IJARES/June 2015/Volume-3/Issue-6/1846-1850 **ISSN 2347- 9337**

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND SCIENCE

IMPLEMENTATION OF TRUST RELATIONS IN MOBILE SOCIAL SYSTEMS

K.Prasanna Kumari[1], B.V.S.P.Pavan Kumar[2]

[1]M.Tech Student, Dept of CSE, Malla Reddy Engineering College for Women, Hyderabad, T.S, India

[2]Assistant Professor, Dept of CSE, Malla Reddy Engineering College for Women, Hyderabad, T.S, India

ABSTRACT:

Distributed systems are susceptible to sybil attacks, where an opponent influences bogus identities to compromise efficiency of the systems. In Service-oriented mobile social networks it is important to provide trust relations among service providers as well as users. Trust evaluation of service providers is an important component towards the achievement of location-based services within an independent network. Trustworthy service evaluation systems (TSE) facilitate service providers to receive user feedback, well-known as service reviews about their services. TSE is found in social networks and are significant marketing tools for service providers who target global market. In designing of TSE for Service-oriented mobile social networks security mechanisms have to be included to oppose the attacks. We put forward a basic trustworthy service evaluation as well as an extended Sybil-resisted TSE structure for Service-oriented mobile social networks. In both systems, no trusted authorities are concerned, and vendor in the neighbourhood continues reviews that are left by users. We introduce two typical sybil attacks, that cause massive damage to the basic trustworthy service evaluation.

Keywords: Sybil attacks, Service-oriented mobile social networks, Trustworthy service evaluation, Trusted authorities.

1. INTRODUCTION:

In recent times, Location-based services come out as an essential need of mobile users. It can be included into a variety of types of networks to acquire capable applications while their functioning has numerous exceptional and autonomous research issues [1]. Location-based services necessitate an efficient way to make an impact on local users and earn their trust with the intention that service providers can get hold of profits. In recent times, sybil attacks within social networks are paying significant attention. Service-oriented mobile social networks are promising networking platforms on which several individuals are capable to correspond with local service providers by means of handheld wireless communication devices. In Service-oriented mobile social networks it is important to provide trust relations among service providers as well as users. Mobile social networks of service oriented are independent and distributed networks where no third trustworthy authority exists for bootstrapping trust associations. For users in mobile social networks of service oriented the challenging issues are towards facilitating trust evaluation of service providers. Trust evaluation of service providers is an important component towards the achievement of location-based services within an independent network. In our work we put forward a system of trustworthy service evaluation to facilitate users to allocate service reviews [2]. We introduce two typical sybil attacks, that cause massive damage to the basic trustworthy service evaluation.

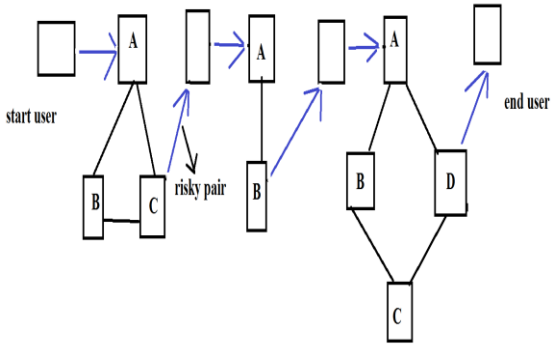

Fig1: A hybrid arrangement

2. OVERVIEW OF SYBIL ATTACKS:

Trustworthy service evaluation systems (TSE) facilitate service providers to receive user feedback, well-known as service reviews about their services. TSE is regularly maintained by means of a trusted authority who is trustworthy to host genuine reviews. TSE is found in social networks and are significant marketing tools for service providers who target global market. By TSE, the service providers gain knowledge of service experiences of users

and improve their service strategy eventually. In designing of TSE for Service-oriented mobile social networks security mechanisms have to be included to oppose the attacks. Notorious sybil attacks moreover cause vast damage to efficiency of trustworthy service evaluation systems. Distributed systems are susceptible to sybil attacks, where an opponent influences bogus identities to compromise efficiency of the systems. We put forward a basic trustworthy service evaluation as well as an extended Sybil-resisted TSE structure for Service-oriented mobile social networks. In both systems, no trusted authorities are concerned, and vendor in the neighbourhood continues reviews that are left by users. We introduce two typical sybil attacks, that cause massive damage to the basic trustworthy service evaluation. Under sybil attacks, basic trustworthy service evaluation system cannot effort as likely since a single user can misuse pseudonyms to make multiple unlinkable fake reviews in short period. To resist such attacks, in sybil-resisted TSE structure pseudonyms are fixed with a trapdoor; if any user leaves numerous false reviews in the direction of a vendor in a predefined instance, its real identity will be exposed to public. Since TSE assigns numerous pseudonyms towards a registered user, the sybil attacks can effortlessly occur in the TSE. Sybil attack 1: is an attack that is launched by malevolent users: One registered user leaves numerous reviews in direction of a vendor within a time slot, where reviews are fake and unconstructive to the service. Sybil attack 2: an attack is launched by means of malevolent vendors by means of colluded users. A malevolent vendor enquires one registered user to leave numerous reviews in the direction of itself in a time slot, where reviews are constructive to the service [3][4]. These two sybil attacks construct imprecise information, which is unreasonable to moreover vendors or else users, and disrupt efficiency of the TSE. We put forward an additional security mechanism to efficiently oppose sybil attacks by means of restricting each user to make only one review toward a vendor within a predefined time slot.

3. SCHEMING OF TRUSTWORTHY SERVICE EVALUATION SYSTEMS:

In basic trustworthy service evaluation, a user, subsequent to being serviced by vendor, submits a review towards the vendor, which subsequently accumulates review in its confined repository. Review

submission might necessitate cooperations from additional users; the user forwards its review towards a nearby user who desires to submit a review towards the similar vendor and expect that user to submit their reviews mutually. For the duration of review submission, integrity of data, as well as non-repudiation are obtained by applying conventional cryptography methods on review content. In the basic trustworthy service evaluation reviews are controlled to reflect their adjacency all the way through user cooperation. Vendor's basically rejecting or else modifying reviews will break reliability of review structure, as a consequence being detected by public. As a result, in basic trustworthy service evaluation, we assume a hybrid arrangement as shown in fig1; consist of a chain as its skeleton. The basic trustworthy service evaluation was extended towards a Sybil-resisted TSE structure which successfully prevents sybil attacks. The sybil attack 1 is commenced by means of a group of registered users who aims at informing other users bad service from a vendor although service of the vendor is good. Sybil attack 2 is commenced by means of a vendor as well as a group of registered users who intends at raising status of the service from a vendor although the service of vendor is not that superior [5]. In Sybil-resisted TSE structure we introduce a new solution to put off two sybil attacks. In Sybil-resisted TSE structure we believe that a user has no need to make numerous reviews in the direction of a vendor within a short period and allows a user to leave merely one review towards a vendor in support of a predefined time slot. If a user produces numerous reviews with similar pseudonyms, linkability of the reviews are simply verified by public; if a user makes numerous reviews with dissimilar pseudonyms toward a vendor within a time slot, its actual identity is uncovered towards the public [6].

4. CONCLUSION:

In recent times, sybil attacks within social networks are paying significant attention. Service-oriented mobile social networks are promising networking platforms on which several individuals are capable to correspond with local service providers by means of handheld wireless communication devices. Mobile social networks of service oriented are independent and distributed networks where no third trustworthy authority exists for bootstrapping trust associations. Trustworthy service evaluation

systems (TSE) facilitate service providers to receive user feedback, well-known as service reviews about their services. In designing of TSE for Service-oriented mobile social networks security mechanisms have to be included to oppose the attacks. By TSE, the service providers gain knowledge of service experiences of users and improve their service strategy eventually. In our work we put forward a system of trustworthy service evaluation to facilitate users to allocate service reviews. We put forward a basic trustworthy service evaluation as well as an extended Sybil-resisted TSE structure for Service-oriented mobile social networks. In both systems, no trusted authorities are concerned, and vendor in the neighbourhood continues reviews that are left by users. We introduce two typical sybil attacks, that cause massive damage to the basic trustworthy service evaluation. Under sybil attacks, basic trustworthy service evaluation system cannot effort as likely since a single user can misuse pseudonyms to make multiple unlinkable fake reviews in short period. Since TSE assigns numerous pseudonyms towards a registered user, the sybil attacks can effortlessly occur in the TSE.

REFERENCES

[1] 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.

[2] D. Quercia and S. Hailes, "Sybil Attacks Against Mobile Users: Friends and Foes to the Rescue," Proc. IEEE INFOCOM, pp. 336- 340, 2010.

[3] R. Lu, X. Lin, X. Liang, and X. Shen, "A Dynamic Privacy- Preserving Key Management Scheme for Location-Based Services in VANETs," IEEE Trans. Intelligent Transportation Systems, vol. 13, no. 1, pp. 127-139, Mar. 2012.

[4] R. Lu, X. Lin, T. Luan, X. Liang, and X. Shen, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs," IEEE Trans. Vehicular Technology, vol. 61, no. 1, pp. 86-96, Jan. 2012.

[5] X. Boyen and B. Waters, "Full-Domain Subgroup Hiding and Constant-Size Group Signatures," Proc. 10th Int'l Conf. Practice and Theory Public Key Cryptography, pp. 1-15, 2007.

[6] X. Liang, Z. Cao, J. Shao, and H. Lin, "Short Group Signature without Random Oracles," Proc. Ninth Int'l Conf. Information and Comm. Security (ICICS), pp. 69-82, 2007.