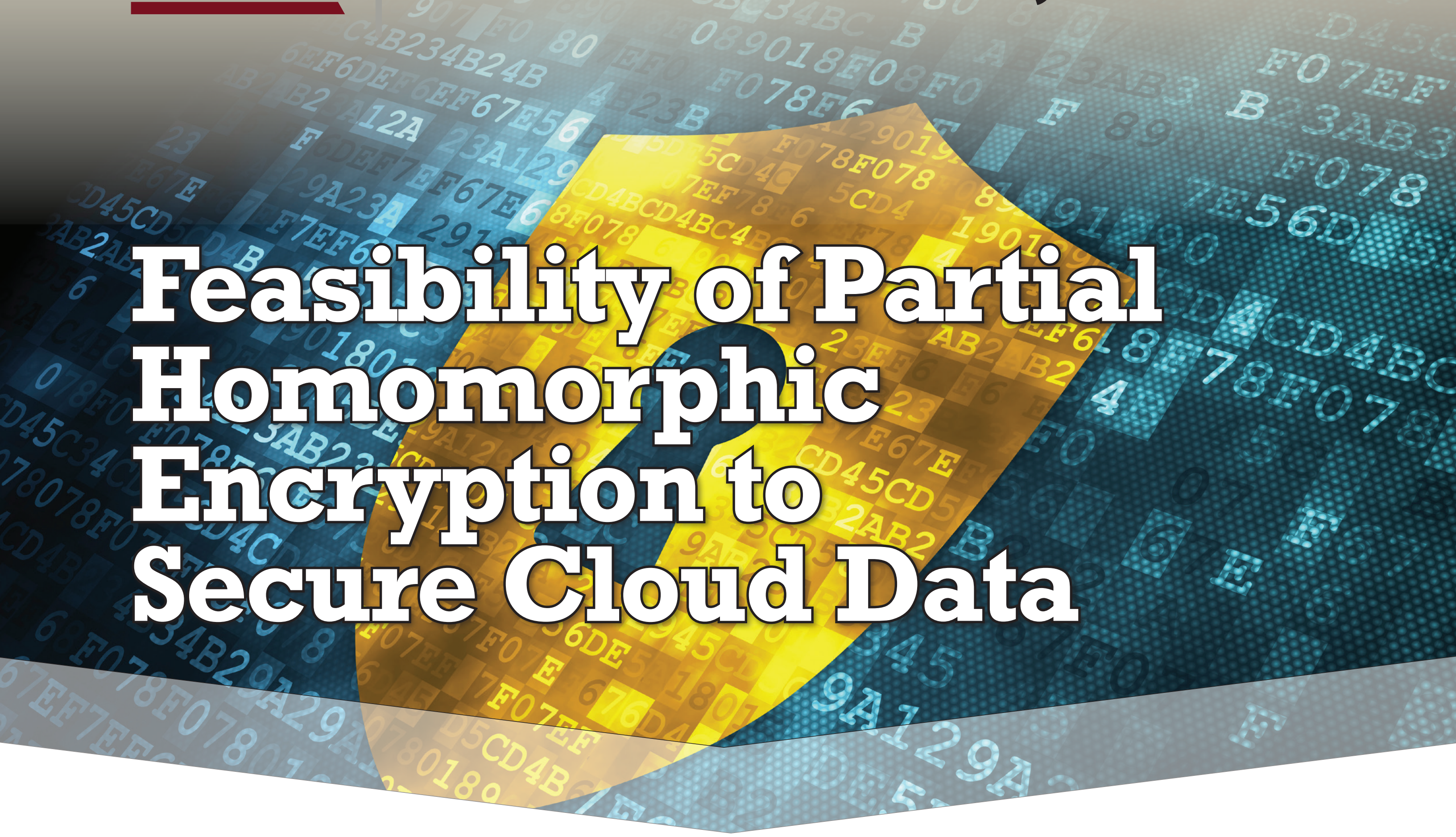
IDA | Research Summary



Feasibility of Partial Homomorphic Encryption to Secure Cloud Data

The Department of Defense is adopting a cloud computing model, but storing sensitive data in the cloud raises security issues. IDA previously demonstrated the feasibility of using partial homomorphic encryption (PHE) as part of a database encryption scheme in which standard Structured Query Language (SQL) queries are performed on encrypted data. PHE allows manipulation of encrypted data to perform certain computations without first decrypting the underlying data, thus reducing threats posed by cloud providers, employees, and others. The present work extends that concept by demonstrating the feasibility of operating a full-scale Oracle Enterprise Resource Planning (ERP) system on PHE data.

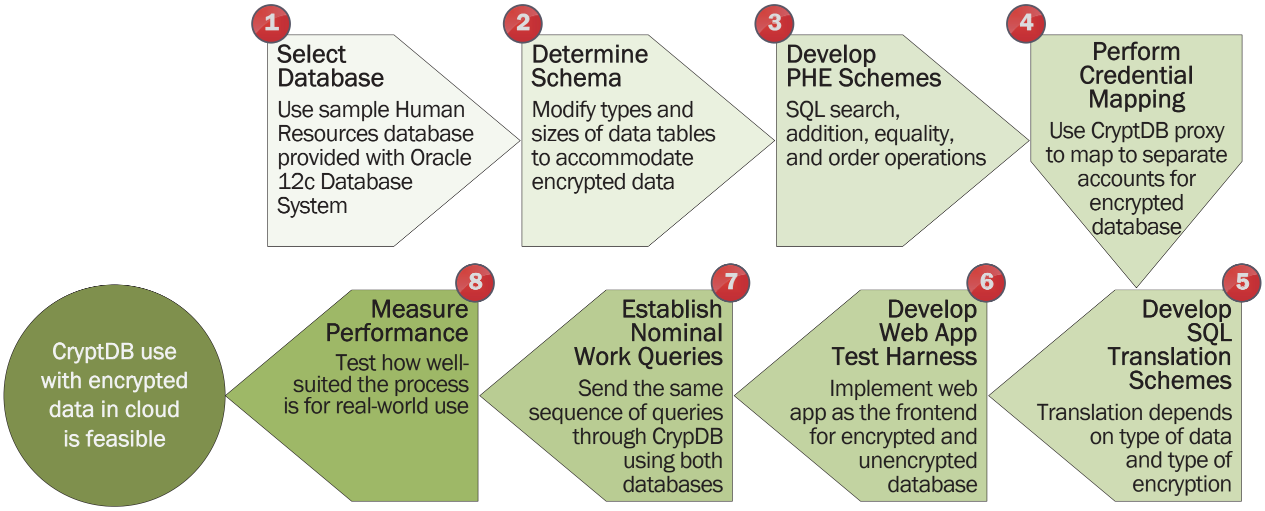
The demonstration required accommodating extra features such as stored procedures, views, and multiuser access controls. IDA was able to implement these features using encrypted data without changing the underlying ERP application code. So that the concept would work with Oracle's ERP SQL database, we first rewrote CryptDB—an open-source system that executes confidential SQL queries over encrypted data using efficient encryption-aware SQL schemes.

We added new abilities to address features of Oracle ERP that make computing with encrypted data even more complicated—features such as key reference integrity and multiple accounts with different permissions. We then used a test ERP application to compare functionality and performance between the original unencrypted database and the encrypted database.

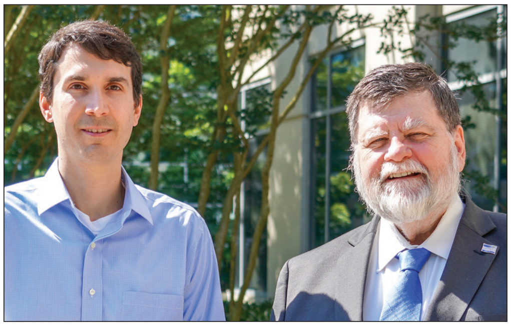
(continued)

April 2020
NS D-12086

The steps we followed are depicted below.


1
Select Database
Use sample Human Resources database provided with Oracle 12c Database System
2
Determine Schema
Modify types and sizes of data tables to accommodate encrypted data
3
Develop PHE Schemes
SQL search, addition, equality, and order operations
4
Perform Credential Mapping
Use CryptDB proxy to map to separate accounts for encrypted database
5
Develop SQL Translation Schemes
Translation depends on type of data and type of encryption
6
Develop Web App Test Harness
Implement web app as the frontend for encrypted and unencrypted database
7
Establish Nominal Work Queries
Send the same sequence of queries through CrypDB using both databases
8
Measure Performance
Test how well-suited the process is for real-world use
CryptDB use with encrypted data in cloud is feasible

We assessed functionality, bulk encryption, and operational performance and found that converting an existing database to an encrypted database scaled well in database size and computational resources with delays in transfer of data (latency) necessary for operating on encrypted data being within a small factor of those for unencrypted data. These results demonstrate the feasibility of running an ERP system with an encrypted database in an untrusted cloud hosting environment using CryptD.



Kevin E. Foltz (kfoltz@ida.org) and **William R. (Randy) Simpson** (wsimpson@ida.org) are both members of the research staff in the Information Technology and Systems Division of IDA's Systems and Analyses Center. Kevin holds a PhD in electrical engineering from the California Institute of Technology, and Randy holds a PhD in aerospace engineering from the Ohio State University.

This publication is based on "Extending CryptDB to Operate and ERP System on Encrypted Data," by K. E. Foltz and W. R. Simpson in *Proceedings of the 20th International Conference on Enterprise Information Systems (ICEIS 2018)*, Volume 1, March 2018. Research was sponsored by the DoD Deputy Chief Information Officer for Cybersecurity and the United States Air Force Chief Technology Offecer.

4850 Mark Center Drive
Alexandria, VA 22311-1882
ida.org