IJRRECS/April 2014/Volume-2/Issue-4/2158-2163 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

A SECURE DATA ANALYSIS SYSTEM FOR GRANTING OF TRUTHFUL INFORMATION

Aakula Srilatha[1], G.Pavani[2]

[1]M.Tech Student, Dept of CSE, Bandari Srinivas Institute of Technology, Chevella, R.R Dist., A.P, India

[2]Assistant Professor, Dept of CSE, Bandari Srinivas Institute of Technology, Chevella, R.R Dist., A.P, India

ABSTRACT:

Maintenance of data confidentiality and privacy, have turn out to be a challenging issue with advancements made in communication and information technology. Secure multiparty computation has in recent times come into sight as a response to the setback. In secure multiparty computation, it was generally believed that participating parties make available straightforward inputs and these protocols necessitate participating parties to carry out high-priced computations. The ability to converse and allocate data has several benefits, and the thought of an omniscient data source carries enormous value to study and building models of accurate data analysis. In view of the fact that data analysis algorithms can be seen as a particular case, changing non-cooperative computation representation for our purposes is an accepted choice. In non-cooperative computation, every party participates in a procedure to gain knowledge of the output of some function over the combined inputs of the parties.

Keywords: Privacy, Secure multipary computation, Non-cooperative computation, Data analysis.

1. INTRODUCTION:

Although secure multiparty computation protocols promise that nothing other than the concluding data analysis result is made known [6]. It is not possible to authenticate whether contributing parties are straightforward concerning their confidential input data. Several procedures of privacy-

preserving data analysis have been considered by means of cryptographic techniques. The thought of an omniscient data source carries huge value to explore and building precise data analysis representations and the capability to converse and distribute data has numerous benefits [4]. The participating parties gain knowledge of only the concluding result and whatever can be inferred from the concluding result and their individual inputs if a procedure meets the secure multiparty computation definitions. The computation representation of secure multiparty does not assurance that information provided by participating parties is honest. The present methods of secure multiparty computation cannot put off input alteration by means of participating parties unless appropriate incentives are set [8]. Since the protocols of secure multiparty computation based necessitate participating parties to carry out high-priced computations, if any party does not desire to gain knowledge of data models and examination results, the party should not contribute in the protocol [1]. The honesty of the private input data was not assured by the supposition when participating parties would like to gain knowledge of the final result completely. All the existing techniques imagine that each participating party make use of its accurate data throughout the distributed data mining protocol implementation. Besides existing techniques that believe model of honest butcurious, there are methods expanded against malevolent adversaries [11]. A large extent of work seeks to comprise a model of game-theoretic in pattern secure multiparty computation. As a substitute of considering players who are honest or else malicious, the effort merely considers players to be reasonable in the sense of game theoretic [13].

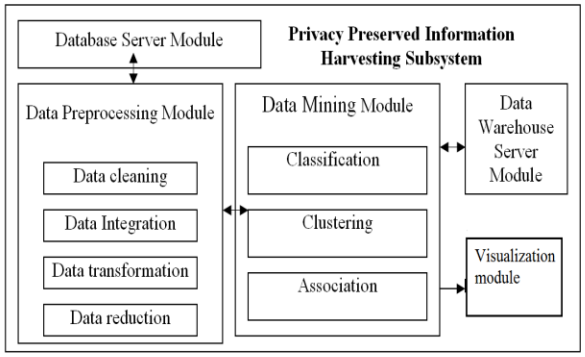

Fig1: An overview of privacy preserving

2. METHODOLOGY:

With potentially contradictory interests in numerous real life circumstances, information needed for construction of data analysis models are dispersed between multiple parties [3]. For the most part maintaining privacy of data, by means of

progression in information and communication expertise, privacy and protection have turn out to be a demanding concern. We generally believe in secure multiparty computation, that participating parties make available straightforward inputs [14]. By means of the fact that learning the truthful data analysis representation is in the most excellent attention of all contributing parties justifies the supposition. Data are normally assumed to be moreover vertically or horizontally partitioned. Various sites accumulate the identical set of information in relation to unlike in the horizontally partitioned information [9]. By means of cryptographic techniques numerous privacy-preserving data analysis procedures shown in fig1 have been considered. Since data analysis algorithms can be seen as a particular case, changing non-cooperative computation representation for our purposes is an accepted choice [7]. The representation model of non-cooperative computation makes the following suppositions such as correctness: The primary precedence for each participating party is to gain knowledge of the accurate result; exclusiveness: If feasible, each participating party have a preference to learn the right result completely [2] [15]. Learning the accurate consequence is the most significant objective of each party. The representation of non-cooperative computation was approved which is considered for parties who want to jointly calculate the accurate function results on their confidential inputs [12]. Aspects such as confidentiality and voyeurism could be also measured in the non-cooperative computation representation setting. The non-cooperative computation representation setting was made used where each party wants to gain knowledge of the data mining result accurately, if promising prefers to gain knowledge of it completely [5]. Revealing only the consequence does not disobey privacy was taken granted. The representation of non-cooperative computation is able to be seen as an instance of be validating game theoretical facts in a dispersed computation setting. In the representation model of non-cooperative computation, every party participates in a procedure to gain knowledge of the output of some function over the combined inputs of the parties [10]. To a trusted third party initially all participating parties transmit their confidential inputs securely, and subsequently trusted third party computes

and sends backside the consequence to each participating party.

3. RESULTS:

In deterministic non-cooperative computation several functions like set union, set intersection and sum, are not present however they can be able to be used in an incentive-compatible way in privacy-preserving distributed data analysis functions. In secure multiparty computation domain expansively the effects of an antagonist that controls numerous parties have been considered. By means of binary vectors functions calculating dot product is in deterministic non-cooperative computation, then by means of the results, we can terminate that calculating a support count up of an item set is in addition in deterministic non-cooperative computation. In several functions, primitives like set union and intersection and sum are not used only, and they frequently act as subroutines. The subroutines can merely return arbitrary shares of the accepted results to have an entirely protected protocol. The general consequences point towards that any function could be estimated confidentially specifically not anything other than the function consequence is revealed if an adversary is computationally enclosed and does not manage the bulk of the parties.

4. CONCLUSION:

By means of progression in information and communication expertise, privacy and protection, for the most part maintaining privacy of data, have turn out to be a demanding concern. The non-cooperative computation representation setting was made used where each party wants to gain knowledge of the data mining result accurately, if promising prefers to gain knowledge of it completely. The representation model of non-cooperative computation makes the following suppositions such as Correctness: The primary precedence for each participating party is to gain knowledge of the accurate result. Exclusiveness: If feasible, each participating party have a preference to learn the right result completely. Even though the method of privacy-preserving data analysis assurance that not anything other than the final effect is disclosed, whether or not participating parties make available honest input data cannot be confirmed. In recent times, secure multiparty computation has come into sight as a response to the setback. Several data analysis of privacy-preserving

procedures has been considered by means of cryptographic methods. Various functions like set union, set intersection and sum, are not in deterministic non-cooperative computation, on the other hand they can be able to be used in an incentive-compatible way in privacy-preserving distributed data analysis functions. In a dispersed computation setting the non-cooperative computation representation is able to be seen as an instance of be validating game theoretical facts.

REFERENCES:

[1] R. Layfield, M. Kantarcioglu, and B. Thuraisingham, "Incentive and Trust Issues in Assured Information Sharing," Proc. Fourth Int'l Conf. Collaborative Computing: Networking, Applications and Worksharing, p. 113, 2009.

[2] Murat Kantarcioglu and Wei Jiang, "Incentive Compatible Privacy-Preserving Data Analysis" IEEE Transactions on Knowledge and Data Engineering, Vol. 25, No. 6, June 2013.

[3] "Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," Official J. European Communities, vol. 281, pp. 31-50, Oct. 1995.

[4] H. Kargupta, K. Das, and K. Liu, "A Game Theoretic Approach toward Multi-Party Privacy-Preserving Distributed Data Mining," Proc. 11th European Conf. Principles and Practice of Knowledge Discovery in Databases, pp. 523-531, Sept. 2007.

[5] R. McGrew, R. Porter, and Y. Shoham, "Towards a General Theory of Non-Cooperative Computation (Extended Abstract)," Proc. Conf. Theoretical Aspects of Rationality and Knowledge
(TARK IX), 2003.

[6] I. Abraham, D. Dolev, R. Gonen, and J. Halpern, "Distributed Computing Meets Game Theory: Robust Mechanisms for Rational Secret Sharing and Multiparty Computation," Proc. 25th Ann. ACM Symp. Principles of Distributed Computing, pp. 53-62, 2006.

[7] S. Izmalkov, S. Micali, and M. Lepinski, "Rational Secure Computation and Ideal Mechanism Design," Proc. 46th Ann. IEEE Symp. Foundations of Computer Science (FOCS '05), pp. 585-594, 2005.

[8] G. Jagannathan and R.N. Wright, "Privacy-Preserving Distributed k-Means Clustering over Arbitrarily Partitioned Data," Proc. ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining, pp. 593- 599, Aug. 2005

[9] I. Ashlagi, A. Klinger, and M. Tenneholtz, "K-NCC: Stability Against Group Deviations in Non-Cooperative Computation," Proc. Third Int'l Conf. Internet and Network Economics, pp. 564-569, 2007.

[10] M. Kantarco_glu and C. Clifton, "Privacy-Preserving Distributed Mining of Association Rules on Horizontally Partitioned Data," IEEE Trans. Knowledge and Data Eng., vol. 16, no. 9, pp. 1026-1037, Sept. 2004.

[11] O. Goldreich, S. Micali, and A. Wigderson, "How to Play Any Mental Game - A Completeness Theorem for Protocols with Honest Majority," Proc. 19th ACM Symp. the Theory of Computing, pp. 218-229, 1987.

[12] Y. Shoham and M. Tennenholtz, "Non-Cooperative Computation: Boolean Functions with Correctness and Exclusivity," Theoretical Computer Science, vol. 343, nos. 1/2, pp. 97-113, 2005.

[13] W. Du and Z. Zhan, "Building Decision Tree Classifier on Private Data," Proc. IEEE Int'l Conf. Data Mining Workshop Privacy, Security, and Data Mining, C. Clifton and V. Estivill-Castro, eds., vol. 14, pp. 1-8, Dec. 2002.

[14] G. Jagannathan and R.N. Wright, "Privacy-Preserving Distributed k-Means Clustering over Arbitrarily Partitioned Data," Proc. ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining, pp. 593- 599, Aug. 2005.

[15] M.J. Atallah, M. Bykova, J. Li, and M. Karahan, "Private Collaborative Forecasting and Benchmarking," Proc. Second ACM Workshop Privacy in the Electronic Soc. (WPES), Oct. 2004.