IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Secure Searchable Encryption Framework for Data Security using Personal Data Storage (PDS) Module

KOTTU SATYA NAGA DIVYA [#1], A.DURGA DEVI [#2]

[#1] MCA Student, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

[#2] Assistant Professor, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

ABSTRACT

Recently, Personal Data Storage (PDS) has gained a substantial change to the way people can store and control their personal data, by moving from a service-centric to a user-centric model. PDS offers individuals the capability to keep their data in a unique logical repository, that can be connected and exploited by proper analytical tools, or shared with third parties under the control of end users.In current day's the cloud based service is mostly adopted by healthcare providers in order to store and access the valuable health information of patients under secure manner.Thus is mainly came into existence due to the reason like lot of end users or E-Health systems try to exchange the PDS data among one another and this may be within distance or sometimes more far distance. Hence we proposed a novel methodology called Secure Personal Data Storage (PDS) for storing the patients health information in a secure manner

1. 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 hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

In the existing cloud servers, there was no concept like encryption of cloud data and also there was no facility like key generation and maintenance of data. The current cloud storage is almost centralized and all the data which is stored along with details of data owners and data users is clearly visible by the cloud server department, which is almost

a big problem in the current cloud service providers. In the existing clouds there is no security for the personal health records which is generated by the hospitals and also there is no security for the reports generated by the PDR.

PURPOSE

As we all know that till now no cloud service provider is providing privacy for the data in terms of encryption and also authorization of data for the valid users. manner. This is mainly came into existence due to the reason like lot of end users or E-Health systems try to exchange the PDS data among one another and this may be within distance or sometimes more far distance. Hence we proposed a novel methodology called Secure Personal Data Storage (PDS) for storing the patients health information in a secure manner.

OBJECTIVE

The main objective of this present application is design a secure application in order to secure the sensitive data under secure manner inside the cloud server using PDS.

2. LITERATURE SURVEY

INRODUCTION

Literature survey is the most important step in software development process. Before developing the tool, it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, then next steps are to determine which operating system and language used for developing the tool. Once the programmers start building the tool, the programmers need lot of external support. This support obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system.

1) A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing

AUTHORS: K. Liang et al

In this paper, for the first time, we define a general notion for proxy re-encryption (PRE), which we call deterministic finite automata-based functional PRE (DFA-based FPRE). Meanwhile, we propose the first and concrete DFA-based FPRE system, which adapts to our new notion. In our scheme, a message is encrypted in a ciphertext associated with an arbitrary length index string, and a decryptor is legitimate if and only if a DFA associated with his/her secret key accepts the string. Furthermore, the above encryption is allowed to be transformed to another ciphertext associated with a new string by a semitrusted proxy to whom a re-encryption key is given. Nevertheless, the proxy cannot gain access to the underlying plaintext. This new primitive can increase the flexibility of users to delegate their decryption rights to others. We also prove it as fully chosen-ciphertext secure in the standard model.

2) Fine-grained twofactor access control for Web-based cloud computing services

AUTHORS: J. K. Liu, M. H. Au, X. Huang, R. Lu, and J. Li

In this paper, we introduce a new fine-grained two-factor authentication (2FA) access control system for web-based cloud computing services. Specifically, in our proposed 2FA access control system, an attribute-based access control mechanism is implemented with the necessity of both a user secret key and a lightweight security device. As a user cannot access the system if they do not hold both, the mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for web-based cloud services. In addition, attribute-based control in the system also enables the cloud server to restrict the access to those users with the same set of attributes while preserving user privacy, i.e., the cloud server only knows that the user fulfills the required predicate, but has no idea on the exact identity of the user. Finally, we also carry out a simulation to demonstrate the practicability of our proposed 2FA system.

3) Ciphertext-policy attributebased encryption

AUTHORS: J. Bethencourt, A. Sahai, and B. Waters

In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous AttributeBased Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe auser's credentials, and a party encrypting data determinesa policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, we provide an implementation of our system and give performance measurements.

4) Arbitrary-state attributebased encryption with dynamic membership

AUTHORS: C.-I. Fan, V. S.-M. Huang, and H.-M. Ruan

Attribute-based encryption (ABE) is an advanced encryption technology where the privacy of receivers is protected by a set of attributes. An encryptor can ensure that only the receivers who match the restrictions on predefined attribute values associated with the ciphertext can decrypt the ciphertext. However, maintaining the correctness of all users' attributes will take huge cost because it is necessary to renew the users' private keys whenever a user joins, leaves the group, or updates the value of any of her/his attributes. Since user joining, leaving, and attribute updating may occur frequently in real situations, membership management will become a quite important issue in an ABE system. In this paper, we will present an ABE scheme which is the first ABE scheme that aims at dynamic membership management with arbitrary states, not binary states only, for every attribute. Our work also keeps high flexibility of the constraints on attributes and makes users be able to dynamically join, leave, and update their attributes. It is unnecessary for those users who do not change their attribute statuses to renew their private keys when some user updates the values of her/his attributes. Finally, we also formally prove the security of the proposed scheme without using random oracles.

5) **HASBE: A hierarchical attributebased solution for flexible and scalable access control in cloud computing.**

AUTHORS: Z. Wan, J. Liu, and R. H. Deng

Cloud computing has emerged as one of the most influential paradigms in the IT industry in recent years. Since this new computing technology requires users to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. Several schemes employing attribute-based encryption (ABE) have been proposed for access control of outsourced data in cloud computing; however, most of them suffer from inflexibility in implementing complex access control policies. In order to realize scalable, flexible, and fine-grained access control of outsourced data in cloud computing, in this paper, we propose hierarchical attribute-set-based encryption (HASBE) by extending ciphertext-policy attribute-set-based encryption (ASBE) with a hierarchical structure of users. The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of ASBE. In addition, HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. We formally prove the security of HASBE based on security of the ciphertext-policy attribute-based encryption (CP-ABE) scheme by Bethencourt and analyze its performance and computational complexity. We implement our scheme and show that it is both efficient and flexible in dealing with access control for outsourced data in cloud computing with comprehensive experiments

3. EXISTING SYSTEM

In the existing cloud servers, there was no concept like encryption of cloud data and also there was no facility like key generation and maintenance of data. The current cloud storage is almost centralized and all the data which is stored along with details of data owners and data users is clearly visible by the cloud server department, which is almost a big problem in the current cloud service providers. In the existing clouds there is no security for the personal health records which is generated by the hospitals and also there is no security for the reports generated by the PDR.

LIMITATION OF EXISTING SYSTEM

The following are the limitation of existing system. They are as follows:

1. In the existing or current clouds the following are the main limitations that are available
2. All the existing schemes are limited upto data storage and retrieval in a plain text manner.
3. All the current cloud servers don't have a facility to store the data in an encrypted manner.
4. The existing cloud servers are almost operated in a centralized manner, where all the access can be viewed and monitored by the cloud service providers.

4. PROPOSED SYSTEM

As we all know that till now no cloud service provider is providing privacy for the data in terms of encryption and also authorization of data for the valid users. manner. Thus is mainly came into existence due to the reason like lot of end users or E-Health systems try to exchange the PDS data among one another and this

may be within distance or sometimes more far distance. Hence we proposed a novel methodology called Secure Personal Data Storage (PDS) for storing the patients health information in a secure manner.

ADVANTAGES OF THE PROPOSED SYSTEM

The following are the advantages of the proposed system. They are as follows:

1. For PDR data storage our application is fully secure
2. Here Authority will try to allow or deny the access of un-authorized users.
3. Here if any un-authorized user try to access the data illegally that will be identified by the cloud server and the cloud will de-activate them.

5. IMPLEMENTATION

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. We have implemented the proposed concept on Java programming language with JEE as the chosen language in order to show the performance this proposed novel IPath protocol. The front end of the application takes JSP,HTML and Java Beans and as a Back-End Data base we took My-SQL Server. They are totally 4 modules present in this project. They are as follows:

1. Data owner Module
2. User and Physician Module
3. Cloud Service Provider (CSP)
4. Public Data Storage (PDS)Module

Now let us discuss about each and every module in detail as follows:

5.1 Data Owner Module

In the first module, we develop the Data Owner Module. Owner Will Signup and Wait for the approval Key of admin. After Getting key Owner can login using the key, and upload any records related to users medical Information on the cloud.In this module, data owner will check the progress status of the file upload by him/her. It has large data needed to be stored and shared in cloud system. In our scheme, the entity is in charge of defining access structure and executing **Encrypt** operation. And it uploads ciphertext to CSP. After the completion, owner logout the session.

5.2 User and Physician Module

In this module, we develop the User Module. User Will registries and login on the user's page. We develop the module, such that, the User will search for his/her medical records by given user medical record id on the page. User will get search results of the medical records related to the id and he/she will request admin to access the document which is encrypted one by the admin. After Getting decrypt key from the admin, he/she can access to the medical records. User logouts the session. It wants to access a large number of data in cloud system. The entity first downloads the corresponding ciphertext. Then it executes **Decrypt** operation of the proposed scheme.

5.3 Cloud Service Provider (CSP)

Here cloud server module is one which can store all the information in an encrypted manner and this will give authorization for the end users. This will try to store all the data in a secure manner and try to store the data in a encrypted manner.This will verify the user identities and then try to download the data.

5.4 Public Data Storage (PDS)Module

Here PDS is one who gives permission for either file upload or download for the data owners and data users.If the PDS give permission then only file can be given access or else the file cannot be decrypted.

6. OUTPUT SCREENS

RESEARCHER LOGIN

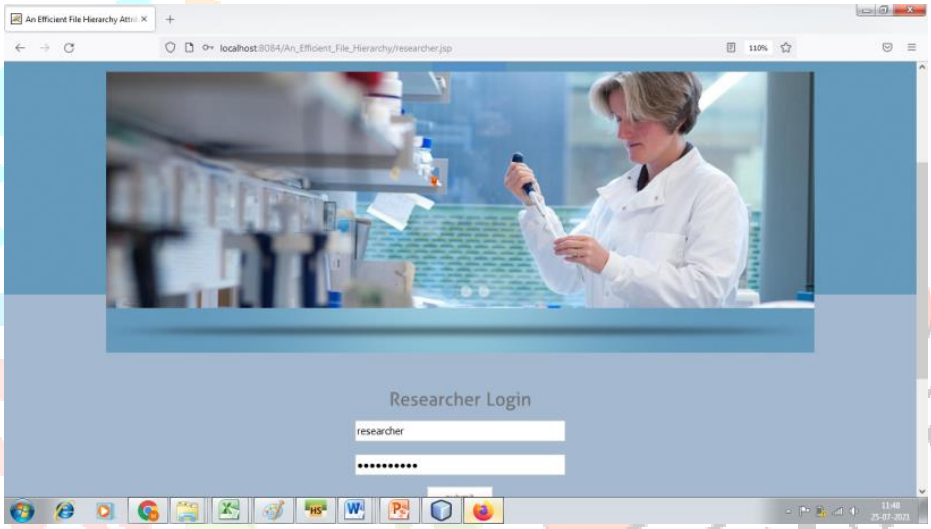


Figure Represents the researcher try to login

OWNER LOGIN PAGE

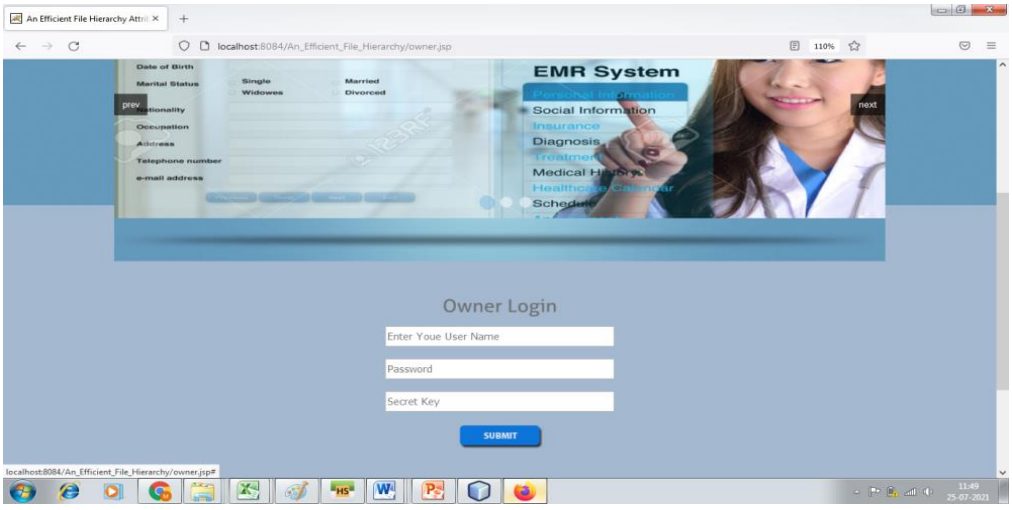


Figure Represents the Owner Home Page

OWNER HOME PAGE

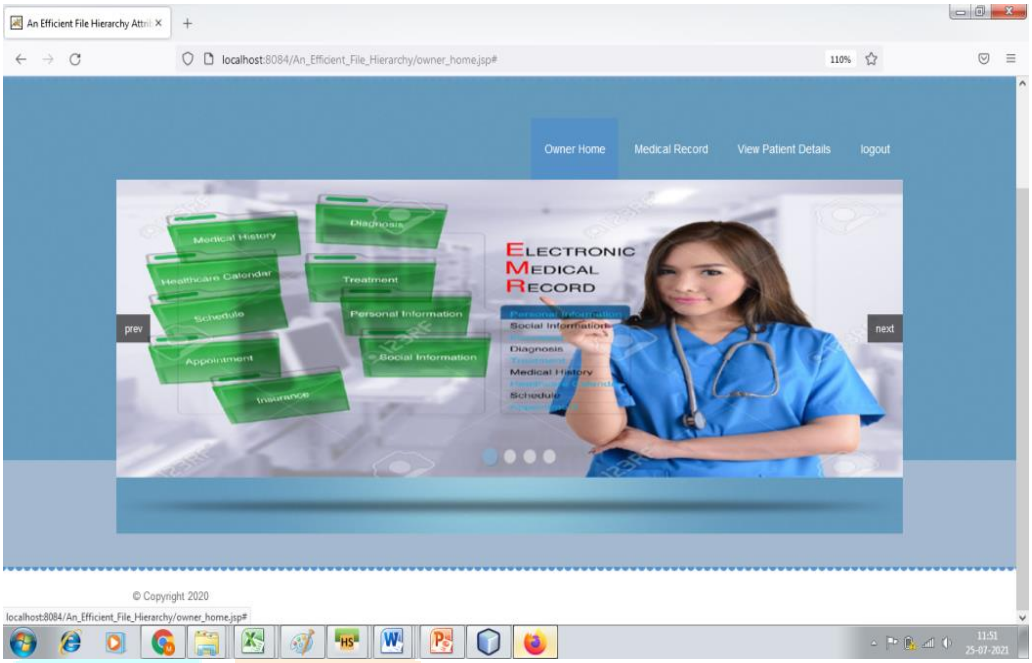
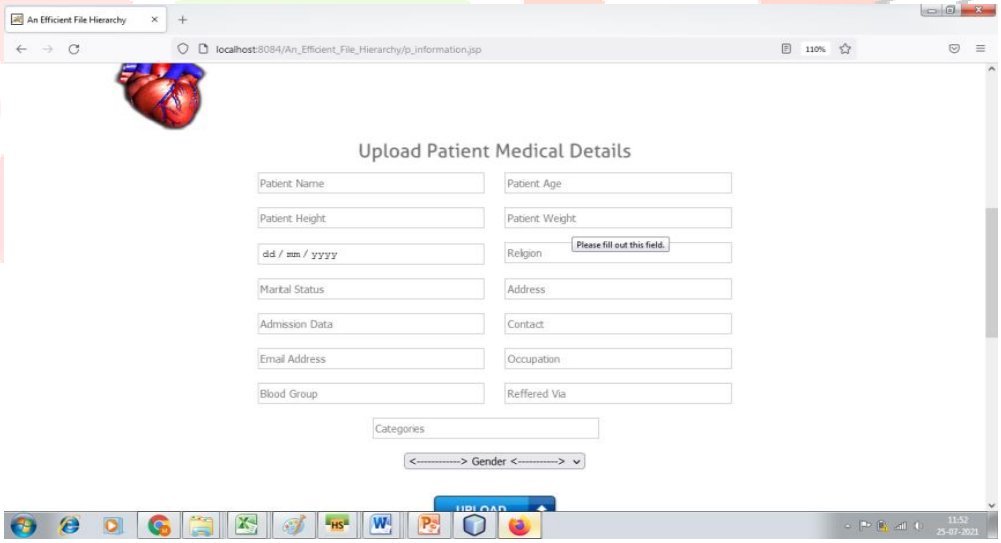


Figure Represents the owner Home Page

OWNER UPLOAD MEDICAL DATA



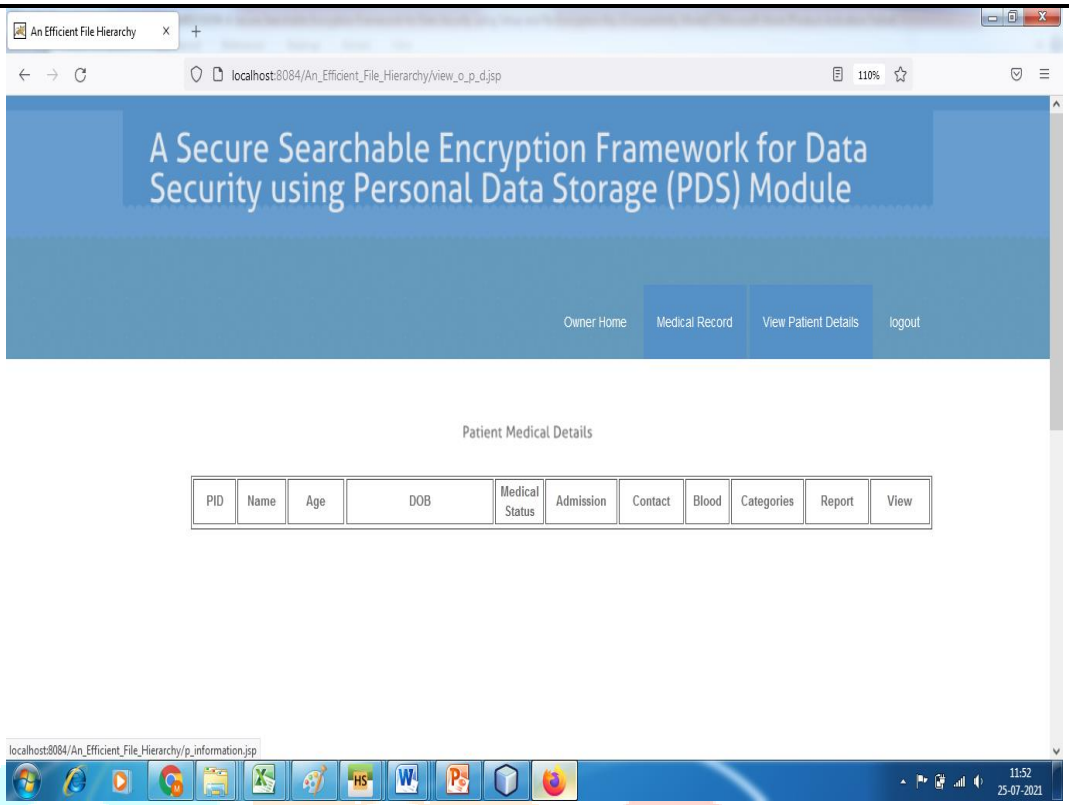


Figure Represents the owner Medical Data

7. CONCLUSION

We for the first time designed a secure application which can able to store a lot of valuable and personal data storage of several patients under a secure manner by using this current application. Hence we proposed a novel methodology called Secure Personal Data Storage (PDS) for storing the patients health information in a secure manner.

8. REFERENCES

[1] C.-K. Chu, W.-T. Zhu, J. Han, J.-K. Liu, J. Xu, and J. Zhou, "Security concerns in popular cloud storage services," *IEEE Pervasive Comput.*, vol. 12, no. 4, pp. 50–57, Oct./Dec. 2013.

[2] T. Jiang, X. Chen, J. Li, D. S. Wong, J. Ma, and J. Liu, "TIMER: Secure and reliable cloud storage against data re-outsourcing," in *Proc. 10th Int. Conf. Inf. Secur. Pract. Exper.*, vol. 8434. May 2014, pp. 346–358.

[3] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloudbased revocable identity-based proxy re-encryption scheme for public clouds data sharing," in *Proc. 19th Eur. Symp. Res. Comput. Secur.*, vol. 8712. Sep. 2014, pp. 257–272.

[4] T. H. Yuen, Y. Zhang, S. M. Yiu, and J. K. Liu, "Identity-based encryption with post-challenge auxiliary inputs for secure cloud applications and sensor networks," in *Proc. 19th Eur. Symp. Res. Comput. Secur.*, vol. 8712. Sep. 2014, pp. 130–147.

[5] K. Liang *et al.*, "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 10, pp. 1667–1680, Oct. 2014.

[6] T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo, and J. Zhou, "*k*-times attribute-based anonymous access control for cloud computing," *IEEE Trans. Comput.*, vol. 64, no. 9, pp. 2595–2608, Sep. 2015.

[7] J. K. Liu, M. H. Au, X. Huang, R. Lu, and J. Li, "Fine-grained two factor access control for Web-based cloud computing services," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 3, pp. 484–497, Mar. 2016.

[8] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology*. Berlin, Germany: Springer, May 2005, pp. 457–473.

[9] 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.*, Oct. 2006, pp. 89–98.

[10] W. Zhu, J. Yu, T. Wang, P. Zhang, and W. Xie, "Efficient attribute-based encryption from R-LWE," *Chin. J. Electron.*, vol. 23, no. 4, pp. 778–782, Oct. 2014.

[11] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in *Proc. IEEE Symp. Secur. Privacy*, May 2007, pp. 321–334.

[12] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proc. 14th ACM Conf. Comput. Commun. Secur.*, Oct. 2007, pp. 456–465.

[13] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," in *Proc. 10th Int. Workshop Inf. Secur. Appl.*, Aug. 2009, pp. 309–323.

[14] X. Xie, H. Ma, J. Li, and X. Chen, "An efficient ciphertext-policy attribute-based access control towards revocation in cloud computing," *J. Universal Comput. Sci.*, vol. 19, no. 16, pp. 2349–2367, Oct. 2013.

[15] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan, "CP-ABE with constant-size keys for lightweight devices," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 5, pp. 763–771, May 2014.