# CONCLUSION

In this paper, we presented a proxy-invisible condition-hiding proxy re-encryption scheme which supports keyword search that can be applied to securing data sharing and delegation in e-healthcare systems. With our new system, a doctor, Alice (delegator), may construct a conditional authorization for a doctor, Bob (delegate), by specifying a re-encryption key. With the re-encryption key, the cloud server can per- form cipher text transformation so that Bob is able to access the PHRs original encrypted under Alice's public key, thus enabling secure delegation. The cloud server can operate search over encrypted PHRs on behalf of the doctor with-out learning information about the keyword or the under- lying condition. Specifically, we achieved the property of proxy-invisible in the system. We have also obtained the property of collusion-resistance in the system, where a delegator's (Alice) private key is still secure even a dishonest cloud server colludes with the delegate (Bob). We have demonstrated security through a rigorous proof, and the performance analysis confirms that our proposed scheme DSAS is efficient and practical.