International Journal of Innovative
Computing, Information and Control
Volume **7**, Number **5(A)**, May **2011**

ICIC International ©2011 ISSN 1349-4198
pp. **2247–2256**

IC-LOCK APPROACH: A KEY MANAGEMENT SOLUTION FOR OUTSOURCED DATABASE

Kevin I-J Ho[1], Chun-Wei Liao[2,3] and Wei-Bin Lee[2,*]

[1]Department of Computer Science and Communication Engineering
Providence University
No. 200, Chung Chi Road, Sha-Lu, Taichung 43301, Taiwan
ho@pu.edu.tw

[2]Department of Information Engineering and Computer Science
Feng Chia University
No. 100, Wenhwa Road, Seatwen, Taichung 40724, Taiwan
*Corresponding author: wblee@fcu.edu.tw

[3]Department of Information Management
Hsiuping Institute of Technology
No. 11, Gungye Road, Dali City, Taichung 41280, Taiwan
leggy@mail.hit.edu.tw

Received January 2010; revised May 2010

Abstract. *Outsourced databases are now in widespread use by enterprises. A database service provider contracts with a data owner to sell storage space and make a profit. The data owner pays for the service and transmits data for storage in a database at a service provider's site through the Internet. In a high-risk network environment, a service provider may want to ensure that the received data are originally generated by the payer. A data owner may similarly worry about leaking his sensitive data to others, including the distrusted service provider. Thus, it is necessary to provide data confidentiality services to data owners and data integrity services to both service providers and data owners. In addition, using a symmetric cryptosystem to provide data confidentiality services usually requires many encryption keys; as such, determining how to manage those keys while minimizing the associated burden is a challenge. Accordingly, a key management scheme called the IC-Lock approach is proposed to simultaneously guarantee both integrity and confidentiality. Moreover, if necessary, the approach's modular design makes the approach flexible enough to adopt new components for performance and security consideration.*

Keywords: Confidentiality, Database-as-a-service, Integrity, Key management, Outsourced database

1. **Introduction.** Cloud computing is the third revolution of IT industry, following the Internet revolution. Cloud storage is a service of Cloud computing in which a third-party service provider rents storage space out to a data owner. Through data outsourcing, the data owner can reduce costs associated with purchasing expensive hardware and software. However, data security worries data owners. As data leave its owner and reside on the premises of the service provider – even if the data owner may not fully trust the management of data and services – the process requires a security mechanism to reassure the data owner when utilizing this service. For example, if hospitals want to rent a database from service providers to store or back up health information and medical images, they have to consider data security in order to obtain compliance with regulations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). According to HIPAA requirements, any health information that identifies an individual or can be