International Research Journal of Computer Science (IRJCS)
Issue 02, Volume 07 (February 2020)
ISSN: 2393-9842
www.irjcs.com

# CIPHERTEXT-POLICY ATTRIBUTE-BASED SIGNCRYPTION WITH VERIFIABLE OUTSOURCED DESIGNCRYPTION FOR SHARING PERSONAL HEALTH RECORDS

**Mohammed Asadulla Sami**
Dept. of Information Science and Engineering, Atria College of Engineering, Bengaluru-24
Asadulla411@gmail.com;
**Srinivas B V,**
Assistant Professor/ISE, Atria College of Engineering, Bengaluru-24

**Manuscript History**
Number: **IRJCS/RS/Vol.07/Issue02/FBCS10080**
Received: 27, January 2020
Final Correction: 06, February 2020
Final Accepted: 09, February 2020
Published: **February 2020**
**Citation:** Asadulla & Srinivas (2020). Ciphertext-Policy Attribute-Based Signcrption with Verifiable outsourced Designcryption for Sharing Personal Health Records.International Research Journal of Computer Science (IRJCS), Volume VII, 10-15. **doi://10.26562/IRJCS.2020.FBCS10080**
**Editor:** Dr.A.Arul L.S, Chief Editor, IRJCS, AM Publications, India


**Abstract** Personal Health Record (PHR) is a patient-centric model of health information exchange, which greatly facilitates the storage, access and share of personal health information. In order to share the valuable resources and reduce the operational cost, the PHR service providers would like to store the PHR applications and health information data in the cloud. The private health information may be exposed to unauthorized organizations or individuals since the patient lost the physical control of their health information. Ciphertext-Policy Attribute-Based Signcryption (CP-ABSC) is a promising solution to design cloud-assisted PHR secure sharing system. It provides fine-grained access control, confidentiality, authenticity and sender privacy of PHR data. However, a large number of pairing and modular exponentiation computations bring heavy computational overhead during designcryption process. In order to reconcile the conflict of high computational overhead and low efficiency in the designcryption process, an outsourcing scheme is proposed in this paper. In our scheme, the heavy computations are outsourced to Ciphertext Transformed Server (CTS), only leaving a small computational overhead for the PHR user.
**Index Terms**—Personal health record system; Attribute based signcryption; Cloud Computing; Outsourcing computation;

## I. INTRODUCTION

With the rapid development of cloud computing, a large number of companies and individuals utilize the public cloud to store and share data. By outsourcing data in the cloud, the users no longer need to maintain the local storage. Instead, users can store the data in a pay-peruse manner and save the cost of hardware and software deployment. Taking Personal Health Record (PHR) system for example, many PHR services are outsourced to the cloud server to enjoy the benefits of cloud computing. The users can access their PHR data from cloud rather than from the PHR service providers. Undoubtedly, the cloud-assisted PHR system attracts a lot of attention from government and industry. On the other hand, the PHR data collected from patients might be polluted if the malicious adversary delivers the false data to the PHR service provider. Therefore, the most crucial question is how to ensure the PHR data is only available to the users who are authorized by the PHR owner. And how to ensure the data collected from patients is authentic without disclosing the identity of the patients.

## II. PROBLEM STATEMENT

- **Existing system**

Taking Personal Health Record (PHR) system for example, many PHR services are outsourced to the cloud server to enjoy the benefits of cloud computing.

The users can access their PHR data from cloud rather than from the PHR service providers. Undoubtedly, the cloud-assisted PHR system attracts a lot of attention from government and industry. However, it brings a series of questions about security and privacy of the sensitive personal health information of the patients.

- **Limitations of existing system**

An unauthorized user may access or modify the PHR data stored in the cloud server. On the other hand, the PHR data collected from patients might be polluted if the malicious adversary delivers the false data to the PHR service provider.

- **Proposed system**

Proposed system contains a new Ciphertext-Policy Attribute- Based Signcryption with Outsourced Designcryption (CPOABSC) scheme in the cloud-based PHR system. As far as we know, this is the first time to equip the secure outsourcing to the ABSC scheme. The design philosophy behind our verifiable outsourcing of designcryptionan is novel. The major computation in the designcryption process is outsourced to the untrusted cloud server. Only constant computation is required to be run on the PHR user side. Moreover, the result returned by the untrusted cloud server can be verified by the associated user. And the extra communication overhead in our scheme is actually tolerable. The high-level description of our protocol is illustrated in Fig. 1.

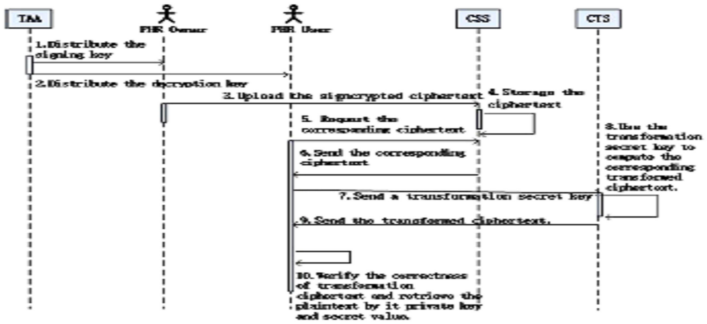


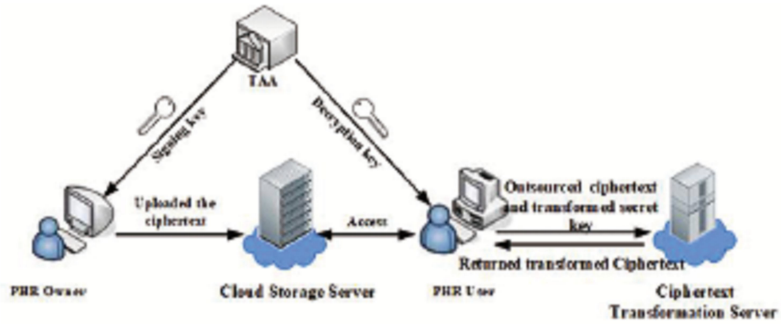

Fig. 1: High-level description of our protocol

**The main contributions are as follows:**

1) Firstly, we formalize the framework of CP-OABSC. After that, the verifiability for the CP-OABSC has also been modeled formally. The design philosophy behind our verifiable outsourcing of designcryption can be viewed as the sophisticated combination of ABE schemes with verifiable outsourcing decryption and server-aided signature verification.

2) In order to reduce the expansion rate of ciphertext, we utilize a mixed signcryption technology, in which an attribute-based encryption method is used to encapsulate the symmetric key and a symmetric encryption algorithm is used to encrypt the PHR data.

3) We also prove the correctness and security of the proposed scheme and its complexity and efficiency are also analyzed. We further compare our scheme with other ABSC schemes in terms of signing key size, decryption key size and ciphertext size, the computational cost of signcryption and designcryption



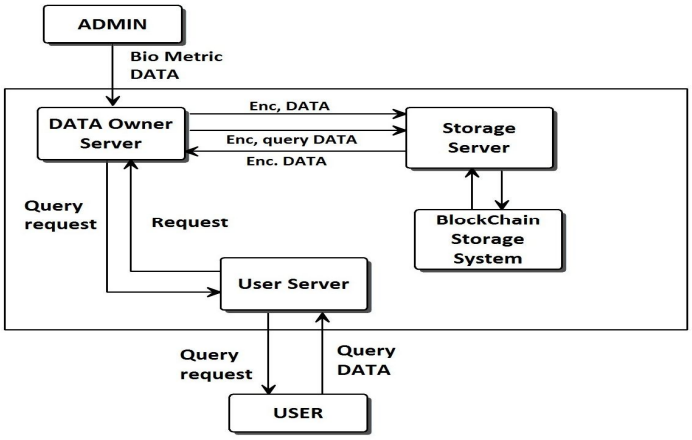

- **Advantages of proposed system**

An authorized user can access or modify the PHR data stored in the cloud server.
It's more secure.

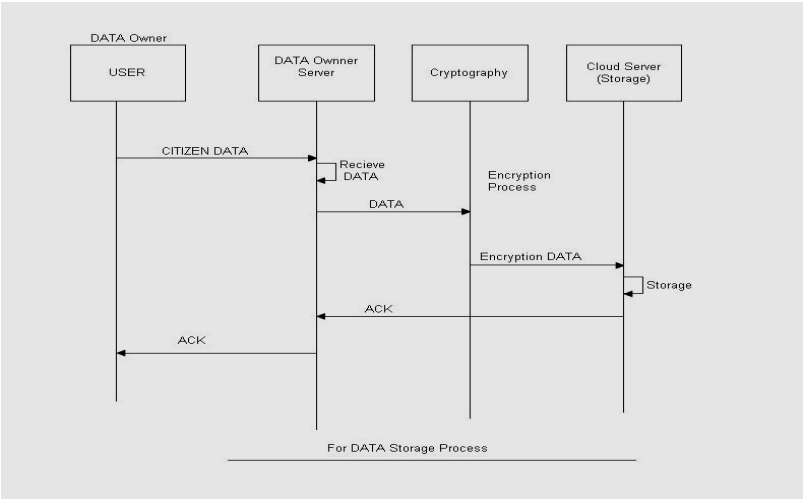
## III. SYSTEM DESIGN

System design can be explained by using any or all of the following methods:

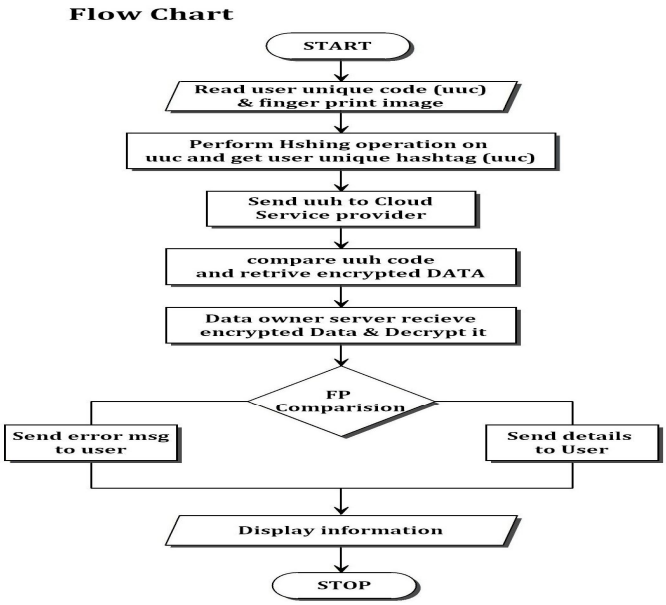
- **System Architecture**




- **Sequence Diagram**




- **Flowcharts**



## IV. REQUIREMENTS

- **Hardware requirements**

System : Pentium IV 2.4 GHz.
Hard Disk : 500 GB.
Ram : 4 GB

- **Software requirements**

Operating system : Windows XP / 7,8
Coding Language : Java (Jdk 1.7)
Web Technology : Servlet, JSP
Web Server : TomCAT 6.0
IDE : Eclipse Indigo
Database : My-SQL 5.0
UGI for DB : SQLyog
JDBC Connection : Type 4 Driver

## V. IMPLEMENTATION

- Implementation plan **(or)** Pseudo code/algorithm

## VI. RESULT/ TESTING ANALYSIS

Include the results of the testing done by any or all of the following methods.

- **Unit testing**

Initialization testing is the first level of dynamic testing and is first the responsibility of developers and then that of the test engineers. Unit testing is performed after the expected test results are met or differences are explainable/acceptable**.**

- **Integration testing**

All module which make application are tested . Integration testing is to make sure that the interaction of two or more components produces results that satisfy functional requirement**.**

- **System testing**

To test the complete system in terms of functionality and non functionality. It is black box testing, performed by the Test Team, and at the start of the system testing the complete system is configured in a controlled environment.

- **Results and analysis using**

| | |
|---|---|
| Name of Test: - | Login as Admin |
| Items being tested: - | Admin model |
| Sample Input: - | Correct Username & Password is given as inputs |
| Expected output: - | Depending on the correct inputs, it must login as Admin |
| Actual output: - | Login successful |
| Remarks: - | Pass. |

## VII. CONCLUSION

To eliminate the computational overhead of the designcryption process at PHR user side, we studied the attributed-based signcryption scheme [8] and presented an efficient and secure CP-ABSC with variable outsourced designcryption scheme. With the help of cloud servers (CSS and CTS), our scheme only needs small modular exponentiation operation to PHR user. Thus, the user saves both bandwidth and local computation time significantly. It greatly improves the efficiency of PHR system. Furthermore, we provided the security proof to show that our scheme is CPA-secure. And the experimental evaluation result demonstrates that the proposed scheme is secure and practicable. Despite our scheme has only achieved CPA security, we argue that most existing ABSC schemes also can only achieve CPA security. So, the CPA security model has been widely accepted in the public key cryptosystem recently. Furthermore, in both of the CPA and CCA2 security model, the adversary can query the decryption key and transformation secret key of any non-targeted user, reflecting that in the real world, the adversary has the ability to collect decryption key and transformation secret key of any non-targeted user. But beyond that, in the CCA2 security model, the adversary can also decrypt any non-target challenge ciphertext. It also reflects that in the real world adversaries can obtain the plaintext information in any non-challenge ciphertext. To achieve the CCA2 security, one more decryption oracle should be available to the CPA adversary during the Phase 1 and Phase 2. Since the decryption oracle is added to the CPA security model, the adversary can query decryption oracle to any non-challenge ciphertext. Then, the adversary may use a challenge ciphertext to replace a non-challenge ciphertext and perform a decryption query on this ciphertext. In this way, the adversary can obtain the target plaintext, and then the adversary can win the security game trivially. In order to prevent the adversary from partially replacing the challenge ciphertext, the plaintext information is obtained by querying decryption oracle. A common method is to sign the generated ciphertext during the encryption process and perform authentication during the decryption process [48]. Our future work consists of designing efficient and provably secure ABSC scheme, which achieves CCA2 security.

## REFERENCES

1. A.Sahai and B.Waters, ``Fuzzy identity-based encryption,'' in Advances in Cryptology_EUROCRYPT, vol. 3494. Berlin, Germany: Springer, 2005, pp. 457_473.
2. V.Goyal, O. Pandey, A. Sahai, and B.Waters, ``Attribute-based encryption for _ne-grained access control of encrypted data,'' in Proc. 13th ACMConf. Comput. Commun. Secur., 2006, pp. 89_98. A. Lewko and B. Waters, ``Unbounded HIBE and attribute-based encryption,'' in Advances in Cryptology_EUROCRYPT, vol. 6632. Berlin, Germany: Springer, 2011, pp. 547_567.
3. J. Bethencourt, A. Sahai, and B. Waters, ``Ciphertext-policy attribute based encryption,'' in Proc. IEEE Symp. Secur. Privacy (SP), May 2007, pp. 321_334.
4. A.Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, ``Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption,'' in Advances in Cryptology_EUROCRYPT, vol. 6110. Berlin, Germany: Springer, 2010, pp. 62_91.
5. H.Maji, M. Prabhakaran, and M. Rosulek, ``Attribute-based signatures: Achieving attribute-privacy and collusion-resistance,'' IACR Cryptol. ePrint Arch., Tech. Rep. 2008/328, 2008, p. 328. [Online]. Available: http://eprint.iacr.org/2008/328
6. M.Gagné, S. Narayan, and R. Safavi-Naini, ``Threshold attribute-based signcryption,'' in Security and Cryptography for Networks, vol. 6280. Berlin, Germany: Springer, 2010, pp. 154_171.
7. Y.S.Rao, ``A secure and ef_cient ciphertext-policy attribute-based signcryption for personal health records sharing in cloud computing,'' Future Gener. Comput. Syst., vol. 67, pp. 133_151, Feb. 2017.
8. J. Lai, R. H. Deng, C. Guan, and J.Weng, ``Attribute-based encryption with veri_able outsourced decryption,'' IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1343_1354, Aug. 2013.
9. B.Qin, R.H.Deng, S. Liu, and S. Ma, ``Attribute-based encryption with ef_cient veri_able outsourced decryption,'' IEEE Trans. Inf. Forensics Security, vol. 10, no. 7, pp. 1384_1393, Jul. 2015.
10. S.Lin,R.Zhang, H. Ma, and M.Wang, ``Revisiting attribute-based encryption with veri_able outsourced decryption,'' IEEE Trans. Inf. Forensics Security, vol. 10, no. 10, pp. 2119_2130, Oct. 2015