International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IJIEMR Transactions, online available on 12th Dec 2021. Link :http://www.ijiemr.org/downloads.php?vol=Volume-10&issue=Issue 12

DOI: 10.48047/IJIEMR/V10/ISSUE 12/15

Title **Analysis of High-Density Rating and Co-Visit Behaviors for Malicious Injection Attacks**

Volume 10, ISSUE 12, Pages: 77-85

Paper Authors

Kiran Kumar Polu , Dr. J. Suresh Babu

Analysis of High-Density Rating and Co-Visit Behaviors for Malicious Injection Attacks

Kiran Kumar Polu , Dr. J. Suresh Babu

Abstract_E-commerce, financial transaction platforms, and even social networks all make use of personalised recommender systems. The ratings and reviews provided by users are helpful for other users to gain a more in-depth review of the products, and they are also helpful for online businesses to make focused improvements on the products. However, recommender systems are inherently open and vulnerable, making them susceptible to manipulation by malevolent users. However, improving the detection performance for defending malicious threats like profile injection attacks and co-visitation injection attacks is hampered by three difficult issues: (1) the coexistence of different types of malicious attacks in real-world data; (2) the difficulty of striking a balance between the commonalities and specialisations of rating behaviours in terms of accurate detection; and (3) the similarity in rating behaviours between attackers and anchor users that result from the consistency of attack intent. Throughout this paper, we differentiate malicious injection behaviours for recommender systems using a unified detection technique we call IMIA-HCRF. First, the building of an association graph and the strengthening of dense behaviours, both of which may be modified to diverse threats, are implemented to empirically eliminate disrupted data. Then, higher order potentials are used to further segment the continuous boundary of dense rating (or co-visitation) behaviours, which is then used to define the relevant injection behaviours. The proposed IMIA-HCRF has been shown to exceed all baselines on a variety of criteria through extensive experimentation on both synthetic and real-world data. IMIA-detection HCRF's performance improves upon the baselines in terms of FAR (false alarm rate) while maintaining the maximum DR by 7.8% for mixed profile injection assaults and by 6% for mixed co-visitation injection attacks (detection rate). In addition, testing with real-world data demonstrate that IMIA-HCRF outperforms the baselines by an average of 11.5% in FAR.

1.INTRODUCTION

Sites like Amazon, TripAdvisor, YouTube, TaoBao, etc. all use personalised recommender systems to help users find content and services that are a good fit for them, whether that's clothing or a hotel room [1, 2]. In particular, in the last two decades [1], collaborative recommendation techniques (crts) such as ubcf, ibcf, co-visitation based, etc., have been created. To put it simply, crts count on the fact that users who have previously shown affinity for one another will continue to do so in the future. As a result of their transparency and inherent weaknesses [4]-[6], [7] and false co-visitation injection attacks [3] crts are extremely susceptible to profile injection attacks (also known as shilling attacks]. Figure 1 shows how malicious actors can manipulate recommendations (shaking consumers' confidence) or lower the quality of recommnedations by injecting a sufficient number of well-designed fake profiles (e.g., ratings and reviews) into the systems and empirically rating higher scores (termed push or promotion attacks [9]) or lower scores (called nuke or demotion attacks [9]) toward targeted items. The public is severely harmed by these types of attacks, and business owners and consumers alike lose faith as a result. As a result, there is a growing need to safeguard the privileges of individual users.

2.LITERATURE SURVEY

2.1 G. Adomavicius and A. Tuzhilin, "Toward the next generation of recommender 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.

In this work, we provide an introduction to recommender systems and discuss the latest generation of recommendation algorithms, which can be broadly categorised into three subfields: content-based, collaborative, and hybrid. In addition to outlining the many ways in which conventional recommendation methods fall short, this study explores how they may be expanded upon to increase recommendation efficacy and expand the scope of use for recommender systems. These enhancements allow for better user and item comprehension, contextual information integration, multi-criteria rating support, and more adaptable, less obtrusive recommendations.

2.2 X. Luo, M. Zhou, Y. Xia, Q. Zhu, A. C. Ammari, and A. Alabdulwahab, "Generating highly accurate predictions for missing QoS data via aggregating nonnegative latent factor models," IEEE Trans. Neural Netw. Learn. Syst., vol. 27, no. 3, pp. 524–537, Mar. 2016

In the field of service computing, automatically selecting Web services is a hot topic. Accurate QoS forecasts from previously invoked services are crucial to end users at this stage. Through the development of an ensemble of nonnegative latent factor (NLF) models, this work seeks to provide extremely accurate forecasts for missing QoS data. The reasons for this are as follows: 1) the satisfaction of nonnegativity constraints can more accurately represent the value-adding aspect of QoS data, hence improving prediction accuracy; and 2) Given that QoS prediction is a learning activity, it's possible that a well-designed ensemble model might help enhance forecast accuracy even further. First, we put into action an NLF model for estimating quality of service. Next, a diversified NLF model is created by sampling features and injecting randomness, and an ensemble is constructed from this model. On two large, real-world data sets, comparison results show that the proposed ensemble can outperform numerous widely used and state-of-the-art QoS predictors in terms of prediction accuracy.

2.3S. Günnemann, N. Günnemann, and C. Faloutsos, "Detecting anomalies in dynamic rating data: A robust probabilistic model for rating evolution," in Proc. 20th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (KDD), 2014, pp. 841–850

Amazon, TripAdvisor, and Yelp are just a few examples of popular review sites. Insights about the development of a product's quality can be gained through a temporal study of rating data, as ratings are not static but are given at different times. Specifically, we answer the following question in this work: Given user ratings for a product or service that have been timestamped, how can we identify patterns in user rating behaviour and periods in which ratings exhibit unusual patterns? We propose a Bayesian model that uses a series of categorical mixture models to represent the ratings data. The input to our method does not need to be aggregated like it is in other approaches; instead, we use the raw time-stamped data. To account for the time-dependent effects of the ratings, the categorical mixtures are constrained: In general, ratings behaviour should evolve gradually over time, with anomalies allowed only during certain time windows. Our approach uses a state space model on the innate parameters of the categorical distributions to automatically detect the periods where anomalies occur and to capture the temporal implications of the general behaviour. An effective approach based on variational inference and dynamic programming is proposed by us for learning our model. We demonstrate the efficacy of our approach and share exciting findings across a variety of real-world datasets in our experimental study.

3.PROPOSED WORK

This work explores a unified detection technique for detecting malicious injection attempts with higher order conditional random fields (named IMIA-HCRF). First, we conduct an empirical study of the distribution of rating and co-visiting behaviours, and then we implement the building of a behaviour association graph and an improvement of dense behaviours to lessen the impact of disturbed data on improving detection performance.

We then investigate unary and pairwise qualities of nodes (users or items) inside the built association graph in an effort to combine topological characteristics of behavioural association linkages while maintaining the advantage of traditional and intrinsic behaviour traits. In particular, higher-order conditional random fields can be used to further divide the continuous boundary between dense and mixed rating behaviours or co-visitation behaviours based on weighted node and link properties. At last, the globally optimal segmentation and suspected items can be used together to identify harmful users and objects.

As a first step, the system suggests a method for improving dense rating (profile injection) behaviours and co-visitation injection behaviours by omitting perturbed data and representing sparse behaviours, which also allows for the possibility of integrated detection of multiple injection attack behaviours.

Second, the method proposes including unary potential and pair wise potential of higher order conditional random fields for informative representations of rating and covisitation behaviours, by looking at features of both nodes and edges of the behaviour association graph.

Third, it learns to spot both profile injection attacks and co-visitation injection assaults using a single, unified detection strategy. The implementation of mixed profile injection attacks and mixed covisitation injection attacks with varying circumstances is also included.

The suggested IMIA-HCRF is superior to the baselines, as shown by the evaluation and analysis of comparative tests on synthetic data and real-world data.

3.1 IMPLEMENTATION

Admin

In this module, the Admin has to login by using valid user name and password. After login successful he can do some operations such as View All Users,AddProducts,View All Posts with Ratings,View All Recommended Posts, View All Friend Request and Response,View All Malicious Injection Attackers,View All

Product Reviews,View search Transaction,View Rating Results.

Add Products Posts

In this module, the admin can add the post by including product name, price, description and corresponding product image.

View all posts

In this module, the admin can view the post by searching keyword and can get all the information about the product like product name, price, description and corresponding product image.

User

In this module, there are n numbers of users are present. User should register before doing some operations. After registration successful he has to login by using authorized user name and password. Login successful he will do some operations like View My Details,Search Friends And Request,View Friend Requests,View All Friends,Search Products, Recommend To Friend, View All Product Recommends,View My Search History.

Searches for good reviews and bad review

In this module, user searches for reviews for the post and can get the following information like product name, price, description and corresponding product image. The user can recommend the product and can give review using sentiment words(such as good or bad product like that) based on brand, Quality, Price.

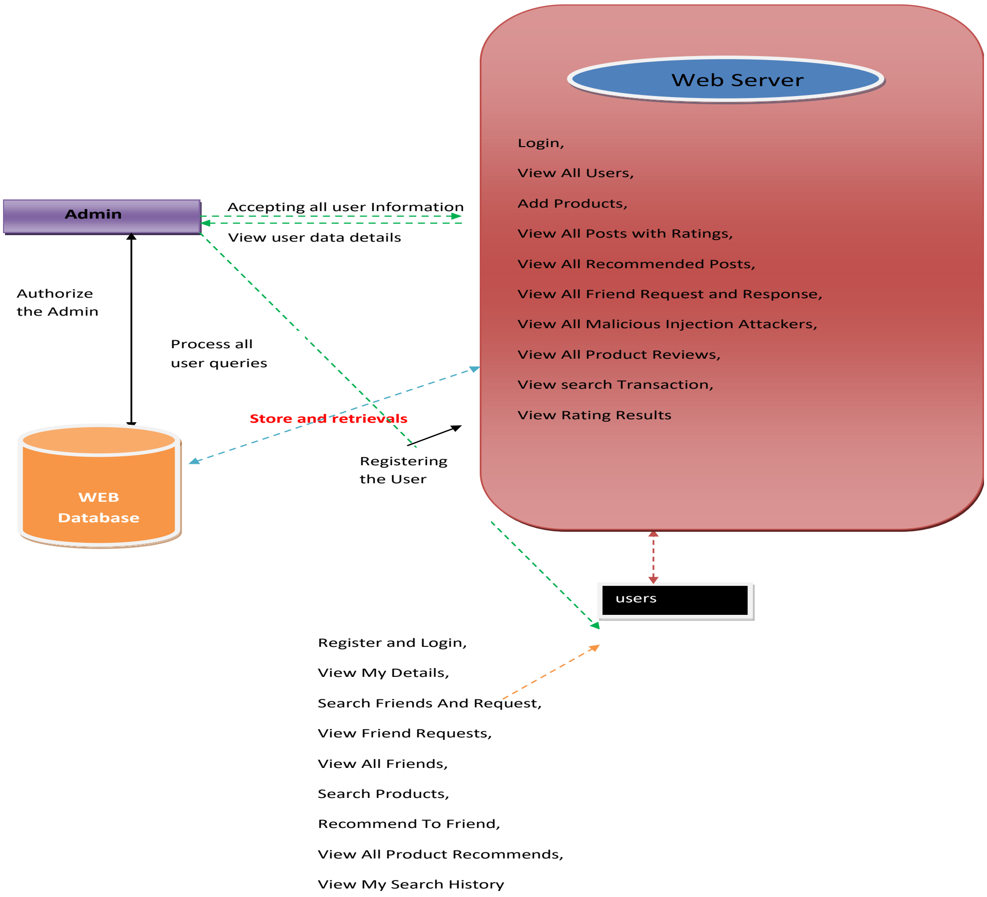
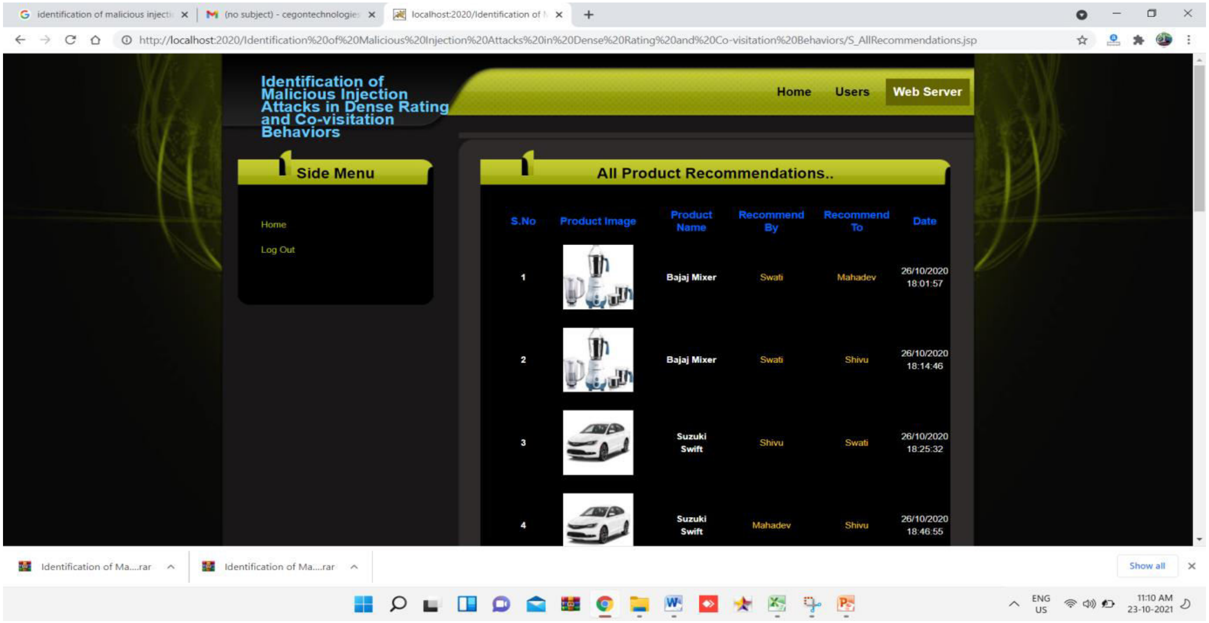


Fig 1:Architecture

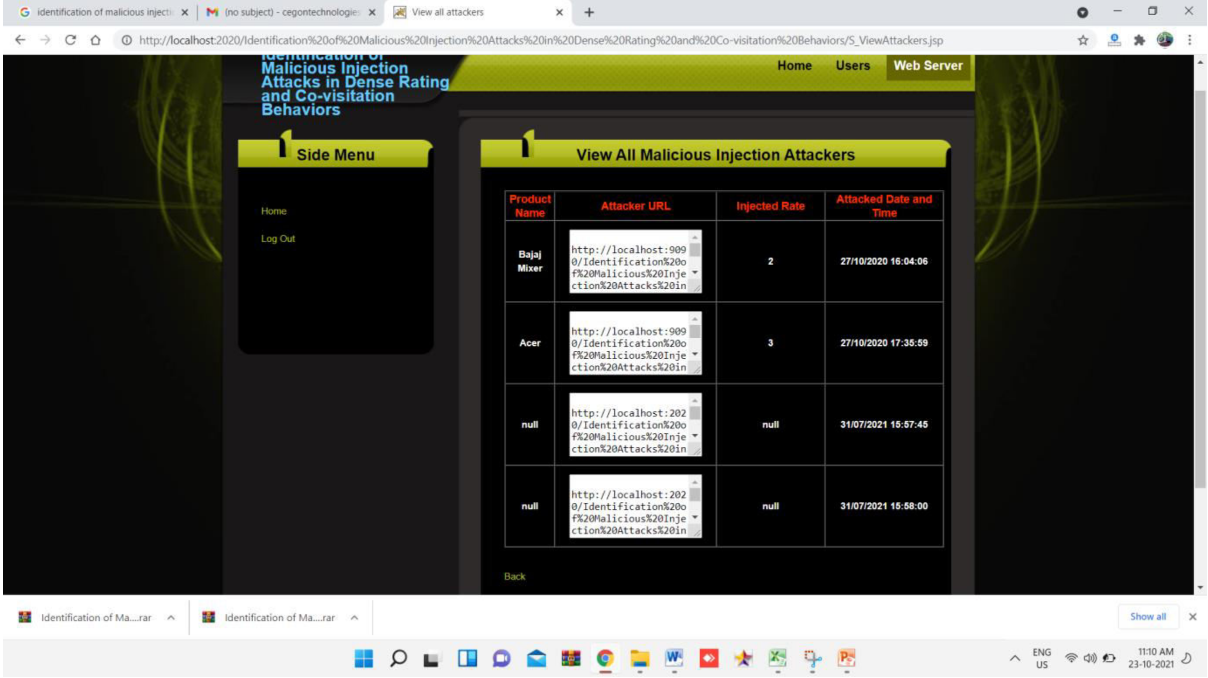
4.RESULTS AND DISCUSSION


identification of malicious injecti
(no subject) - cegontechnologies
localhost:2020/Identification of
http://localhost:2020/Identification%20of%20Malicious%20Injection%20Attacks%20in%20Dense%20Rating%20and%20Co-visitation%20Behaviors/S_AllRecommendations.jsp
Identification of Malicious Injection Attacks in Dense Rating and Co-visitation Behaviors
Home
Users
Web Server
Side Menu
Home
Log Out
Identification of Ma....rar
Identification of Ma....rar
Show all
ENG US
11:10 AM 23-10-2021

All Product Recommendations..

S.No	Product Image	Product Name	Recommend By	Recommend To	Date
1		Bajaj Mixer	Swati	Mahadev	26/10/2020 18:01:57
2		Bajaj Mixer	Swati	Shivu	26/10/2020 18:14:46
3		Suzuki Swift	Shivu	Swati	26/10/2020 18:25:32
4		Suzuki Swift	Mahadev	Shivu	26/10/2020 18:46:55

Fig 1:View All Recommended Products


identification of malicious injecti
(no subject) - cegontechnologies
View all attackers
http://localhost:2020/Identification%20of%20Malicious%20Injection%20Attacks%20in%20Dense%20Rating%20and%20Co-visitation%20Behaviors/S_ViewAttackers.jsp
Identification of Malicious Injection Attacks in Dense Rating and Co-visitation Behaviors
Home
Users
Web Server
Side Menu
Home
Log Out
Back
Identification of Ma....rar
Identification of Ma....rar
Show all
ENG US
11:10 AM
23-10-2021

View All Malicious Injection Attackers

Product Name	Attacker URL	Injected Rate	Attacked Date and Time
Bajaj Mixer	http://localhost:9090/Identification%20of%20Malicious%20Injection%20Attacks%20in	2	27/10/2020 16:04:06
Acer	http://localhost:9090/Identification%20of%20Malicious%20Injection%20Attacks%20in	3	27/10/2020 17:35:59
null	http://localhost:2020/Identification%20of%20Malicious%20Injection%20Attacks%20in	null	31/07/2021 15:57:45
null	http://localhost:2020/Identification%20of%20Malicious%20Injection%20Attacks%20in	null	31/07/2021 15:58:00

Fig 2:View Malicious Injections Attacks

5.CONCLUSION

In this study, we describe a divide-and-conquer approach to identifying profile injection attacks and co-visitation injection attacks against online recommender systems. Experiments conducted on both synthetic and real-world data demonstrate that harmful injection behaviours can be detected by eliminating noisy data, identifying dense behaviours, and performing possible segmentation. Nonetheless, it is far from perfect in terms of protecting against a wide variety of injection attempts and achieving the gold standard (DR of 100% and practically zero FAR).

Therefore, more study is needed before we can rely exclusively on the removal of skewed data and potential segmentation and representation as an online detection strategy. Building a more solid behaviour model of nodes and links, or coming up with a more efficient algorithm with powerful generalisation capacity to reduce behavioural variability, are also potential strategies for improving performance. The other option is to create a discrimination system that is better able to handle dense behaviours.And as new dangers emerge for recommender systems, like data poisoning attacks on factorization-based collaborative filtering [36], poisoning attacks to graph-based recommender systems [37], and adversarial attacks on an oblivious recommender [38], it's important to study how to build a flexible and selective detection framework to protect against these dangers.

REFERENCES

[1] G. Adomavicius and A. Tuzhilin, “Toward the next generation ofrecommender systems: a survey of the state-of-the-art and possibleextensions,” IEEE Transactions on Knowledge and Data Engineering,vol. 17, no. 6, pp. 734–749, 2005.

[2] X. Luo, M. Zhou, Y. Xia, Q. Zhu, A. Ammari, and A. Alabdulwahab,“Generating highly accurate predictions for missing qos-data via aggregatingnon-negative latent factor models,” IEEE Transactions on NeuralNetworks and Learning Systems, vol. 27, no. 3, pp. 524–537, 2016.

[3] G. Yang, N. Gong, and Y. Cai, “Fake co-visitation injection attacksto recommender systems,” Network & Distributed System SecuritySymposium (NDSS), pp. 1–15, 2017.

[4] R. Burke, B. Mobasher, and C. Williams, “Classification features forattack detection in collaborative recommender systems,” InternationalConference on Knowledge Discovery and Data Mining, pp. 17–20, 2006.

[5] N. Gunnemann, S. G□unnemann, and C. Faloutsos, “Robust multivariateautoregression for anomaly detection in dynamic product ratings,” Proceedingsof the 23rd international conference on World Wide Web, pp.361–372, 2014.

[6] S. Gunnemann, N. G□unnemann, and C. Faloutsos, “Detecting anomaliesin dynamic rating data: A robust probabilistic model for rating evolution,”In KDD’2014, pp. 841–850, 2014.

[7] Z. Wu, J. Wu, J. Cao, and D. Tao, “HySAD: A semi-supervised hybridshilling attack detector for trustworthy product recommendation,” InKDD’2012, pp. 985–993, 2012.

[8] M. Fang, N. Gong, and J. Liu, “Influence function based data poisoningattacks to top-n recommender systems,” Proceedings of The WebConference (WWW), pp. 3019–3025, 2020.

[9] I. Gunes, C. Kaleli, A. Bilge, and H. Polat, “Shilling attacks againstrecommender systems: A comprehensive survey,” Artificial IntelligenceReview, vol. 42, no. 4, pp. 1–33, 2012.

[10] Z. Yang, L. Xu, Z. Cai, and Z. Xu, “Re-scale AdaBoost for attackdetection in collaborative filtering recommender systems,” Knowledge-Based Systems, vol. 100, pp. 74–88, 2016.

[11] Z. Yang, Z. Cai, and X. Guan, “Estimating user behavior toward detecting anomalous ratings in rating systems,” Knowledge-Based

Systems,vol. 111, pp. 144–158, 2016.

[12] W. Zhou, Y. S. Koh, J. H. Wen, S. Burki, and G. Dobbie, “Detection ofabnormal profiles on group attacks in recommender systems,” Proceedingsof the 37th international ACM SIGIR conference on Research ondevelopment in information retrieval, vol. 1, pp. 955–958, 2014.

[13] N. Gong, M. Frank, and P. Mittal, “Sybilbelief: A semi-supervised learningapproach for structure-based sybil detection,” IEEE Transactions onInformation Forensics and Security, vol. 9, no. 6, pp. 976–987, 2014.

BIOGRAPHY

Kiran Kumar Polu completed his Bachelor of Computer Applications from Sri Vekateswara University, Tirupathi, Master of Computer Applications from IGNOU, New Delhi and M.Tech in Computer Science and Engineering from Narayana Engineering College. His areas of interest include Machine Learning, IoT and Digital Forensics.

Dr. J. Suresh Babu is currently working as head & Professor, Department of MCA in Narayana Engineering College, Nellore. He received his Ph.D in Computer Science from Vikrama Simhapuri University, Nellore and PhD area Geographical Information Systems . He has got 14 years of teaching experience. He has attended many Faculty Development Programs and Workshops. He has published 12 research papers in various National and International journals and 4 International Conferences.