Privacy-Preserving Auction for Big Data Trading Using Homomorphic Encryption

Abstract—Cyber-Physical Systems (smart grid, smart transportation, smart cities, etc.), driven by advances in Internet of Things (IoT) technologies, will provide the infrastructure and integration of smart applications to accelerate the generation and collection of big data to an unprecedented scale. As now a fundamental commodity in our current information age, such big data is a crucial key to competitiveness in modern commerce. In this paper, we address the issue of privacy preservation for data auction in CPS by leveraging the concept of homomorphic cryptography and secured network protocol design. Specifically, we propose a generic Privacy-Preserving Auction Scheme (PPAS), in which the two independent entities of Auctioneer and Intermediate Platform comprise an untrusted third-party trading platform. Via the implementation of homomorphic encryption and one-time pad, a winner in the auction process can be determined and all bidding information is disguised. Yet, to further improve the security of the privacy-preserving auction, we additionally propose an Enhanced Privacy-Preserving Auction Scheme (EPPAS) that leverages an additional signature verification mechanism. The feasibilities of both schemes are validated through detailed theoretical analyses and extensive performance evaluations, including assessment of the resilience to attacks. In addition, we discuss some open issues and extensions relevant to our scheme.

Conclusion

In this paper, we have addressed the issue of protecting information privacy during the data auction in the thirdparty auction platform. We have leveraged the concept of homomorphic encryption to design a Privacy-Preserving Auction Scheme (PPAS). In order to carry out a privacy-preserving auction, we selected a set of
crypto-primitives and designed algorithms in our system to enable the efficiency of the auction process. To further improve the security and resistance to attacks of PPAS, we proposed the Enhanced Privacy-Preserving Auction Scheme (EPPAS). The prototypical system of the auction scheme has been implemented to conduct thorough experimental evaluation.

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb

**SOFTWARE REQUIREMENTS:**

- Operating system : Windows 7/UBUNTU.
- Coding Language : Java 1.7, Hadoop 0.8.1
- IDE : Eclipse
- Database : MYSQL

**REFERENCES**
