Efficiently Deployable & Efficiently Searchable Encryption (EDESE) – Applications, Attacks, and Countermeasures

Robert H. DENG[1] [0000−0003−3491−8146]

School of Information Systems
Singapore Management University, Singapore
robertdeng@smu.edu.sg

Abstract. The volume of data stored in the public cloud is growing exponentially. With this growth, the risk of data breaches and the challenges of data protection grow just as rapidly. As more organizations opt for using encryption to protect their data in the cloud and in web services, the ability to efficiently search over encrypted data becomes increasingly important.

Though numerous searchable encryption (SE) schemes have appeared in the literature, Efficiently Deployable & Efficiently Searchable Encryption (EDESE) is the most popular SE scheme being deployed in practical applications at the expense of information leakages that were considered acceptable. In this talk, we first look at single user EDESE and multiuser EDESE schemes and their real-world deployments. We then review some of the recent attacks to EDESE that can accurately recover the underlying keywords of query tokens based on partially known documents and the L2 leakage. Finally, we discuss possible means to counter such attacks.

Bio: Robert Deng is AXA Chair Professor of Cybersecurity, Director of the Secure Mobile Centre, and Deputy Dean for Faculty & Research, School of Computing and Information Systems, Singapore Management University (SMU). His research interests are in the areas of data security and privacy, network security, and applied cryptography. He received the Outstanding University Researcher Award from National University of Singapore, Lee Kuan Yew Fellowship for Research Excellence from SMU, and Asia-Pacific Information Security Leadership Achievements Community Service Star from International Information Systems Security Certification Consortium. He serves/served on the editorial boards of ACM Transactions on Privacy and Security, IEEE Security & Privacy, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, Journal of Computer Science and Technology, and Steering Committee Chair of the ACM Asia Conference on Computer and Communications Security. He is a Fellow of IEEE and Fellow of Academy of Engineering Singapore.