As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 7(12): 225-229, 2021

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0712044
Available online at: http://www.ijmtst.com/vol7issue12.html

False Reviews in Online Product Review Systems using Heterogeneous Graph Transformer

Mory Keita[1], Dr.R.Tamilkodi[2] and N.Durga Devi[3]

[1]PG Student, Dept of CA, Godavari Institute of Engineering and Technology(Autonomous),Rajahmundry, AP
[2]Professor, Dept of CA, Godavari Institute of Engineering and Technology(Autonomous),Rajahmundry, AP
[3]Assistant Professor, Dept of CA, Godavari Institute of Engineering and Technology(Autonomous),Rajahmundry, AP

To Cite this Article
Mory Keita, Dr.R.Tamilkodi and N.Durga Devi. False Reviews in Online Product Review Systems using Heterogeneous Graph Transformer. *International Journal for Modern Trends in Science and Technology* 2021, *7* pp. 225-229. https://doi.org/10.46501/IJMTST0712044

Article Info
Received: 12 November 2021; Accepted: 05 December 2021; Published: 16 December 2021

ABSTRACT

It is possible to leave reviews for products or services you have bought through online product review platforms. Customers are often duped and businesses suffer as a result of false reviews that have been submitted by dishonest people. As a result of the complexity of user interactions and the structure of graph-structured data, traditional fraud detection algorithms are unable to cope. In recent years, graph-based solutions have been presented to deal with this scenario, however few earlier research have observed the camouflage fraudster's behaviour and inconsistencies diverse nature. A lack of attention to these two issues has resulted in poor performance from existing approaches. Fraud Aware Heterogeneous Graph Transformer (FAHGT) is proposed as an alternative paradigm to deal with camouflages and inconsistencies together. For heterogeneous graph data, FAHGT employs a type-aware feature mapping technique that uses multiple relation scoring algorithms to relieve inconsistencies and uncover camouflage. Neighbors' characteristics are combined to provide an informative depiction. When applied to real-world datasets, experimental findings show that FAHGT outperforms the currently available baselines.

KEYWORDS: FAHG, Fraud Detection, GNN, Data Mining

1. INTRODUCTION

E-commerce, social networking, and other types of online entertainment made possible by Internet service providers have created new opportunities for scammers. In order to post spam or acquire user data, fraudsters appear to be genuine users. Consequently, there are a large number of connections between Internet companies. Traditional machine learning methods are incapable of analysing data in graph form. Current methods use a network-based approach to identify fraudsters' features and structure by analysing the data. GNNs have been used in a variety of industries, including product evaluation, mobile application distribution, cybercrime detection, and financial service fraud detection. As a result, most current GNN-based solutions only employ homogeneous GNNs and ignore the network's topology and hidden node properties. A number of approaches to this issue have been proposed, including [4], [5], and [10]. Fraud detection has three inconsistencies, according to GraphConsis [4], and two camouflage behaviours have been provided by CAREGNN. [5] What you need to know about these issues: A generative language model may be used to generate domain-independent bogus reviews [11] for crowd workers who associate with trustworthy persons [3], [6],

or [11] [3] [6]. When two people with different interests get together over a shared passion, such as cuisine or movies, they may develop a connection that transcends their differences. Individual user habits cannot be seen because of the way the data is pooled. When two people have a same interest, it is more probable that they will feel distrustful of one other as a result of this commonality.

2. PROPOSED SYSTEM

Similarity scores between node embeddings do not differentiate between various kinds of nodes, hence they are used to solve the inconsistency issue. For GNN-based fraud detection, CAREGNN adds an adaptive neighbour selection and relation aware aggregater to better combat hidden fraudsters. The graph's heterogeneity is still affecting its performance. FaHGT is introduced in this research, where we present a label-aware neighbour selector to handle the camouflage problem and a heterogeneous mutual attention to resolve the inconsistency issue. Known as the "score head mechanism," this method unifies the two methods of implementation. FAHGT's usefulness and efficiency have been shown on a variety of real-world datasets. There is evidence that FAHGT can outperform current GNNs in terms of KS and AUC, and GNN-based fraud detectors.

3. PROPOSED SYSTEM ARCHITECTURE

In order to access administrative functions, you'll need a working account and password. In order to carry out certain actions such as viewing and authorising users, adding and viewing categories and subcategories, he must first successfully log in to the system. To this list, please add: a list of the most popular products, Analyze product reviews for any fraudulent activity, look at user search history, see product rankings and comments, or look at user search activity. An administrator may use this module to see a list of all users and grant them access to the admin area.There are n people in the room at any one time. ' Users should first log in and set up an account before attempting any actions. Assuming his registration was successful, he will be able to log in using his legitimate user name and password. Once he's logged in, he'll proceed to do various tasks. Register and Login, My Profile, Search Products & Give Review, View Top Products, My Search History are all available to registered users.

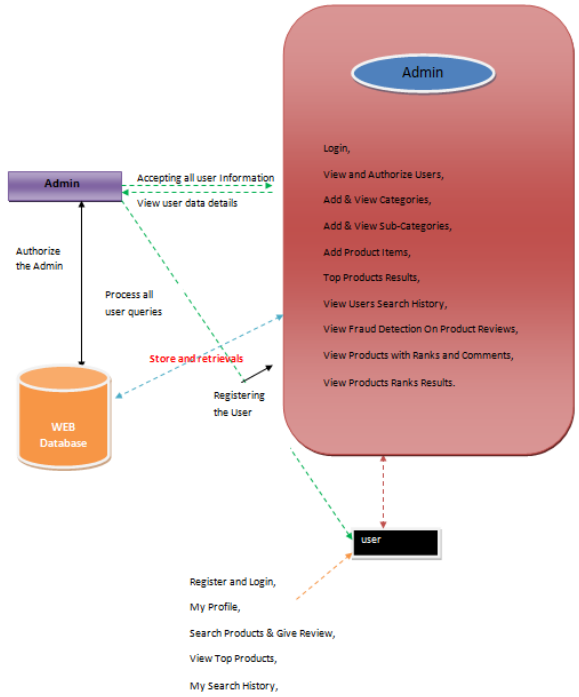

Fig.1: System Architecture

4. EXPERIMENTAL RESULTS

Admin has to login with valid username and password. After login successful he can do some operations such as View and Authorize Users,Add & View Categories, Add & View Sub-Categories, Add Product Items, Top Products Results,View Users Search History,View Fraud Detection On Product Reviews, View Products with Ranks and Comments, View Products Ranks Results. The administrator checks all of the user's information before granting them access to the system. User Name, Address, Email Id, and Phone Number. There are n number of users in the user. Before attempting to accomplish anything, a user must first register. On order to log in, he must provide a user name and password that are both genuine. Some actions will be carried out after a successful login. My Profile, Search Products & Give Reviews, View the Top Products, My Search History, and Register and Login. This includes the user's name and contact information, as well as their profile picture.

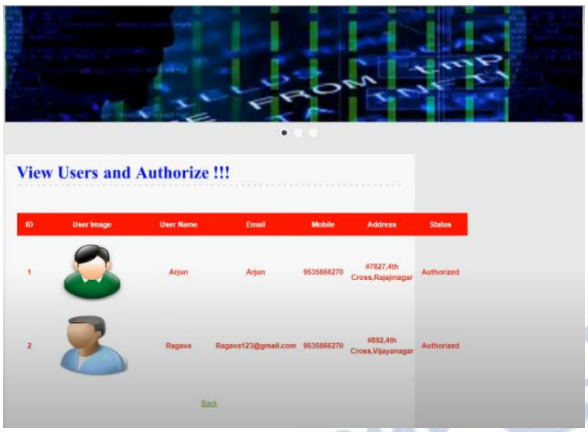

Fig5.1:View Users and Authorize

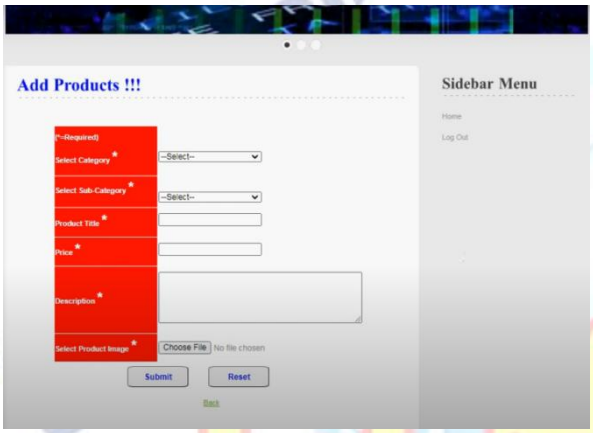

Fig5.2: Add Products

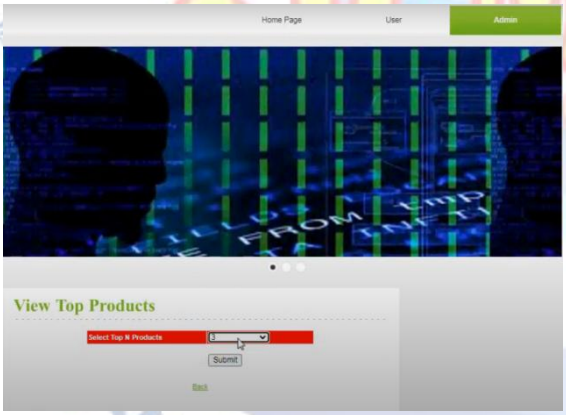

Fig5.3: View Top Products

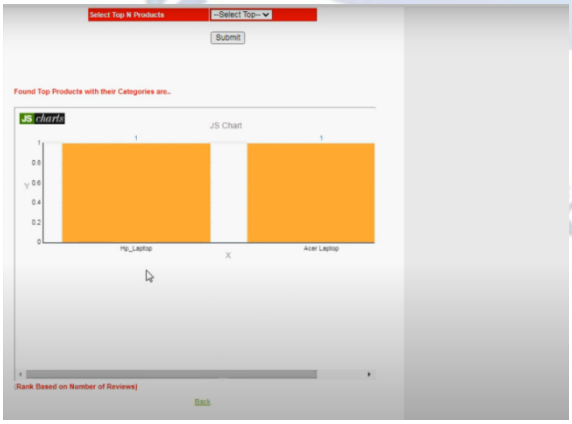

Fig5.4: Top Products with their Category

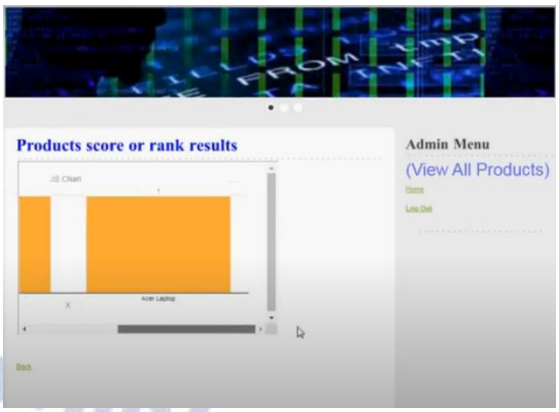

Fig5.5: Products Score Rank Results

Fig5.6: View Review Status

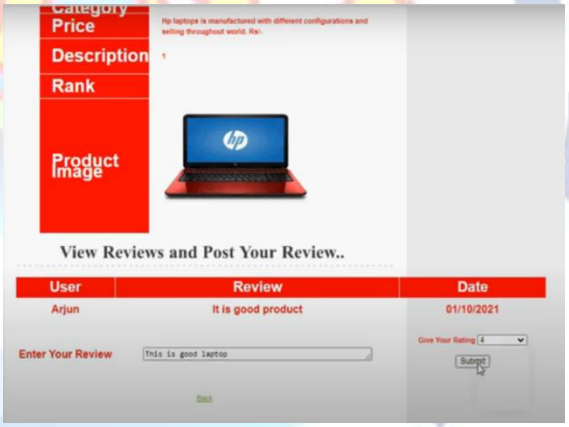

Fig5.7: View Reviews and Post Reviews

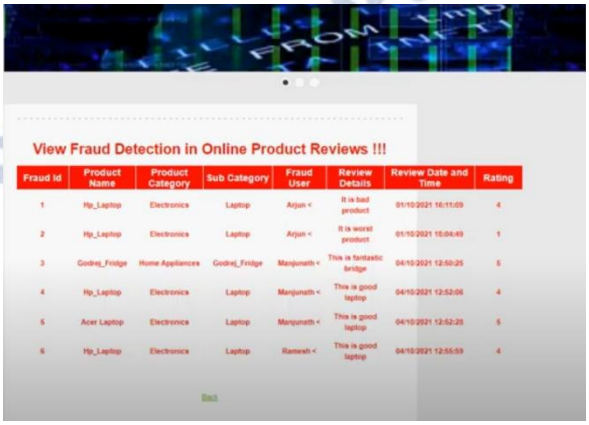

Fig5.8: Fraud Detection in Product Reviews

5. COMPARATIVE STUDY

Using three separate datasets, FAHGT was compared to three different baselines and the findings are shown in Table 1. Using the data, it is evident that FAHGT is superior to the other treatments. Network structure and neighbor qualities are both helpful in fraudster prediction, notwithstanding the poor results of logistic regression. GraphSAGE, GCN, GAT, and all GNN baselines in Table 1 use the same homogenous graph and treat all relationships equally. Additional baselines are also examined in multi-relational graphs. Because the results of homogeneous GNNs are equivalent to those of multi-relation approaches like GraphConsis and SemiGNN, previously recommended graph-based fraud detectors are not suited for heterogeneous networks. Single and multi-relation GNNs both suffer from poor performance if node properties are aggregated into several kinds. FAHGT and its variations can better identify camouflage behavior, remove unnecessary nodes, and better manage heterogeneous network information by integrating information from nodes that are aware of their type and label. In addition to FAHGT and its offshoots, as well.

Table1: Overall Result the Performance of FAHGT and Various Baselines on Three Datasets

Dataset	Baby			Musical Instruments			Automotive		
Model	F1	KS	AUC	F1	KS	AUC	F1	KS	AUC
LR	50.84	61.41	86.72	73.20	67.05	89.18	48.14	47.92	80.35
GCN	55.20	60.97	87.13	74.60	68.68	91.00	52.67	51.31	81.90
GAT	57.48	63.73	88.25	74.61	70.11	91.16	56.90	49.95	81.43
GraphSAGE	58.50	64.67	89.10	71.63	68.97	91.14	61.55	50.62	83.11
GeniePath	60.58	64.14	89.16	73.83	70.54	90.80	59.93	49.14	80.82
SemiGNN	65.40	65.52	88.88	74.73	69.77	91.23	46.77	54.80	84.12
GraphConsis	60.64	64.37	88.58	74.07	68.58	90.85	56.41	52.98	84.19
CAREGNN	61.66	46.37	79.50	59.59	54.09	82.62	44.82	45.81	77.30
FAHGT-l	61.55	63.82	88.67	74.67	68.84	90.02	58.19	51.76	82.96
FAHGT-h	62.91	65.23	89.25	74.25	71.26	91.49	**61.85**	**55.48**	84.24
FAHGT	**65.58**	**67.37**	**90.69**	**76.14**	**71.41**	**91.61**	58.85	53.85	**85.09**

6. CONCLUSION

A unique heterogeneous graph neural network (FAHGT) is proposed for the identification of fraudulent users in online review platforms. Using heterogeneous mutual attention for autonomous meta route creation is the best way to manage inconsistent features. The label aware scoring is designed to filter out loud neighbours in order to discover camouflage activities. For the final feature aggregation, the "score head mechanism" combines two neural modules, they are both used in the final feature summary to calculate edge weight. It has been shown via experiments on actual commercial data that FAHGT is quite effective at detecting fraud.. As shown by the hyper-parameter sensitivity and visual examination, our model is very reliable. Finally, FAHGT can reduce inconsistency and discover concealment, leading to best-in-class performance in most situations. In the future, we'd want to extend our model to handle dynamic graphs data and identify fraud in other industries, such as robust item suggestion in E-commerce or loan default prediction in financial services.

REFERENCES

[1] V. S. Tseng, J. Ying, C. Huang, Y. Kao, and K. Chen, "Fraudetector: A graph-mining-based framework for fraudulent phone call detection," in Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Sydney, NSW, Australia, August 10-13, 2015, L. Cao, C. Zhang, T. Joachims, G. I. Webb, D. D. Margineantu, and G. Williams, Eds. ACM, 2015, pp. 2157–2166.[Online]. Available: https://doi.org/10.1145/2783258.2788623

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

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

[4] 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.

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

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

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

[8] 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.

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

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

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

[12] Z. Zhang, P. Cui, andW. Zhu, "Deep learning on graphs: A survey," TKDE, 2020.

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

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

[15] T. Kipf and M. Welling, "Semi-supervised classification with graph convolutional networks," in ICLR, 2017.

[16] W. Hamilton, Z. Ying, and J. Leskovec, "Inductive representation learning on large graphs," in NeurIPS, 2017.

[17] P. Veli˘ckovi´c, G. Cucurull, A. Casanova, A. Romero, P. Lio, and Y. Bengio, "Graph attention networks," in ICLR, 2017.

[18] X. Wang, H. Ji, C. Shi, B. Wang, Y. Ye, P. Cui, and P. S. Yu, "Heterogeneous graph attention network," in WWW, 2019, pp. 2022–2032.

[19] S. Zhou, J. Bu, X. Wang, J. Chen, and C. Wang, "Hahe: Hierarchical attentive heterogeneous information network embedding," arXiv preprint arXiv:1902.01475, 2019.

[20] S. Wang, Z. Chen, D. Li, Z. Li, L.-A. Tang, J. Ni, J. Rhee, H. Chen, and P. S. Yu, "Attentional heterogeneous graph neural network: Application to program reidentification," in Proceedings of the 2019 SIAM International Conference on Data Mining. SIAM, 2019, pp. 693–701.

[21] Y. Zhang, Y. Xiong, X. Kong, S. Li, J. Mi, and Y. Zhu, "Deep collective classification in heterogeneous information networks," in Proceedings of the 2018 World Wide Web Conference, 2018, pp. 399–408.

[22] C. Zhang, D. Song, C. Huang, A. Swami, and N. V. Chawla, "Heterogeneous graph neural network," in KDD, 2019, pp. 793–803.

[23] Z. Hu, Y. Dong, K.Wang, and Y. Sun, "Heterogeneous graph transformer," in WWW, 2020, pp. 2704–2710.

[24] G. Wang, S. Xie, B. Liu, and S. Y. Philip, "Review graph based online store review spammer detection," in ICDM. IEEE, 2011, pp. 1242–1247.

[25] W. Yu, W. Cheng, C. C. Aggarwal, K. Zhang, H. Chen, and W. Wang, "Netwalk: A flexible deep embedding approach for anomaly detection in dynamic networks," in KDD, 2018, pp. 2672–2681.