Y. Bhargav *et al*, International Journal of Computer Science and Mobile Applications,
Vol.1 Issue. 5, November- 2013, pg. 18-37 **ISSN: 2321-8363**

Homomorphic Recommendations for Data Packing- A Survey

Y. Bhargav[1], P. Sreenivasa Moorthy[2]

[1]M.Tech. Student, CSE Dept, CMR Institute of Technology, Hyderabad, A.P
Email-id: bhargav.y9959@gmail.com

[2]Associate Professor, CSE Dept., CMR Institute of Technology, Hyderabad, A.P
Email-id: moorthypsm@gmail.com

Abstract

Recommender systems have become an important tool for personalization of online services. Generating recommendations in online services depends on privacy-sensitive data collected from the users. Traditional data protection mechanisms focus on access control and secure transmission, which provide security only against malicious third parties, but not the service provider. This creates a serious privacy risk for the users. In this paper, we aim to protect the private data against the service provider while preserving the functionality of the system. We propose encrypting private data and processing them under encryption to generate recommendations. By introducing a semitrusted third party and using data packing, we construct a highly efficient system that does not require the active participation of the user. We also present a comparison protocol, which is the first one to the best of our knowledge, that compares multiple values that are packed in one encryption. Conducted experiments show that this work opens a door to generate private recommendations in a privacy-preserving manner.

We have developed an approach for privacy-preserving Recommender Systems based on Multi-Agent System technology which enables applications to generate recommendations via various filtering techniques while preserving the privacy of all participants. We describe the main modules of our solution as well as an implemented application based on this approach. This paper also describes various limitations of current recommendation methods and discusses possible extensions that can improve recommendation capabilities and make recommender systems applicable to an even broader range of applications. These extensions include, among others, an improvement of understanding of users and items, incorporation of the contextual information into the recommendation process, support for multcriteria ratings, and a provision of more flexible and less intrusive types of recommendations.

Index Terms- Homomorphic encryption; privacy; recommender systems; secure multiparty computation

Full Text: www.ijcsma.com/publications/november2013/V1I517.pdf