International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October 2016

Performance analysis on adaptive control for security using Trust management using IOT in OSN

Kancharla Sai Krishna[1] & Bagam Laxmaiah[2]

[1]M-Tech Dept of CSE Sarada Institute Of Technology And Science , Khammam.

[2]Associate Professor & HOD Dept of CSE Sarada Institute Of Technology And Science , Khammam

Abstract

A social Internet of Things (IoT) framework can be seen as a blend of conventional distributed systems and informal communities, where "things" self-sufficiently set up social connections as per the proprietors' interpersonal organizations, and look for trusted "things" that can give administrations required when they come into contact with each other deftly. We propose and investigate the outline thought of versatile trust administration for social IoT frameworks in which social connections develop powerfully among the proprietors of IoT gadgets. We uncover the configuration tradeoff between trust merging versus trust variance in our versatile trust administration convention outline. With our versatile trust administration convention, a social IoT application can adaptively pick the best trust parameter settings in light of changing IoT social conditions such that trust evaluation is exact as well as the application execution is amplified. We propose a table-lookup technique to apply the investigation comes about powerfully and exhibit the plausibility of our proposed versatile trust administration plan with two certifiable social IoT administration arrangement applications.

Keywords: Trust management, Internet of things, social networking, performance analysis, adaptive control, security.

1. Introduction

A social Internet of Things (IoT) system can be viewed as a mix of traditional peer-to-peer (P2P) networks and social networks, where “things” autonomously establish social relationships according to the owners’ social networks, and seek trusted things that can provide services needed when they come into contact with each other opportunistically in both the physical world and cyberspace. It is envisioned that the future social IoT will connect a great amount of smart objects in the physical world, including radio frequency identification (RFID) tags, sensors, actuators, PDAs, and smartphones, as well as virtual objects in cyberspace such as data and virtual desktops on the cloud. The emerging paradigm of the social Internet of Things (IoT) has attracted a wide variety of applications running on top of it, including e-health, smart-home,

smart-city, and smart-community. We will use the terms things, objects, and devices interchangeably in the paper. Such future social IoT applications are likely oriented toward a service oriented architecture where each thing plays the role of either a service provider or a service requester, or both, according to the rules set by the owners. Unlike a traditional service-oriented P2P network, social networking and social relationship play an important role in a social IoT, since things (real or virtual) are essentially operated by and work for humans. Therefore, social relationships among the users/owners must be taken into account during the design phase of social IoT applications. A social IoT system thus can be viewed as a P2P owner-centric community with devices (owned by humans) requesting and providing services on behalf of the owners. IoT devices establish social relationships autonomously with other devices based onsocial rules set by their owners, and interact with each other opportunistically as they come into contact. To best satisfy the service requester and maximize application performance, it is crucial to evaluate the trustworthiness of service providers in social IoT environments. This paper concerns trust management in social IoT environments. The motivation of providing a trust management system for a social IoT system is clear: There are misbehaving owners and consequently misbehaving devices that may perform discriminatory attacks based on their social relationships with others for their own gain at the expense of other IoT devices which provide similar services. Further, misbehaving nodes with close social ties may collude and monopoly a class of services. Since trust provisioning in this environment inherently is fully integrated with service provisioning (i.e., one must decide whether or not to use a service provided by a device based on the trust toward the device), the notion of trust-based service management is of paramount importance. There is a large body of trust management protocols for P2P service computing systems. These P2P service systems share a common characteristic with social IoT systems in that services are provided by nodes in the system so that trust evaluation of nodes is critical to the functioning of the system. However, trust protocols for P2P service computing systems lack consideration of the social aspects of IoT device owners, and are not applicable to a social IoT system comprising real or virtual heterogeneous “things” with ownership, friendship and community of interest relationships connected with each other by various ways (via the Internet), and operated by their owners with a variety of social behaviors to collect information, provide services, provide recommendations, make decisions, and take actions. On the other hand, trust protocols for social networks are more concerned with trust assessment of social entities based on

frequency, duration and nature of contacts (such as conversation and propagation) between two social entities, without considering P2P service computing environments in which IoT devices seek and provide service when they come into contact with each other opportunistically. To date there is little work on trust management for social IoT systems, especially for dealing with misbehaving owners of IoT devices that provide services to other devices in the system. We compare and contrast our trust protocol design principles with prior work in Section 7 Related Work.

1.1 ADAPTIVE TRUST MANAGEMENT PROTOCOL:

In this paper we propose a versatile trust administration convention for social IoT frameworks. Our technique is reasonable to be connected to social IoT trial stages as examined. We will likely upgrade the security and expansion the execution of social IoT applications. We expect to outline and approve a versatile trust administration convention that can progressively conform trust plan parameter settings because of changing environment conditions to give exact trust appraisal (regarding real status) and to boost application execution. The requirement for versatile trust administration originates from the way that social connections amongst proprietors and in this way social practices of proprietors are developing. A case is that proprietors conveying IoT gadgets can frequently move from an amicable situation (e.g., a social club) to an antagonistic domain (e.g., an area one doesn't go regularly).

We are especially inspired by trust convention outline that can manage getting out of hand hubs. Such a convention must have alluring trust joining, precision, and strength properties. Our commitment in respect to existing trust administration conventions for IoT frameworks is that we build up a versatile trust administration convention in social IoT frameworks. Not at all like trust frameworks intended for P2P systems, sensor systems, delay tolerant systems, and versatile impromptu systems, our trust administration convention takes progressively changing social connections among the "proprietors" of gadgets in IoT frameworks into record and show that the attractive union, precision, and strength properties are fulfilled by broad recreation. Further, utilizing two genuine social IoT applications, we exhibit that our versatile trust administration convention is able to do adaptively modifying the best trust parameter setting because of powerfully changing situations to enhance trust evaluation precision and to boost application execution, in spite of the nearness of acting up hubs upsetting the usefulness of a social IoT framework.

Client Centric Social IoT Environments:

We consider a client driven social IoT environment with no brought together trusted power. Each IoT gadget has itsexceptional personality which can be accomplished through standard systems, for example, PKI. A gadget speaks with different gadgets through the overlay interpersonal organization conventions, or the fundamental standard correspondence system conventions (wired or remote). Each gadget has a proprietor who could have numerous gadgets. Social connections between proprietors are interpreted into social connections between IoT gadgets as takes after: Each proprietor has a rundown of companions (i.e., different proprietors), speaking to its social connections. This companionship list shifts powerfully as a proprietor makes or denies different proprietors as companions. On the off chance that the proprietors of two hubs are companions, then it is likely they will be helpful with each other. A gadget might be conveyed or worked by its proprietor in certain group interest situations (e.g., work versus home or a social club). Hubs having a place with a comparable arrangement of groups likely have comparable interests or abilities. Our social IoT model depends on social connections among people who are proprietors of IoT gadgets. We take note of that the gadget to-gadget self-governing social relationship is likewise a potential for the social IoT worldview.

2. Related Work

The trustworthy IoT applications in past are only considered as an imitation level, because nobody is interested in trust of next person to reveal the private information, basically this kind of information are highly leaked via Service Providers. Service providers take advantage of this dynamic and ever-growing technology landscape by proposing innovative context-dependent services for mobile subscribers. Location-based Services (LBS), for example, are used by millions of mobile subscribers every day to obtain location-specific information.

Privacy of a user's location or location preferences fully depends upon the Service providers or the third party vendors. For instance, such information can be used to de-anonymize users and their availabilities, to track their preferences or to identify their social networks. For example, in the taxi-sharing application, a curious third-party service provider could easily deduce home/work location pairs of users who regularly use their service.

Disadvantages:

- Service Providers takes an advantage of this kind of data sharing and Third Party providers or their devices can easily catch the location of the source person intend.
- Privacy of a user's location or location preferences, with respect to other users

and the third-party service provider, is a critical concern in such location sharing based applications.

- Without effective protection, even parse location information has been shown to provide reliable information about a users' private sphere, which could have severe consequences on the users' social, financial and private life. Even service providers who legitimately track users' location information in order to improve the offered service can inadvertently harm users' privacy, if the collected data is leaked in an unauthorized fashion or improperly shared with corporate partners.
- Possibility to redirect the destination parties to the favorable place of the Service providers or third party providers.

3. Implementation

3.1 Proposed System:

In the proposed System we formulate trustworthy IoT Systems. The motivation of providing a trust management system for a social IoT system is clear: There are misbehaving owners and consequently misbehaving service providers that may perform discriminatory attacks based on their social relationships with others for their own gain at the expense of other IoT devices which provide similar services. Further, misbehaving users with close social ties may collude and monopoly a class of services. Since trust provisioning in this environment inherently is fully integrated with service provisioning (i.e., one must decide whether or not to use a service provided by a device based on the trust toward the device), the notion of trust-based service management is of paramount importance. In this system we propose an adaptive trust management protocol for social IoT systems. Our method is suitable to be applied to social IoT experimental platforms. Our goal is to enhance the security and increase the performance of social IoT applications. We aim to design and validate an adaptive trust management protocol that can dynamically adjust trust design parameter settings in response to changing environment conditions to provide accurate trust assessment (with respect to actual status) and to maximize application performance. The need for adaptive trust management stems from the fact that social relationships between owners and thus social behaviors of owners are evolving. An example is that owners carrying IoT devices can often move from a friendly environment (e.g., a social club) to a hostile environment (e.g., a neighborhood one does not go often).

Advantages

- Addresses the privacy issue in LSBSs by focusing on a specific algorithm called Location Safe Algorithm.

- Given a set of user location preferences, the LSA is to determine a location among the proposed ones such that the maximum distance between this location and all other user's locations is minimized, i.e. it is fair to all users.
- The Secure Hash Algorithm (SHA) is implemented to provide the optimal location oriented transmission with privacy preserving concern.

In this method we achieve two processes simultaneously without the help of third party service providers. There are: o Location Check-Ins o Location Sharing

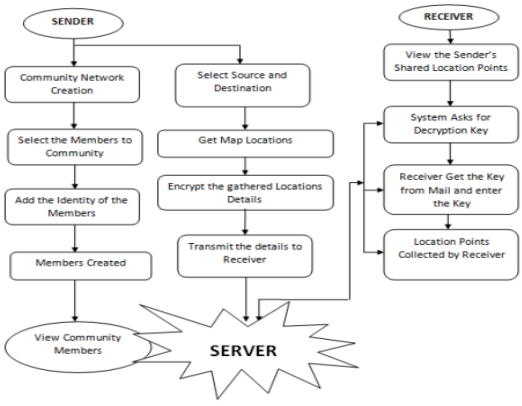

Fig. 1 System Architecture.

4. Experimental Work

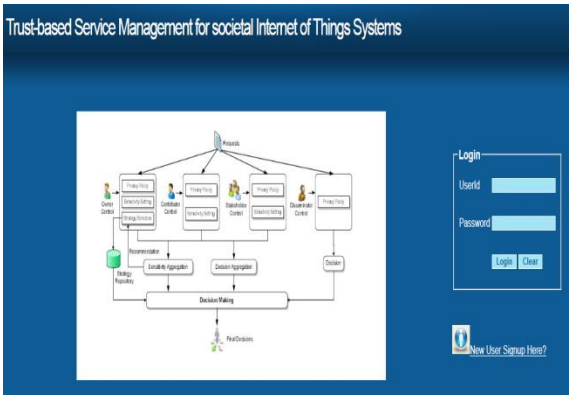

Fig 2: System Home Page.

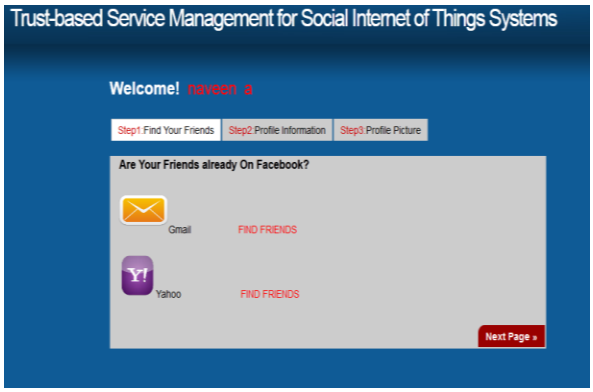

Fig 3: User Home Page.

5. Conclusion

In this system, we developed and analyzed an adaptive trust management protocol for social IoT systems and its application to service management. Our protocol is distributed and each node only updates trust towards others of its interest upon encounter or interaction events. The trust assessment is updated by both direct observations and indirect recommendations, with parameters □and □being the respective design parameters to control trust propagation and aggregation for these two sources of information to improve trust assessment accuracy in response to dynamically changing conditions. We analyzed the effect of α and β on the convergence, accuracy, and resiliency properties of our adaptive trust management protocol using simulation. The results demonstrate that (1) the trust evaluation of adaptive trust management will converge and approach ground truth status, (2) one can tradeoff trust convergence speed for low trust

fluctuation, and (3) adaptive trust management is resilient to misbehaving attacks. We demonstrated the effectiveness of adaptive trust management by two real-world social IoT applications. The results showed our adaptive trust-based service composition scheme outperforms random service composition and approaches the maximum achievable performance based on ground truth. We attributed this to the ability of dynamic trust management being able to dynamically choose the best design parameter settings in response to changing environment conditions. There are several future research areas. We plan to further test our adaptive trust management protocol's accuracy, convergence and resiliency properties toward a multitude of dynamically changing environment conditions under which a social IoT application can automatically and autonomously adjust the best trust parameter settings dynamically to maximize application performance. Another direction is to explore statistical methods to exclude recommendation outliers to further reduce trust fluctuation and enhance trust convergence in our adaptive trust management protocol design.

6. References

[1] S. Adali et al., "Measuring Behavioral Trust in Social Networks," IEEE International Conference on Intelligence and Security Informatics, Vancouver, BC, Canada, May 2010.

[2] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," Computer Networks, vol. 54, no. 15, Oct. 2010, pp. 2787-2805.

[3] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The Social Internet of Things (SIoT) - When social networks meet the Internet of Things: Concept, architecture and network characterization," Computer Networks, vol. 56, no. 16, Nov. 2012, pp. 3594-3608.

[4] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," Computer Communications, vol. 54, 2014, pp. 1-31.

[4] F. Bao, and I. R. Chen, "Dynamic Trust Management for Internet of Things Applications," 2012 International Workshop on Self-Aware Internet of Things, San Jose, California, USA, September 2012.

[5] F. Bao, Dynamic Trust Management for Mobile Networks and Its Applications, ETD, Virginia Polytechnic Institute and State University, May 2013.

[6] F. Bao, I. R. Chen, M. Chang, and J. H. Cho, "Hierarchical Trust Management for Wireless Sensor Networks and Its Applications to Trust-Based Routing and Intrusion Detection," IEEE Trans. on Network and Service Management, vol. 9, no. 2, 2012, pp. 161-183.

[7] F. Bao, I. R. Chen, and J. Guo, "Scalable, Adaptive and Survivable Trust Management for Community of Interest Based Internet of Things

Systems," 11th IEEE International Symposium on Autonomous Decentralized System, Mexico City, March 2013.

[8] N. Bui, and M. Zorzi, "Health Care Applications: A Solution Based on The Internet of Things," the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies, Barcelona, Spain, Oct. 2011, pp. 1-5.

[9] B. Carminati, E. Ferrari, and M. Viviani, Security and Trust in Online Social Networks, Morgan & Claypool, 2013.

[10] I. R. Chen, F. Bao, M. Chang, and J.H. Cho, "Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 5, 2014, pp. 1200-1210.

[11] I. R. Chen, F. Bao, M. Chang, and J.H. Cho, "Trust-based intrusion detection in wireless sensor networks," IEEE International Conference on Communications, Kyoto, Japan, June 2011, pp. 1-6.

[12] I.R. Chen, F. Bao, M. Chang, and J. H. Cho, "Trust management for encounter-based routing in delay tolerant networks," IEEE Global Telecommunications Conference (GLOBECOM 2010), 2010, pp. 1-6.

Candidate Details:

KANCHARLA SAI KRISHNA
B-Tech in Sai spurthi Institute Of Science And Technology, B.gangaram, percentage is 60.55% , year of completed April 2013. M-Tech Computer Science And Engineering in Sarada Institute Of Technology And Science, Khammam.

Mail id: ksaikrishna002@gmail.com

Phone number: 9666020297

Guide Details

Bagam Laxmaiah.
Email-d: laxmanmtech99@gmail.com
Phone Number: 8106467177.
Experience: 7 years.
Qualification: M.Tech from JNTU, Hyderabad.
Designation: Associate Professor.
Working: Head of Department, Sarada Institute of Technology Science (SITS), Khammam..