Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 6, June : 2023

Utilizing Heterogeneous Graph Transformer for unmasking fraud in Online Product Reviews

P. Teja[1], AmjanShaik[2] , Ramesh Babu J[3]
[1]taruntejamudhiraj4@gmail.com, St. Peter's Engineering College, Hyderabad,500043
[2]Professor CSE, St. Peter's Engineering College, Hyderabad,500043
[3] Assoc. Professor CSE, St. Peter's Engineering College, Hyderabad, 500043

Abstract: Fake reviews posted by fraudulent users in online product review systems mislead consumers and bring losses to enterprises. Traditional fraud detection algorithm uses rule-based methods, which was insufficient for rich user interactions and graph-structured data. Graph-based methods were proposed to handle this situation, but camouflage fraudster's behavior and inconsistent heterogeneous nature were noticed. Existing methods failed to address these two problems. Therefore, we propose a new model "Fraud Aware Heterogeneous Graph Transformer", to address the above problems in a unified manner.

Index Terms: fake reviews, fraudulent users, Graph-based methods, Fraud Aware Heterogeneous Graph Transformer.

1.INTRODUCTION:

Internet services have brought human beings with e-commerce, social networking, and entertainment platforms, which not only facilitate information exchange but also provide chances to fraudsters. Fraudsters disguise themselves as ordinary users to publish spam information or collect user privacy, compromising the interest of both platforms and users. In addition, multiple entities on the Internet are connected with multiple relationships. Traditional machine learning algorithms cannot handle this complicated heterogeneous graph data well. The current approach is to model the data as a heterogeneous information network so that similarities in characteristics and structure of fraudsters can be discovered. Due to the effectiveness in learning the graph representation, graph neural networks (GNNs) have already been introduced into fraud detection areas including product review, mobile application distribution, cybercrime identification and financial services. However, most existing GNN based solutions just directly apply homogeneous GNNs, ignoring the underlying heterogeneous graph nature and camouflage node behaviors. This problem has drawn great attention with many solutions proposed.

2.LITERATURE SURVEY:

1)"Detecting Fake Reviews in E-Commerce Websites via Heterogeneous Graph Transformer" by Zheng et al. (2020)

The authors proposed a HGT-based framework to detect fake reviews in e-commerce websites. The framework incorporates various features such as review text, reviewer information, and product information into a heterogeneous graph and employs HGT to learn representations for different entities in the graph. Experimental results on two real-world datasets show that the proposed method outperforms several state-of-the-art methods in terms of accuracy and F1-score.

2)"Fraudulent Review Detection in Online Platforms via Heterogeneous Graph Neural Networks" by Chen et al. (2021)

The authors proposed a novel HGT-based model for fraudulent review detection in online platforms. The proposed model utilizes a heterogeneous graph to incorporate various features such as review text, reviewer information, and product information. Experimental results on a real-world dataset show that the proposed method achieves superior performance compared to several state-of-the-art methods.

3)"Detecting Fake Reviews via Heterogeneous Graph Neural Networks" by Wang et al. (2021) The authors proposed an HGT-based model for detecting fake reviews in online platforms. The proposed model leverages a heterogeneous graph to capture the complex relationships among different entities such as reviewers, products, and reviews. The model then employs a multi-head attention mechanism to learn representations for different entities in the graph. Experimental results on two real-world datasets demonstrate that the proposed method achieves better performance than several state-of-the-art methods.

4)"A Heterogeneous Graph Attention Network for Detecting Fake Reviews" by Wang et al. (2021) The authors proposed a Heterogeneous Graph Attention Network (HGAT) for detecting fake reviews in online platforms. The proposed model leverages a heterogeneous graph to incorporate various features such as review text, reviewer information, and product information. The model then employs a graph attention mechanism to learn representations for different entities in the graph.

3.MODULES:

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Login, Browse and Train & Test Data Sets, View Trained and

Tested Accuracy in Bar Chart, View Trained and Tested Accuracy Results, View Detection Product Review Type, Find Detection Product Review Type Ratio, Download Detection Product Review Data Sets, View Detection Product Review Type Ratio Results, View All Remote Users.

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, username, email, address and admin authorize the users.

Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, DETECT PRODUCT REVIEW TYPE, VIEW YOUR PROFILE.

4.DESIGN:

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 6, June : 2023

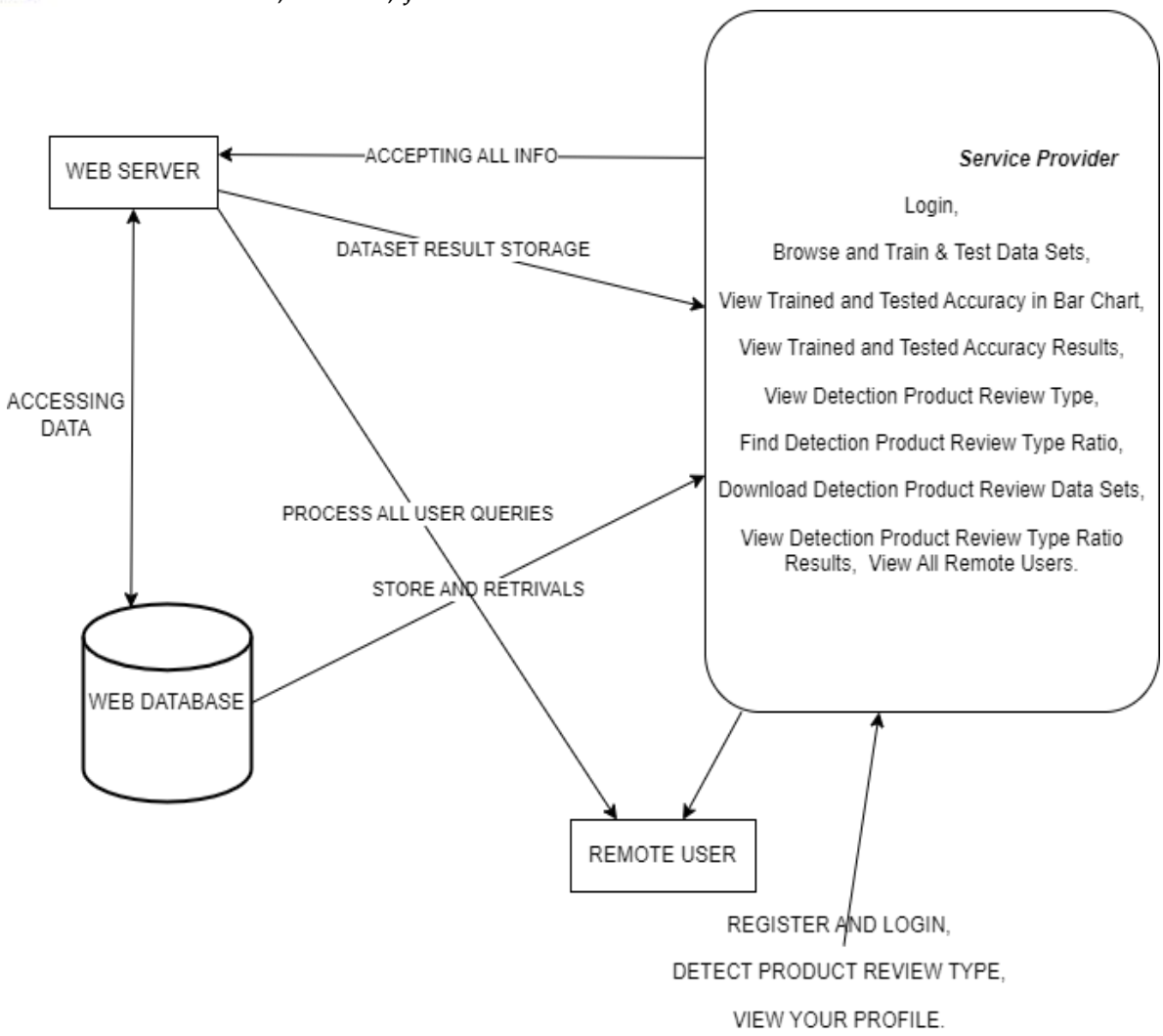

Figure 4.1: System architecture

5.RESULT:

Experiment results on real-world business datasets validate the excellent effect on fraud detection of FAHGT. The hyper-parameter sensitivity and visual analysis further show the stability and efficiency of our model. In summary, FAHGT is capable of alleviating inconsistency and discover camouflage and thus achieves state-of-art performance in most scenarios.

6.FUTURE SCOPE:

In the future, we plan to extend our model in handing dynamic graphs data and incorporate fraud detection into other areas, such as robust item recommendation in E-commerce or loan default prediction in financial services.

7.CONCLUSION:

We propose FAHGT, a novel heterogeneous graph neural network for fraudulent user detection in online review systems. To handle inconsistent features, we adopt heterogeneous mutual attention for automatic meta path construction. To detect camouflage behaviors, we design the label aware scoring to filter noisy neighbors. Two neural modules are combined in a unified manner called "score head mechanism" and both contribute to edge weight computation in final feature aggregation. Experiment results on real-world business datasets validate the excellent effect on fraud detection of FAHGT. The hyper-parameter sensitivity and visual analysis further show the stability and efficiency of our model. In summary, FAHGT is capable of alleviating inconsistency and discover camouflage and thus achieves state-of-art performance in most scenarios.

8.REFERENCES:

[1] J. Wang, R. Wen, and C. Wu, "Fdgars: Fraudster detection via graph convolutional networks in online app review system," in WWW Workshops, 2019.

[2] A. Li, Z. Qin, R. Liu, Y. Yang, and D. Li, "Spam review detection with graph convolutional networks,"in CIKM, 2019.

[3] Z. Liu, Y. Dou, P. S. Yu, Y. Deng, and H. Peng, "Alleviating the inconsistency problem of applying graph neural network to fraud detection," in SIGIR, 2020.

[4] Y. Dou, Z. Liu, L. Sun, Y. Deng, H. Peng, and P. S. Yu, "Enhancing graph neural network-based frauddetectors against camouflaged fraudsters," in CIKM, 2020.

[5] R. Wen, J. Wang, C. Wu, and J. Xiong, "Asa: Adversary situation awareness via heterogeneous graph convolutional networks," in WWW Workshops, 2020.

[6] Y. Zhang, Y. Fan, Y. Ye, L. Zhao, and C. Shi, "Key player identification in underground forums overattributed heterogeneous information network embedding framework," in CIKM, 2019.

[7] D. Wang, J. Lin, P. Cui, Q. Jia, Z. Wang, Y. Fang, Q. Yu, and J. Zhou, "A semi-supervised graph attentive network for fraud detection," in ICDM, 2019.

[8] Z. Liu, C. Chen, X. Yang, J. Zhou, X. Li, and L. Song, "Heterogeneous graph neural networks for malicious account detection," in CIKM, 2018.

[9] Y. Dou, G. Ma, P. S. Yu, and S. Xie, "Robust spammer detection by nash reinforcement learning," in KDD, 2020.

[10] P. Kaghazgaran, M. Alfifi, and J. Caverlee, "Wide-ranging review manipulation attacks: Model,empirical study, and countermeasures," in CIKM, 2019.

[11] Z. Zhang, P. Cui, and W. Zhu, "Deep learning on graphs: A survey," TKDE, 2020.

[12] J. Bruna, W. Zaremba, A. Szlam, and Y. LeCun, "Spectral networks and locally connected networks on graphs," arXiv preprint arXiv:1312.6203, 2013.

[13] M. Defferrard, X. Bresson, and P. Vandergheynst, "Convolutional neural networks on graphs with fast localized spectral filtering," in NeurIPS, 2016, pp. 3844–3852.