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

Contd..

- Privacy-Preserving Auction Scheme (PPAS), in which the two independent entities of Auctioneer and Intermediate Platform comparise 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

EXISTING SYSTEM

- network-connected devices will engender diverse applications for the generation, maximization, and optimization of a variety of resources that span a multitude of domains.
- Furthermore, it is readily evident that emerging networking and computing technologies shall enable easier, faster, and cheaper data collection from such CPS systems.

DISADVANTAGES

- critical challenges must be overcome, such as properly evaluating the price of datasets, enabling fair and secure data trading with the support of network protocols, and ensuring data copyright protection.
- Although data, in the form of digital information/commodity, can be duplicated and assigned with an infinite number of copies, competition among data users would prefer to compete for it.

PROPOSED SYSTEM

- 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.

ADVANTAGES

- Platform run by sellers, meaning that the sellers play the role of the auctioneer, and information from the bidders is open to the sellers during the auction. In addition, with the increasing number of data owners, it is inefficient and inconvenient for each data seller to maintain their own auction platform.
- Thus, a third-party data trading platform in the network environment would be a more realistic approach.

HARDWARE REQUIREMENTS

Processor	:Intel Pentium IV 1GHz
RAM	:256MB (Min)
Hard Drive	:5GB free space
Monitor	:1024 * 768, High Color inch
Mouse	:Scroll Mouse(Logitech)
Keyboard	:104 keys

SOFTWARE REQUIREMENTS

OS	:	Windows XP/7/8
Front End	:	Visual Studio 2010/ netbeans 7.1
Back End	:	SQL Server 2005/ heidisql 3.2
Browser	:	Any Web Browser

CONCLUSION

- 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 privacypreserving auction, we selected a set of crypto-primitivesand 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. The experimental results demonstrate that our proposed scheme is capable of ensuring the determination of an auction winner with a 100% correct rate under normal operations and without leakage of private information.

REFERENCES

[1] R. van der Meulen, “8.4 billion connected ’things’ will be in use in 2017, up 31 percent from 2016,” 2017. [Online]. Available: https://www.gartner.com/newsroom/id/3598917

[2] J. A. Stankovic, “Research directions for the Internet of Things,”IEEE Internet of Things Journal, vol. 1, no. 1, pp. 3–9, Feb 2014.

[3] Q. Yang, D. An, R. Min, W. Yu, X. Yang, and W. Zhao, “Optimal PMU placement based defense against data integrity attacks in smart grid,” IEEE Transactions on Forensics and Information Security (T-IFS), vol. 12, no. 7, pp. 1735–1750, 2017.

[4] J. Lin, W. Yu, X. Yang, Q. Yang, X. Fu, and W. Zhao, “A real-time en-route route guidance decision scheme for transportation-based cyberphysical systems,” IEEE Transactions on Vehicular Technology, vol. 66, no. 3, pp. 2551–2566, March 2017.

[5] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications,” IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125–1142, Oct 2017.