**INTRODUCTION**

Nowadays, with the rapid development of artificial intelligence and the advancement of wearable devices and sensors, e-healthcare sensor network has reached a stage of maturity for adoption and deployment at a commercial scale. E-

healthcare sensor network serving as a mobile platform profoundly benefit patients to obtain medical treatment of high quality and efficiency. As shown in Fig.1, patients' devices collect a large amount of personal healthcare records through sensor devices, which enable doctors to more effectively diagnose and attend to the need of the patients through utilizing these data. Such information also enables medical researchers and analysts to perform analytics to gain better insights on illnesses and devise better treatments. Nevertheless, these data may be stored on cloud storage provided by third-party service providers [10], [16], [34], which introduce potential security issues such as data leakage. This is because neither the patients nor the doctors have control of the information once the data is outsourced. This means the privacy and confidentiality of these outsourced data should be protected in such an environment. For instance, some medical institutions collect and store a large amount of PHRs on cloud servers and authorize the usage of these data to the Center for Disease Control and Prevention (CDC). To facilitate disease prevention and control, doctors in CDC are allowed to study these data with data mining technology. However, in the process of collecting case information from medical institutions and the implementation of traditional data mining technology, the CDC may inevitably expose sensitive data of patients. How to store manage and retrieve the PHRs securely and efficiently is a great challenge.

E-healthcare system requires stronger security and privacy guarantees for practices in terms of both data and access to data. In order to prevent information leakage from the stored PHRs, all PHRs stored on the cloud should be encrypted [11], [14], [15], [26], [27], [42]\_[44]. Although encryption ensures data confidentiality and can be used to address concerns of data privacy and avoids the attacks from malicious users and cloud servers, it also brings inconvenience of usage. For instance, conventional encryption techniques render it dif\_- cult to query these encrypted data [28] because of the useless information retrieval methods based on plaintext. Due to this limitation of conventional, most of the researches employs searchable encryption (SE) cryptosystem to alleviate such concerns. With searchable encryption technology, patients in the e-healthcare system first encrypt the potential keyword as an index and then upload it to the cloud server along with the encrypted PHRs. Then, the authorized doctor or research institution is able to operate encrypted keyword search by sending a trapdoor generated with a certain keyword to the cloud server. With the trapdoor, the cloud server can operate keyword search over the encrypted index and retrieve the corresponding records. Overall, a searchable encryption cryptosystem allows the cloud server to search encrypted data on behalf of users without learning about keywords or plaintext.

With searchable encryption technology, doctors in CDC are able to perform information retrieval over encrypted PHRs and carry out medical treatment. Nevertheless, such a system also implies the doctors need to be available all the time. If the doctor is offline, then medical treatment would not be possible. Proxy re-encryption (PRE) [4], [5], [36] was proposed to solve the above problem by allowing a trusted proxy to securely transform cipher text belonging to one doctor to another so that a doctor can delegate the medical treatment right to the other doctor in his absent. For instance, suppose there are two doctors Alice and Bob. Each patient with Alice's public key can encrypt the healthcare records to Alice. Suppose Alice is on vacation and wishes to delegate the decryption right to Bob. With PRE technology, Alice generates a encryption key based on his private key and Bob's public key, so that with the re-encryption key, the proxy can re-encrypt a cipher text encrypted under Alice's public key into a cipher text of the same message under Bob's public key. However, there are two problems with the existing PRE approach. First, the proxy is too powerful: With the re- encryption key, the proxy can transform all cipher texts of Alice no matter which keyword the cipher text has. Second, inherent from the bidirectional property, it is impossible to provide collusion-resistance when the dishonest proxy colludes with the delegate to export the delegator's private key, which constitutes a serious security issue to the system since now the delegate can impersonate as the delegator. Therefore, it is necessary to restrict the power of proxy server.

A conditional proxy re-encryption searchable (CPRE) [21], [49] system can be deployed to overcome the above issue. In the CPRE system, the delegator generates the re-encryption key with a condition that aims to specify the cipher text that satisfies the condition. Unfortunately, most existing CPRE schemes cannot guarantee the privacy of the condition, which also contains some sensitive information. On the other hand, if a malicious user can distinguish a re-encrypted cipher text from an original cipher text, it will increase the security risk such as that the malicious user knows Alice is not available right now. Thus, it is required for conditional proxy re-encryption to be proxy-invisible, where a malicious user cannot distinguish between the original cipher text and the re-encrypted cipher text.

In summary, existing solutions apply many methods (e.g., searchable encryption, proxy re-encryption, conditional proxy re-encryption) sharing PHRs with doctors or medical research institutions to protect data privacy. However, information retrieve over the encrypted PHRs is still a challenging issue, especially when dealing with massive data at a \_ne- grained level.