**INTRODUCTION**

C LOUD computing has been the remedy to the problem of personal data management and maintenance due to the growth of personal electronic devices. It is because users can outsource their data to the cloud with ease and low cost. The emergence of cloud computing has also influenced and dominated Information Technology industries. It is unavoidable that cloud computing also suffers from security and privacy challenges.

Encryption is the basic method for enabling data confidentiality and attribute-based encryption is a prominent representative due to its expressiveness in user’s identity and data [1]– [4]. After the attribute-based encrypted data is uploaded in the cloud, authorized users face two basic operations: data searching and data sharing. Unfortunately, traditional attribute- based encryption just ensures the confidentiality of data. Hence, it does not support searching and sharing. Suppose in a Person Health Record (PHR) system [5]–[7], a group of patients store their encrypted personal health reports Enc(D1; P1;KW1); \_ \_ \_ ;Enc(Dn; Pn;KWn) in the cloud, where Enc(Di; Pi;KWi) is an attribute-based encryption of the health report Di under an access policy Pi and a keyword KWi. Doctors satisfying the policy Pi can recover the record Di. However, they could not retrieve the specific record by simply typing the keyword. Instead, a doctor Alice needs to first download and decrypt the encrypted records. After decryption, she can use the keyword to search the specific one from a bunch of the decrypted health records. Another inconvenient scenario is that Alice attempts to share a record with her colleague, in the case like she needs to consult the report with a specialist. In this situation, she must download the encrypted files, then decrypt them. Then, after she has acquired the underlying record, she encrypts the record using the policy of the specialist. As a result, this system is very inefficient in terms of searching and sharing.

Additionally, the traditional attribute-based encryption (ABE) technology used in the current PHR systems might cause another issue for keyword maintenance because the ABE algorithm could not scale well for keyword updates once the number of the records significantly increases. For example, after reviewing a health report with the patient self marked “contagious” tag, Alice from hospital A confirmed it is not the contagious condition and corrected the tag to “non- contagious”. In order for Alice to share a health report that is encrypted with a tag “contagious” with another doctor from hospital B, she need to change the tag as “non-contagious” without decrypting the report. As the traditional attribute-based

encryption with keyword search can not support keyword updating, Alice has to generate a new tag for all shared ciphertexts so as to keep the privacy of the keyword. From above scenarios, the traditional attribute-based encryp- tion is not flexible for data searching and sharing. Additionally, attribute-based encryption is not well scaled when there is an update request to the keyword. In order to search and share a specific record, Alice downloads and decrypts the ciphertexts. However, this process is impractical to Alice especially when there is a tremendous number of ciphertexts. The worse situation is the data owner Alice should stay online all the time because Alice needs to provide her private key for the data decryption. Thus, ABE solution does not take the advantages of cloud computing.

An alternative method is to delegate a third party to do the search, re-encrypt and keyword update work instead of Alice. Alice can store her private key in the third party’s storage, and thus the third party can do the heavy job on behalf of Alice. In such an approach, however, we need to fully trust the third party since it can access to Alice’s private key. If the third party is compromised, all the user data including sensitive privacy will be leaked as well. It would be a severe disaster to the users.