INTERNATIONAL JOURNAL OF APPLIED
SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

A TRUST EVALUATION MODEL FOR IDENTIFYING CREDIBLE SERVICE PROVIDERS IN ONLINE NETWORKS

[1]L.Priyanka,[2]Bongani Ravali

[1]Assistant Professor,[2]MCA Student

Depatment Of MCA

Sree Chaitanya College of Engineering, Karimnagar

ABSTRACT

Numerous trust models for Trustworthy Service Recommendation (TSR) in online services have been presented as a result of the widespread use of online services. Reputation-based methods are susceptible to unfair rating assaults and typically lack user choices. The algorithm known as Find Trusted Service Provider is the subject of this study. The Find Trusted Service Provider Algorithm asks neighbour nodes to rate it, and then the neighbour node asks its neighbour node to do the same. The primary goal of customer ratings is to identify reliable sources in online service-oriented trusted networks. Finding the greatest and most reliable service provider can be accomplished by taking into account the ranking, which can be determined by a number of elements depending on the criteria. The service provider with the highest rating may be found by comparing its average ranking. How the procedure proceeds and how to obtain ratings and trust values from other customers are the topics of the suggested algorithm. That allows for the identification of a reliable service supplier.

I. INTODUCTION

The need for trustworthy service providers has never been higher in the connected world of today. Finding someone you can trust is crucial for both your own peace of mind and the effective execution of tasks, whether you're looking for a tech support specialist, contractor, or healthcare professional. Finding reliable service providers inside your current network is essential since the sheer number of possibilities might be daunting.

In this pursuit, a reliable network may be a useful asset. You may successfully negotiate the sometimes muddy seas of choosing a service provider by utilising referrals, reviews, and personal contacts. The significance of building trust in service connections, the advantages of working with a reliable network, and practical methods for locating trustworthy providers that meet your needs are all covered in this introduction.

As we explore this subject, we will go over important things to think about, such confirming credentials, evaluating reputation, and comprehending the subtleties of personal recommendations. You may connect with service providers who not only satisfy your needs but also maintain the professionalism and integrity standards that are essential in any service-oriented relationship by arming yourself with the appropriate information and tools.

II. LITERATURE SURVEY

A Trust and Reputation based Anti-SPIM Method

Instant Messaging (IM) service is a killer application in the Internet. Due to the problem of IM spam (SPIM), building an effective anti-spim method is an important research topic. At present, most of anti-spim solutions are based on email-spam prevention techniques, which are not directly applicable to anti-spim. We present a new anti-spim method SpimRank, which integrates trust and reputation mechanisms with black-list technique. SpimRank also tracks user's historical action to deal with spim attacks in nearly real time, which is applicable to IM environment.

Toward a testbed for evaluating computational trust models

We propose a generic testbed for evaluating social trust models and we show how existing models can fit our tesbed. To showcase the flexibility of our design, we implemented a prototype and evaluated three trust algorithms, namely Eigen Trust, Peer Trust and Appleseed, for their vulnerabilites to attacks and compliance to various trust properties. For example, we were able to exhibit discrepancies between Eigen Trust and Peer Trust, as well as trade-offs between resistance to slandering attacks versus self-promotion.

A Heuristic Algorithm for Trust-Oriented Service Provider Selection in Complex Social Networks

In a service-oriented online social network consisting of service providers and consumers, a service consumer can search trustworthy service providers via the social network. This requires the evaluation of the trustworthiness of a service provider along a certain social trust path from the service consumer to the service provider. However, there are usually many social trust paths between participants in social networks. Thus, a challenging problem is which social trust path is the optimal one that can yield the most trustworthy evaluation result In this paper, we first present a novel complex social network structure and a new concept, Quality of Trust (QoT). We then model the optimal social trust path selection with multiple end-to-end QoT constraints as a Multi-Constrained Optimal Path (MCOP) selection problem which is NP-Complete. For solving this challenging problem, we propose an efficient heuristic algorithm, H_OSTP. The results of our experiments conducted on a large real dataset of online social networks illustrate that our proposed algorithm significantly outperforms existing approaches.

Multi-Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks

Mobile Ad Hoc Networks (MANETs) offer a dynamic environment in which data exchange can occur without the need of a centralized server or human authority, providing that nodes cooperate among each other for routing. In such an environment, the protection of data en route to its destination is still a challenging issue in the presence of malevolent nodes. This paper proposes a message security approach in MANETs that uses a trust-based multipath AOMDV routing combined with soft-encryption, yielding our so-called T-AOMDV scheme. Simulation results using ns2 demonstrate that our scheme is much

more secured than traditional multipath routing algorithms and a recently proposed message security scheme for MANETs (our so-called Trust-based Multipath Routing scheme (T-DSR)), chosen as benchmark. The performance criteria used are route selection time and trust compromise.

An Efficient Multiple Trust Paths Finding Algorithm for Trustworthy Service Provider Selection in Real-Time Online Social Network Environments

Online Social Networks (OSNs) have been used to enhance service provision and service selection, where trust is one of the most important factors for the decision making of service consumers. Thus, it is significant to evaluate the trustworthiness of the service providers along the social trust paths from a service consumer to a service provider. However, there are usually many social trust paths between an unknown service consumer and service provider. Thus, a challenging problem is how to effectively and effciently find those social trust paths that can yield trustworthy trust evaluation results based on the requirements of a service consumer particularly in the real-time OSN environments. In this paper, we first present a contextual trust-oriented social network structure and a concept of Quality of Trust (QoT). We then model the multiple social trust paths finding with end-to-end QoT constraints as the Multiple Constrained K Optimal Paths (MCOP-K) selection problem, which is NP-Complete. To deal with this challenging problem, based on the Monte Carlo method and our optimization search strategies, we propose a new efficient and effective approximation

algorithm D-MCBA. The results of our experiments conducted on a real-world dataset of OSNs illustrate that D-MCBA can efficiently identify the social trust paths with better quality than our previously proposed MONTE K algorithm that is the most promising algorithm for the social trust path finding in OSNs.

Security Trust and Implementation Limitations of Prominent IoT Platforms

Internet of Things (IoT) is indeed a novel technology wave that is bound to make its mark, where anything and everything (Physical objects) is able to communicate over an extended network using both wired and wireless protocols. The term "physical objects" means that any hardware device that can sense a real world parameter and can push the output based on that reading. Considering the number of such devices, volume of data they generate and the security concerns, not only from a communication perspective but also from its mere physical presence outside a secure/monitored vault demands innovative architectural approaches, applications and end user systems. A middleware platform/framework for IoT should be able to handle communication between these heterogeneous devices, their discoveries and services it offers in real time. A move from internet of computers to internet of anything and everything is increasing the span of security threats and risks. A comparative study of existing prominent IoT platforms will help in identifying the limitations and gaps thereby acting as the benchmark in building an efficient solution.

III. SYSTEM ANALYSIS AND DESIGN

EXISTING SYSTEM

There is lot of trustworthy finding methodologies present in the existing system, but they are not accurate enough to find the trustworthy service provider. The existing systems are dealing with minimal number of nodes interaction in order to find the best trustworthy existing in an online service oriented trusted network. Trustworthy finding solutions are not having enough interaction with consumers to get their views and trustiness of the service and the quality of service.

DISADVANTAGE

There are no consumer interactions to find trustworthy in the current system so that system cannot be best solution to the problem. The main disadvantage of the existing system is that no trust values calculated, in such cases consumer difficult to find out the best trustworthy available in service provider.

PROPOSED SYSTEM

Even though there are lot solutions to finding trustworthy methodologies, the proposed algorithm is simple way to find the trustworthy among the service provider. In proposed system, there are only one consumer and many providers. Since the rating of the other consumers can help consumer to detect the best among the all service providers. The trust rate measurements are based on the rating of the other consumers who already used the service of the service provider. The rating scale of 1 to 5 and the average of the given rating provide the best solution to analysis the trustworthy. Among the consumers, rating can give in the various scales of attributes of the service providers and mode of services that they are doing.

ADVANTAGE

The proposed system can have consumer influence to find the trustworthy in trusted network. The scheme that proposed is very simple method among all other methods present in current systems to find the trustworthy. The Best possible solution is available with help of rating system and trust value in this method.

SYSTEM ARCHITECTURE
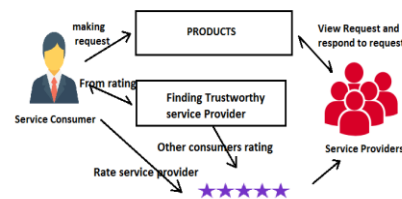
IV. SYSTEM IMPLEMENTATION MODULES

1. ADD RESOURCE

The resources have been uploading in database in order to view for users. Resources can be uploading, modify or delete. The added resources can be visible to user and user can apply with required details. User can add details with their quotation of application. So that user can implement their work.

2. ALLOCATE RESOURCE

The received applications are viewed by admin. Admin then, find the available space and view application and based on that, algorithm applied to sort the best

user to be allocated or the allocation space will be measured according to the quotation of user had submitted. The allocated resource can be utilized by user and admin need to intimate the user that how much resource have been allocated.
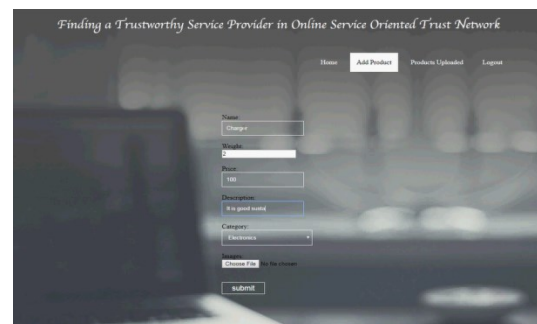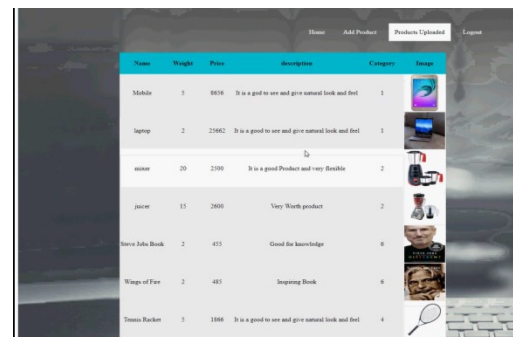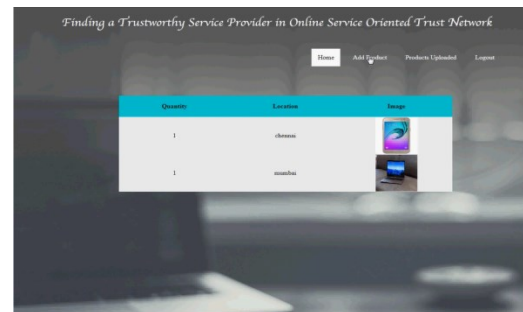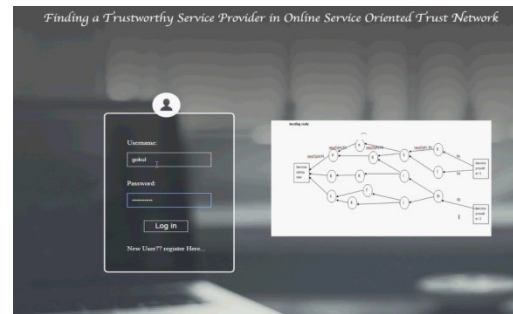
3. USER QUERIES

Users can have queries about the process. This part of project is dedicated to make and get response for queries that are needed to answerable. The major part of the modules is making project as interactive one, queries have been very normally arise to users regarding different details about the process.

4. GRAPH ANALYSIS

Graph analysis is the part where admin can knows the statistics about process of details. The data are taken from the project flow and it shows until updated value. The data are gives clear solution to admin that part of improvement and user satisfaction and other factors.

V. SCREEN SHOTS

VI.   CONCLUSION

The suggested approach is more dependable even if there are several approaches available to address the issue of finding trustworthy. Finding the most reliable network depends on the availability of customers. It is anticipated that this suggested work will be enhanced by additional future effort. This work has several drawbacks, such as the inability of certain users to take it seriously. We can address the shortcomings of the current work in the future by taking into account their shortcomings.

REFERENCES

1. J. Bi, J. Wu and W. Zhang, "A Trust and Reputation Based Anti-SPIM Method", *Proc. IEEE INFOCOM*, pp. 2485-2493, Apr. 2008.

2. Partheeban Chandrasekaran and Babak Esfandiari, *Toward a testbed for evaluating computational trust models*, vol. 2, no. 8, 2015.

3. L. Guanfeng, W. Yan, M.A. Orgun and L. Ee-Peng, "A heuristic algorithm for trust-oriented service provider selection in complex social networks", *Proc. IEEE Int. Conf. Serv. Comput. (SCC)*, pp. 130-137, 2010.

4. C.K. Shyamala, N. Ashok and B. Narayanan, "Trust-based multi-path Security Scheme for Ad-hoc
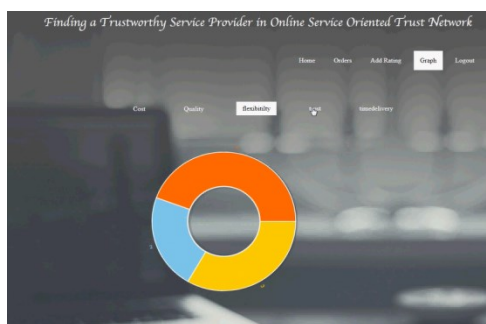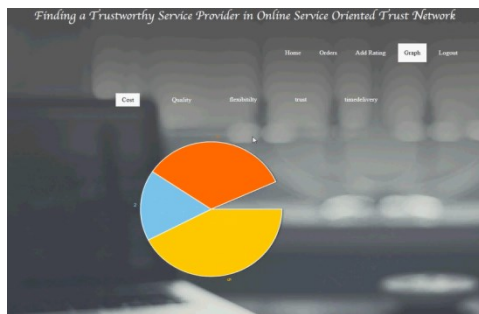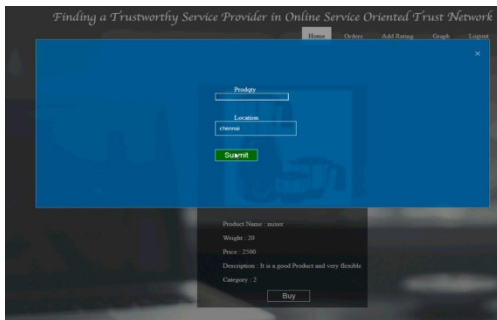
networks", *International Journal of Control Theory and Applications*, vol. 8, pp. 1735-1742, 2015.

5. Yan Wang, Guanfeng Liu and An LiuAn, "Efcient Multiple Trust Paths Finding Algorithm for Trustworthy Service Provider Selection in Real-Time Online Social Network Environments", *IEEE International Conf. Serv. Comput.*.

6. L. Guanfeng, Y. Wang, M. Orgun and E. Lim, "Finding the optimal social trust path for the selection of trustworthy service providers in complex social networks", *IEEE Trans. Serv. Comput.*, vol. 6, no. 2, pp. 152-167, Apr./Jun. 2013.

7. Sathyadevan Shiju, B.S. Kalarickal and M.K. Jinesh, "Security Trust and Implementation Limitations of Prominent IoT Platforms", *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA)*, vol. 2, pp. 85-95, 2015.

8. C.K. Shyamala and T.R. Padmanabhan, "A trust-reputation model offering data retrievability and correctness in distributed storages", *(2014) International Journal of Computers and Applications*, vol. 36, no. 2, pp. 56-63.

9. G. Liu, Y. Wang, M.A. Orgun and H. Liu, "Discovering Trust Networks for the Selection of Trustworthy Service Providers in Complex Contextual Social Networks", *2012 IEEE 19th International Conference on Web Services*, pp. 384-391, 2012.

10. B. Yang, Y. Lei, J. Liu and W. Li, "Social Collaborative Filtering by Trust", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 39, no. 8, pp. 1633-1647, Aug. 2017.

11. B. Zhang, R. Yong, M. Li, J. Pan and J. Huang, "A Hybrid Trust Evaluation Framework for E-Commerce in Online Social Network: A Factor Enrichment Perspective", *IEEE Access*, vol. 5, pp. 7080-7096, 2017.

12. K.B. Yedugiri, S. Chandni, P.S. Raj and S. Souparnika, "Recommender systems - A deeper insight", *International Journal of Applied Engineering Research*, vol. 9, pp. 28521-28531, 2014.

13. M. Jamali and M. Ester, "TrustWalker: A Random Walk Model for Combining Trust-Based and Item-Based Recommendation", *Proc. ACM SIGKDD Intl Conf. Knowledge Discovery and Data Mining (KDD 09)*, pp. 29-42, 2009.

14. Duncan S. Wong, Guanfeng Liu and Yan Wang, Multiple QoT Constrained Social Trust Path Selection in Complex Social Networks, IEEE, 2012.

15. R. Guha, R. Kumar, P. Raghavan and A. Tomkins, "Propagation of Trust and Distrust", *Proc. Intl Conf. World Wide Web (WWW 04)*, pp. 403-012, 2004.