International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 5, 2016. ISSN: 2348-6600
Reference ID: IJCS-140 PAGE NO: 827-835

A Framework of Online Social IoT System and Trust Management Scheme

MAMATHA[1]& Dr.K.Ramakrishna[2]
[1]M-Tech Dept. of IT Sridevi Women's Engineering College Hyderabad
[2]Professor & HOD, Dept. of IT Sridevi Women's Engineering College Hyderabad

***Abstract*—** Internet of things is going to make a world where physical objects are unlined in corporate into information networks in order to render advanced and intelligent services for human being. Trust management plays a vital role in IOT; there is a need for robust and efficient trust management. Various security issues result in several different requirements to the design of trust management. The propose a framework to separate desired properties of trust management for each type of security issues. A Iot of service provider needs to control access to their performance and providing personalized services. This entails that the service provider requests and stores personal attributes. Nevertheless, many service providers are not sure enough about the correctness of attributes that are revealed by the user during registration. Identity management systems purpose to increase the easy to use of authentication procedures. The exhibits a new approach for user-centric identity management scheme, using trusted modules. Along with the review, we also discover some open search query for future work and accordingly present a new idea over the trust management implementation.

Keywords: Data mining, Internet of Things, Secure Computing.

I. 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

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 5, 2016. ISSN: 2348-6600
Reference ID: IJCS-140 PAGE NO: 827-835

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 asocial IoT, since things (real or virtual) are essentially operated by and work for humans. Therefore, social relationshipsamong the users/owners must be taken into account during the design phase of social IoT applications. A social IoTsystem thus can be viewed as a P2P owner-centric community with devices (owned by humans) requesting and providingservices 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 satisfythe service requester and maximize application performance, it is crucial to evaluate the trustworthiness of serviceproviders in social IoT environments.

This paper concerns trust management in social IoT environments. The motivation of providing a trust managementsystem for a social IoT system is clear: There are misbehaving owners and consequently misbehaving devices that mayperform discriminatory attacks based on their social relationships with others for their own gain at the expense of otherIoT devices which provide similar services. Further, misbehaving nodes with close social ties may collude and monopolya 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 notionof trust-based service management is of paramount importance.

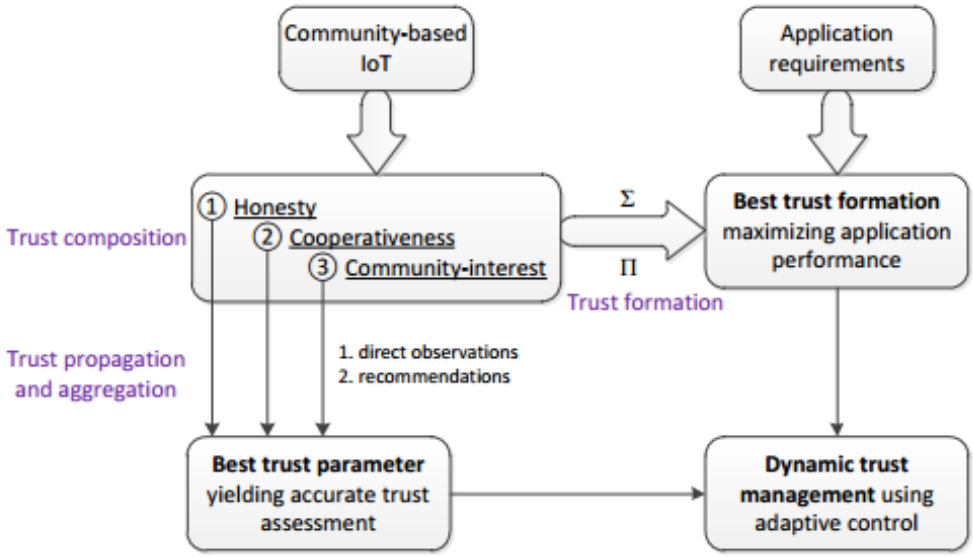
There is a large body of trust management protocols forP2P service computing systems. These P2P service systems share a common characteristic with social IoT systems in thatservices are provided by nodes in the system so that trust evaluation of nodes is critical to the functioning of the system.However, trust protocols for P2P service computing systems lack consideration of

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 5, 2016. ISSN: 2348-6600
Reference ID: IJCS-140 PAGE NO: 827-835

the social aspects of IoT deviceowners, 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), andoperated by their owners with a variety of social behaviors to collect information, provide services, providerecommendations, make decisions, and take actions. On the other hand, trust protocols for social networks are moreconcerned with trust assessment of social entities based on frequency, duration and nature of contacts (such asconversation and propagation) between two social entities, without considering P2P service computing environments inwhich IoT devices seek and provide service when they come into contact with each other opportunistically. To date thereis little work on trust management for social IoT systems, especially for dealing with misbehaving owners of IoT devicesthat provide services to other devices in the system.

II. Adaptive Trust Management

While there is a wealth of social trust metrics available, we choose *honesty*, *cooperativeness*, and *community-interest* as the most striking metrics for characterizing social IoT systems, as illustrated in Figure (2nd level). These trust properties are considered orthogonal but complementary to each other to characterize a node. Each trust property is evaluated separately.



International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 5, 2016. ISSN: 2348-6600
Reference ID: IJCS-140 PAGE NO: 827-835

The Honesty

The *honesty* trust property represents whether or not a node is honest. In IoT, a malicious node can be dishonest when providing services or trust recommendations. We select *honesty* as a trust property because a dishonest node can severely disrupt trust management and service continuity of an IoT application. In an IoT application, a node relies on direct evidence (upon interacting) and indirect evidence (upon hearing recommendations vs. own assessment toward a third-party node) to evaluate the honesty trust property of another node.

The Cooperativeness

The *cooperativeness* trust property represents whether or not the trustee node is socially cooperative with the trustor node. A node may follow a prescribed protocol only when interacting with its friends or nodes with strong social ties (with many common friends), but become uncooperative when interacting with other nodes. In an IoT application, a node can evaluate the cooperativeness property of other nodes based on social ties and select socially cooperative nodes in order to achieve high application performance.

The Community-Interest

The *community-interest* trust represents whether or not the trustor and trustee nodes are in the same social communities/groups (e.g. co-location or co-work relationships) or have similar capabilities (e.g., parental object relationship). Two nodes with a degree of high community-interest trust have more chances and experiences in interacting with each other, and thus can result in better application performance.

III. IoT Trust Management Model

In order to design a trust model for IoT, which could handle the above mentioned challenges and attack models, several IoT trust management systems have been generated, and the trust computation almost falls into the classification in Figure 1. Five design dimensions are introduced in the classification: trust propagation, trust composition, trust update, trust aggregation and trust formation. The most commonly used methods are marked with red color, and then the yellow ones, the blue ones mean the fewest visited methods.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 5, 2016. ISSN: 2348-6600
Reference ID: IJCS-140 PAGE NO: 827-835

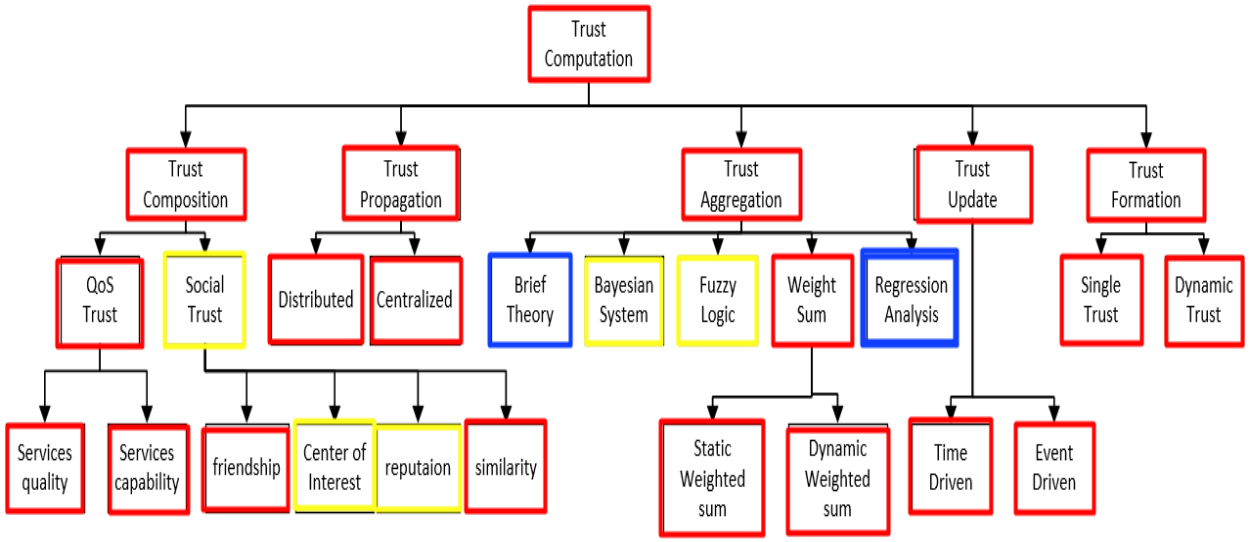


Figure 1. Trust Computation Classification Tree

3.1 Trust Composition

Trust composition determines which kind of trust values should be taken into consideration. Usually, the QoS (quality of service) and social trust are two main components. QoS trust means that the performance of an IoT node could serve. It is usually measured by packet delivery ratio, load balance, energy consumption etc. Social trust is the evaluation of social contact, the social relationship is divided by community of interest (CoI). When a node has several choices, it would first select those nodes who have social connections rather than unrelated devices.

3.2 Trust Propagation

In general, centralized and distributed systems are prevalent methods used in IoT trust system. Distributed trust propagation defines that IoT devices store trust observations towards their peer nodes without the use of a centralized server. The nodes in a distributed system using their constrained storage space to restore historical transaction information and handle the forwarding packages. Centralized trust propagation refers to those models which need unified services to deal with the entity requesting and a centralized entity to restore the trust values. The trust could only be acquired from the central server and the server is well assigned according to different communities.

3.3 Trust Aggregation

Trust aggregation provides a concept that gathers all the feedback from directed or undirected peer observation of the trust evaluation. Weighted sum method [16], [17], as the prevalent technique to be

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 5, 2016. ISSN: 2348-6600
Reference ID: IJCS-140 PAGE NO: 827-835

used, refers to add weights to direct or indirect trust. It could be developed in both fixed and dynamic way. Belief theory method [18], known as Dempster–Shafer theory as well, is a framework used for balancing uncertainty. It could also serve as connected to other probability theories frameworks. Bayesian inference [19] becomes a popular trust computation model because of it's easy to implementation and well statistical basis. With Bayesian inference, parameters in the model with a probability distribution are updated upon new events. Regression Analysis [20] is a statistical way to estimate relationships between trust and a set of variables characterizing the behavior of a node.

3.4 Trust Update

In general, there are two schemes involving the trust model: time-driven scheme and event-driven scheme. The time-driven scheme decreased the importance of trust reports that were made a long time ago. Usually, the latest evaluated trustworthiness get bigger weights. Event-driven scheme refers to a node's trustworthiness get updated after an event or transaction is made. We can also combine these two methods into one equation by assigning different weights or coefficients.

3.5 Trust Formation

Trust formation provides the scheme to form the overall trust by using different trust criteria. Single trust refers to the scheme that only one trust property is involved in a trust protocol. For example, quality of services is considered the single most important metric in social IoT. Dynamic trust implements the common belief that trust evaluation should be multidimensional. Various trust properties such as intimacy, honesty, unselfishness and competence should be deemed to assess the overall trust value of a node.

IV. 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 withdifferent gadgets through the overlay interpersonal organization conventions, or the fundamental standardcorrespondence 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

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 5, 2016. ISSN: 2348-6600
Reference ID: IJCS-140 PAGE NO: 827-835

(i.e., different proprietors), speaking to its social connections. Thiscompanionship list shifts powerfully as a proprietor makes or denies different proprietors as companions. On the offchance that the proprietors of two hubs are companions, then it is likely they will be helpful with each other. A gadgetmight 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.

Oursocial IoT model depends on social connections among people who are proprietors of IoT gadgets. We take note of thatthe gadget to-gadget self-governing social relationship is likewise a potential for the social IoT worldview.

V. CONCLUSION

In this system, we developed and analyzed an adaptive trust management protocol for social IoT systems and itsapplication to service management. Our protocol is distributed and each node only updates trust towards others of itsinterest upon encounter or interaction events. The trust assessment is updated by both direct observations and indirectrecommendations, with parameters α and β being the respective design parameters to control trust propagation andaggregation for these two sources of information to improve trust assessment accuracy in response to dynamicallychanging conditions.

We analyzed the effect of α and β on the convergence, accuracy, and resiliency properties of our adaptive trustmanagement protocol using simulation. The results demonstrate that (1) the trust evaluation of adaptive trustmanagement will converge and approach ground truth status, (2) one can tradeoff trust convergence speed for low trustfluctuation, and (3) adaptive trust management is resilient to misbehaving attacks. We demonstrated the effectiveness ofadaptive trust management by two real-world social IoT applications.

The results showed our adaptive trust-based service composition scheme outperforms random service composition andapproaches the maximum achievable performance based on ground truth. We attributed this to the ability of dynamictrust management being able to dynamically choose the best design parameter settings in response to changingenvironment conditions. There are several future research areas.We plan to further test our adaptive trust management protocol's accuracy,

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 5, 2016. ISSN: 2348-6600
Reference ID: IJCS-140 PAGE NO: 827-835

convergence and resiliency propertiestoward a multitude of dynamically changing environment conditions under which a social IoT application canautomatically and autonomously adjust the best trust parameter settings dynamically to maximize applicationperformance. Another direction is to explore statistical methods to exclude recommendation outliers to further reducetrust fluctuation and enhance trust convergence in our adaptive trust management protocol design.

VI. 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 Thingsvision: 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 Internetof 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, May2013.

[6] F. Bao, I. R. Chen, M. Chang, and J. H. Cho, "Hierarchical Trust Management for Wireless Sensor Networks and Its Applications to Trust-BasedRouting 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 ThingsSystems," 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 AppliedSciences in Biomedical and

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 4, Issue 2, No 5, 2016. ISSN: 2348-6600
Reference ID: IJCS-140 PAGE NO: 827-835

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 onCommunications, 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.