CAM: Cloud-Assisted Privacy Preserving Mobile

Health Monitoring

**CONCLUSION**

In this paper, we design a cloud-assisted privacy preserving mobile health monitoring system, called CAM, which can effectively protect the privacy of clients and the intellectual property of mHealth service providers.To protect the clients’ privacy, we apply the anonymous Boneh–Franklin identity-based encryption (IBE) in medical diagnostic branching programs. To reduce the decryption complexity due to the use of IBE, we apply recently proposed decryption outsourcing with privacy protection to shift clients’pairingcomputation to the cloud server.To protect mHeath service providers’ programs, we expand the branching program tree by using the random permutation and randomize the decision thresholds used at the decision branching nodes. Finally, to enable resource-constrained small companies to participate in mHealth business, our CAM design helps them to shift the computational burden to the cloud by applying newly developed key private proxy reencryption technique. Our CAM has been shown to achieve the design objective.