ISSN:0975-9646

Privacy Preserving in Collaborative Data Publishing

K. Reddi Kumari
Department of CSE
M. Tech student MITS,
Madanapalle

P.Rajarajeswari
Department of CSE
Assoc. Professor, MITS,
Madanapalle.

Dr.D.Vasumathi
Professor,
JNTU,
Hyderabad

Abstract-Security and maintaining privacy of data, have become a challenging issue with innovations in information technology. The quantity of data that is streaming on internet is growing at an exponential rate. The capability to interconnect and sharing data has several advantages, and it carries a notable value to research and designing data analysis models. Due to the increasing issue of identity theft, it is difficult to avoid the maltreatment of data. For this reason, we need to maintain the security of data by means of a third party which is taking care of the data being shared. Secure multiparty computation is one of the model, which acts as a third party to achieve it. But this model does not guarantee that organizations are providing truthful data and provides communication between two organizations only. For this reason we are proposing game theoretic mechanism to encourage honest behavior among organizations in sharing private data correctly and it provide communication among multiple organizations. In this work, we will study the incentive issues present in another data analysis models.

Index Terms: Game theory, Non Cooperative Computation, Multi Party Computation.

I.INTRODUCTION

Nowadays, data management applications have evolved from pure storage and retrieval of information to finding interesting patterns and associations from large amounts of data. With the advancement of Internet and networking technologies, more and more computing applications, including data mining programs, are required to be conducted among multiple data sources that scattered around different spots, and to jointly conduct the computation to reach a common result. However, due to legal constraints and competition edges, privacy issues presentin the area of distributed data mining, thus leading to the interests from research community of both data mining.

II. RELATED WORK

Privacy-preserving data mining (PPDM) is an evolving research area that reports the integration of privacy preserving issues to data mining procedures. In this work, we propose a privacy-preserving (PP) Cox model for persistence evaluation, and study a real clinical back ground where the data is horizontally spread among various organizations. Here the proposed model is based on linearly launching the data to a subordinate dimensional area over an ideal plotting acquired by resolving a linear programming hindrance. Our method differs from the generally used unplanned estimate method since it as an alternative finds an estimate that is best at conserving the attributes of the data that are vital for the particular issue at present. Since our projected method generates a meager mapping.

In supplement to present practices that study truthful but-inquiring model, there are methodologies progressed against malicious opponents. Authors examine how to avoid dishonest about inputs exploiting “input-consistency checks”. Generally, authors advise inspection whether the inputs meet some circumstances that are known to be correct about the inputs. Although such method could be beneficial in reality, it cannot avoid untruthfulness about inputs that meet the area limit. In our present case, we suggested an altered explanation.

III. SECURE MULTI PARTY COMPUTATION

In existing system, cryptographic techniques are used for designing the PPDA protocols. In this secure multiparty computation is used. It provides communication between two parties only. The data analysis results are calculated without verifying the correctness of input data given by private organizations. In existing system, we assume that the organizations are providing true input for calculating analysis results.

- Secure Multiparty Computation
- Cryptographic techniques

DRAWBACKS

- Impossible to check the correctness of input data given by organizations.
- Participating parties can modify the input using SMC techniques.
- SMC techniques can provide access between two parties only.

IV. NON – COOPERATIVE COMPUATATION

In this work, we propose a method called Non – Cooperative computation for establishing communication among multiple organizations in order to access data from multiple organizations. This method provide many - to - many communication. Using this method, it is possible to verify the correctness of input given by private parties. By the incorporation of Trusted Third Party, this method guarantees privacy in data sharing and encourage honest behavior among private parties.

PROPOSED METHODS

- **Non – Cooperative Computation**
- **Deterministic NCC**

The study of game theory is related to the motivation of participant organizations, which are known as players. They participated in analysis task in order to achieve some goal and the choices they make to do so. Among the all options, game theory assumes that each participating party wishes to maximize their own benefit.A two-party protocol is proposed to securely compute JC. The protocol consists of two stages**.**The working of protocol is as follows.It contains client Login, Database, Work Allocation, Worker Page, Computing, Reposting, and Work Grouping. First computation node will start running. After party node enter user name and password that is validated by compatible node. Then computation node assigns the work to the data mining nodes. Data mining node finishes his work and reposted to the compatible node. TTP collects the inputs of parties and group of parties input for particular work presented by party nodes.

VI.CONCLUSION

In this work, as a future work there is a scope to investigate which type of PPDA assignments are incentives compatible relating to the NCC model. In this work, we propose a method called Non – Cooperative computation for establishing communication among multiple organizations in order to access data from multiple organizations. This method provides many - to - much communication. Using this method, it is possible to verify the correctness of input given by private parties. By the incorporation of Trusted Third Party, this method guarantees privacy in data sharing and encourage honest behavior among private parties. Within this work.

REFERENCES

[1] I. Abraham, D. Dolev, R. Gonen, and J. Halpern. Distributed computing meets game theory: Robust mechanisms for rational secret sharing and multiparty computation. In Proceedings of the twenty-fifth annual ACM symposium on Principles of distributed computing, pages 53–62. ACM New York, NY, USA, 2006.

[2] R. Agrawal and E. Terzi. On honesty in sovereign information sharing. Lecture Notes in Computer Science, 3896:240, 2006.

[3] Rakesh Agrawal and RamakrishnanSrikant. Fast algorithms for mining association rules. In VLDB '94, pages 487–499, Santiago, Chile, September 12-15 1994. VLDB.

[4] I. Ashlagi, A. Klinger, and M. Tenneholtz. K-NCC: Stability Against Group Deviations in Non-Cooperative Computation. LECTURE NOTES IN COMPUTER SCIENCE, 4858:564, 2007.

[5] Mikhail J. Atallah, Marina Bykova, Jiangtao Li, and MercanKarahan. Private collaborative forecasting and benchmarking. In Proc. 2d. ACM Workshop on Privacy in the Electronic Society (WPES), Washington, DC, October 28 2004.

[6] B. Chor and E. Kushilevitz. A zero-one law for boolean privacy. In STOC '89, pages 62–72, New York, NY, USA, 1989. ACM Press.

[7] www.doe.gov, doe news, feb. 16 2005.

[8] Wenliang Du and Zhijun Zhan. Building decision tree classifier on private data. In Chris Clifton and Vladimir Estivill-Castro, editors, IEEE International Conference on Data Mining Workshop on Privacy, Security, and Data Mining, volume 14, pages 1–8, Maebashi City, Japan, December 9 2002. Australian Computer Society.

[9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities, No I.(281):31–50, October 24 1995.

[10] KeinosukeFukunaga. Introduction to Statistical Pattern Recognition. Academic Press, San Diego, CA, 1990.