World of Computer Science and Information Technology Journal (WCSIT)
ISSN: 2221-0741
Vol. 11, No. 3, 13-16, 2021

Logistic Regression for Detecting Untrustworthy Recommendations in Pervasive Environments

Mohammad Said El-Bashir
Prince Hussein Bin Abdullah College for Information Technology
AL al-Bayt University, Mafraq, Jordan

Abstract— In recent research, the assessment of the trustworthiness of a certain recommender in pervasive environments is examined upon their previous interactions. However, when it is the initial interaction for a certain user, then recommendations cannot be assessed against trustworthiness. One of the approaches is to refer to a previous interaction of one of the users. However, this approach may give good results but it may also lead into wrong recommendations. In this paper, a method for detecting untrustworthiness in pervasive environments is proposed. After digitizing the data attributes, logistic regression is applied. The data attributes used are the recommendations not users information. The proposed method achieved promising results, which are comparable with other research.

Keywords- Trust model; pervasive environments; logistic regression.

I. INTRODUCTION

Over the past years, pervasive environments were widely used with the development of wireless networks. Moreover, hand held devices were used for applications and services over the internet. Interacting entities in such environment without background of each other leads to the need of security management [1]. Trustworthiness based on certain parameters may make communication over such environment possible. To give more security, adding authentication or limitation of services is an attempt to protect of certain attack. It is important to differentiate untrustworthy or trustworthy entities in pervasive environment. Due to that, a trust model may be applied to assess the trustworthiness of entities interacted in such an environment [2] [3]. Using previous data collected of certain user interactions to be utilized in the model to predict its trustworthiness unless user has no previous interactions. It would be effective if the fair data is provided, otherwise it will be misleading for unfair data [4].

Several online markets use marking to evaluate their entities such as a scale from 1 to 5 or rating of (excellent, very good, good, fair , bad, very bad) [5]. Moreover, comments provided for more explanation for users [6]. This will help to get feedback by recommending or not for a specific entity, which is viewed in public. This could make benefit in such cases but still have some disadvantages [7]. Sometimes fake feedback is provided number of times, which make the rate steady in a misleading direction. This problem could be solved by constructing a trust model which can overcome this problem such in [8] [9] and [10]. Their system used several factors like score, context and timestamp.

This paper proposes an approach for the same data set used by [8] [9] and [10] by applying logistic regression detection model (LRD).

The paper in the next section provides a literature review of previous research. After that, methodology is presented. Results and conclusion are discussed and elaborated after that. Finally, conclusions and future research directions are composed.

II. Literature Review

Several research has been done to develop a trust model in the environment of pervasive computing. Although it suffers from unfair feedback which leads to defect in the evaluation. Several methods proposed to deal with these kind of problems.

A proposed method by Xiong et al. named PeerTrust, which evaluates the trustworthiness through peer to peer feedback network in a decentralized environment with number of factors [11]. Another method proposed by Weng et al. depending on the entropy to determine unfair recommenders. The proposed algorithm depends on giving initial rating from other entities, which may be different [12]. A method of formal trust model with multi-hop protocol is proposed by Ahamed et al. along with statistical measurements including mean and the standard deviation [13].

Iltaf et al. proposed an approach to filter recommendations based on comparing similarity. The most different considered dishonest [14]. Barmade et al. applied association rules in a method to detect outliers in a transactional data [15]. He et al developed an algorithm to Find frequent pattern outlier factor (FindFPOF) to detect outliers [16]. D'Angelo et al. proposed a method, which work like human by applying Apriori algorithm to make use of recommender's behavior then applying naïve

bayes to classify user trustworthiness [9]. D'Angelo et al. in 2019 proposed different method by applying association rules to ensure trustworthiness of data from a recommender [10].

More and more methods were proposed in the literature with different approaches [17]. However, different methods could be applied such as statistical and machine learning algorithms.

III. Proposed Method

A reputation score is utilized by several online shops. The study of the behavior of a user may give an indication of its trustworthiness. A method is proposed upon user behavior represented in such parameters. These parameters are gathered together to get a dataset in the form of tuples. Dataset then entered into logistic regression model to make a decision.

A. Data Set

Data set represents a simulation of roguish internet users. It is constructed with Java Language [8]. The data is used to construct a pervasive environment model to test the users interaction trustworthiness. Three types of attack Bad Mouthing (BM), Ballot Stuffing (BS) and Random Opinion (RO) were emulated based on time, counting and context. Recommendations are assumed to be all fair. A percentage of 10% to 50% for all the experiments of unfair recommendations [9]. If entities are reliable then its trustworthy (T), otherwise its untrustworthy (U) [8].

Each entity identification (EID) defined by some attributes. Attributes include counting trust (CT), counting un-trust (CU), last time (LT), transactions context (TC) and trust Score (TS). CT provides the number of trustworthy subsequent occurrences [8]. CU provides the number of untrustworthy subsequent occurrences. LT the last time a specific context provided. TC represents the category of transaction (e-commerce, social network, game and others) [9].

B. Logistic Regression

Logistics regression is from the widely applied machine learning approaches for different types of applications. It works by capturing a vector of variables estimating the input variable value to be applied after that for a classification process [18]. Logistic regression function for the classification process is linearly defined in Equation (1) as follows:

$$logistic(S) = \beta_0 + \beta_1 X_1 + \cdots + \beta_k X_k \quad (1)$$

Where, S is the probability of presence of feature of interest

$X_1, X_2, \dots, X_k$ is the classifier value and $\beta_0, \beta_1, \dots, \beta_k$ are the interception variables [18]

IV. Results and Discussion

Data set which described in details above in previous section. The data set took in its consideration three types of attacks Bad Mouthing (BM), Ballot Stuffing (BS) and Random Opinion (RO). Provided also a Trustworthy (T) and Untrustworthy (U) interactions. For each attack, there is trustworthy and untrustworthy recommendations. Unfair recommendations from 10% to 50%. Data were digitized then a logistic regression detection (LRD) method is performed. The results are shown below in Table I, Table II and Table III. A comparison with previous research were shown in Table IV, Table V and Table VI.

A. Performance Measurements

Some type of measurements are used for the assessment of the proposed method performance and for the comparison with previous work. The performance measurements include Sensitivity (S) also known as True Positive Rate (TPR), False Positive Rate, Accuracy (ACC) and Precision (P). In order to calculate these performance measures, we need to extract how many true positives (TP) which is number of unfair recommendations properly classified. True negative (TN) which refers to the number of fair recommendations classified properly. False positive (FP) which is the number of unfair recommendations classified wrongly as fair. False negative (FN) which is the fair recommendations classified wrongly as unfair. The equations to calculate sensitivity, false positive rate, accuracy and precision are shown below in Equation 2, Equation 3, Equation 4 and Equation 5 respectively: [19]

$$S = \frac{TP}{TP+FN} \quad (2)$$

$$FPR = \frac{FP}{TN+FP} \quad (3)$$

$$ACC = \frac{TP+TN}{TP+FP+TN+FN} \quad (4)$$

$$P = \frac{TP}{TP+FP} \quad (5)$$

Matthews correlation coefficient (MCC) indicates the quality of classification. Its value range from -1 to +1. The more near to +1 the better the results are. The equation of MCC show in Equation 6 below: [19]

$$MCC = \frac{TP \times TN - FP \times FN}{\sqrt{(TP+FP) \times (TP+FN) \times (TN+FP) \times (TN+FN)}} \quad (6)$$

B. Results of BM, BS and RO Attacks

Bad Mouthing (BM) attack for unfair recommendations from 10% to 50% results are shown in Table I below. Best results appear when unfair recommendation is of 40%. High Sensitivity average of 97.67%. False positive rate average is 16.08%, which is not very bad but it needs to be lower than that. High precision rate and accuracy of 96.18%, 95.77% respectively. MCC also gave very good indication with 0.86.

TABLE I. BAD MOUTHING PERFORMANCE MEASUREMENTS RESULTS

Attack	**S**	**FPR**	**P**	**ACC**	**MCC**
BM10%	100	30	99.0476	99.0683	0.832666
BM20%	88.3495	28.4483	84.6512	82.2981	0.610502
BM30%	100	13.7931	98.6532	98.7578	0.922203
BM40%	100	0	100	100	1
BM50%	100	08.1633	98.556	98.7578	0.95137

The same experiment has been run on Ballot Stuffing with the same unfair recommendations from 10% to 50%. The results shown in Table II below where results did not vary so much when unfair recommendations is changed. Average sensitivity reached 97.9%. False positive rate 42.9% in average, which is higher than for BM. Similarly to BM precision and accuracy in average, obtained a high score of 95.9% and 94.4% respectively. Still MCC give a good indication with a rate of 0.6.

Random opinion attack results shown in Table III. The results achieved in general is less than with BM and BS. Average sensitivity resulted of an 88.7%. A higher false positive rate of 57.3%, which is not much acceptable. Precision and Accuracy were very good rates of 81.5% and 80.6% respectively. MCC still achieved an acceptable indication of 0.39.

TABLE II. BALLOT STUFFING PERFORMANCE MEASUREMENTS RESULTS

Attack	S	FPR	P	ACC	MCC
BS10%	98.7179	60	98.0892	96.8944	0.431499
BS20%	98.6799	21.0526	98.6799	97.5155	0.776272
BS30%	98.6348	55.1724	94.7541	93.7888	0.556381
BS40%	97.5265	43.5897	94.198	92.5466	0.61472
BS50%	95.9707	34.6939	93.9068	91.3043	0.647052

TABLE III. RANDOM OPINION PERFORMANCE MEASUREMENTS RESULTS

Attack	**S**	**FPR**	**P**	**ACC**	**MCC**
RO10%	100	96.875	90.3427	90.3727	0.168024
RO20%	100	93.75	81.1321	81.3665	0.225183
RO30%	97.7778	38.1443	85.6031	86.9565	0.681622
RO40%	76.1658	27.907	80.3279	74.5342	0.477438
RO50%	69.5652	29.8137	70	69.8758	0.397523

C. Comparison with previous research

In order to check for the performance of the proposed method, it is compared with a research done by Gianni D'Angelo et al. in 2019. The researchers applied an association rules on the same data set used in this research and the results illustrated in Table IV, Table V and Table VI with a comparison with our approach. Our proposed LRD method has higher sensitivity rate than Gianni et al. method in all attacks. False positive rate for Gianni et al. method is lower than our proposed LRD method, which give some advantage for Gianni et al. method. Our proposed LRD achieved better precision in general in comparison to Gianni et al. except in RO attack Gianni et al. is slightly higher. MCC is higher for Gianni et al. on BS and RO attacks, while it is lower than our proposed LRD method on BM attack. In general, both methods gave similar indication.

TABLE IV. COMPARISON OF PROPOSED METHOD WITH PREVIOUS IN TERMS OF BAD MOUTHING

BM	**S**	**FPR**	**P**	**MCC**
Proposed LRD	98.2443	18.107	96.8277	0.830485
D'Angelo et. Al (2019) [10]	88.67	05.86	71.66	0.7576

TABLE V. COMPARISON OF PROPOSED METHOD WITH PREVIOUS IN TERMS OF BALLOT STUFFING

BS	**S**	**FPR**	**P**	**MCC**
Proposed LRD	97.9508	41.0959	95.9839	0.631409
D'Angelo et. Al (2019) [10]	77	03.8	69.72	0.6978

TABLE VI. COMPARISON OF PROPOSED METHOD WITH PREVIOUS IN TERMS OF RANDOM OPINION

RO	**S**	**FPR**	**P**	**MCC**
Proposed LRD	91.1269	43.8923	82.8894	0.514011
D'Angelo et. Al (2019) [10]	81.72	12.26	83.33	0.6941

V. CONCLUSIONS AND FUTURE DIRECTIONS

A method named LRD for the detection of untrustworthy recommendations were proposed. These recommendations were used to entities bought online from electronic shops. The untrustworthy recommendation are represented in three types of attacks. The attacks are Bad Mouthing, Ballot Stuffing and Random Opinion. In LRD method, data is digitized then logistic regression is applied. A data set [8] were used for testing our method and results were obtained. Sensitivity, false positive rate, accuracy, precision and Matthews correlation coefficient are the performance measures used to assess the quality of the proposed method. The results were promising and comparable with previous research. Our proposed method achieved high sensitivity, accuracy and precision while false positive rate need to be less since it is relevant with detecting untrustworthy recommendations. Future work may include applying different machine learning methods or even can applying deep learning approaches.

REFERENCES

[1] A. Jsang, R. Ismail, C. Boyd, "A survey of trust and reputation systems for online service provision," Decision Support System, vol. 43, no. 2, p. 618–644, 2007.

[2] F. Almenrez, A. Marn, D. Daz, A. Corts, C. Campo, C. GarcRubio, "Trust management for multimedia P2P applications in autonomic networking, Ad Hoc Netw," MultimediaAdHocandSensorNetworks, vol. 9, no. 4, p. 687–697, 2011.

[3] T. Sun, M.K. Denko, "A distributed trust management scheme in the pervasive computing environment," ACM Comput. Surv., p. 1219–1222, 2007.

[4] G. Carullo, A. Castiglione, A. De Santis, F. Palmieri, "A triadic closure and homophily-based recommendation system for online social networks," World Wide Web, vol. 18, no. 6, p. 1579–1601, 2015.

[5] G. Carullo, A. Castiglione, G. Cattaneo, A.D. Santis, U. Fiore, F. Palmieri, "Feeltrust: providing trustworthy communications in ubiquitous mobile environment," Proceedings of the IEEE 27th International Conference on Advanced Information Networking and Applications (AINA), p. 1113–1120, 2013.

[6] A . Manna, A . Sengupta, C. Mazumdar, "A survey of trust models for enterprise information systems," Procedia Comput. Sci., vol. 85, p. 527–534, 2016.

[7] R. Malaga, "Web-based reputation management systems: problems and suggested solutions," Electronic Commerce Research, p. 403–417, 2001.

[8] G. D'Angelo, S. Rampone, F. Palmieri, "An artificial intelligence-based trust model for pervasive computing," Proceedings of the 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), p. 701–706, 2015.

[9] G. D'Angelo, S. Rampone, F. Palmieri, "Developing a trust model for pervasive computing based on apriori association rules learning and Bayesian classification," Soft Comput., p. 6297–6315, 2017.

[10] Gianni D'Angelo , Francesco Palmieri , Salvatore Rampone, "Detecting unfair recommendations in trust-based pervasive environments," Information Sciences, vol. 486, p. 31–51, 2019.

[11] L. Xiong, L. Liu, "PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities," IEEE Transactions on Knowledge and Data Engineering, vol. 16, no. 7, p. 843–857, 2004.

[12] J. Weng, C. Miao, A. Goh, "Protecting Online Rating Systems from Unfair Ratings," International Conference on Trust, Privacy and Security in Digital Business, p. 50–59, 2005.

[13] S.I. Ahamed, M.M. Haque, M.E. Hoque, F. Rahman, N. Talukder, "Design, analysis, and deployment of omnipresent formal trust model (FTM) with trust bootstrapping for pervasive environments," Journal of Systems and Software, vol. 83, no. 2, p. 253–270, 2010.

[14] N. Iltaf, A. Ghafoor, U. Zia, " A mechanism for detecting dishonest recommendation in indirect trust computation," EURASIP Journal on Wireless Communications and Networking, vol. 189, 2013.

[15] A. Barmade , M.M. Nashipudinath, "An efficient strategy to detect outlier transactions," International Journal of Soft Computing and Engineering (IJSCE), vol. 6, no. 174-178, p. 3, 2014.

[16] Z. He, X. Xu, J.Z. Huang, S. Deng, "Fp-outlier: frequent pattern based outlier detection," Computer Science and Information Systems, vol. 2, no. 1, pp. 103-118, 2005.

[17] F. Hendrikx, K. Bubendorfer, R. Chard, "Reputation systems: a survey and taxonomy," Journal of Parallel and Distributed Computing, vol. 75, pp. 184-197, 2015.

[18] Dobson, A. J., and A. G. Barnett. , An Introduction to Generalized Linear Models, Chapman and Hall/CRC. ,Taylor & Francis Group, 2008.

[19] A. Tharwat, "Classification assessment methods," Applied Computing and Informatics, vol. 17, no. 1, pp. 168-192, 2020.

AUTHORS PROFILE

Mohammad Said El-Bashir is an Assistant Professor at the Department of Computer Science faculty of computer science, Prince Hussein Bin Abdullah College for Information Technology, Al Al-Bayt University (Jordan). As he supervised several master students and been an examiner to master thesis for several times. His research is in the field of Machine Learning and Multimedia and has published several journal papers in that field.