A Trust Computational System For Service Oriented IOT

Shweta, Dr. Sunil Kumar

Abstract: Internet of Things has made noteworthy benefits over old style communication technologies. IoT has done a lot in modern day and have totally changed the scenario of technologies. This paper helps in providing an overview of Internet of Things. Counting on an ample literature review, the main objectives of this research paper is to provide a trust computational model for service oriented IoT environment. Most of the existing trust model doesn't consider service Provider claim which affect the efficiency of trust management system. The proposed Trust model ORC is unique which consider three major parts Observation, Recommendation and Certification for computing subjective trust along with several parameters of Trust. The proposed model is able to remove the Biasness towards the new nodes in the system. Also certain weightage is given to the all ORC model parameters which help in reducing risk factor by giving preference to the Direct Observation as here node has most reliable analysis but the service provider. Fuzzy logic along with the weighted sum is used as trust aggregation. Also Trust Computing Algorithm has been proposed to evaluate trust In IoT environment.

Index term: Internet of things, Trust computation, service-oriented, Trust management, aggregation, weighted sum,direct trust, indirect trust.

1. INTRODUCTION

Internet of Things is helpful in connecting the pervasive environment to the real world including small real objects to the living large objects like human being [1]. IoT has its application in almost every part of our life and things are interconnected here. In order to connect or take use of some part, one needs to avail services from this environment which is also known as service oriented IoT. In service-Oriented IoT. Trust plays an important role which helps in reducing risk factor, increase efficiency of the system. Trustworthiness system enhances the usability of the system. Since IoT is growing very rapidly which results in large number of service providers for a particular service. It is very difficult to select one from an unknown environment. Thus trust management is helpful. More the trust factor, more reliable will be the service provider. In this paper, a unique Trust computational model is proposed which consider several attributes of trust. This paper is organized as follows: Second section describes background history related to our proposed work. 3rd part describe proposed trust model with its algorithm and its parameters important in trust management. Section 4 explains performance evaluation of our proposed work as compared to the traditional model. Conclusion and future scope is covered in last section of this paper.

2. Literature Review

Internet of things is a Covering a large part of our today's life. Service oriented IoT is an important part of it where a consumer node A request services from the IoT environment nodes. Trust plays an important role in this process. It helps in reducing risk factor and improving quality and efficiency of the system. Trust is Subjective in nature which helps in building a positive expectation between service provider and service requestor. There are many Trust model but these models are very limited in context of Internet of Things. Mostly existing frameworks are based on Reputation, social relationship, privacy and security. Privacy and security related trust issues are explored in [2][3][4]. A trust computational model based on fuzzy was designed by Chen et al in [5] which consider reputation to calculate the trust. Trust is ranged from -1 to 1 in the paper. Gligor et al [6] presented behavior theory while evaluating trust between human and computers by proposing Channel framework and some entities. In this paper, Trust was total based on the recommendations which make validation very difficult. Yan et al designed a trust model in [7] by considering three layers of IoT system i.e. physical layer, network layer and the application layer. Service oriented IoT works in Application Layer. Zhang et al[8] proposed dynamic trust model using dynamic weight adjustment factor. Bao et al[9] proposed Hierarchical trust management protocol with QoS and social trust considering honesty as trust matrices [10]. Since, very little research work is done on trust computation considering various parameter. This paper present trust model based on three major attributes as observation, feedback recommendations and Providers specifications.

3. Proposed Trust Model

The traditional models follow recommendation from the neighbor nodes in order to evaluate trust value for the service provider. But trust composed of many attributes and parameters. Considering more parameter will leads to more effective trust model. In fig 1, the proposed trust model is categorized into three major features which are Consumer Direct Observation, Indirect recommendation from intermediate nodes, and Certification from service provider which works as a proof for their claim.

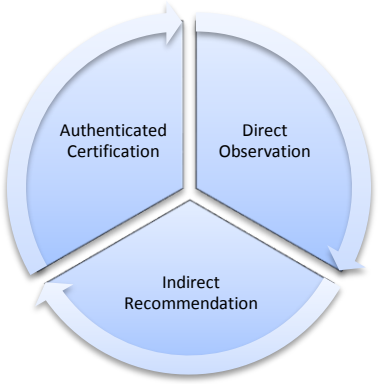

Fig 1. *Three pillar of Trust Evaluation process (ORC)*

In a trust management model, trust evaluation is a key step. While evaluating Trust, three major parts are considered i.e. Observation, Recommendation and Certification (ORC). The ORC trust Model uses fuzzy logic to aggregate the

trust value where a probabilistic approach is used to give weightage to the all three essential parts of the system.

A. Direct Observation (O): since IoT has a vast network and consider recommendation for every neighbor node is quit time consuming. In the service oriented IoT network, some service provider had direct previous experience with the consumer. While requesting for new services, if a consumer experience a service provider with which they have already dealt with then we evaluate that service provider on the basis of the direct observation of the consumer.

Trust(O) = -1 (distrust)
0 (No Trust Experience)
0.5 (very old trust value)
1 (Trustworthy) (1)

B. Indirect Recommendation (R): In IoT system when we are requesting new services from the multi service provider environment then indirect recommendation plays a very important role. When service provider are new to us, then selecting randomly is quiet risky process. Hence indirect recommendation is considered based on the feedbacks provided by the neighbor node.

Trust (R) = -1(negative Feedback)
1 (Good Feedback)
0(No past experience) (2)

C. Authenticated Certification (C): In order to improve trust value we consider trust value to the several certifications from the trusted third party. Like quality assurance certificate from ISO or any medical certificate of good internship practices for Doctors in healthcare environment. These certificates or medals helps in proving the claim done by service providers.

Trust(C) = -1(Fake Certifications)
1(Authnt credentials)
0(No Certificates) (3)

Selecting the service provider on the bases of direct and indirect recommendation leads to poor trust evaluation value of new nodes which results in starvation stage. This part helps in removing Biasness towards new nodes.

3.1 Trust Computation Algorithm ORCA:

In the IoT environment, whenever a consumer wants to avail some service, there will be several service providers available which claim to provide best service that match the user requirements. So in order to select most trustworthy service provider, Trust computation is done using the following algorithm steps:

INPUT : Consumer node requests the service in the IoT environment.
OUTPUT : Computed Trust Value of the service Providers
ALGORITHM STEPS :
Step 1: Arrange the entire service providers (n) in a queue and select the one on the Front pointer (i) of the queue;
Step 1: Traverse the Consumer Database for the service provider and extract their trust value as Trust(O) as in equation (1).
Step 2: Traverse the intermediate nodes of the consumer and evaluate the trust value as Trust(R) on the bases of their feedback and recommendation using equation (2);
Step 3: extract all the claimed Trust values for the service Provider as Trust(C) as in equation (3);
Step 4: Set the weighting factor as Wo, Wr, Wc for all the three calculated trust in previous steps;
Step 5: Compute Trust as Tr(SPi) = Wo*Trust(O)+ Wr*Trust(R)+ Wc*Trust(C);
Step 6: Compare the computed Trust value Tr(SPi) with the predefined Threshold value.
If Tr(SPi) < Threshold then Add to the list Scepticism Service Providers;
If Tr(SPi) > Threshold then Add to the list TrustFull Service Providers along with their current time Tj;
Step 7: Set i=i+1 and GoTo step 1;
Step 8: Repeat step 1 to 7 until queue is empty;
Step 9: Arrange the Service Providers in the Trustful list on the bases of their trust value along with the timestamp and cost value. Return topmost service provider as most Trustworthy.
Step 10: End

Once the trust is computed for the entire service providers queue, consumer selects the service provider with their cost value.

3.2 Trust Updation:

Trust value will be timely updated and old and static service provider will be removed from the database which will improve time and space complexity. Trust updation can be done on :

- Event basis
- Timely basis.

In event basis. Trust is updated whenever any new request is made by the consumer but on timely basis, a time period is set and trust is updated within the time interval. If a service provider is not active for a long time then its all entry will be eliminated from the database.

3.3 Trust Propagation:

Whenever data needs to be transferred from one node to another then there is a need of trusted path between them so that information is not leaked. Sender and receiver can be consumer and the service provider. The intermediate nodes are used to transfer data between them. This propagation is done using nature inspired optimization algorithm such as moth flame optimization[8][9], firfly, glow worm etc. these optimization algorithm extract necessary nodes which result in reduced overload and better performance. The trust propagation is also done by identifying malicious nodes in the IoT system.

3.4 Trust Conflict Resolution:

While computing trust value using the algorithm ORC, some service provider may get same trust value which occur conflict stage. So in order to select the one from same trustworthiness, consumer may select the service provider with lowest price or with lowest time constraint. This is done on the requirement preference of consumer. If consumer

wants service within time constraint, then service provider with lowest time bound will be preferred, but if consumer wants cheaper one, then service provider with lowest cost will be preferred.

4. Performance evaluation

Our proposed model aggregate direct trust with indirect trust using Fuzzy logic and consider the authenticated certification as a high weightage parameter while evaluating trust, while the traditional models are recommendation based. In this section a performance comparison is shown between traditional trust model and the proposed trust model in terms of:

- Number of nodes
- Utility score
- Starvation

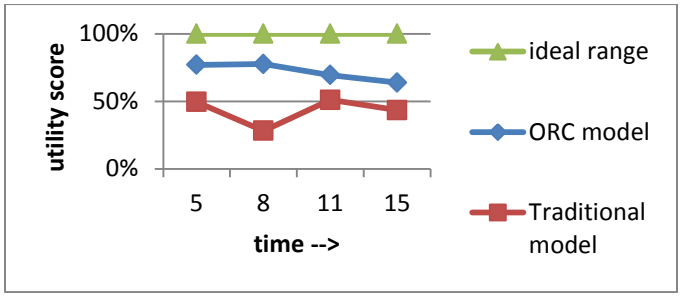

***Fig 3** utility score analysis of models*

A MatLab simulation is done to demonstrate the effectiveness of our proposed model with the Traditional Trust Model in terms of Utility score. Here Utility score in fig 3 representing goodness is compared for both the models. Since our proposed model consider the credential certifications with guaranty from the service provider authenticated from the trust party like government and a high weightage is given to such service provider hence its utility score came out to be more efficient and our proposed model leads to have less risk as compared to the traditional model. Furthermore, traditional trust model based on recommendation only keep on gathering feedbacks from the neighbor nodes but our proposed model gives a high weightage to the direct observation, if any which helps in having more customer satisfaction and negligible impact of fake recommendations from malicious nodes.

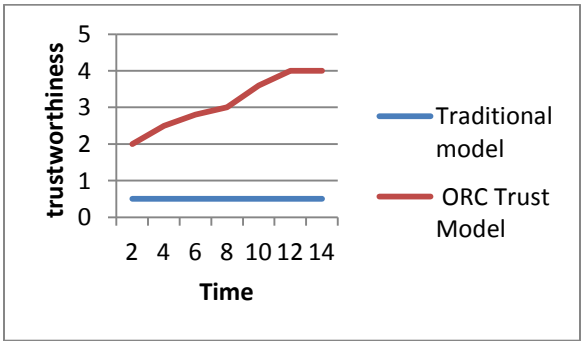

***Fig 4** Starvation condition for new SP nodes*

Thus if a node is having direct observation for a service provider then its computation time doesn't change if number of nodes increases. The proposed trust model consider Certification claim of service providers from the trusted third party which helps in removing biasness towards the old node in the system. Since there is are no recommendations or observation for new service provider, their trust value results in poor evaluated trust which also effect overall trust in later stages also. This condition is known as starvation. Considering service provider's specification helps in giving some initial weight to service provider which is shown in fig 4. Where red line shows the increase in trust value at every time cycle while blue line of traditional model shows that trust is negligible in starting and stays zero in future also. Static comparative evaluation of our trust model to that of existing model is summarized in table 1.

***Table1.** Trust evaluation using various parameters*

Paper id	Trustworthiness	Conflict resolution	direct and indirect observation	Starvation handling
S Sicari	Yes	No	Yes	No
F. Fei	Yes	No	No	No
T. Jim	Yes	Yes	No	No
J. Zhang	Yes	No	No	No
F. Bao	Yes	Yes	yes	No
Proposed work	Yes	Yes	Yes	yes

5. Conclusion and future scope

In this paper, a novel trust evolution model for IoT environment has been proposed by aggregating direct trust with indirect trust and also considering the service provider quality constraints. The aggregation is done using fuzzy logic along with the weighted sum. Our Proposed Trust Aggregation is done with direct observation, Authenticate Certificates and indirect Recommendations (ORC) which result in a combine evolution of consumer, service provider details and the intermediate recommendation nodes. Highest weightage is given to direct observation of consumer, followed up by certification authenticate from the trusted third party and later by the indirect recommendations. Authenticate certification helps in removing starvation condition for the new service provider. Thus it eliminates biasness in the system. In future, fuzzy logic can be replaced with more effective neural network technique and some more parameters can be considered to make our system more effective by reducing conflicts in trust evaluation. Since IoT environment is very vast, thus malicious node detection can be done which can prevent our system from harmful attacks which would result in improved system performance and reducing the risk factor.

6. Reference:

[1]. T. L. Koreshoff, T. Robertson, and T. W. Leong, "Internet of Things : a review of literature and products," In Proceedings of the 25th Australian Computer-Human Interaction Conference: Augmentation, Application, Innovation, Collaboration, pp. 335–344, 2013.

[2]. 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.

[3]. F. Fei, S. Li, H. Dai, C. Hu, and W. Dou, “A K-Anonymity Based Schema for Location Privacy Preservation,” IEEE Transactions on Sustainable Computing, vol. PP, no. 99, pp. 1-1, 2017.
[4]. T. Jim, “SD3: a trust management system with certified evaluation,” in Proceedings 2001 IEEE Symposium on Security and Privacy S&P, 2001, pp. 106-115.
[5]. J. Guo, I.R. Chen, and J.J.P. Tsai “A Survey of Trust Computation Models for Internet of Things Systems,” Computer Communications, vol. 97, 2017, pp. 1-14.
[6]. V. Gligor and J. Wing, "Towards a theory of trust in networks of humans and computers," in the 19th international workshop on security protocols, ser. LNCS, 2011.
[7]. Z. Yan, P. Zhang and A. Vasilakos, "A Survey on Trust Management for Internet of Things," Journal of Network and Computer Applications, vol. 42, pp. 120-134, 2014.
[8]. J Zhang, R S Hankaran, MA Orgun, et al., in Proc. of 2010 IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC), Hong Kong, China. A dynamic trust establishment and management framework for wireless sensor networks (2010), pp. 484–491.
[9]. F Bao, IR Chen, MJ Chang, et al., Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE Trans. Netw. Serv. Manag.. **9**(2), 169–183 (2012).
[10]. Y. Zhou, “Hybrid Artificial Glowworm Swarm Optimization Algorithm for Solving System of Nonlinear Equations Hybrid Artificial Glowworm Swarm Optimization Algorithm for Solving System of Nonlinear Equations,” Journal of Computational Information Systems 6, no. October, pp.3431-3438, 2015.
[11]. Y.Zhou, “Hybrid Artificial Glowworm Swarm Optimization Algorithm for Solving System of Nonlinear Equations Hybrid Artificial Glowworm Swarm Optimization Algorithm for Solving System of Nonlinear Equations,” Journal of Computational Information Systems 6, no. October, pp.3431-3438, 2015.