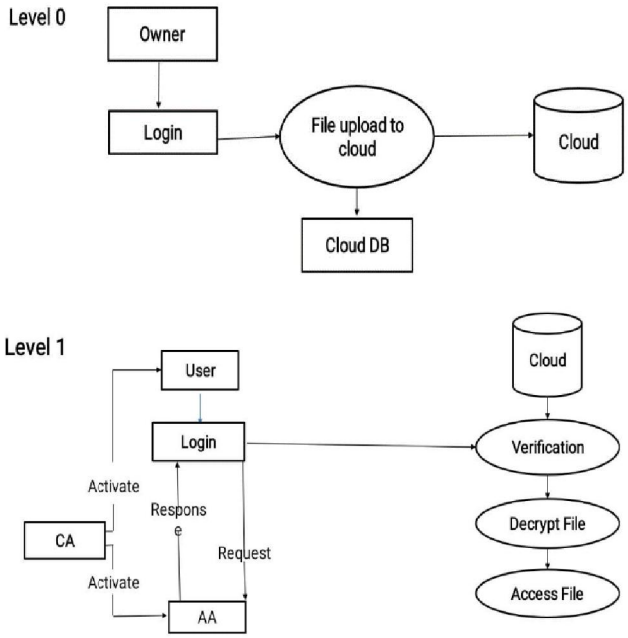
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

IV. PROPOSED SYSTEM DESIGN AND METHODOLOGY

Data Flow Diagram: Data flow diagram represents the information flow and shows how the data enters into the system and leaves the system, what changes the information and where the data is stored.

Level-0: It describes how the admin will login into Cloud data and uploads the file into the Cloud database and sets the timelimit to view thefile.

Level 1: The Certificate Authority (CA) will activate Attribute Authority (AA) and User. The User will send request to Attribute Authority to view the file then Attribute Authority sends response with the Secret Key. User will be verified as valid user, now the file will be decrypted and user can able to view the file.



Data Flow Diagram

Use Case diagram

Use Case Diagram is to depict the dynamic aspect of a system. Use case diagram summarize the details of the system's users and interactions with the system. It collects the system's requirement, which includes both internal and external influences. It represents the dynamic behaviour of a system and how an entity known as actors from the external environment can interact with the system. It sums up the system functionality by incorporating use cases, actors and their relationships. It consists of the use cases, actors and associations.

Use cases: The horizontally shaped ovals are the use cases that represent the different uses that a user might have.

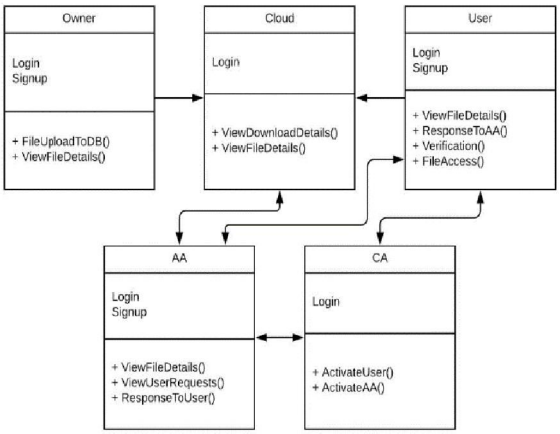
Actors: Actors are the stick figures that represent the people actually employing the use cases.

Associations: A line between the actors and use cases.

Sequence Diagram: Sequence Diagrams are the interaction diagrams. That presents how the operations are carried out. Sequence diagrams captures the interaction between objects in the context of a collaboration. It shows the order of interaction and it is also a time focus using the vertical access of the diagram.

Class Diagram: Class diagram is a static view of an applications that analyses and designs. Class diagram describes the major responsibilities and importance of a system. It is a base for the component diagram and deployment diagram. It incorporates forward and reverse engineering.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023



Class Diagram

Modules split up

1. Certificate Authority
2. Attribute Authorities
3. Data Owners
4. Cloud Server
5. Data Consumers

Certificate Authority

It is a globally trusted authority in the system. It sets the system and accepts the registration of all the consumers and attribute authority in the system. Each legal consumer in the system, the certificate authority assigns a unique user identity and generates a global public key for this consumer. The certificate authority is not involved in any management of attribute and the secret keys creation that are associated with the attributes.

Attribute Authorities

Each AA is an independent AA and this is answerable for revoking user's attributes and entitling according to the role or identity based on its domain. In this scheme, each and every attribute is associated with a single AA, but each AA can managea number of attributes. Every AA has a full control on its semantics and structure of the attributes. This is responsible for generating a public key for each attribute it manages and it generates a secret key for each consumer reflecting their attributes.

Data Owners

The data is divided into several parts according to the logic granularities and encrypts that each data part with different by using the encryption technique. Then, the owner defines the view policies on attributes from multiple attribute authorities and the owner encrypts the files with the help keys under the policies.

Data Users

Each user is having a global identity in the system. The data user can be entitled a set of attributes which may come from multiple AA's. The consumer willreceive a secret key associated with its attributes entitled by the corresponding Attribute Authorizes.

Cloud Server

The data owner sends the encrypted data file to the cloud server together with the ciphertexts. It does not rely on the server to do the data views control. Here the views control happens within the cryptography. Only when the user's attributes satisfy the access policy defined in the cipher text; the data user is able to decrypt the ciphertext. Therefore, the data consumers with different attributes can decrypt different no. of keys and obtain different granularities of information from the same data.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

Algorithms worked on:

Timestamp MA-ABE

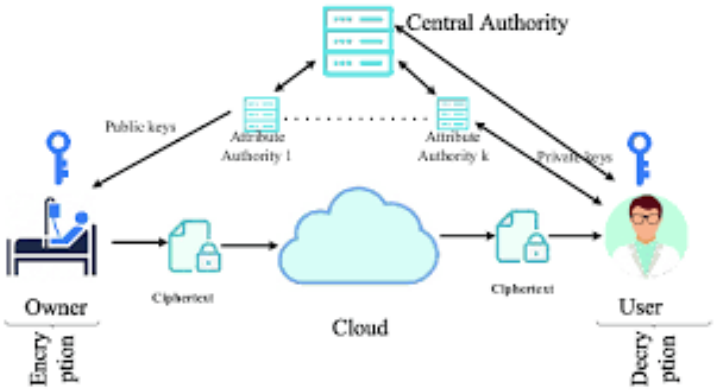
Multi-Authority Attribute Based Encryption
System (setup)
Init: fix y1…..yk
System public key: Y0
Attribute-Authority (Key generation)
Authority Secret key: tk1, tk2…..tkn
Authority Public key: Tk1, Tk2…. Tkn
Secret key for user named as u from authority named as k
Encryption for the attributes set: E= Y0s m, {Ek,i = Tsk,i } Decryption for the attributes set: m=E/Y0s

Elliptic curve cryptography- It's a key based technique for encrypting data. It focuses on pairs of public and private keys for decryption and encryption of web traffic.

- By using this expensive Bilinear Pairing is reduced and it will enhance the immediate revocation of the attributes.
- It allows smaller keys compared to non-elliptic curve cryptography to furnish equivalent security approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields.
- It generates very faster key generation, smaller keys, ciphertexts, moderately fast encryption and decryption, right protocols for authenticated key exchange.

Attribute based encryption (ABE)- It is a public key cryptographic technique that furnishes secure data sharing among multiple users which can achieve both privacy and access control, it is flexible that is extensible one to many encryptions based on ciphertext attributes decryption is possible only if the set of attributes of the consumer key matches to the ciphertext attributes. Only group of consumers satisfying the determined access protocols that can read the ciphertext.

Multi-Authority Attribute Based Encryption (MA-ABE)– multinomial number of independent authorities is present to monitor the attributes and distributes the secret keys and messages are decrypted.



MA-ABE Architecture

V. EXISTING SYSTEM

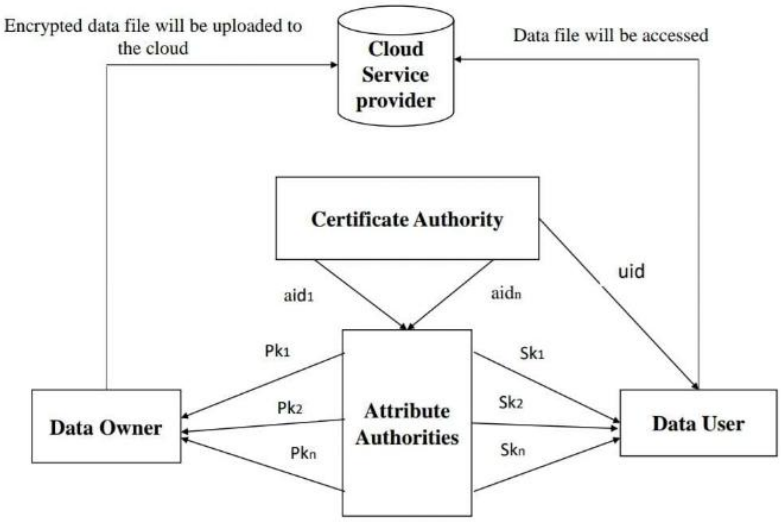
One common way is to resort to the traditional public key encryption technology to encrypt data.
Attribute based encryption (ABE). It used to be considered one of the most promising technologies for pall storehouse, since it ensures the data possessors to enjoy non-interactive and fine- granulated control over translated data. The largely computational outflow, since the being Multi-authority ABE schemes are all grounded on the precious bilinear pairing operations.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

DISADVANTAGES

- It'll induce high calculation cost using precious Bilinear Pairing.
- There's no immediate access cancellation in Multiauthority- ABE.

VI. PROPOSED SYSTEM



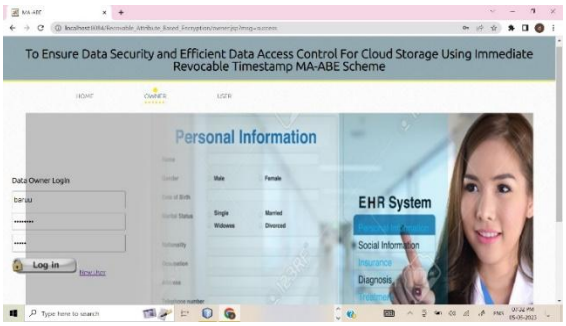
System Architecture

The proposed effective revocable multi-authority Attribute based encryption (Multiple Authority-ABE scheme using elliptic wind cryptography for pall storehouse. The proposed scheme satisfies the indistinguishable or interchangeable under adaptive chosen plaintext attack in which that assuming the hardness of the decisional Diffie- Hellman problem. Compared with the other schemes, the proposed scheme gets its advantages in that it's further provident in calculation and storehouse. Timestamp is enforced for the train attributes.

ADVANTAGES

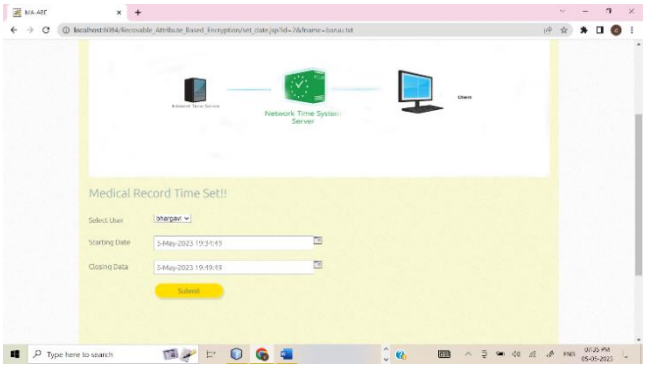
- Effective automatic train access control.
- It reduces communication and computational cost for data proprietor.

VII. TESTING ANALYSIS



Login page

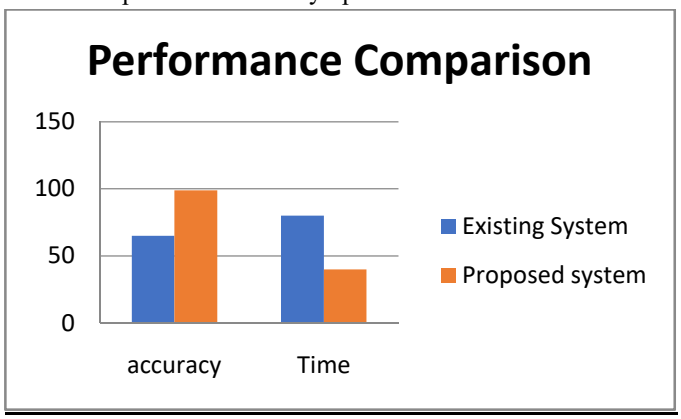
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023



Time seal for the uploaded file

VIII. RESULTS AND DISCUSSION

- ✓ Security evidence demonstrates that the proposed scheme use of the data confidentiality
- ✓ Effective automatic train access control using Diffie Hellman.
- ✓ It reduces communication and computational cost for data proprietor.
- ✓ No reliance on untrusted third parties for security operation.



Test Case#	TC01
Test Name	User input Validation Test
Test Description	To test whether it's accepting all the valid input or not
Input	Name, username, password, email as valid input
Expected Output	It should read and store the values in database
Actual Output	It Read and stored in database
Test Result	Success

Test Case#	TC02
Test Name	User input Validation Test
Test Description	To test whether it's accepting all the valid input or not
Input	Name, username, password, email as empty
Expected Output	It should show alert message
Actual Output	It shown the alert message
Test Result	Success

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

Test Case#	TC03
Test Name	File Upload
Test Description	To test whether its uploading Data in cloud
Input	.txt/.java/.html file
Expected Output	It Should encrypt and connect to cloud and upload to cloud
Actual Output	It stored encrypted data in cloud
Test Result	Success

Test Case#	TC04
Test Name	File Upload
Test Description	To test whether its uploading Data in cloud
Input	No cloud connection
Expected Output	Show the alert cloud not connected
Actual Output	Shown the alert cloud not connected
Test Result	Success

Test Case#	TC05
Test Name	File Access
Test Description	To test whether file access control
Input	File
Expected Output	Allow the user attribute based on file access control
Actual Output	Given file access control based on attributes.
Test Result	Success

IX. CONCLUSION

Security evidence demonstrates that the proposed scheme uses the data confidentiality. Effective automatic train access control using Diffie Hellman. It reduces communication and computational cost for data proprietor. No reliance on untrusted third parties for security operation. This paper proposes an effective Multi-Authority-ABE system for pall storehouse, which is on thebase of the elliptic wind cryptography and Diffie-Hellman problem. The proposed scheme does not need any bilinear pairing operations any further. The interpretation key is introduced into the trait to achieve the traitrevocation.by using the unique identity tied to the secret keys of attributes, conspiracy resistant is realized. It's showed in the performance analysis that the proposed scheme is high- effectiveness in storehouse as well as calculation cost.

REFERENCES

[1] Yang Ming, Baokang HE and Chenhao Wang, "Efficient Revocable Multi-Authority Attributed based Encryption for cloud storage" Chang'an University Mar 2021.
[2] K. Fan, T. Liu, Y. Yang and K. Zhang, H. Li, ''A secure and efficient outsourced computation on data sharing scheme for privacy computing,'' J. Parallel Distrib. Comput., vol. 135, pp. 169–176, Jan. 2020.
[3] K. Sethi, P. Bera and A. Pradhan, ''Practical traceable multi-authority CP-ABE with outsourcing decryption and access policy updation,'' J. Inf. Secur. Appl., vol. 51, Apr. 2020, Art. no. 102435.
[4] Q. Xu, C. Tan, W. Zhu, Y. Xiao, F. Cheng and Z. Fan,''Decentralized attribute-based conjunctive keyword search scheme with online/offline encryption and outsource decryption for cloud computing,'' Future Gener. Comput. Syst., vol. 97, pp. 306–326, Aug. 2019.
[5] S. Ding, H. Liand C. Li, ''A novel efficient pairing-free CP-ABE based on elliptic curve cryptography for IoT,'' IEEE Access, vol. 6, pp. 27336–27345, May 2018.
[6] Z. Liu, Z. L. Jiang, S. M. Yiu and X. Wang, ''Practical attribute-based encryption: Outsourcing decryption, attribute revocation and policy updating,'' J. Newt. Compute. Appl., vol. 108, pp. 112–123, Apr. 2018.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

[7] M. Chase, ‘‘Multi-authority attribute-based encryption,’’ in Proc. Theory Cryptogr. Conf. Berlin, Germany: Springer, Feb. 2007, pp. 515–534.
[8] J. Li, W. Yao, Y. Zhang, J. Han and J. Shen, ‘‘User collision avoidance CP-ABE with efficient attribute revocation for cloud storage,’’ IEEE Syst. J., vol. 12, no. 2, pp. 1767–1777, Jun. 2018.