HONEST OR DISHONEST PERSONS IN PERVASIVE COMPUTING BY USING BAYES CLASSIFIERS

Dr.R.Venkatesh Babu, Dr.G.Ayyppan, Dr.A. Kumaravel
Dean Academic, BIHER, BIST, Bharath University, Chennai
Associate Professor, Department of Information Technology, BIHER, BIST, Bharath University, Chennai.
Professor and Head, Department of Information Technology, BIHER,BIST, Bharath University, Chennai.

Abstract - In current years pervasive computing focuses of IoT markets, Big data, Cognitive computing and analytics, new business models and services, home appliances, and support for wearable and IOT connected devices. In this work, the proposed system focuses several Bayes classifiers are used for final decision making expressed in term of probability of user trustworthiness and also analysis some common issues and then propose a pervasive computing architecture based on a simple but helpful of the Bayes classifiers are more trustable model.

Keywords: Pervasive computing, Bayes classifier, ICT, Counting Trust, Counting Un-trust

I. INTRODUCTION

The growing evolution of information and communication technology (ICT) systems is moving beyond the big desktop computers and tends to increasingly smaller and more powerful devices providing advanced computing capabilities and multiple heterogeneous wireless communications interfaces. The main advantage of pervasive computing environments is to make life more comfortable by providing mobile devices and digital infrastructures capable of offering the distribution of any type of service within environments where people live, work or socialize. However, at the same time pervasive computing presents many risks and security-related issues that open many questions that remain to be answered. The fact that pervasive systems are typically embedded or invisible and participate in the provision of the required service without the conscious or explicit knowledge of the user complicates the design further. Moreover, the various devices operating in pervasive environments need to perform mutual interactions without knowing each other in advance, by also distinguishing themselves in a fully autonomous way without requiring any human intervention. So, it is quite difficult for users to know when these devices are present and exchange personal information such as their identities, preferences, roles and current positions. For example, while surfing the Internet, our browser habits are continuously tracked by third parties for user profiling, social networks connections suggestion and targeted advertising purposes.

The paper is structured as follows. First, in Sect. 2, the background and related works are discussed. Second, in Sect. 3, the materials and methods are used in this research work. Second, in Sect. 4, the results and discussions are presented. Finally, in Sec.5, Conclusions of this research work.

II. LITERATURE SURVEY

In this section presents the background work of this research work. in this work, by extending the preliminary results reported in a pervasive computing architecture based on a trust model that dynamically takes trust decisions based on different contexts and different sources of trust information[1,2]. Many works in the trust modeling domain are based on the following dimensions and history, recommendation and context[3]. Based on above approaches, trust has been represented and estimated in many different ways, such as statistical analysis [4], probability [5] and directed graphs[6].

Providing a quite complete survey of the entire collection of trust-related works in computer science is out of our scoe, and we can refer to the already existing surveyson such topic [7,8 and 9].

The Bayes theorem is used as a tool for designing Bayesian trust model that promotes a probabilistic view of the trust[8,9]. Due to the numerous advantages of the Bayes network such as dynamic updating, this approach makes the trust models more suitable to be used in pervasive computing environments since it can dynamically adapt to the different situations. Inspired from these works, we introduce a way to recognize the adopted behavioral schemes by the entities for both when they are acting in good and bad faith.

III. MATERIALS AND METHODS

In this section presents the materials and methods of this research work.

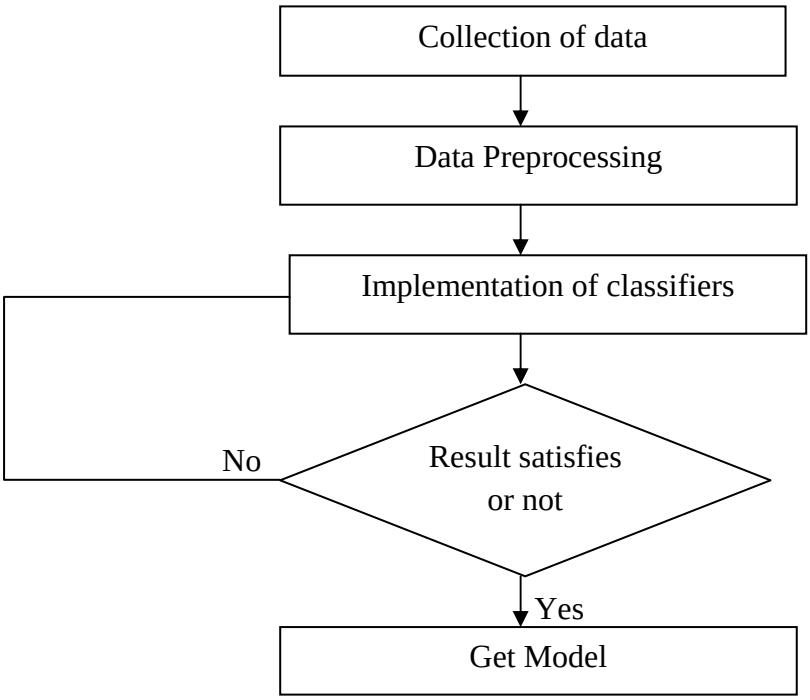

Figure 1: Proposed system

Dataset Description:

The dataset borrowed from https://archive.ics.uci.edu/ml/datasets/Dishonest+Internet+users+Dataset. The data has created based on three types of attack. The user gains a reputation based on counting based, time based, context based attacks. The proposed solution enables to evaluate the trustworthiness of each user by monitoring the behavior of each other during their interaction on the network.

Table 1: List of Attributes

S.No	Abbreviation	Attribute Name	Description
1	CT	Counting Trust	Counting of trustworthy transactions
2	CU	Counting Un-trust	Counting of untrustworthy transactions (belonging to a specific context)
3	LT	Last Time	The last experience in a specific context took place (belonging to a specific context)
4	TC	Transactions Context	Type of transaction {game, e-commerce, social network and others }
5	TS	Trust Score	an entity gives to another entity at the end of each direct interaction
6	S	Status	Fair, Unfair

IV. RESULTS AND DISCUSSIONS

In this section presents the results and interpretations of this research work. The below table represents the time taken to build the BayesNet model has 0.04 seconds, the time taken to build the NaiveBayes ha 0.01 seconds, the time taken to build the NaiveBayesMultinomialText has 0 seconds and the time taken to build the NaiveBayesUpdateable has 0 seconds.

Table 2: Bayes classifiers and their accuracies with time to build the model

S.No	Name of the Classifier	Accuracy	Time taken to build model (In seconds)
1	BayesNet	94.72%	0.04
2	NaiveBayes	94.72%	0.01
3	NaiveBayesMultinomialText	84.78%	0
4	NaiveBayesUpdateable	94.72%	0

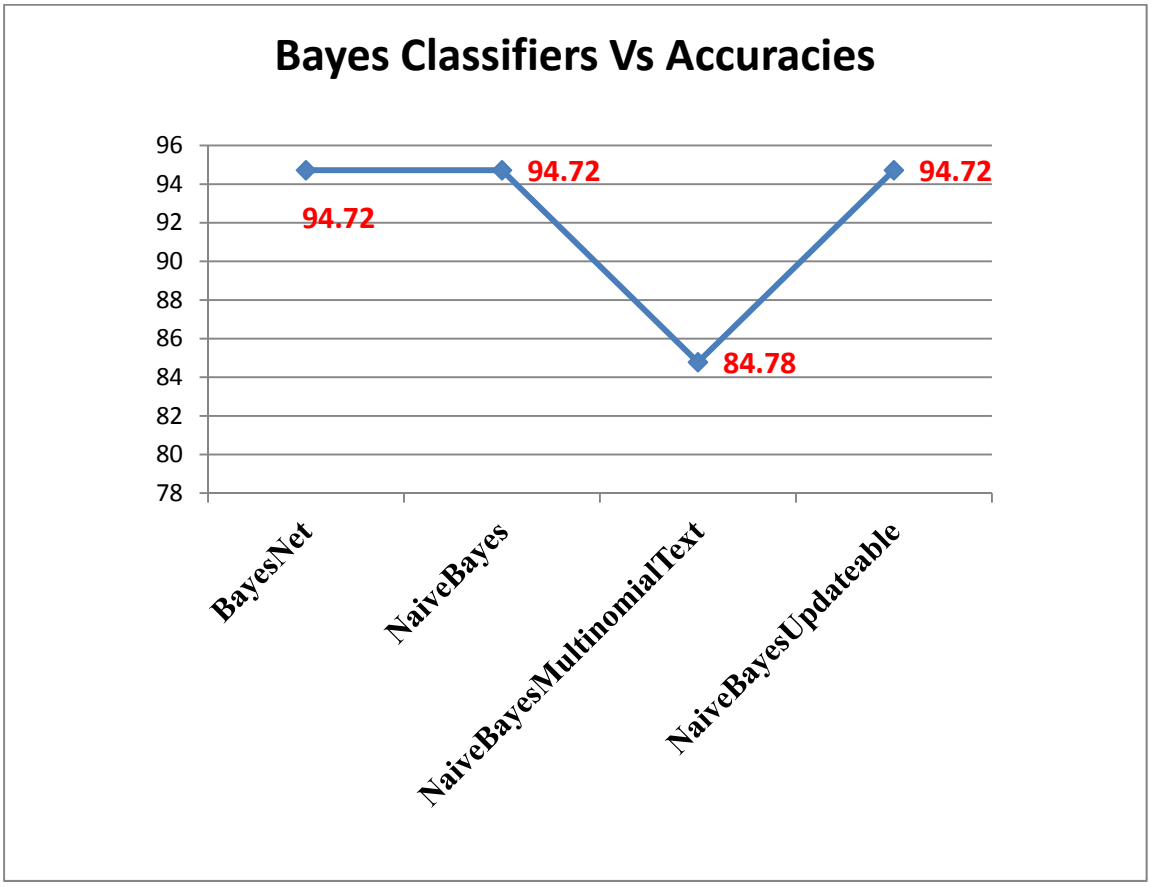

Figure 2: Graphical representation of Bayes classifiers Vs Accuracies

Above diagram depicts on BayesNet has 94.72% accuracy level, NaiveBayes has 94.72% accuracy level, NaiveBayesMultinomialText classifier has 84.78% accuracy level and NaiveBayesUpdateable classifier has 94.72% accuracy level. BayesNet, NaiveBayes and NaiveBayesUpdateable classifier have same accuracy level but NaiveBayesMultinomialText classifier has odd man out of other classifiers.

V. CONCLUSION

Our experimental results show that the proposed trust model is able to recognize the tactics used by the malicious entities for three typical attacks: counting-based, time-based and context-based. Moreover, the proposed trust model learns such tactics as soon as they appear, which would not be discovered by the conventional approach in which only the global score is used as trustworthiness measure. Furthermore, the problem of the trust evaluation at the first interaction is resolved by using the recommenders, which are also used in order to achieve faster and more accurate trust evaluation. In this research work recommends the proposed model by using the NaiveBayesUpdateable classifier compare than other Bayes classifier models.

REFERENCES

[1] G. D'Angelo, S. Rampone, F. Palmieri, "Developing a Trust Model for Pervasive Computing Based on Apriori Association Rules Learning and Bayesian Classification", SOCO – Soft Computing Journal, Vol.21, n.21, pp. 6297-6315, 2017. DOI: 10.1007/s00500-016-2183-1.

[2] G. D'Angelo, S. Rampone and F. Palmieri, "An Artificial Intelligence-Based Trust Model for Pervasive Computing," 2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), Krakow, 2015, pp. 701-706. DOI: 10.1109/3PGCIC.2015.94

[3] Khiabani H, Sidek ZM, Manan JlA (2010) Towards a unified trust model in pervasive systems. In: 2010 IEEE 24th international conference on advanced information networking and applications workshops (WAINA). IEEE, pp 831–835

[4] Kurniawan A, Kyas M (2015) A trust model-based Bayesian decision theory in large scale internet of things. In: 2015 IEEE tenth international conference on intelligent sensors, sensor networks and information processing (ISSNIP). IEEE, pp 1–5.

[5] Gonzalez JM, Anwar M, Joshi JB (2011) A trust-based approach against ip-spoofing attacks. In: 2011 Ninth annual international conference on privacy, security and trust (PST). IEEE, pp 63–70.

[6] Theodorakopoulos G, Baras JS (2006) On trust models and trust evaluation metrics for ad hoc networks. IEEE J Sel Areas Commun 24(2):318–328

[7] Wei Z, Tang H, Yu FR, Mason P (2014) Trust establishment based on bayesian networks for threat mitigation in mobile ad hoc networks. In: 2014 IEEE military communications conference (MILCOM).IEEE, pp 171–177.

[8] Kantor PB, Rokach L, Ricci F, Shapira B (2011) Recommender systems handbook. Springer, Berlin.

[9] Denko MK, Sun T, Woungang I (2011) Trust management in ubiquitous computing: a Bayesian approach. Comput Commun 34(3):398–406.

[10] https://www.theticblog.com/pervasive-computing-cutting-edge-technology/

[11] 1https://www.monitis.com/blog/how-to-make-your-website-load-faster/