AMPLYFING RECOMMENDER SYSTEM WITH NETWORK REPRESENTATION LEARNING

DR. Rajesh Khanna, Associate Professor CSE, Vaagdevi College of Engineering (Autonomous), India
V. Bhaskar, UG student, CSE, Vaagdevi College of Engineering(Autonomous),India
S. Chandana, UG student, CSE, Vaagdevi College of Engineering(Autonomous),India
P. Sai Krishna, UG student CSE, Vaagdevi College of Engineering(Autonomous),India

ABSTRACT
With the popularity of social network applications, more and more recommender systems utilize trust relationships to improve the performance of traditional recommendation algorithms. Social-network-based recommendation algorithms generally assume that users with trust relations usually share common interests. However, the performance of most of the existing social-network-based recommendation algorithms is limited by the coarse-grained and sparse trust relationships. In this paper, we propose a network representation learning enhanced recommendation algorithm. Specifically, we first adopt a network representation technique to embed social network into a low-dimensional space, and then utilize the low-dimensional representations of users to infer fine-grained and dense trust relationships between users. Finally, we integrate the fine-grained and dense trust relationships into the matrix factorization model to learn user and item latent feature vectors. The experimental results on real-world datasets show that our proposed approach outperforms traditional social-network-based recommendation algorithms.

INTRODUCTION
In the era of big data, it becomes increasingly difficult to find valuable related information from massive unstructured data. Recommender systems infer users' latent preferences by analyzing their past activities and provide them with personalized recommendation services [1]. Therefore recommender systems have become an effective means to solve the problem of information overload. In recent years, such research directions have drawn great attention from academia and industry. Typical applications of recommender systems include Amazon's product recommendation, Netflix's movie recommendation, last.fm's music recommendation, LinkedIn's friend recommendation, and Google News's news recommendation.
Collaborative filtering (CF) [2] is the most widely used recommendation technique in the research of recommender systems. However, the problems of data sparsity and cold start have significantly negative impact on the performance of collaborative filtering methods. As an example, owing to data sparsity, traditional collaborative filtering algorithms cannot accurately calculate the similarities between users or between items; or cannot accurately learn latent user and item feature vectors from users' past activities.
The emergence of social networks brings an opportunity to alleviate the problems of data sparsity and cold start in traditional collaborative filtering algorithms. Some researchers utilize the rich information contained in social networks to propose some social-network-based reco- mendation algorithms. Typical social-network-based recommendation algorithms include SoRec [3], RSTE SocialMF [4], TrustMF [5] and so on. Social-network-based recommendation algorithms generally assume that users with trust relations usually share common interests. However, in the original social network, the trust relationship is usually binary, that is, only 0 or 1 is used to denote the trust relationship between users where 1 denotes there is a trust relation between two users, and the degree of trust is 1 and 0 indicates that there is no trust relationship between users. Intuitively, the granularity of such a representation is too coarse to specify the different levels of trust among users.
In fact, many users are very likely to trust one another because of their shared connections, although they have not built any direct trust connections. In the process of designing recom- mendation

models, the quality of recommendation algorithms can be enhanced by considering such indirect and implicit trust relationships. However, such implicit trust relationships between users are often ignored in the traditional social- network-based recommendation models.

In order to tackle the above problems, this research pro- poses a network representation learning enhanced recom- mendation algorithm. Speci_cally, we _rst adopt a network representation technique [6] to embed social network into a low-dimensional space, and then utilize the low-dimensional representations of users to infer _ne-grained and dense trust relationships between users. Finally, we integrate the _ne- grained and dense trust relationships into the social-network- based recommendation model to learn latent feature vectors of users and items more precisely. The empirical results on real-world datasets indicate that our proposed approach out- performs traditional social-network-based recommendation algorithms.

LITERATURE SURVEY

A break in the clouds: Towards a cloud definition

This paper discusses the concept of Cloud Computing to achieve a complete definition of what a Cloud is, using the main characteristics typically associated with this paradigm in the literature. More than 20 definitions have been studied allowing for the extraction of a consensus definition as well as a minimum definition containing the essential characteristics. This paper pays much attention to the Grid paradigm, as it is often confused with Cloud technologies. We also describe the relationships and distinctions between the Grid and Cloud approaches

Practical techniques for searches on encrypted data

It is desirable to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. But this usually implies that one has to sacrifice functionality for security. For example, if a client wishes to retrieve only documents containing certain words, it was not previously known how to let the data storage server perform the search and answer the query without loss of data confidentiality. In this paper, we describe our cryptographic schemes for the problem of searching on encrypted data and provide proofs of security for the resulting crypto systems. Our techniques have a number of crucial advantages. They are provably secure: they provide provable secrecy for encryption [8], in the sense that the untrusted server cannot learn anything about the plaintext when only given the ciphertext; they provide query isolation for searches, meaning that the untrusted server cannot learn anything more about the plaintext than the search result; they provide controlled searching, so that the untrusted server cannot search for an arbitrary word without the user's authorization; they also support hidden queries, so that the user may ask the untrusted server to search for a secret word without revealing the word to the server. The algorithms we present are simple, fast (for a document of length , the encryption and search algorithms only need stream cipher and block cipher operations), and introduce almost no space and communication overhead, and hence are practical to use today.

Searchable symmetric encryption: Improved definitions and efficient constructions.

Searchable symmetric encryption (SSE) [9] allows a party to outsource the storage of his data to another party in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research and several security definitions and constructions have been proposed. In this paper we begin by reviewing existing notions of security and propose new and stronger security definitions. We then present two constructions that we show secure under our new definitions. Interestingly, in addition to satisfying stronger security guarantees, our constructions are more efficient than all previous constructions. Further, prior work on SSE only considered the setting where only the owner of the data is capable of submitting search queries. We consider the natural extension where an arbitrary group of parties other than the owner can submit search queries. We formally define SSE in this multi-user setting, and present an efficient construction.

PROBLEM STATEMENT

The multi-keyword search schemes can realize many multi-keyword search related functions such as conjunctive keyword search, disjunctive keyword search and subset search. Ballardetal. Proposed [10] two different conjunctive keyword search schemes, which only return the files containing all the searched keywords, on the basis of Shamir secret sharing and bilinear pairings, respectively. Their scheme is proven secure in the standard model. And disjunctive keyword search scheme was proposed in later, which can return files containing the subset of query keywords. Meanwhile predicate encryption schemes were also presented in order to support both conjunctive keyword search and disjunctive keyword search.

3.1 DISADVANTAGES

The data owner has to rebuild the search index tree, which is time-consuming.Traditional solutions have to suffer high computational costs

PROPOSED SYSTEM

We will propose a secure and effective multi-keyword ranked search scheme supporting update operations efficiently. The index tree based on Bloom filter will be designed to improve the search efficiency. And our scheme utilizes vector space model to build an index vector for every file in the outsourcing dataset. The cosine similarity measure is used to compute the similarity score of one file to the search query and TF×IDF weight will be used to improve the search accuracy.

SYSTEM ARCHITECTURE

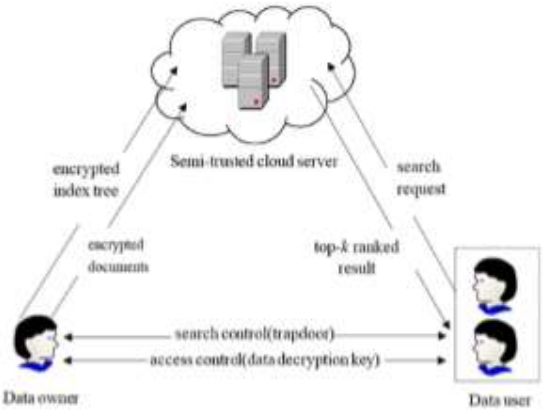


FIGURE 1. Architecture of the search over encrypted cloud data.

IMPLEMENTATION

6.1 OWNER

In this application the owner is one of the main module for uploading the files and view the uploads file which are uploaded by the owner before do all these operations the owner should register with the application and the owner should authorized by the cloud.

6.2 USER

In this application the user also a modules to perform the bloom filter operation to access the files from the cloud, before do the search operations the user should get the search permission from the cloud then only the user can search the files after get the details of the searched file, if the user want to download the user should get the trapdoor key from the trapdoor Generator, then the user can able to download the file.

To do all these operation the user should register with application and the user should accessed by the cloud.

6.3 TRAPDOOR GENERATOR

The trapdoor is used to generate the trapdoor key for the requested users.Here the trapdoor should login directly with the application.

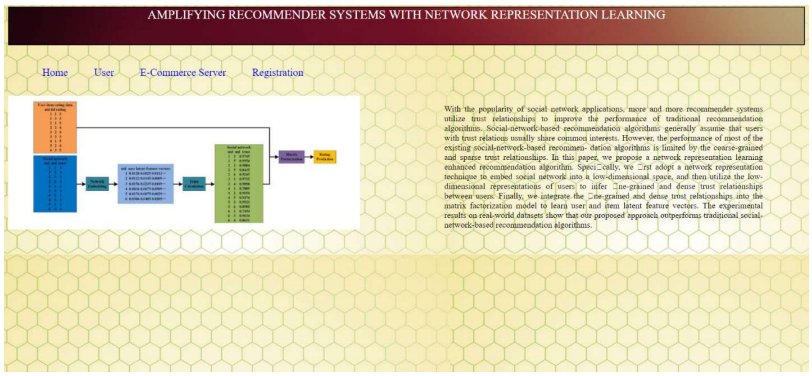
6.4 CLOUD

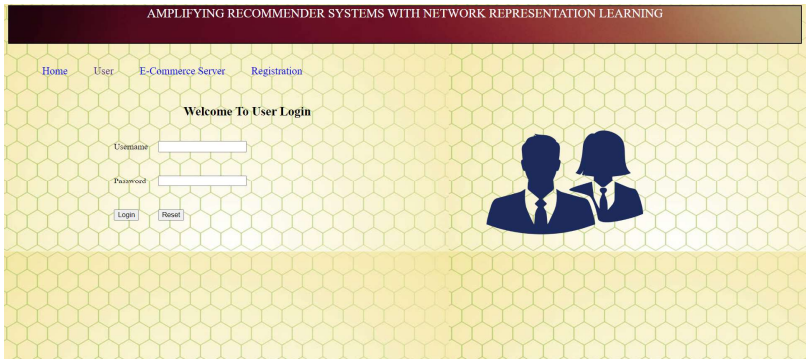
The cloud is the main module to operate this project in the users activation s , owner activation and also the cloud can check the following operations like search permission provides to the users, can check the top-k searched keyword, top-k similarity in chart, top-k searched keyword in chart.Primarily the cloud should login. Then only the cloud can perform the above mentioned actions.\

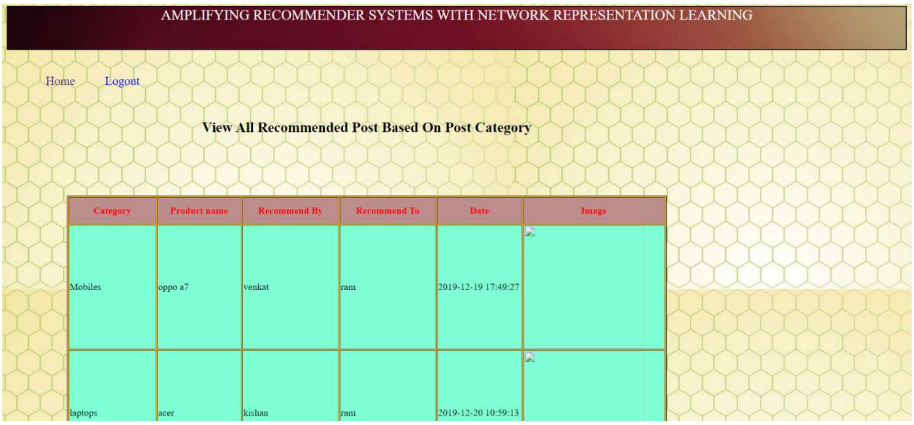
6. 5 ATTACKER

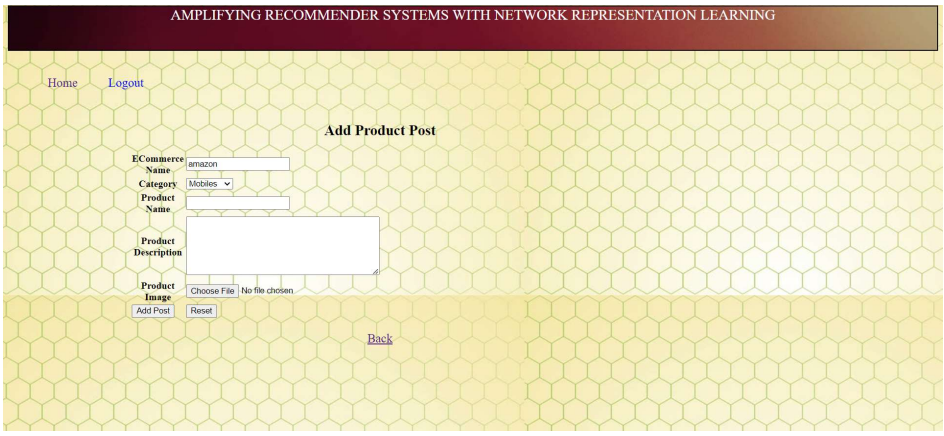
The attacker is the unauthorized perform to attack the owner files.

1. OUTPUT EXPERIMENTS









CONCLUSION

Traditional social-network-based recommendation algorithms generally utilize the coarse-grained trust relationships to generate recommendations, which seriously hinders the performance of recommendation algorithms. To tackle this problem, we proposed a network representation learning enhanced recommendation algorithm in this study. Specically, we _rst adopt a network representation learning technique to embed a social network into a low dimensional space, and then utilize the low-dimensional representations of users to infer _ne-grained dense trust relationships between them. Finally, we integrate the _ne-grained dense trust relationships into the classic matrix factorization model to learn latent user and item feature vectors. Experimental results on real-world datasets show that our proposed approach out- performs traditional social-network-based recommendation algorithms.

REFERENCES

[1] G. Adomavicius and A. Tuzhilin, ``Toward the next generation of recom-mender systems: A survey of the state-of-the-art and possible extensions,"*IEEE Trans. Knowl. Data Eng.*, vol. 17, no. 6, pp. 734_749, Jun. 2005.

2] J. S. Breese, D. Heckerman, and C. Kadie, *Empirical Analysis of PredictiveAlgorithms for Collaborative Filtering*. Burlington, MA, USA: MorganKaufmann, 1998, p. 18.

[3] H. Ma, H. Yang, M. R. Lyu, and I. King, ``SoRec: Social recommen-dation using probabilistic matrix factorization," in *Proc. CIKM*, 2008,pp. 931_940.

[4] H. Ma, I. King, and M. R. Lyu, ``Learning to recommend with social trustensemble," in *Proc. SIGIR*, 2009, pp. 203_210.

[5] M. Jamali and M. Ester, ``A matrix factorization technique with trustpropagation for recommendation in social networks," in *Proc. RecSys*,2010, pp. 135_142.

[6] B. Yang, Y. Lei, D. Liu, and J. Liu, ``Social collaborative _ltering by trust,"in *Proc. IJCAI*, 2013, pp. 2747_2753.

[7] J. Tang, M. Qu, M. Wang, M. Zhang, J. Yan, and Q. Mei, ``LINE: Large-scale information network embedding," in *Proc. 24th Int. World Wide WebConf. Steering Committee*, 2015, pp. 1067_1077

[8] P. Resnick, N. Iacovou, M. Suchak, P. Bergstrom, and J. Riedl,``GroupLens: An open architecture for collaborative _ltering of netnews,"in *Proc. CSCW*, 1994, pp. 175_186.

[9] G. Linden, B. Smith, and J. York, ``Amazon.com recommendations: Item-to-item collaborative _ltering," *IEEE Internet Comput.*, vol. 7, no. 1,pp. 76_80, Jan./Feb. 2003.

[10] B. M. Sarwar, G. Karypis, J. A. Konstan, and J. Riedl, ``Item-basedcollaborative _ltering recommendation algorithms," in *Proc.WWW*, 2001,pp. 285_295.

