International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 6, Issue 1 (June '2020)

CLOUD BASED SECURE SHARING IN DISTRIBUTED MEDICAL RECORDS USING MULTIPLE AUTHORITY BLOCKCHAIN TECHNIQUE

J.Valarmathi,
Assistant professor,
PG & Research Dept. of Computer Science & Applications,
Vivekanandha College of Arts and Sciences for Women(Autonomous)
Elayampalayam, Tiruchengode, Namakkal Dist.

V.T.Kruthika,
Assistant professor,
PG & Research Dept. of Computer Science & Applications,
Vivekanandha College of Arts and Sciences for Women(Autonomous)
Elayampalayam, Tiruchengode, Namakkal Dist.

Abstract: Cloud based data is safer than local database and client-server records. records in the cloud, which will make lots of security related challenges to the PMR privacy and confidentiality. E-health records are sensitive and should be stored in a medical database in encrypted format.. There are lots of security issues related with the storage of sensitive personal health our proposed scheme leverages the RSA function to enable each authority to limit the search capability of different clients based on clients' privileges.. The Cryptographic techniques can be employed to protect the medical data in cloud environment. This method used for security is multiple authority ABE technique which focuses on the multiple data owner and divide the users in the PMR system into multiple secure domains which leads to key distribution complexity for owners and users. In the proposed system DAE(distributed attribute based encryption) scheme Personal Medical Records can be accessed from any hospital using a single key thereby reducing the complexity of key management.

Keywords: Cloud Computing, Key Managament, RSA, Distributed Attribute Based Encryption, Personal Health Record

1. INTRODUCTION

Online medical record systems play an big role in the digital transformation of healthcare, which allows a patient to create, manage, and control her private personal health record (PHR) via the online. To less security the local computation and communication overhead, most emedical records service are outsourced to a third-party such as public cloud. However, such outsourcing may be to a variety of privacy issues because of the risk of data leakage. Therefore, cloud services should provide appropriate strategies to protect emedical records. The most normal method of addressing data privacy is to use algorithm to encrypt data before uploading to the cloud. Once data are encrypted and outsourced, the cloud server can no longer perform keyword search, because the admin is not expected to obtain any information about the records.

After a particular thing, only the authorized client who has the key or security permissions can decrypt the data. Accordingly, in a PHR system, medical data owners are usually required to encrypt their PHRs. As a practical method, data owners also need to provide corresponding access policies to access their PHRs and determine which keywords they can search. However, it isimportant to achieve the aforementioned requirements over encrypted data. Here, to search the records of all patients medical data with the keyword "inda", all the records must be downloaded from the cloud and then decrypted to search the records. This technic introduces huge computation and communication costs.

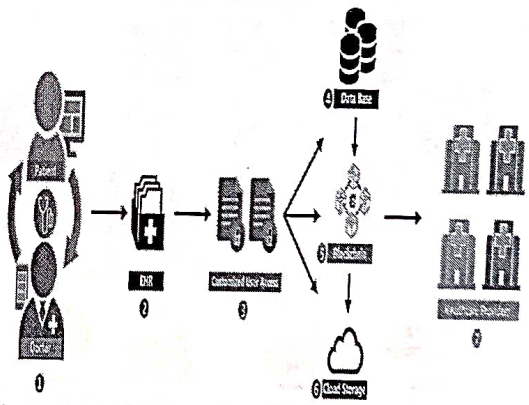

Figure 1.Healthcare data management Architecture in blockchain

However, existing searchable encryption schemes consider the single authority method, this is not possible meet the requirement of PHR systems in which more than one authority exist and the data records and queries are encrypted via different keys. To provide our design, we consider the following reason in a smart PHR system. Therefore, the search cabacity of the clients must be managed so that they are only allowed to perform queries for authorized persons. To assume that there are various doctors in different hospitals and they can write information to PHRs.

Due to the real nature of the data, the access right will be restricted to certain clients only. For example, a doctor could be authorized to read the records of their treated patients only, whereas a cardiologist could be authorized to read all records relating to heart conditions.

In addition, patients may be go to more than one or two hospital, and doctors may want to read patient's health records for diagnosis in another hospital. Therefore, the clients should be forced with read and search data under a scenario of multiple authorities. Furthermore, due to the privacy of medical health data, the access control of the health data should be refined to authorized keywords for searching. For example, cardiologists are only authorized to query medical health information about heart disease and cannot search a patient's history of skin diseases.

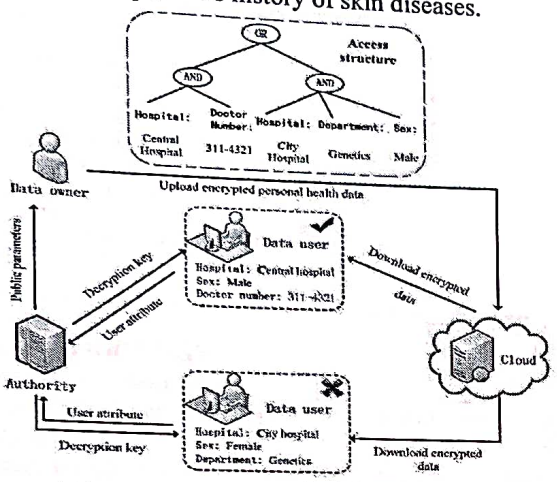

Figure 2: Distributed M-Healthcare

The needs mentioned above motivate us to focus on addressing the medical health data authorization management issue and propose a practical and privacy based encrypted data search solution for multiauthority medical databases. To ensure that the patient only performs the valid queries on authorized keywords, we adopt the RSA function to give the search capability for a set of authorized keywords, and then assign these capabilities to different patients.

The patient can use the obtained capability to compute the search words of the authorized keywords by herself, while the RSA algoritham achieves a non-interactive setting, meaning that the authority only needs to calculate and send the search capability once for all authorized persons. To realize search capability control in multi-authority method, a new scheme must be designed so that search capabilities can be assigned to patients(clients) from multiple authorities. One simple solution is to adopt an attribute based encryption (ABE) scheme to encrypt search sensitive information under a set of policies, and only the patients who satisfy these However, under method single authority ABE, different copies of the encrypted search capability must be generated for different users under different authorities, which will introduce more computation and communication overhead and complicate the authorization process.

To address this challenge, we deploy a multi-authority attribute-based encryption primitive to our system.the search capability once for all authorized users and generates only one copy of the search capability under a set of policies from different authorities. When the clients satisfy these policies, they can decrypt the valid search token.

2. LITRATURE SURVEY

The exchange of Personal Health Records (PHR) in cloud computing is a promising platform of medical health information exchange. The correctness, security and efficiency of this scheme are also true. In order to address this security loophole, we suggest a promising results. Uur propose new method for fine-grained access control and sign-thenencrypt data. We call our new primitive Ciphertext-Policy Attribute-Based Signcryption (CP-ABSC) which satisfies the requirements of cloud computing technic for PHR. CP-ABSC combines the merits of digital signature and encryption to provide confident, authenticity, unforgeability, anonymity and collusion resistance.

3. PROBLEM STATEMENT

This work to considers a secure encrypted medical data search system architecture that involves multiple authorities for smart emedical systems. As depicted in Figure. 1, a medical treatment may involve multiple authorities. For example, a nurse is responsible for filling in your medical health records, the staff of the insurance company helps patients insurence medical claims, and bankers paying for the current treatment received at the hospital. All these authorities need access to the patient's health data in the hospital such as medical records and invoices. Figure. 1 provides a brief explanation of the proposed encrypted medical health database system and functions used by each party.

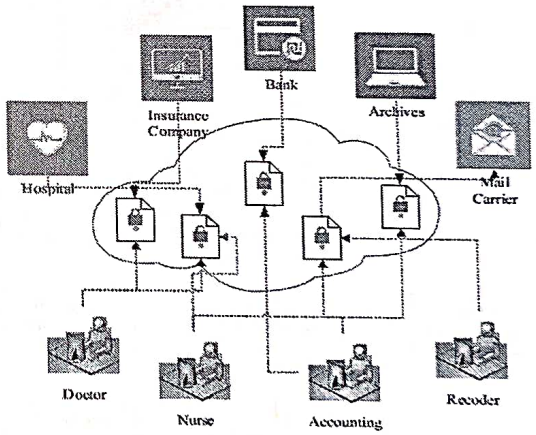

Figure 3. The system architecture overview

3.1 EXISTING MODEL

The basic encrypting these medical records will eliminate data utility and interoperability of the existing medical database system because encrypted medical records are no longer searchable.

3.1.1 Drawbacks

- Searchable encryption scheme consider the single authority.
- Existing searchable scheme not able to achieve forward privacy.

3.2 PROPOSED SYSTEM

we present the first multi-uthority/multiclient dynamic searchable encryption system.

- Multi-Authority.
- Multi-Client.

- Non-interactive.
- Forward Privacy.

3.2.1 Advantages Of Proposed System

- protect the privacy of authority databases.
- reduce the risk of attack from more powerful adversaries.
- adaptive attacks from malicious clients.

3.2.3 Proposed Algorithm

- **Matching Hash to Prime and RSA Functions**

Algorithm 1 Hash Keyword to Prime [35]

Input: keyword $x \in W$, functions $h : W \rightarrow \{0,1\}^k \in \mathcal{H}, F_k : \{0,1\}^* \rightarrow \{0,1\}^k \in \mathcal{F}$
Output: prime integer $w \in P_{2k}$

```
foundprime ← False
r ← 0
while foundprime = False do
    w ← 2 · Int(h(x)) + Int(F_k(Bin(r)))
    if w is prime then
        foundprime ← True
    end if
    r ← r + 1 mod 2k
end while
return w
```

4. METHODOLOGY

Our Contribution

In this paper, our proposed system to implement the first multi-authority/multiclient dynamic searchable encryption system, which can implement fine-grained access control on encrypted PHRs stored via outsourced storage services. The proposed system can be listed below:

Multi-Authority

Our system supports encrypted medical data search under scenarios in which all health data records are encrypted by multiple authorities. By deploying an improved multi-authority attribute-based encryption scheme, all authorities can distribute their search capability to patients under different authorities withoutadditional negotiations.

Multi-Client

Due to the use of ABE algorithm, this work satisfies multi-client requirement as well as. Because all search keywords are encrypted under an access policy before being sent to the patients(Clients), only the allowed clients with corresponding attributes can obtain a valid search keyword tokens. In fact, the user side is controlled by providing different search for authorized keywords.

Non-interactive

Our system also provides an efficient approach to enable noninteractive authorized search. Once the authority determines the set of authorized keywords for the client, it only performs a one-time calculation to generate the partial search token for the client. Moreover, the size of the partial search keyword in our scheme is constant, regardless of the number of authorized tokens.

Forward Privacy

Because of the dynamic setting, our design also supports forward privacy such that an adversary or server will not know the relationship between the updated keywords and documents. This feature thwarts the file injection attacks which may emerge in the update process and compromise the confidentiality of the records and queries.

Encrypted Data Search

The first searchable encryption scheme was proposed by Chor et al. [4] in 1995, and it was based on symmetric encryption in a single writer/single reader (S/S) model. In their work, a retrieval scheme is described that enables the client to access and retrieve documents stored in the third party without leaking any of the information, which provided us an encrypted data search technique. After Chor's work, searchable symmetric encryption was deeply studied, with most research focused on improving search performance, search pattern and security. However, with the data sharing cycle taking its toll on sensitive encrypted data and the inability of S/S model searchable encryption to meet the continuously increasing demands, a multi-client searchable encryption system is proposed to realize encrypted search among a number of clients. For example, Sun et al.constructed a noninteractive searchable encryption system based on Cash's work for multiple clients.

Grained Access Control

Attribute-based encryption(ABE) protocol provides finegrained access control for encrypted data based on client's attributes. Such protocol allows the client whose attributes satisfy the access policy to decrypt the encrypted messages that are encrypted under certain policies.

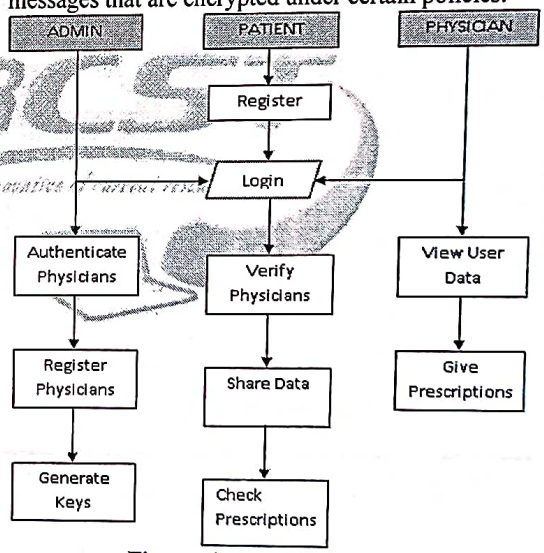

Figure 4. System Flow Diagram

The first attributebased encryption scheme is proposed by Sahai and Waters, and the prototype of attribute-based encryption is derived from a fuzzy identity-based encryption. Classical attributebased encryption system can be divided into two categories:Ciphertext-policy (CP) ABE and Key-policy (KP) ABE. The CP-ABE was first proposed by Bethencourt et al., who use system attributes to describe the client's credentials; moreover, private keys are computed with respect to a set of attributes and the access policy determines which clients have the ability to decrypt the encrypted data. In KP-ABE, the role of access policy and attributes are converted, and the access policy is used to design the client's private key and ciphertext is generated

with respect to a set of attributes. The first KP-ABE is suggested by Goyal et al..

5. RESULTS

Here show some sample outputs for medical records to distributed multiple patients usings blockchain technologies.

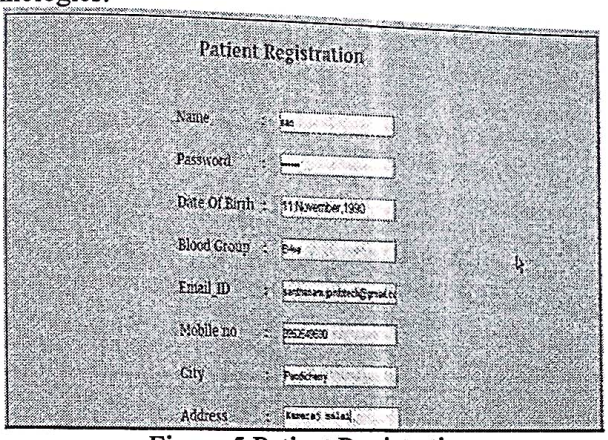

Figure 5 Patient Registration

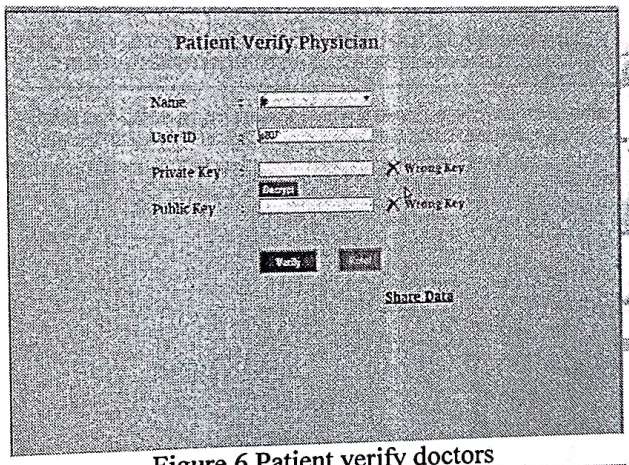

Figure 6 Patient verify doctors

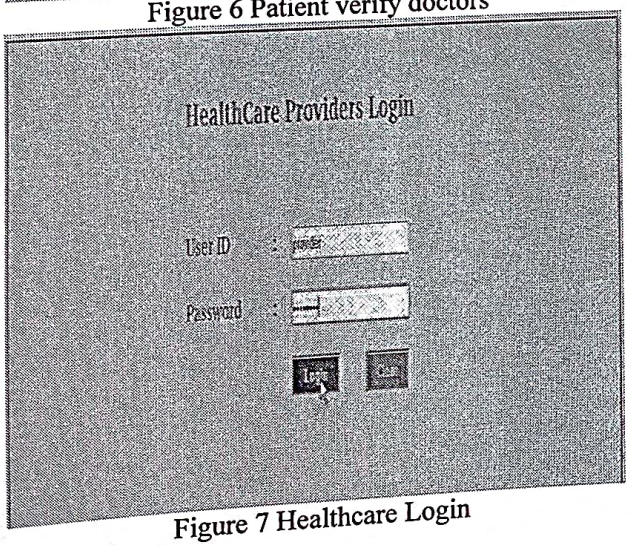

Figure 7 Healthcare Login

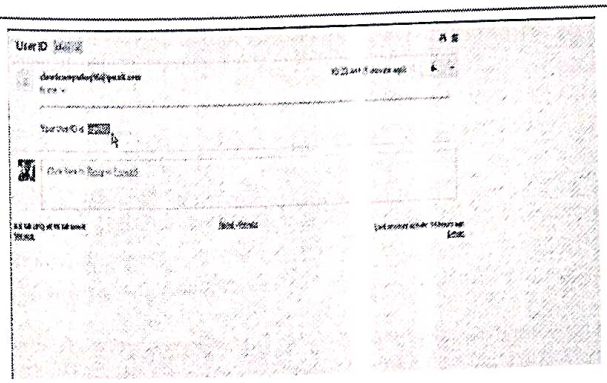

Figure 8 User verify from Healthcare provider

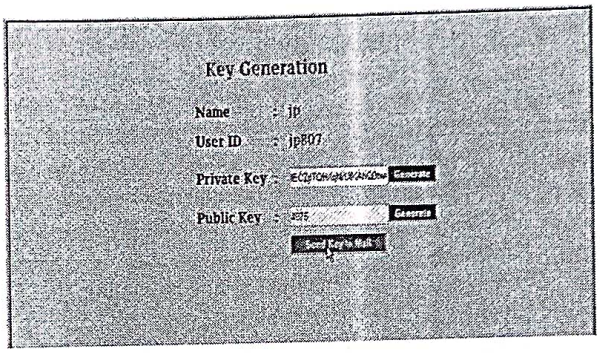

Figure 9 Key Generation

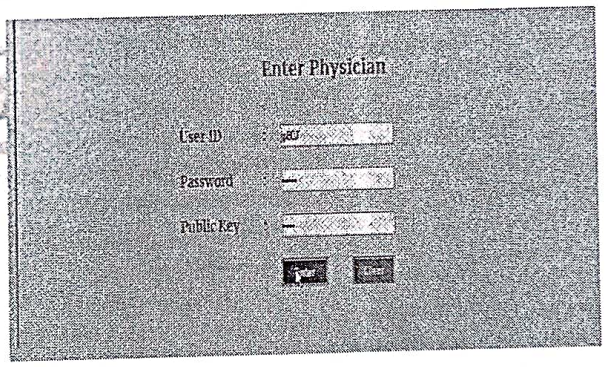

Figure 10 Physician Login

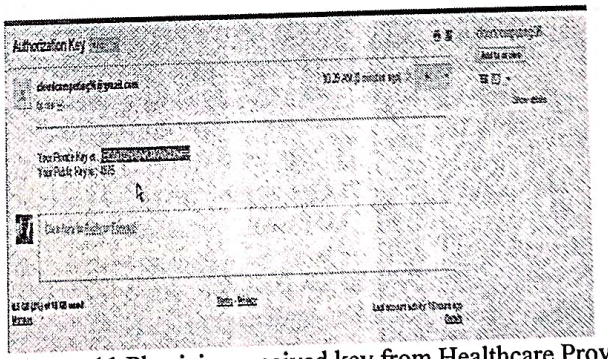

Figure 11 Physician received key from Healthcare Provider

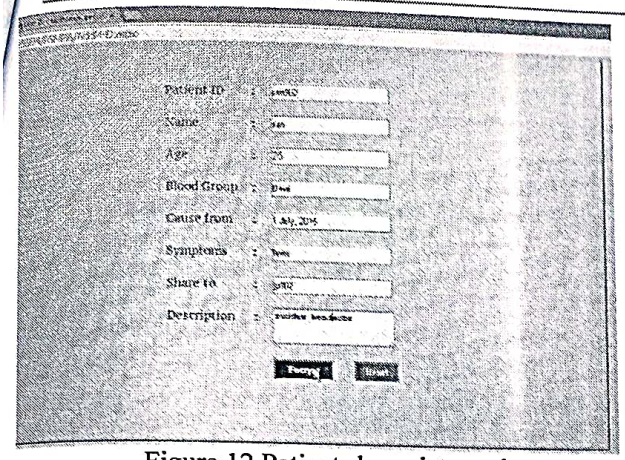

Figure 12 Patient share data to doctor

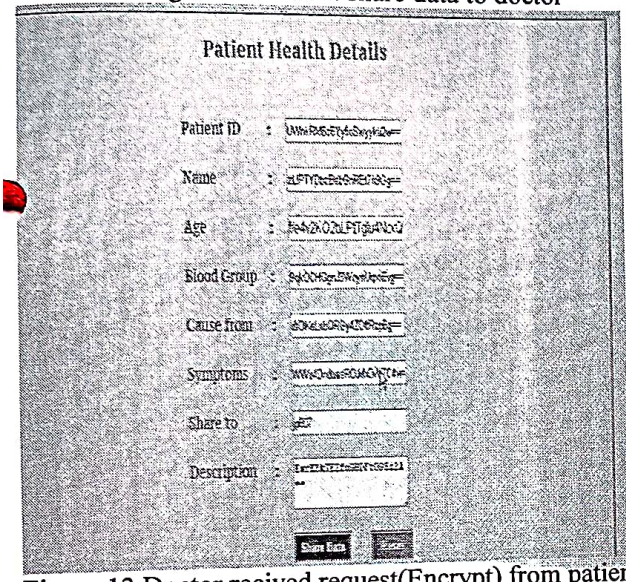

Figure 13 Doctor recived request(Encrypt) from patient

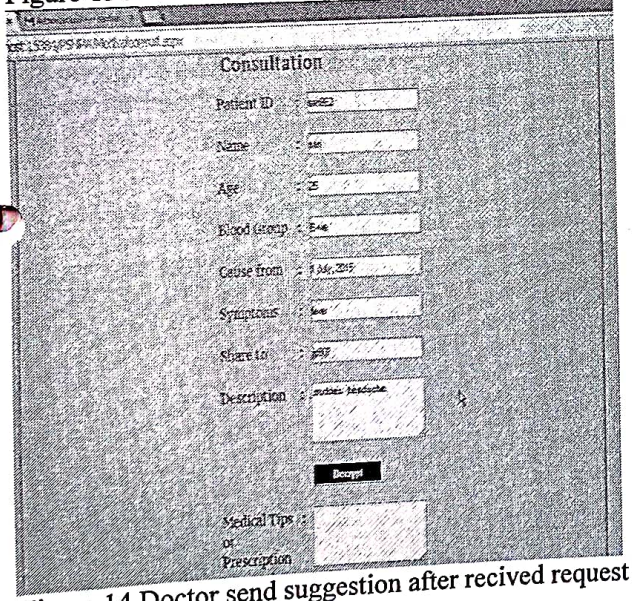

Figure 14 Doctor send suggestion after recived request from patients

6. CONCLUSION

In this paper, we present a practical and efficient authorized encrypted search scheme for multi-authority medical databases, and it also supports forward security. Our construction is L-adaptive-secure with the designed leakage functions, which are also non-interactive. The proposed system shows how to build a fine-grained encrypted database search system for multiple authorities. In addition, we also present an analysis of our framework properties. There are some interesting open problems that deserve further investigation, such as, designing more practical Boolean query searchable encryption with forward security, exploiting the method of simplifying access control for data owners or clients etc.

7. REFERENCE

[1]. J. Liu, X. Huang, and J. K. Liu, "Secure sharing of personal health records in cloud computing: Ciphertext-policy attributebased signcryption," Future Generation Comput. Syst., vol. 52, pp. 67–76, 2015.

[2]. M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, 2013.

[3]. Y. Zhang, J. Katz, and C. Papamanthou, "All your queries are belong to us: The power of file-injection attacks on searchable encryption," in Proc. of 25th USENIX Secur. Symp., 2016, pp. 707– 720.

[4]. B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval," in Proc. of 36th Annu. Symp. on Foundations of Comput. Sci., 1995, pp. 41–50.

[5]. X. Yuan, X. Wang, C. Wang, C. Qian, and J. Lin, "Building an encrypted, distributed, and searchable key-value store," in Proc. Of the 11th ACM on Asia Conf. on Comput. and Commun. Security, 2016, pp. 547–558.

[6]. S. Lai, S. Patranabis, A. Sakzad, J. K. Liu, D. Mukhopadhyay, R. Steinfeld, S.-F. Sun, D. Liu, and C. Zuo, "Result pattern hiding searchable encryption for conjunctive queries," in Proc. of the 2018 Conf. on Comput. and Commun. Secur. ACM, 2018, pp. 745–762.

[7]. S.-F. Sun, X. Yuan, J. K. Liu, R. Steinfeld, A. Sakzad, V. Vo, and S. Nepal, "Practical backward-secure searchable encryption from symmetric puncturable encryption," in Proc. of the 2018 Conf. on Comput. and Commun. Secur. ACM, 2018, pp. 763–780.

[8]. L. Xu, X. Yuan, C. Wang, Q. Wang, and C. Xu, "Hardening database padding for searchable encryption," in Proc. of the 2019 Conf. on Int. Conf. on Comput. Commun. IEEE, 2018.

[9]. S. K. Kermanshahi, J. K. Liu, and R. Steinfeld, "Multi-user cloudbased secure keyword search," in Proc. of 22nd Aus. Conf. on Inf. Secur. and Privacy, 2017, pp. 227–247.

[10]. X. Yang, T. Lee, J. K. Liu, and X. Huang, "Trust enhancement over range search for encrypted data," in Proc. of 2016 IEEE Trustcom/BigDataSE/ISPA, 2016, pp. 66–73.