Evaluation of Trust Methods for Service Selection in IoT

Shweta, Sunil Kumar

Abstract: ***Internet of things is combining virtual world and real world together. In order to perform particular service, there are many similar service providers, which make selection quiet difficult for the end users. Hence trust plays a vital role..Trust computational model helps in evaluating the Trust for the purpose of reliable service management. It helps in reducing Risk factor and uncertainty. Current research lacks in comprehensive study on trust management in IoT. This paper categorizes existing Trust computational models into five basic building steps. Each step is elaborated into certain important attributes and properties. Several trust computational model are studied and classified according to these properties and attributes. Further we also provided important parameter of each trust step. This paper also discussed the open research issues in this area.***

Keywords: Internet of things, trust management, services

I. INTRODUCTION

Internet of Things (IoT) was first proposed in 1998 by Kevin Ashton [1]. At that time it was linked to the RFID technology. Today, IoT include any device which is directly or indirectly connected to internet. It integrates the physical world with the real world which also includes real places and human being [2][10]. The term "things" includes both small device like sensors [3], RFID tags , wearable devices, cell phones and the large devices like automobile, large vehicles, robot etc. The main concept of IoT is going digital so that people get comfortable environment where information sharing is quiet easy task and everyone is interconnected. The connection can be between people-people, people-things, and things-things. Digital India is an innovative idea of such system. Also AMRUT (Atal Mission for Rejuvenation, and urban Transformation) is introduced in India for providing basic services and IOT. In order to interconnect everybody, one need a virtual space or the cyberspace where cities can be visualized as a geographical connection of people , services and their activities where they can carry out their daily activities like online shopping, gaming, health care, smart learning etc. Smart city is an application of IoT where an innovative link is formed between technology, electronics, mechanical devices and people all around [2].

IoT can be considered as set of nodes which are interconnected to each other. These nodes can be virtual or physical. Nodes can communicate with other nodes in order to fulfill certain task such as service oriented IoT system.

Revised Manuscript Received on December 22, 2018.

Shweta, Research scholar, GJU, Hisar, India
Sunil Kumar, Asst. prof., GJU, Hisar, India

In order to coordinates with other IoT nodes providing the similar services, trust plays an important role. Since, trust reduces the risk factor and increases the reliability of the system which results in increasing the system performance.

But, evaluating the trust in the system is quite challenging due to several subjective properties of the trust [4][5][6][7]. There are many fake service providers which compromise with the quality and the service for their own benefits. This affects the other IoT service provider giving the same services. Hence evaluating the trustworthiness of system is very important [8][9]. The main problem is to design an efficient and effective trust evaluation model specifically in the service oriented system where the client (node requesting for the service) can evaluate the trustworthiness of the server (node providing the service) by considering the direct or indirect experience (recommendation or feedback) with that client node. IoT system has many similar properties with the P2P MANETs [9][11][12][13].

Trust computation is very essential as it helps in effectiveness of system, reduced the risk factor of the client, and it also decrease its uncertainty. Trust is directly proportional to the reputation of the service provider. Trust is formed on basis of various factors such as quality, reliability, security, agile monetization, robustness and the connectivity.

Due to subjective properties of the trust, it is very difficult to evaluate the trust in form of model. In this paper, various trust models are studied and reviewed specifically for the service oriented IoT environment. Existing trust models are classified on the bases of several attributes and their properties. Various attacks and their defense mechanism are also taken into consideration.

The rest of the paper is divided into following sections which are as follows: section 1 discusses the most essential 5 steps to compute the trust and their detail explanations. Second section composed of compressive study of all the technique used by the existing researcher and their classification in tabular form. Last section composed of the conclusion of this paper.

II. TRUST EVALUATION STEPS

In order to understand the existing trust model, we have classified the trust in five basic steps. These are the basic steps to evaluate the trustworthiness of the system. Every step is framed using various attributes which has further several properties.

Figure 1 shows the five basic building blocks which are essential to build a trustworthiness system model.

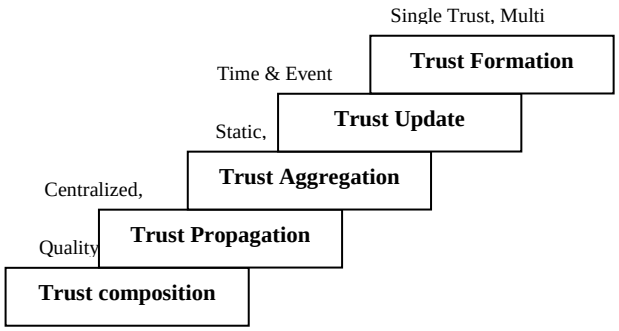

Fig. 1 Basic Building Blocks of Trust

These five steps: Composition, Propagation, Aggregation, Update and Formation play a vital role in order to build a Trust evaluation Model [11]. Every step is composed of several Attributes and these attributes further have several properties. Existing trust model differ in the properties they are using with their attributes. Detail description of each step is explained below.

Trust composition

The trust composition determines the basic amount of trust evaluated based on the quality of the service and based on the social circle of the service node. The two major attributes of Trust Composition are Quality of Service (QoS) and virtual Trust.

Quality of service Trust (QoS)

The performance of system decide the Quality of service provided to the client request. There are several properties to measure the performance of the system (illustrated in figure 1) such as honesty, proficiency, capabilities, consistency, cooperativeness etc. In order to evaluate these properties, researchers have used subjective approach such as ranking, threshold etc. Nitti et al [14] used the performance of the transaction in order to measure the QoS trust.

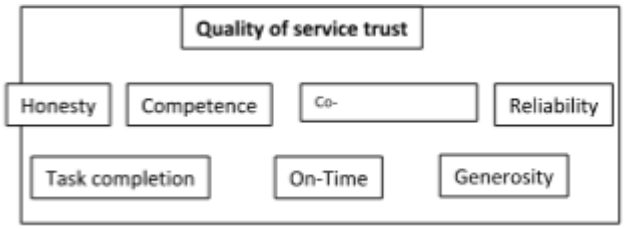

Fig. 2 Parameters of QoS

Virtual Trust

Virtual trust state the social reputation of the service provider. It can be considered using the feedbacks, rating, and recommendation from different person form the virtual world. There are various properties which are illustrate din figure 3. These helps in calculating the social trust such as connectivity, intimacy, sincerity, generosity etc. social trust consider it performance based on its social recommendation. This shows that IoT service provider wants to deliver quality of product. Chen et al [15] used social network, virtual friends and the community of interest properties for trust composition. Whereas Chen et al [16] considered social connections, its honesty, and intimacy for the same.

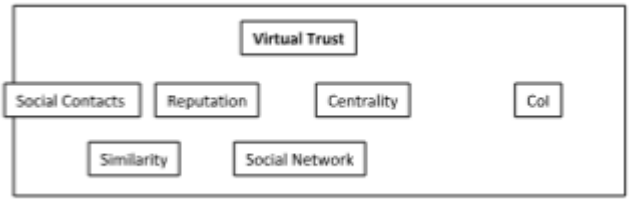

Fig. 3 Parameters of Social Trust

Trust Propagation

Trust propagation states the way trust facts and observations moves from one person to other. It can propagate using to famous scheme -distributed or the centralized.

Distributed

In the distributed scheme, trust observation of a node is propagated to other node with or without the use of a centralized node. Here direct propagation from one node to other node can also be done. There are various standard methods for such propagation such as making linked list table, hash table etc which are explained in figure 4. Distributed scheme for social IoT system was done by Chen et al [15]. Whereas Chen et al [17] propagate the Trust information to other nodes by maintaining a log table holding the forwarding information with the help of neighbor nodes.

Fig. 4 various ways to propagate trust

Centralized

Unlike the distributed scheme, in centralized scheme, propagation of trust data is done using a centralized entity such as clouds or a centralized virtual trust etc. here the presence of centralized entity is essential. Some of the centralized entity is explained in figure 5. Saied et al [18] select an appropriate IoT node to provide the service by managing a centralized trust information table, whereas Nitti et al [14] uses centralized hash table which stores the feedbacks of the entities.

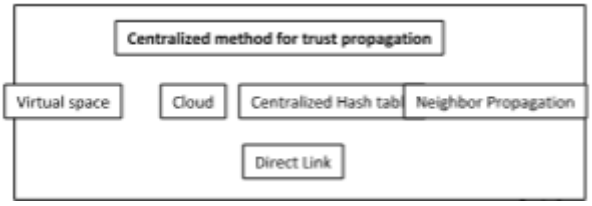

Fig. 5 Trust propagation method for Centralized Entity

Trust Aggregation

Aggregating all the trust information collected from direct or indirect observation refers to as trust aggregation. It can hold the direct experience of the node or the feedbacks, recommendation, ranking or other type of nodes social information which helps in calculating an overall trust factor. These are also classified in the figure 6. Standard aggregation techniques can be used here such as static sum, dynamic sum, fuzzy logic, regression analysis. In this paper we have analyzed the static, dynamic, and fuzzy technique of previous research.

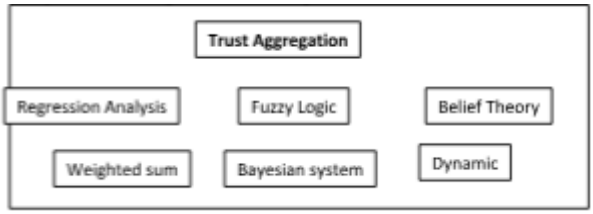

Fig. 6 Trust aggregation Technique

Static

Static sum refers to the subjective properties of the trust without considering the weight factor. It uses the subjective beliefs of the system. Here three major parameters are considered which are true, false and uncertain.

Dynamic

Dynamic aggregation techniques consider trust as not static and therefore it aggregate the trust by considering the weight factor. Certain weight is given to the properties and their attribute and later considers those weights for aggregating the final result value. Reputation system such as [20][21][22] uses weighted sum for aggregating the trust value. Here high weight is given to those raters who have high reputation.

Trust update

Trust update refers to the timely updating of trust information and conclusion. After evaluating the trust for a particular IoT service node, it became crucial to maintain the trust information as it can't be static. Trust can be updated on timely or on every event bases.

Event driven

Event Driven method update the trust information only when a certain task is performed. Whenever any IoT node provide a service to any client in the system and when that client enters a feedback in the cloud with the help of trust manager or that information is stored in its own database. Figure 7 illustrate a flow chart for updating the trust using event driven approach.

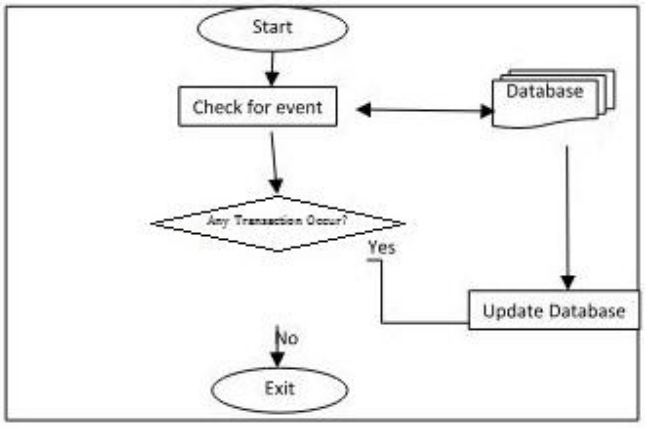

Fig. 7 Flow chart for the event driven approach

Time driven

In this approach, trust database is updating periodically without waiting for any transaction to happen. This time can be of seconds, hours, days or even of months. After every update trust aggregation is reapplied to calculate the final result. More frequent is the updation, better is the trust computational value. If the trust is not updated over a large decay of the time then trust outcome value may not be equally effective.

Trust formation

Trust formation refers to the number of properties used in order to evaluate the trust. Since there are lots of parameters with their attributes at each level, trust formation is classified as single trust or the multi trust based on the number of factors used for the overall process.

Single trust

In single trust, only single trust property is mainly taken into account while calculating the trust of the system such as Quality or timely delivery etc. Chen et al [19] considered the Quality of service as the only main attribute to evaluate the trust of the service oriented IoT where the trust is calculated only if the quality of the service is good. But this leads to the biasness in the system.

Multi trust

Unlike the single trust, multi trust uses the multidimensional properties of the system such as honesty, completeness, quality, reliability etc. Chen et al [15] computed trust of MANET by considering several trust attributes, which includes honesty, selfishness, competence etc .

III. COMPACT CLASSIFICATION OF EXISTING MODELS

Due to the high subjective properties of trust, very limited work is done in literature in aspect of trust evaluation models for IoT. In this section, the primary most essential steps of trust computational model are considered as the base for classification of all existing models.

For the more clear understanding of the models, these steps are

further classified on the basis of their attributes. Table 1 gives a summarized view of these attributes. More attributes are followed, better would be the trust model.

Table. 1 Comparative study of existing trust computation models using several essential attributes of trust with their parameters

Paper Author	Performance	Social	Distributed	Centralized	Static weighted sum	Dynamic Weighted sum	Time Driven	Event Driven	Trust
Gu et all [23]	Yes	No	No	Yes	No	No	No	No	Single
Wang [13]	Yes	No	No	Yes	No	No	No	No	Single
Namal [24]	Yes	No	No	Yes	Yes	No	Yes	No	Single
Mendoza [25]	Yes	No	Yes	No	Yes	No	No	Yes	Single
Bao [26]	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Multi
Chen [27]	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Multi
Chen [28]	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Multi
IR Chen [17]	Yes	No	Yes	No	Yes	Yes	No	Yes	Single
Mahalle [29]	Yes	No	Yes	No	Yes	Fuzzy	No	Yes	Single
Saied [18]	Yes	No	No	Yes	No	Yes	No	Yes	Single
Nitti [14]	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Single
Bao [30]	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Single
Chen [31]	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Single

IV. CHALLENGES IN EVALUATING TRUST COMPUTATIONAL MODEL

While designing a trust model there are certain challenges such as: 1) how to select the base value i.e. the very first value in aggregation system. 2) Which aggregation factor should be selected so that we get most efficient model. 3) Various transitivity factors and 4) Ranking i.e. how to rank different service provider of the same service on the basis of their trust. 5) How to categories Users while considering their feedbacks such as authorized un-authorized, or based on the attributes like honesty, selfishness or behavior analyzing 6) trust development method to be followed like ranking, recommendation, certification, past experience , guarantee etc,

V. GRAPHICAL EVALUATION

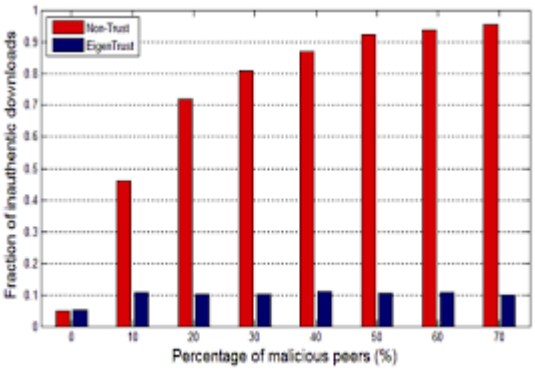

Fig. 7 inauthentic downloads with percentage of malicious peers

VI. CONCLUSION

In this paper, a basic building block for trust is designed using the five most important steps. These steps are trust composition, trust propagation, trust aggregation, trust formation and trust update. These basic steps are also used to classify the already existing trust models. A summarized table is framed in order to explain all attributes of the trust. In order to get a more efficient trust model it is essential to follow most of the attributes. We have also discussed various challenges for evaluating the trust in IoT.

REFERENCES

1. D.L. Brock, "The electronic product code(epc) a naming scheme for physical objects, "Auto-ID center, white paper , Jan 2001.
2. International telecommunication union, "ITU internet reports 2005: the internet of things", international telecommunication union, workshop report, Nov 2005.
3. V. Gazis, M. Gortz, M. Huber, A. Leonardi, K. Mathioudakis, A. Wiesmaier, F. Zeiger, E.Vasilomanolakis," A survey of technologies for internet of things", IEEE information technology and electrical engineering.
4. Huansheng Ning, Hong Liu, and Laurence T Yang. Cyberentity security in the internet of things. *Computer*, (4):46–53, 2013.
5. Michele Nitti, Roberto Girau, Luigi Atzori, Antonio Iera, and Giacomo Morabito. A subjective model for trustworthiness evaluation in the social internet of things. In *Personal Indoor and Mobile Radio Communications (PIMRC), 2012 IEEE 23rd International Symposium on*, pages 18–23. IEEE, 2012.
6. S Sicari, A Rizzardi, LA Grieco, and A Coen-Porisini. Security, privacy and trust in internet of things: The road ahead. *Computer Networks*, 76:146–164, 2015.
7. Zheng Yan, Peng Zhang, and Athanasios V Vasilakos. A survey on trust management for internet of things. *Journal of network and computer applications*, 42:120–134, 2014.
8. R.Lacuesta, G. Palacios-Navarro, C. Cetina, L. Penalver, J. Lloret, "Internet of things: where to be is to trust,"*EURASIP Journal on Wireless Communications and Networking*, 2012.
9. Li, and J. Wu, "Uncertainty Modeling and Reduction in MANETs,"*IEEE Transactions on Mobile Computing*, vol. 9, no. 7, pp.1035-1048, 2010.

10. Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.
11. H. Cho, A. Swami, and I. R. Chen, "A survey on trust management for mobile ad hoc networks,"*IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, 2011, pp. 562-583.
12. W. Li, and A. Joshi, "Coping with Node Misbehaviors in Ad Hoc Networks: A Multi-dimensional Trust Management Approach,"*2010 Eleventh International Conference on Mobile Data Management*, Kansas City, USA, 2010, pp. 85-94.
13. J. Wang, S. Bin, Y. Yu, X. Niu, "Distributed trust management mechanism for the internet of things,"*Applied Mechanics and Materials*, Vol. 347-350, pp. 2463-2467, 2013.
14. M. Nitti, R. Girau, and L. Atzori, "Trustworthiness Management in the Social Internet of Things,"*IEEE Transactions on Knowledge and Data Management*, vol. 26, no. 5, 2014, pp. 1253-1266.
15. I.R. Chen, J. Guo, and F. Bao, "Trust Management for SOA-based IoT and Its Application to Service Composition," *IEEE Transactions on Service Computing*, 2016.
16. I.R. Chen, and J. Guo, "Dynamic Hierarchical Trust Management of Mobile Groups and Its Application to Misbehaving Node Detection," *28th IEEE International Conference on. Advanced Information Networking and Applications*, Victoria, Canada, May 2014, pp. 1-6.
17. D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang "TRM-IoT: a trust management model based on fuzzy reputation for Internet of Things." *Computer Science and Information Systems*, vol. 8, no. 4, 2011, pp. 1207-1228.
18. Y.B. Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the Internet of Things: A context-aware and multi-service approach,"*Computers and Security*, vol. 39, 2013, pp. 351–365.
19. I.R. Chen, J. Guo, and F. Bao, "Trust Management for SOA-based IoT and Its Application to Service Composition," *IEEE Transactions on Service Computing*, 2016.