ISSN:2249-5789

Service Oriented Smartphone Based Social Network: An Enhancement In Trustworthyness

MS.DEEPA BAGDE, PROF.SULABHA PATIL, PROF.NEHA MOGRE
Department of Computer Science and Engineering
Tulsiramji Gaikawad College Of Engineering And Technology
Nagpur,India
Email id: deepa_78384@yahoo.co.in
Contact no.: 9890718385

***Abstract*—** In this, we propose a Trustworthy Service Evaluation (TSE) system to enable users to share service reviews in service-oriented mobile social networks (S-MSNs). Each service provider independently maintains a TSE for itself, which collects and stores users' reviews about its services without requiring any third trusted authority. The service reviews can then be made available to interested users in making wise service selection decisions. We also verify the users for trustworthiness. Services are also trustworthy by detecting the Sybil attacks.

Keywords— Mobile social networks, trust evaluation, Sybil attack, trustworthiness, email verification, expert review.

Introduction

In service-oriented mobile social network environments, computing resources are modelled as services, which can be used directly or composed into other services. Services are being widely adopted in modern distributed environments, such as for cloud computing. In many domains, often multiple services provide similar functional properties. For example, several practical services, offered by airlines and travel agencies, provide airline tickets. Therefore, distinguishing and selecting services with the desired non-functional characteristics becomes essential both for direct interaction and for specifying composite services. We address the problem of selecting services based on criteria such as user requirements and service qualities. Recent research on trust modelling provides us with a promising starting point for a solution to service selection. Trust is a key basis of interaction in an open setting, indicating the relationships between the parties involved. For example, in a service-oriented context, a party Alice may trust another party Bob, because Alice expects Bob will provide a service of the desired functionality and quality. We define trust-aware service selection as selecting desired services based on the trust placed in their ability to deliver specified values of the specified qualities.

In the S-MSNs, service providers (restaurants and grocery stores) offer location based services to local users and aim to attract the users by employing various advertising approaches, for example, sending e-flyers to the nearby passengers via wireless connections. Unlike the global counterparts, the interests of the local service providers are in serving the users in close geographic vicinity because most users choose services based on the comparison of the service quality and the distance advantage. In the S-MSNs, to establish the trust relations between the service providers and the user is particularly important. With a higher reputation, a service provider is more likely to be chosen by the users. However, the S-MSNs are autonomous and distributed networks where no third trusted authority exists for bootstrapping the trust relations. Therefore, for the users in the S-MSNs, how to enable the trust evaluation of the service providers is a challenging problem.

Estimating trust from direct experience with a service is not straightforward, because some services may not directly expose details of their composition to their consumers. A consumer may interact with a composite service without knowing much about the qualities of the services that underlie it. In such a case, evaluating the trustworthiness of a service is nontrivial. For example, a consumer may book an itinerary at a travel agency, which may use underlying services for flights, hotels, and ground transportation. Suppose the consumer is not satisfied with the composite service because of its late response time. The service selection should penalize the composite service, as well as some or all of the constituent

ones. If the hotel service, for instance, is determined to be the cause of an unsatisfactory quality value, the service selection should reflect the changes in the way that consumers or other composite services would become reluctant to interact with it. Also, as the amount of experience of the rater (as captured in the model) increases, the model should be able to suggest superior compositions.

Trustworthy service evaluation (TSE) systems enable service providers or any third trusted authority to receive user feedback, known as service reviews or simply reviews, such as compliments and complaints about their services or products. By using the TSE, the service providers learn the service experiences of the users and are able to improve their service strategy in time. In addition, the collected reviews can be made available to the Public, which enhances service advertising and assists the users in making wise service selections. The TSE is often maintained by a third trusted authority who is trusted to host authentic reviews. Popular TSE can be found in web based social networks such as Facebook and online stores like eBay. They are important marketing tools for service providers who target the global market.

Related work

Distributed systems are vulnerable to sybil attacks, where an adversary manipulates bogus identities or abuse pseudonyms to compromise the effectiveness of the systems. For example, in the peer-to-peer networks, Douceur indicated that the sybil attacks can compromise the redundancy of distributed storage systems. In the sensor networks, Karl of and Wagner showed that the sybil attacks can damage the routing efficiency. Newsome et al. Proposed many defense mechanisms, such as, radio resource testing, key validation for random key predistribution, and position verification. In vehicular ad hoc networks, Lu et al. proposed an efficient detection mechanism on double registration, which can be conducted to mitigate the possible sybil attacks. The sybil attacks in social networks have attracted great attention recently. In social networks, Wei et al. mentioned the existence of a trusted authority can mitigate the effect of the sybil attacks, but they considered that such requirements impose additional burdens on users which is not acceptable. In this paper, we study the sybil attacks in the S-MSNs, where the registered users can legally apply for multiple pseudonyms and alternatively use the pseudonyms for preserving their identity and location privacy. In the meantime, the lack of the in-network third trusted authority makes it very difficult to detect the sybil attacks. We identify two typical types of the sybil attacks, propose a sophisticated pseudonym design, and built the SrTSE based on the bTSE to resist the two sybil attacks.

Mobile social networks extend social networks in the by allowing mobile users to discover and interact with existing. Despite their promise to enable exciting applications, serious security and privacy concerns have hindered wide adoption of these networks. The Sybil attack was first introduced by Douceur in the context of peer-to-peer networks. In this, we investigate the Sybil attack, which is a harmful attack in sensor networks. In Sybil attack, a malicious node behaves like it was a larger number of nodes, like by impersonating other nodes or simply by claiming false identities. In this paper, we examine how the Sybil attack can used to attack several protocols in wireless sensor network. So first consider attacks on distributed storage an algorithm, similar to the Douceur describes in the peer-to-peer environment. To defend the Sybil attack, we can value that each node identity is an identity presented by the corresponding physical node. There are two types to validate an identity we define the Sybil attack and establish taxonomy of that attack by distinguishing different attack types. The definition and taxonomy are important in understanding and analysing the threat that defences of Sybil attack. We present several novel methods by which a node can be verified whether other identities are Sybil identities. A Sybil attack is like computer hacker attack on a peer-to-peer (P2P) network. It is named by the novel Sybil, which recounts medical treatment of a woman with extreme dissociative identity disorder. The attack target only reputation system of the P2P program and also allows the hacker to have an unfair advantage in influencing the reputation and the score of files stored on the P2P network. Several factors determine that how a Sybil attack can be equally affects the reputation system and how easy it is to make an entity; finally whether the program accepts non-trusted entities and their input. Validating accounts can be the best way for administrators to prevent these kinds of attacks, but this sacrifices the anonymity of users.

Formulation of Present Work

In proposed system, we require service providers to maintain the TSE by themselves. In the meantime, we consider the users participate in the TSE in a cooperative manner. We will study possible malicious behaviors conducted by the service providers and the users. For ease of presentation, we refer to service providers as vendors in the sequel.

Because of the proposed system, there are many advantages that are offers to the user of the service, which are, it first identify three unique review attacks, i.e., review linkabilityttack, review rejection attack, and review modification attack in the bTSE and also one of the advantage is the third trusted authority to receive user feedback.

Due to the lack of centralized control, the S-MSN is vulnerable to various security threats. The group authorities are trusted but not a part of the network. In the following, we describe several malicious attacks that aim particularly at the TSE.

Review attack 1: Review linkability attack is executed by malicious users, who claim to be members of a specific group, but disable the group authority to trace the review back to its unique identity, thus breaking review linkability.

Review attack 2: Review rejection attack is launched by the vendor when a user submits a negative review to it. In the

attack, the vendor drops the review silently without responding to the submission request from the user, and hides public opinions and misleads users.
Review attack 3: Review modification attack is performed by the vendor toward locally stored review collections. The vendor inserts forged complimentary reviews, or modifies/ deletes negative reviews in a review collection. Such attacks aim at false advertising by breaking review integrity and influencing user behaviors.

An S-MSN contains multiple vendors offering different or similar services to users. Because each vendor maintains the TSE independently for itself, without loss of generality we consider an S-MSN with a single vendor. There is no third trusted authority in the network. For simplicity, the vendor is assumed to offer a single service. However, the TSE may be trivially extended to multivendor multiservice scenarios by assigning unique identifiers to different vendors and services.

We present the bTSE based on the above-defined models. In the bTSE, a user, after being serviced by the vendor, submits a review to the vendor, which then stores the review in its local repository. Review submission may need cooperation from other users; the user forwards its review to a nearby user who wants to submit a review to the same vendor and expects that user to submit their reviews together. User cooperation increases SR and reduces SD at the cost of additional transmission efforts.
During review submission, data integrity, authenticity, and nonrepudiation can be obtained by directly applying traditional cryptography techniques such as hashing and digital signature on review content.

In this social network, we divide the whole project into three main modules. In the first module the client i.e. users need to register first and after registration user account is created and cab be to login.

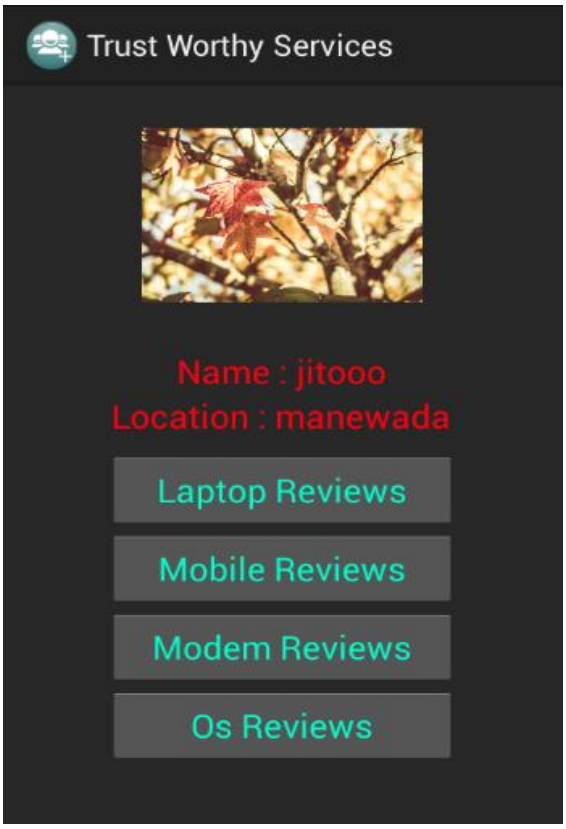
In the second module server is design to save the data in the database. User is not directly added in the database until and unless the verification is done. For the verification of user we provide the verification link to the users email address which is to be genuine.

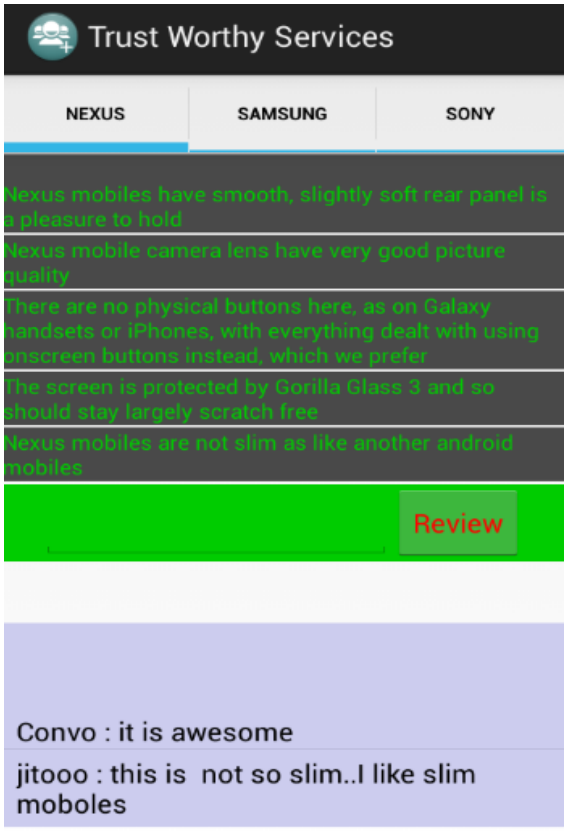
As soon as the user clicked on verification link sent for verification, they added to the social network.

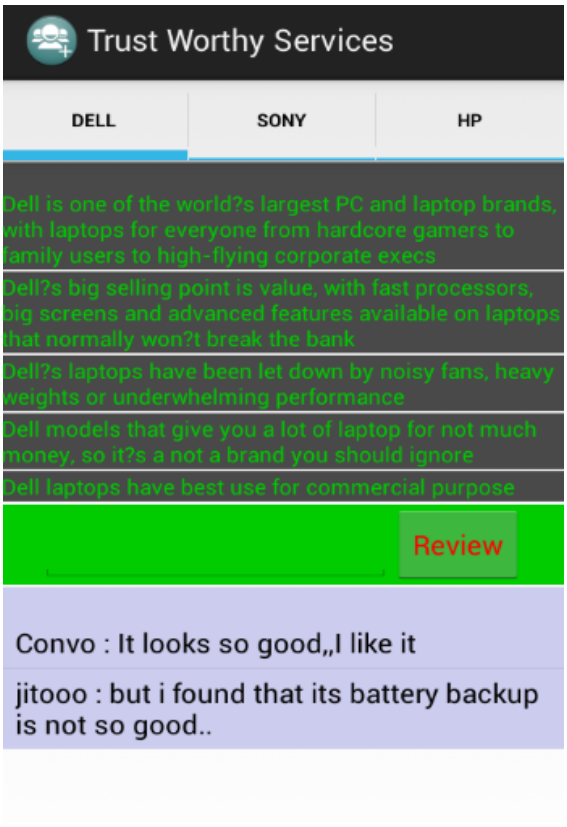
Along with the verification link we create the list of products which is to be selected by the users for reviews. The products are like laptops, mobiles and operating systems.

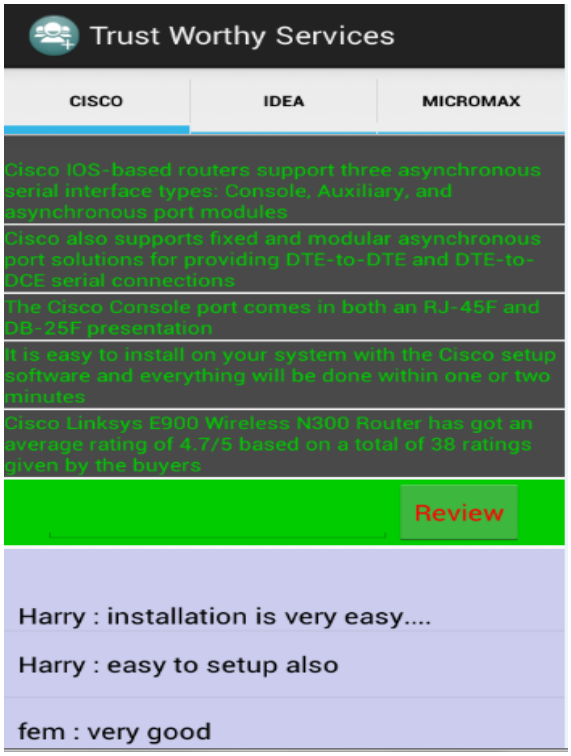
In the third and final module Both Client and Server Communication Part is added. In this we have added the 5 Expert reviews which will help users to decide about products. These reviews will guide the user and includes both positive as well as negative points about the product. After expert reviews the users can provide unlimited review about the products and cannot be edited or deleted by any other user or administrator as well.
For the security we implement AES algorithm and another technique which is use is the Aggregate Signature technique.

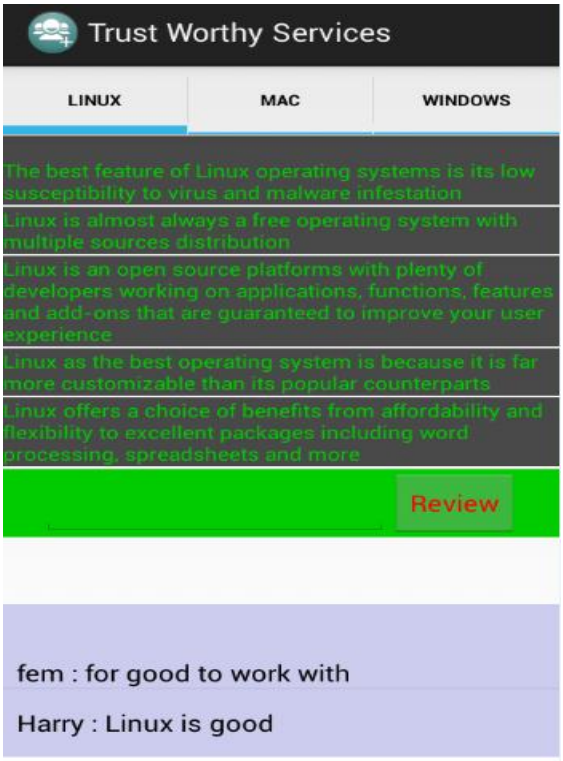
Analysis of Results

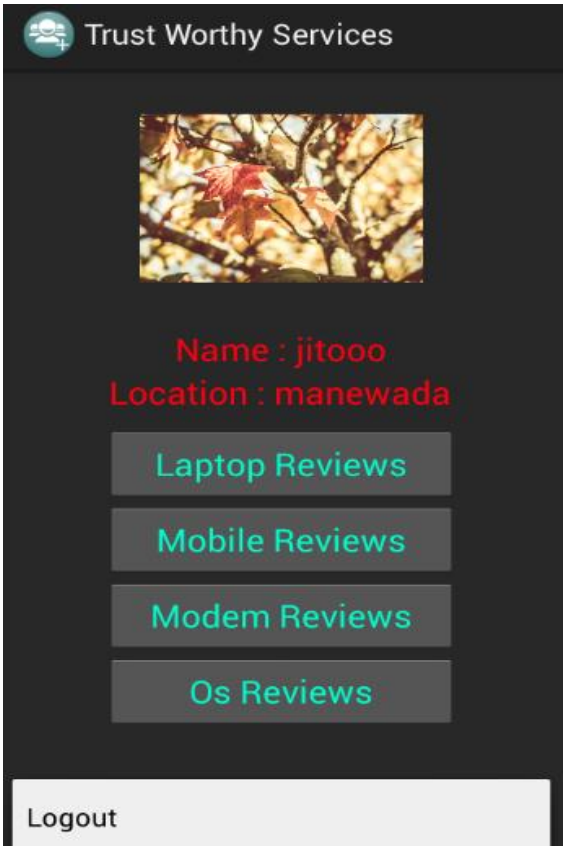

Trust Worthy Services
Name : jitooo
Location : manewada
Laptop Reviews
Mobile Reviews
Modem Reviews
Os Reviews


Trust Worthy Services
NEXUS
SAMSUNG
SONY
Nexus mobiles have smooth, slightly soft rear panel is a pleasure to hold
Nexus mobile camera lens have very good picture quality
There are no physical buttons here, as on Galaxy handsets or iPhones, with everything dealt with using onscreen buttons instead, which we prefer
The screen is protected by Gorilla Glass 3 and so should stay largely scratch free
Nexus mobiles are not slim as like another android mobiles
Review
Convo : it is awesome
jitooo : this is not so slim..I like slim moboles


Trust Worthy Services
DELL
SONY
HP
Dell is one of the world?s largest PC and laptop brands, with laptops for everyone from hardcore gamers to family users to high-flying corporate execs
Dell?s big selling point is value, with fast processors, big screens and advanced features available on laptops that normally won?t break the bank
Dell?s laptops have been let down by noisy fans, heavy weights or underwhelming performance
Dell models that give you a lot of laptop for not much money, so it?s a not a brand you should ignore
Dell laptops have best use for commercial purpose
Review
Convo : It looks so good,,I like it
jitooo : but i found that its battery backup is not so good..


Trust Worthy Services
CISCO
IDEA
MICROMAX
Cisco IOS-based routers support three asynchronous serial interface types: Console, Auxiliary, and asynchronous port modules
Cisco also supports fixed and modular asynchronous port solutions for providing DTE-to-DTE and DTE-to-DCE serial connections
The Cisco Console port comes in both an RJ-45F and DB-25F presentation
It is easy to install on your system with the Cisco setup software and everything will be done within one or two minutes
Cisco Linksys E900 Wireless N300 Router has got an average rating of 4.7/5 based on a total of 38 ratings given by the buyers
Review
Harry : installation is very easy....
Harry : easy to setup also
fem : very good





Conclusion

In this paper,we have proposed a trustworthy social network in which each service provider as well as users should be trustworthy. For service providers to be trustworthy we have added the expert comments which guide the users to choose the service. For users to be trustworthy we have created the verification link in which each user is verified by their email address.

Each user is able to post their own review and can be read other users review about the particular service. But they cannot delete or edit the review of other user as well as their own. We have implemented AES algorithm and Aggregate signature technique and resist the Sybil attack.

References

[1] Xiaohui Liang, Xiaodong Lin, and Xuemin (Sherman) Shen, "Enabling Trustworthy Service Evaluation in Service-Oriented Mobile Social Networks" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014.

[2] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure Friend Discovery in Mobile Social Networks," Proc. IEEE INFOCOM, pp. 1647-1655, 2011.

[3] X. Liang, X. Li, R. Lu, X. Lin, and X. Shen, "Seer: A Secure and Efficient Service Review System for Service-Oriented Mobile Social Networks," Proc. IEEE 32nd Int'l Conf. Distributed Computing Systems (ICDCS), pp. 647-656, 2012.

[4] X. Liang, X. Li, T. Luan, R. Lu, X. Lin, and X. Shen, "Morality- Driven Data Forwarding with Privacy Preservation in Mobile Social Networks," IEEE Trans. Vehicular Technology, vol. 61, no. 7, pp. 3209-3222, Sept. 2012.

[5] T.H. Luan, L.X. Cai, J. Chen, X. Shen, and F. Bai, "VTube: Towards the Media Rich City Life with Autonomous Vehicular Content Distribution," Proc. IEEE CS Eighth Ann. Conf. Sensor, Mesh and Ad Hoc Comm. Networks (SECON), pp. 359-367, 2011.

[6] J.R. Douceur, "The Sybil Attack," Proc. Revised Papers First Int'l Workshop Peer-to-Peer Systems (IPTPS), pp. 251-260, 2002.

[7] J. Newsome, E. Shi, D.X. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses," Proc. Third Int'l Symp. Information Processing in Sensor Networks (IPSN), pp. 259-268, 2004.