Computers and Electrical Engineering 000 (2016) 1–15

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

# When social objects collaborate: Concepts, processing elements, attacks and challenges ☆

Wazir Zada Khan [a,*], Mohammed Y Aalsalem [a], Muhammad Khurram Khan [b], Quratulain Arshad [a]

[a] Farasan Networking Research Laboratory, Faculty of CS & IS, Jazan University, Saudi Arabia
[b] Center of Excellence in Information Assurance, King Saud University, Saudi Arabia

ARTICLE INFO

*Article history:*
Received 29 February 2016
Revised 10 November 2016
Accepted 10 November 2016
Available online xxx

*Keywords:*
Social internet of things
Social collaborative internet of things
Objects social relationship
Trust and reputation management

ABSTRACT

Social Collaborative Internet of Things (SCIoT) is a more elaborative form of Social Internet of Things (SIoT) in which, social objects collaborate by interacting and sharing information to achieve a common goal. In order to collaborate, smart objects need to be grouped and work together by developing a trusted environment and cooperative relationships among them. Trust management plays an important role in such SCIoT scenarios where smart objects have to establish social relationships. Also, these smart objects select other objects in their vicinity as friend or foe based on their trust upon those objects to establish an effective successful collaboration. In this paper, we contribute to present a survey of existing trust management schemes for SIoT, compare them by outlining their features and identify their drawbacks, etc. Furthermore, as far as our knowledge is concerned, we are the first to propose the definition of SCIoT, a hierarchical model of SCIoT for its important processes and a few application scenarios. In addition, we present a threat model to categorize the possible attacks that can be launched on SCIoT. Finally, we also highlight some challenges in the SCIoT.



## 1. Introduction

The vision of Internet of things (IoT) was emerged in 1999 and the term was coined by Kevin Ashton. Initially, it was introduced to promote RFID technology. IoT gained popularity in 2010 with its potential to provide great benefits to humans and making lives easier by practically eliminating time and space through the swiftness of smart devices. The smart devices involved in IoT are capable of talking directly to other smart devices, exchanging important data or information between them.

Wong et al. [1] first introduced the concept of Intelligent Products or Smart Products defining the two levels of product intelligence. The first level of intelligence is information oriented in which a product is allowed to exchange information related to its key features and location etc. The second level of intelligence is decision oriented in which a product is allowed to determine and control its functioning like recording its self-distribution and self-manufacturing. According to [2], theories of pervasive and ubiquitous computing and ambient intelligence emphasize on interaction of humans with their

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. E. Ahmed.

* Corresponding author.
*E-mail addresses:* wazirzadakhan@jazanu.edu.sa, wazirzadakhan@yahoo.com (W.Z. Khan), aalsalem.m@jazanu.edu.sa (M.Y. Aalsalem), mkhurram@ksu.edu.sa (M.K. Khan), brightsuccess_12@yahoo.com (Q. Arshad).

http://dx.doi.org/10.1016/j.compeleceng.2016.11.014
0045-7906/

environment and thus these cannot be used as a synonym for intelligent products. Similarly, the concept of intelligent products/agents is also different from the paradigm of IoT. Intelligent products involve the exchange of intelligence of products whereas IoT focuses on connectivity and information exchange between smart objects/things. The concept of semantic gadgets was introduced by Lassila and Adler [3] who described them as "*devices capable of performing discovery and utilization of services without human guidance or intervention, thus enabling formation of device coalitions*" . On the other hand, Vazquez et al. [4] proposed semantic device as a system "*able to spontaneously discover, exchange and share context information with other fellow semantic devices as well as augment this context information via reasoning in order to better understand the situation and perform the appropriate reactive response*" . Some other related work in this regard can be found in [5-8].

With the evolution of IoT paradigm, the smart devices or objects become social, since they used to mediate human social relationships. The vision of Social Internet of Things (SIoT) involves social objects which communicate and establish social relationships with other objects. When these social objects collaborate to achieve some common goal, they are said to be involved in a social collaborative IoT environment.

The focus of this paper is Social Collaborative Internet of Things (SCIoT). SCIoT is the elaborative form of SIoT involving such social objects that are talkative inherently and collaborative natively in the sense of sharing all the information they can. They are also capable of interacting on behalf of their owner using social networking applications like twitter, flickr, facebook and digg. In order to achieve a collaborative activity using specialized knowledge or information, intelligent social smart objects need to collaborate with each other. Digital objects are able to carry out simple tasks efficiently that can help people in their everyday activities, thus simplifying their lives. In order to perform complex tasks in unexpected situations, a higher level of intelligence, cooperation and collaboration is required. Thus, in SCIoT, the collaborating smart social objects collaborate intelligently and cooperate efficiently in a trustworthy environment to achieve a common goal. SCIoT involves such collaborating objects that leverage their cognitive reasoning (intelligence), situational awareness (sensing) and social communications (relationships) for achieving common complex goals and tasks or to provide specific services.

The foundation of SCIoT is based on collaboration of networking objects for achieving a common goal. The collaboration of social objects is dependent upon the services they provide rather than on the social relations as in SIoT. In SIoT systems, involved objects retain their individuality whereas SCIoT systems require the collective efforts and active participation of all the involved objects for achieving a common goal. SCIoT and SIoT are both situation oriented since their preference is highly dependent upon the scenarios and situation in which the participating objects are involved. Community problems can be resolved by deploying SCIoT systems that involve social collaborative IoT objects. Thus, SCIoT is preferable for communities of social objects that have more often a common goal and need common services. SIoT involves social objects that have different goals and they achieve their own goals without collaboration but they can provide services on the basis of their social relationships. Hence, the major difference between SIoT and SCIoT is that SIoT involves trusted social relationships of smart social objects to provide services. On the other hand, in SCIoT various smart social objects collaborate with each other to provide a common service or to achieve a common shared goal.

Trust and cooperation are important elements in SCIoT to complete these common goals. The foundation of these elements is the social relationships with the involvement of other elements as honesty, community interest etc. Trust is a multi-dimensional concept and has been a well-studied area from different disciplines. Tyrone et al. [9] define trust as "*the firm belief in the competence of an entity to act dependably, securely and reliably within a specified context*" . The authors have assumed that the trust of an entity depends upon reliability and timeliness of some specific situation. Social trust forms the basis of building trust among online communities since trust is considered to be a vital feature of human social networks as well as online communities. Likewise, trust is widely accepted as major component of object's (thing's) social relationships. Various trust management schemes have been proposed for SIoT that are analyzed in Section 3. On the other hand since SCIoT is in its infancy, security, privacy and trust challenges in SCIoT (as described in Section 6) are still remained to be solved.

This paper has three major portions. In the first part, we present a background for SIoT and the comparison of trust management schemes for SIoT. The second part involves the proposal of SCIoT hierarchical model for its important processes, possible attacks on SCIoT and a threat model for SCIoT. The final third part of this paper highlights some important challenges in SCIoT that need to be solved.

In this paper we contribute to the following:

1. The existing trust management schemes particularly proposed for SIoT are explored and analyzed.
2. A comparison of these techniques is presented outlining their features and pointing out their drawbacks. The comparative analysis of these schemes based on the eight taxonomies is also presented
3. The definition of SCIoT is proposed. A hierarchical model of SCIoT highlighting its important processes and a few application scenarios are also proposed.
4. A threat model for SCIoT is proposed and the possible attacks that can be launched on SCIoT are categorized according to the dimensions of the proposed threat model.
5. Some important issues and challenges that can be raised in SCIoT scenarios are also highlighted that need to be resolved in the near future.

The rest of the paper is organized as follows: Section 2 presents the background of SIoT. Section 3 analyzes and compares existing trust management schemes in SIoT. Section 4 proposes the definition, processes and application scenarios of SCIoT. Section 5 identifies several possible attacks on SCIoT and proposes a threat model to categorize the attacks according to the

Please cite this article as: W.Z. Khan et al., When social objects collaborate: Concepts, processing elements, attacks and challenges, Computers and Electrical Engineering (2016), http://dx.doi.org/10.1016/j.compeleceng.2016.11.014