Adaptive Trust Management for Social Internet of Things

Pasupulati Naveena[1], Kailasa Madhusudhan Reddy[2]
[1]*Student, Master of Computer Applications, SKIIMS, Srikalahasti, Andhra Pradesh, India*
[2]Asst.Professor, *Master of Computer Applications, SKIIMS, Srikalahasti, Andhra Pradesh, India*

***Abstract*- Social Internet of Things is a new paradigm where Internet of Things merges with Social Networks, allowing people and devices to interact, facilitating information sharing and enabling a variety of attractive applications. However, face to this new paradigm, users remains suspicious and careful. They fear disclosure of their data and violation of their privacy. Without trustworthy technologies to ensure user's safe communications and trust worthy interactions, the SIoT will not reach enough popularity to be considered as a well-established technology .Accordingly, trust management becomes a major challenge to ensure reliable data analysis, qualified services and enhanced security. It helps people exceed their fears and promotes their acceptance and consumption on IoT services. However, current research still lacks a comprehensive study on trust management in SIoT. In this paper, we expose basic concepts, properties and models proposed for the trust management in SIOT environments. Furthermore, we discuss unsolved issues and future research trends.**

***Index Terms*- Social Internet of Things, Social Networks, Trust Management, and Trust attacks.**

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 [40], actuators, PDAs, and smart phones, as well as virtual objects in cyberspace such as data and virtual desktops on the cloud [2]. 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 [9, 23], smart-home, smart-city, and smart-community [27]. 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 on social 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.

II. SYSTEM ANALYSIS

Existing System: There is little work on trust management in IoT environments for security

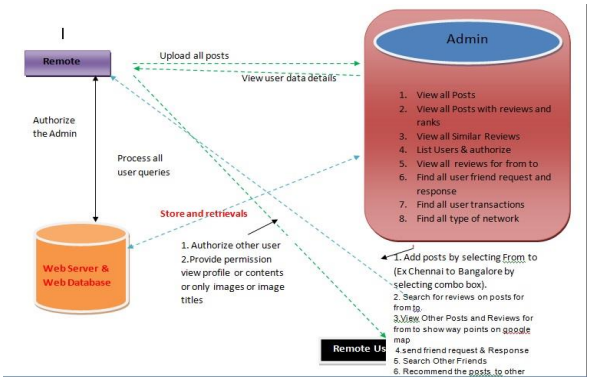
enhancement, especially for dealing with misbehaving owners of IoT devices that provide services to other IoT devices in the system. Chen *et al*. the system proposed a trust management model based on fuzzy reputation for IoT systems. However, their trust management model considers a very specific IoT environment populated with wireless sensors only, so they only considered QoS trust metrics like packet forwarding/delivery ratio and energy consumption for measuring trust of sensors. On the contrary, our work considers both QoS trust deriving from communication networks and social trust deriving from social networks which give rise to social relationships of owners of IoT devices in the social IoT environment. Saied et al.

An existing system proposed a context-aware and multiservice approach for trust management in IoT systems against malicious attacks. However it requires the presence of centralized trusted servers to collect and disseminate trust data, which is not viable in IoT environments. Relative to existing system, our trust protocol is totally distributed without requiring any centralized trusted entity.

Proposed System: The system proposed an *adaptive trust management* protocol for social IoT systems. Our method is suitable to be applied to social IoT experimental platforms as discussed in this system. Our goal is to enhance the security and increase the performance of social IoT applications.

The need for *adaptive* trust management stems from the fact that social relationships between owners and thus social behaviours 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 neighbourhood one does not go often).

III. SYSTEM ARCHITECTURE



IV. MODULES

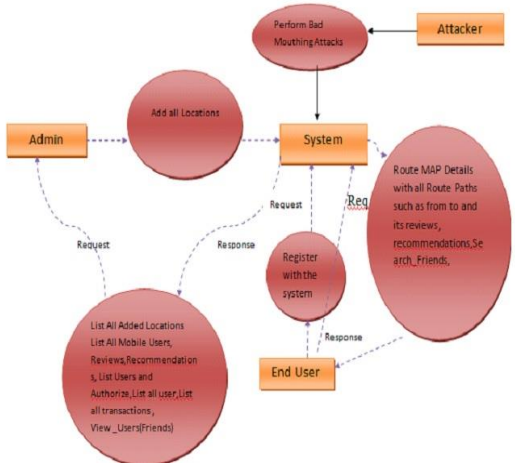
4.1. Data Owner: In this module, the data owner uploads their data with its File in the cloud server. For the security purpose the data owner encrypts the data File and then store in the cloud. The Data owner can have capable of manipulating the encrypted data file and also performs the following operations like 1. Browse file and enc, Uploads files with current enc (secret key) and MAC, Verify data, View all updated files with current file keys.

4.2. Admin Server: he cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them and do the following operations like View all User Files ,Authorize an end user ,Response File Request, View all attackers ,View all End Users, View all Data Owners, View Search Transaction, Store and view all meta data of the files, View all files with encrypted secret keys (fname,oname,secret key),Dec RSA secret keys and auto update current keys based on the time period, View all old and current keys, Set time period to update the secret keys and update keys based on time periods.

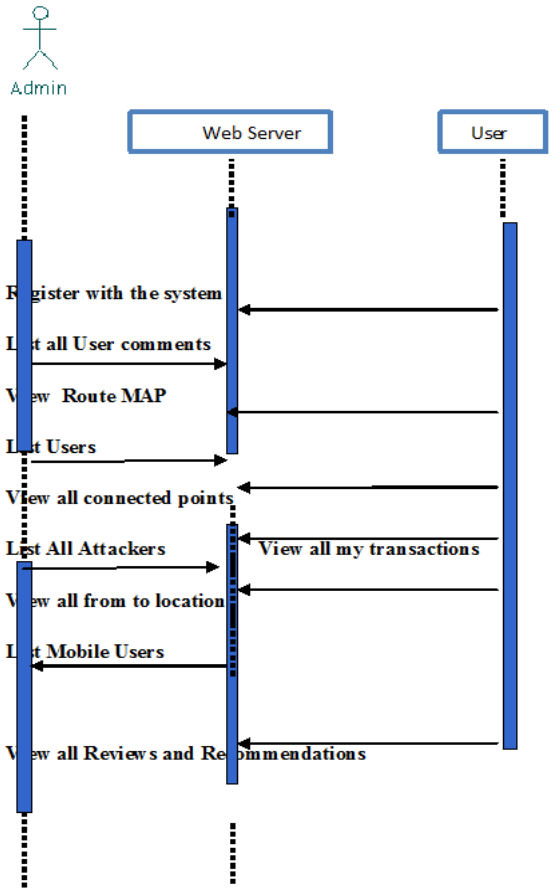
4.3. End User: The Cloud User who has a large amount of data to be stored in cloud and have the permissions to access and manipulate stored data and performs the following operations such as Searches for files based on Content's keyword, Requests for File.

V. DESIGN

DFD Diagram

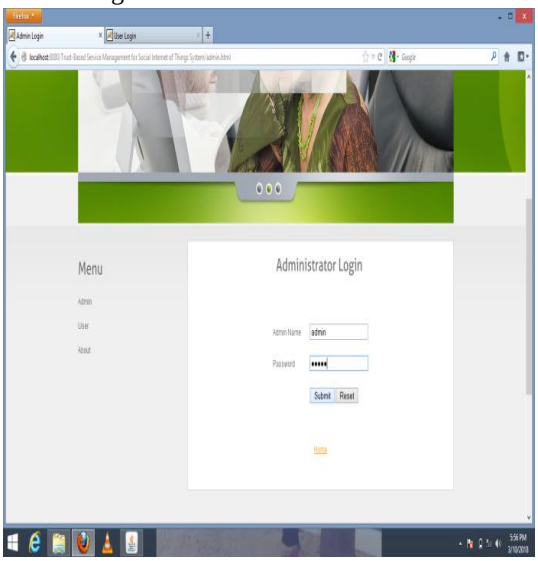


Sequence Diagram:

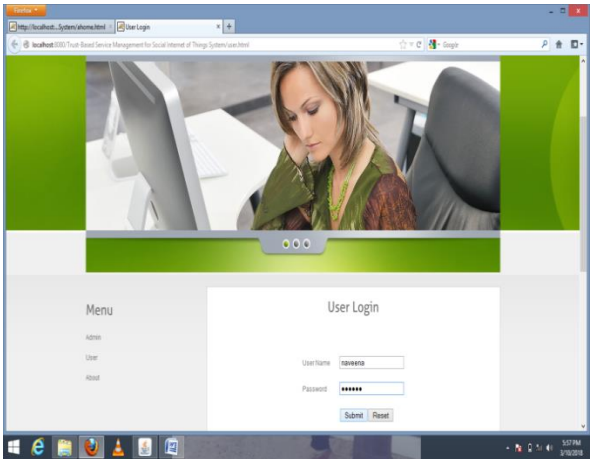


VI. SCREEN SHOTS

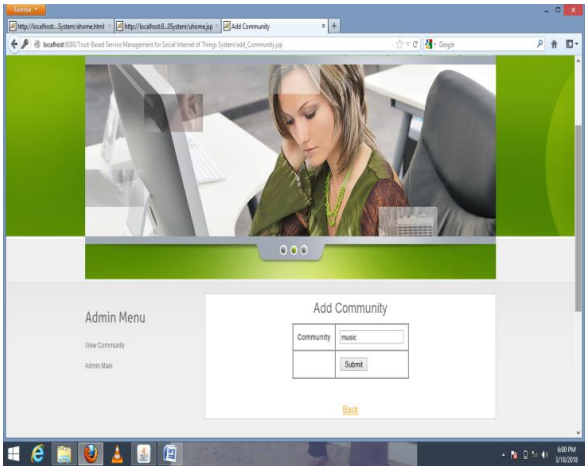
Admin Login:



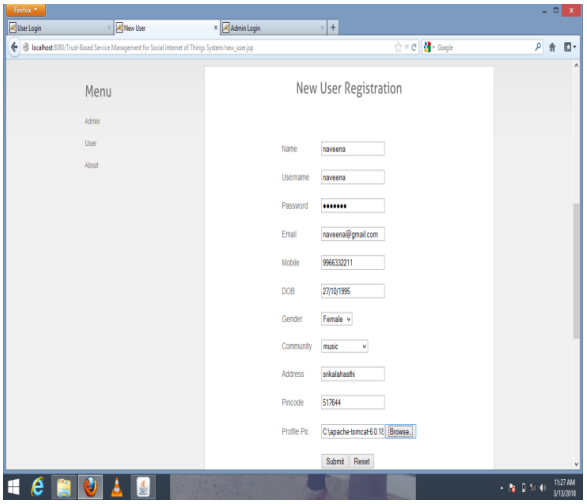
User login:



Add community:



New user registration:



VII. FUTURE ENHANCEMENTS

Aiming at achieving both data integrity and trust in social networks, we propose Trust Based induction. TBI should introduce an auditing entity with a

intenance of a Map Reduce cloud like thing in social network in the next version, which helps clients generate data tags before uploading as well as audit the integrity of data having been stored in cloud. In addition, it enables secure reduplications through introducing a Proof of Ownership protocol and preventing the leakage of side channel information in data reduplication. Compared with previous work, the computation by user in Trust based Induction is greatly reduced during the file uploading and auditing phases. It is an advanced construction motivated by the fact that customers always want to encrypt their data before uploading, and allows for integrity auditing and secure reduplication directly on encrypted data.

One way to counter these malicious behaviours is to introduce *behaviour induction*, a process in which a person or group influences the behaviour of another person or group through the induction of behavioural attitudes. Popular behaviour-induction approaches adopted in social networks include political restriction and employing people to publish positive information.

To address these issues, we propose a novel trust agent-based behaviour-induction approach for social network environments. Given a specified restricted negative behaviour, the agent how to induct, persuade, encourage, or induce social network participants to avoid this kind of negative behaviour as much as possible. Specifically, we introduce a trust agent (whose behaviour is designed according to the corresponding participants) aimed at eliciting maximized trust from other social network participants. In addition, we generate a dynamic control mechanism

to coordinate participant behaviour in social networks and avoid a restricted negative behaviour.

VIII. CONCLUSION

In this paper, 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 α and β 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.

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.

[5] 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.

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

[7] 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.

[8] 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.