# IBEET-AOK: id-based encryption with equality test against off-line KGAs for cloud medical services

**Yan XU, Ming WANG,**
**Hong ZHONG, Sheng ZHONG**

Frontiers of Computer Science, DOI: 10.1007/s11704-020-9396-2

# Problem & Idea

- Problem:
  - When the equality test is performed on ciphertext, the attacker can perform offline keywords guessing attack (KGA) to obtain private information.
- Idea:
  - This paper uses an aided-server to transform the keywords. The equality test on the keywords after transformation will not reveal the privacy information of users. The system model of IBEET-AOK in the cloud medical services is shown in Fig. 1.

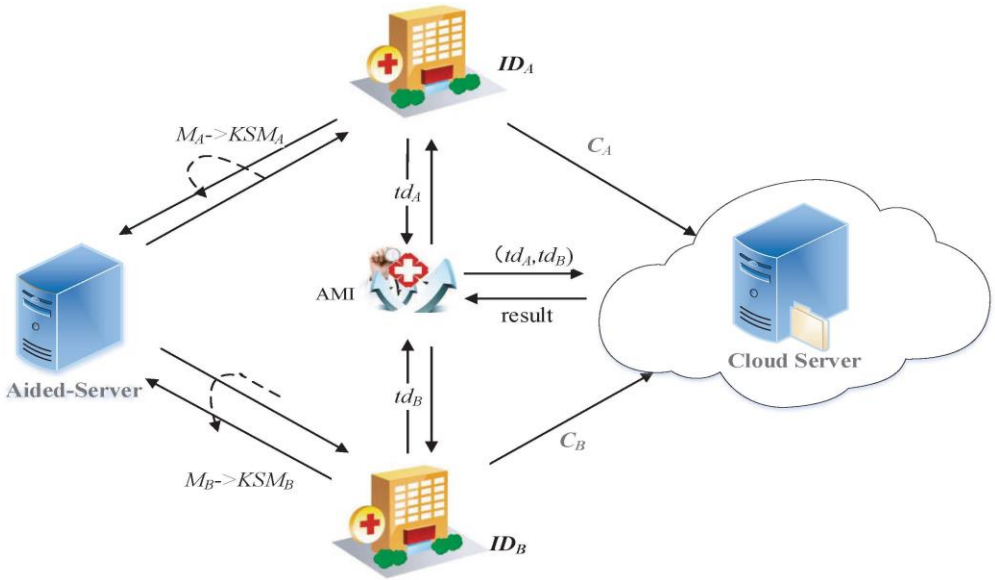


Fig. 1: System model of IBEET-AOK in the cloud medical services

# Main Contributions

- An ID-based encryption with equality test against off-line KGAs (IBEET-AOK) for cloud medical services is present, where insider attackers cannot use off-line KGAs to access patients' privacy.
- In IBEET-AOK, only the authorized specified cloud server can execute equality testing, and the nonauthorized server cannot test even if the trapdoor is obtained.
- The simulation results are shown in Fig. 2.

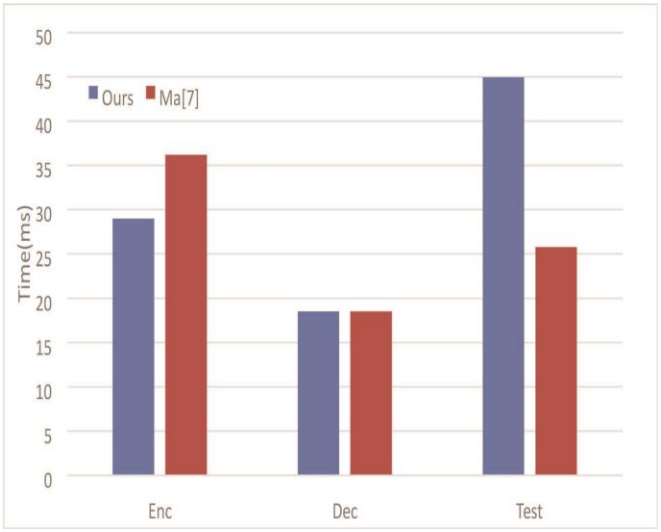


Fig. 2: The simulation results

[7] Sha Ma. Identity-based encryption with outsourced equality test in cloud computing. Information Sciences, 328(20):389–402, 2016.