Wireless Pers Commun (2017) 96:2681–2691
DOI 10.1007/s11277-017-4319-8

Trust Management in the Social Internet of Things

A. Meena Kowshalya[1] · **M. L. Valarmathi**[2]

Published online: 22 May 2017

Abstract Today's electrical and electronic gadgets have become smarter and intelligent. These devices such as sensors, actuators, RFIDs are becoming part of our fabric. Internet of Things (IoT) and Social networking paradigms are not new. The increased pervasiveness has resulted not only in human to thing communication but also thing to thing communication. A new paradigm integrating IoT and Social Networks has emerged in recent years called the Social Internet of Things (SIoT) where objects are not only smarter but also socially conscious. Social Internet of Things is analogous to social network of intelligent objects. Trust is considered as a crucial factor in SIoT for objects to establish reliable autonomous communication. This paper proposes a Trust Management scheme for Social Internet of Things where trust between objects is computed based on Direct Observations, Indirect Recommendations, Centrality, Energy and Service Score of the object. The proposed trust model outperforms the existing trust models leading to a better application performance. The trust model is also tested in the presence of On Off selective forwarding attacks. Experimental results prove that the proposed model is reliable and defendant against On Off selective forwarding attacks.

Keywords Internet of Things (IoT) · Social Internet of Things (SIoT) · Social Networks (SN) · Trust management · On Off attacks

✉ A. Meena Kowshalya
meenakowshalya.gct@gmail.com

[1] Department of Computer Science and Engineering, Government College of Technology, Coimbatore, India

[2] Department of Electrical and Electronics Engineering, ACCET, Karaikudi, India

1 Introduction

The IoT has enabled integration of several heterogeneous technologies and communication solutions [1]. This paradigm has led to the notion of everything, anything and any time access. Social Networks are evolutions beyond IoT. A different perception and visualization of IoT is to make Things sociable i.e., giving IoT a social structure and adding social relationships between objects. The convergence of IoT and Social Networking (SN) leads to what is called a Social Internet of Things. SIoT may be considered as a social networks of intelligent objects [2]. Atzori et al. [3] proposed an architecture for implementing the SIoT. This work gave IoT a social structure; serves as preliminary basics for our work. The actual practice of SIoT is not easy. Major hurdles like heterogeneity, interoperability, fault tolerance, security and privacy issues have to be handled. Out of which Trust Management is very important since if a network comprises of trustworthy nodes, communication will be reliable. Accordingly, Trustworthiness has to be computed for nodes to collaborate with each other securely. The terms nodes and objects are interchangeably used in this paper. Trust management schemes are either centralized or decentralized. In a centralized approach trust scores and peers are managed by a central authority. A Social Internet of Things uses a decentralized approach where objects are independent of each other. A hybrid approach is also practiced depending on the context. The basic assumption followed is when humans move the objects tend to move. Trust is computed based on behavior of objects. The idea of modeling the SIoT environment was obtained recalling the fact of Jon Kleinberg's small world phenomenon. The readers are advised to read [4]. The authors in [5] have studied relationship between objects. Four basic relationships between objects are identified namely parental object relationship, Co - work object relationship, owner object relationship and social object relationship. Figure 1 shows the types of object relationships. When objects of the same manufacturer interact and establish collaboration with each other, the relationship is said to be parent object relationship. When objects move because of their owners they intend to collaborate with other objects at work place and at various locations leading to co work object relationship.

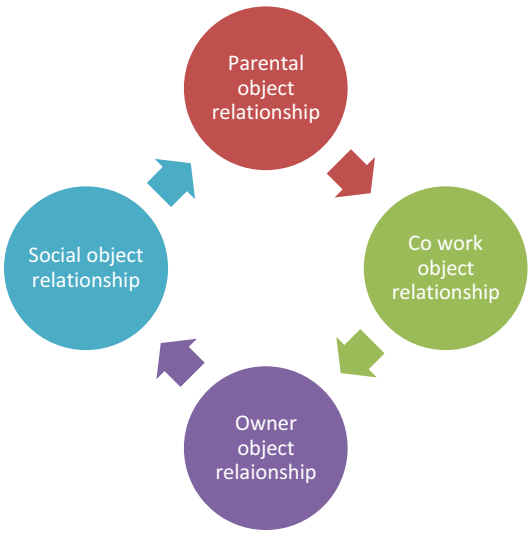

Fig. 1 Types of object relationships

When objects of the same owners establish communication and share information, it leads to a type of collaboration known as owner object relationship. Infrequently, objects also tend to collaborate with devices such as sensors, actuators belonging to their owner's friends. Such collaboration leads to Social object relationship. Meena Kowshalya and Valarmathi [13] proposes that the SIoT network is navigable and service search can be performed efficiently. We propose a new and simple trust management scheme for SIoT based on behavior of objects. An object tends to estimate trust of another object based on its own experience (direct opinion), stores and shares its experience with others, updates trust values and justify trustworthy communication. Trust metrics used includes direct trust, Centrality of the object, Energy, Community Interest, Cooperativeness and Service Score. Trust updates are done periodically in order to make the proposed trust management scheme effective and reliable. The proposed scheme is also tested under On Off selective forwarding attacks.

The major contributions of the paper are:

(a) Establishing a SIoT network and compute the trustworthiness of nodes in the network by First hand information (Direct trust), Second hand recommendation (Indirect trust), Centrality, Energy and Service score.
(b) Analyze the performance of the SIoT network by changing the trust parameters and demonstrate the best application performance.
(c) Prove the reliability of the proposed trust model in presence of On Off selective forwarding attacks.

2 Related Work

This section summaries recent trust management solutions and strategies adopted for SIoT network. Very few works have been done for trust management on SIoT environment. [6] presents techniques to compute and measure dynamic trust based on behavior of mobile nodes. This was later extended for SIoT. Nitti et al. [2] presents an algorithmic approach of computing trust from behaviors of online social network. This paper also lists measurable trust metrics. The authors in [7] combine inferences to arrive at trust and distrust among nodes even if the nodes do not know each other. Wang et al. [8] presents a distributed trust management system for Internet of Things according to the three layering architecture method. Bao and Ing-Ray [9] presents a dynamic Trust Management scheme for communication based SIoT environment. Multiple complex social relationships and basic properties of trust were used for dynamic trust management. As an extension of the previous work, the authors in [10] consider two types of Community of Interest namely Inter Community of Interest and Intra Community of Interest. Given these two as inputs the approach achieves best trust protocol settings. This protocol is scalable when compared to the author's previous work [9]. Mahalle et al. [11] proposed a fuzzy based approach to evaluate trust level across nodes in IoT. The same can be extended for SIoT. This fuzzy based approach is scalable and energy efficient. The authors in [12] have created a framework for inferring trust and distrust relationships in Online Social Networks. The network is decomposed into ego trust sub network and mined for trust and distrust relationship. Graph data mining algorithms are employed for this purpose. It's possible to derive various trust metrics from behavior of objects/nodes/things. According to the trust parameters, Trust is calculated based on first hand information and second hand

recommendation. The authors in [15] proposes a fuzzy trust and reputation system upon a community of sensor nodes in IoT. The algorithm helps sensor nodes to find the most trustworthy assisting node by recording transactions with neighbors and estimating their performance. Direct and indirect trust is computed by using weights on respective nodes. Chen et al. [16] introduces levels of friendships, social relations and social interests into an IoT trust model. It uses dynamic weights to adjust direct trust and indirect trust. It uses a trust decay for removing outdated trust. Saied et al. [17] introduces a context aware multi service approach to estimate trust to overcome the limitations of IoT such as heterogeneity, fault tolerance, service discovery, etc., the authors take into account quality recommendations for updating trust.

3 Trust Management in SIoT

Trust computation is an essential task in SIoT. Social trust is derived from the behavior of objects. Literature lists computation of social trust based on friendship, community of interest, reputation, similarity, etc. To the best of our knowledge this is the first paper that takes into account energy, service score and centrality of object along with direct trust and indirect trust. Any object willing to collaborate needs to compute trust among its peers in order to build a reliable SIoT. The trust value also helps influence the future interactions among objects and their relationships. When objects trust values are higher they tend to share services and resources securely to the extent possible. Besides the existing challenges in building a reliable SIoT, malfunctions and attacks are also an issue. Figure 2 explains the idea of the proposed work. This proposed trust model is defendant against On Off Selective Forwarding attacks and explores vulnerability of trust management strategies. Trust is always assumed to be subjective, context sensitive and unidirectional and may not be transitive.

3.1 Trust metrics

Trust is important and complex concept that helps objects to make decisions in unpredictable circumstances. We use the following trust metrics for computation of trust.

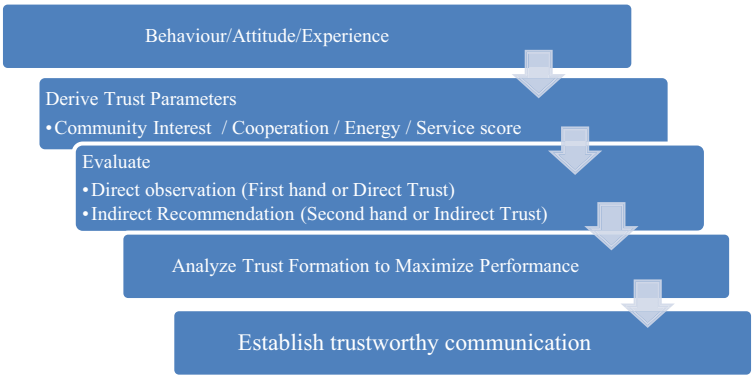

Fig. 2 Computation of trust

3.1.1 Direct Trust

Direct Trust is computed based on the objects own experience with its neighbors. D_{ij} is the Direct Trust of node j as seen by node i during direct contact. For every transaction l, nodes provide feedback f_{ij}^{l} to evaluate the service received. Also, each node maintains a transactional factor tf_{ij}^{l} scoring relevant transactions between each other as 1 and irrelevant transaction as 0.

$$D_{ij} = \frac{\sum_{l=1}^{n} tf_{ij}^{l} f_{ij}^{l}}{\sum_{l=1}^{n} tf_{ij}^{l}} \tag{1}$$

tf_{ij}^{l} is the transactional factor which depicts the relevance of transaction l between node i and j. $tf_{ij}^{l} \in \{0, 1\}$. f_{ij}^{l} is the feedback that node i provides to j, the feedback may be 1 if satisfactory, 0 otherwise. $f_{ij}^{l} \in \{0, 1\}$

$$tf_{ij}^{l} = \begin{cases} 1, & relevant\ trasaction \\ 0, & irrelevant\ trasaction \end{cases}$$

$$f_{ij}^{l} = \begin{cases} 1, & satisfactory\ feedback \\ 0, & otherwise \end{cases}$$

3.1.2 Centrality

G_{ij} is the centrality of the object j with respect to i. It represents how much object j is important for object i and not for the whole network. This metric prevents malicious nodes that build many relationships in the SIoT network.

$$G_{ij} = \frac{|C_{ij}|}{(|F_i| - 1)}. \tag{2}$$

where C_{ij} represents common friends between i and j, F_i represents friends of i.

3.1.3 Cooperativeness

Cooperative trust represents whether or not the trustee object is socially cooperative with the trustor. It's assumed that objects with common friends are cooperative. In a SIoT environment, objects cooperativeness can be predicted by its social ties. Each device/object possesses a list of friends likely to be cooperative.

$$\mathrm{CO_{ij}} = \frac{\mathrm{friends(i)} \cap \mathrm{friends(j)}}{\mathrm{friends(i)} \cup \mathrm{friends(j)}}. \tag{3}$$

3.1.4 Community Interest

Community interest is another factor that enables communication between objects of communal interest. Objects with the same community interest are supposed to interact with each other very often leading to increased application performance.

$$CI_{ij} = \frac{\text{community(i)} \cap \text{community(j)}}{\text{community(i)} \cup \text{community(j)}} \tag{4}$$

3.1.5 Energy

Energy of a node also plays an important role in communication and sharing of information. Almost all devices in SIoT are low power devices and less energy efficient devices. Thus energy of a node is to be given prime importance for collaboration purpose. The reason for considering energy as a factor for determining trust is that, if a node performs On Off selective forwarding attack its energy level will be quiet higher(since the node goes to the Off state during essential transactions) when compared to other peers in the group doing the same task. Energy of node j is computed as

$$E_{residual,j} = E_{initial,j}(t - \Delta t) - E_{consumed,j}(\Delta t) \tag{5}$$

3.1.6 Service Score

When an object provides a requested service it is rewarded with a service score else penalized. The more number of times a node is penalized, more chances that the node can be malicious.

$$\mathrm{S_i} = \begin{cases} 1 * \mathrm{W_s}, & reward \\ -2 * \mathrm{W_s}, & penalty \end{cases} \tag{6}$$

$\mathrm{W_s}$ is the weight of the service score $0 < \mathrm{W_s} < 1$.

3.2 Computation of Trust

We calculate the trust of an node j with respect to node i as

$$T_{ij} = \alpha D_{ij} + (1 - \alpha - \beta)G_{ij} + \lambda CI_{ij} + \gamma CO_{ij} + \omega E_{residual,j} + \eta S_{ij} \tag{7}$$

where $0 < (\eta, \gamma, \lambda, \beta, \alpha, \omega) < 1$, $0 < \mathrm{T_{ij}} < 1$

$\eta, \gamma, \lambda, \beta, \alpha, \omega$ are weights in order to adjust the trust value between 0 and 1. In the implementation $\alpha = 0.6$, $\beta = 0.3$, $\lambda = 0.3$, $\gamma = 0.3$, $\eta = 0.2$, $\omega = 0.2$. We also provide flexibility for node i to evaluate the trust of node j using an intermediate node k (if node i doesn't want direct interaction to compute trust) as

$$T_{ij} = T_{ij}(t)(t - \Delta t) + \kappa R_{kj} + \alpha D_{ik} \tag{8}$$

where $0 < (\alpha, \kappa) < 1$, $0 < \mathrm{T_{ij}} < 1$

where $\alpha = 0.6$ and $\kappa = 0.3$ are the weights in order to adjust the trust value between 0 and 1. $\mathrm{T_{ij}(t)}$ $(t - \Delta t)$ is the past trust value, $\mathrm{R_{kj}}$ is the recommendation that node k provides to node i about node j. There are possible chances of node k being malicious. If node k is malicious it can perform bad mouthing attacks and propagate the same to node i. To prevent this happening, node i uses direct trust $\mathrm{D_{ik}}$ to access node k according to Eq. 1 (Table 1).

Table 1 List of parameters used

Parameter	**Description**
D_{ij}	Direct trust of node j with respect to node i
R_{kj}	Recommendation about node j with respect to node k
T_{ij}	Trust of node j with respect to node j
G_{ij}	Centrality of a node j with respect to node i
D_{ik}	Direct trust of node k with respect to node i
CO_{ij}	Cooperativeness between node i and j
CI_{ij}	Community interest of nodes i and j
$E_{residual,j}$	Energy consumption of node j
S_{ij}	Service score of node j with respect to node i

4 Experimental Results

The dataset was obtained from CRAWDAD [14]. Dataset traces contain Bluetooth device proximity, social profiles (friends and interests) and opportunistic message creation and dissemination of 76 users of Mobiclique application obtained at SIGCOMM Conference 2009, Spain. The dataset was collected by distributing 100 smart phones to users. Traces of object interaction between 100 objects belonging to 76 users were used. Table 2 shows the configuration parameters. The implementations were done using network simulator 3 and Social network visualizer tool SocNetV 1.9. Trace files include information about friends, activity, interests, messages, participants, proximity, reception and transmission. A total of 899 transactions were used for the experiment. A small modification was made to the dataset in order to induce On Off selective forwarding behavior during transactions. The total time of the experimentation was 2 h.

We have compared the proposed trust management scheme with three different trust management schemes namely Fuzzy Trust [15], Context Aware Trust [17] and SOA based Trust [16]. The authors in [15] use a fuzzy based trust and reputation management system for community of sensor nodes. The system evaluates the performance and behavior of nodes and computes trust based on direct observation and indirect recommendation. They use End to End Packet Forwarding Ratio, Absolute Energy Consumption and Packet Delivery Ratio to evaluate their system. Saied et al. [17] uses trust manager who obtains the trust related information. The requesting node queries the trust manager for assistance. Trust manager provides a trust agent based on past history and generate reputation reports. The requesting node report the trust value of every assisting agent and updates the

Table 2 Configuration parameters used

Object interactions	899
Node radius	0.00948
Knowing time	1728000
Simulation seconds	950,400
Cell distance weight	0.8
Node speed multiplier	1
Waiting time exponent	1.35
Waiting time upper bound	216,000
Buckets per side	11

trustworthiness value periodically. Quality of Recommendation (QR) is used as the metric to update trust values. This model is resistive against few attacks. Chen et al. [16] uses similarity measures to compute friendship vectors. They find direct and indirect trust based on similarity scores by using the mean square measurements. None of these trust management schemes are defended against On Off selective forwarding attacks. Figure 3 shows the trust scores of the proposed schemes with the existing trust management models under study (The nodes were chosen randomly assuming all nodes to be honest and no attack exist in the network). The proposed schemes has the best application performance. The performance of [16] and [17] are similar in the first half of the experiment and the performance of [15] and [17] were the same at the latter half of the experiment. Chen et al. [15] and Saied et al. [17] almost converged after the 600th transaction. Figure 4 is analogous to Fig. 3 which depicts the maximum trust value scored every 100th transaction. At the beginning all trust management schemes showed the same performance since the network was initializing. Hence the results show only trust scores from 100 to 899th transactions.

The proposed trust management schemes uses direct trust, Centrality, Energy, Community Interest, Cooperativeness and Service Score to calculate trust. All these metrics contribute to model the behavior of nodes. Out of which direct trust plays an important role as explained in Eq. 1. The reason for choosing $\alpha = 0.6$ is discussed in Fig. 5. When $\alpha = 0.6$ best application performance is rendered by Eq. 7. Figure 6 compares the proposed trust management scheme with the other models under study. The trust value is in between 0 and 1. The maximum trust can be best at 1 and the minimum trust value is 0. A threshold of 0.4 is chosen so that if the trust value falls below the threshold, the node is identified as malicious. When the node is a victim of On Off selective forwarding attack, its trust value calculated based on Eq. 7 will reach the minimum and the node will be isolated from the network. The proposed schemes as shown in Fig. 6 is defended against On Off selective forwarding attacks. The trust value fell down below the threshold, reached the minimum and the node was isolated from the network. Saied et al. [17] is also defended against On Off selective forwarding attack, but took a longer time and did not isolate the node from the network. The node could later recover trust value again and perform malicious attacks. Chen et al. [15, 16] were not defended against the induced attack but the trust score of the node reduced to a small extend. Figure 7 is analogous to Fig. 6 showing the comparison of the proposed schemes with the other models under study. The proposed scheme detected the attack at the 400th transaction and isolated the node at 600th

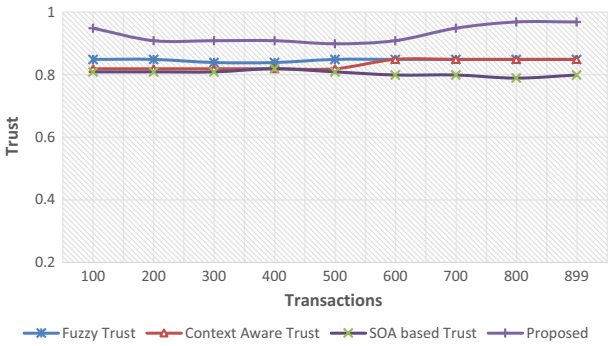

Fig. 3 Trust scores of nodes (assuming all honest)

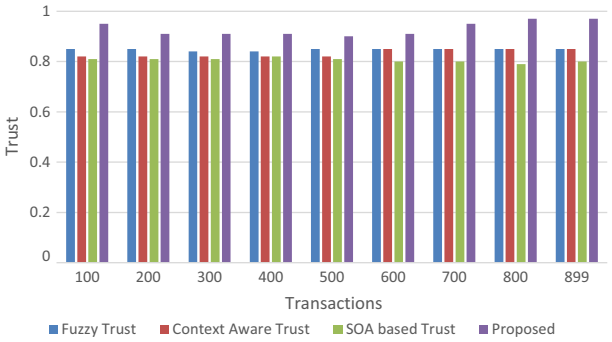

Fig. 4 Comparison of various trust management schemes with the proposed scheme

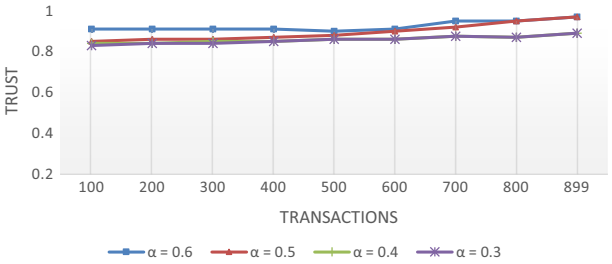

Fig. 5 Performance of varying α value

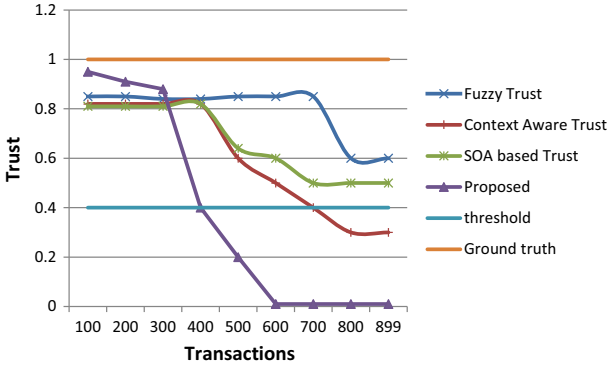

Fig. 6 Comparison of various trust management schemes with the proposed schemes in the presence of On Off selective forwarding attack

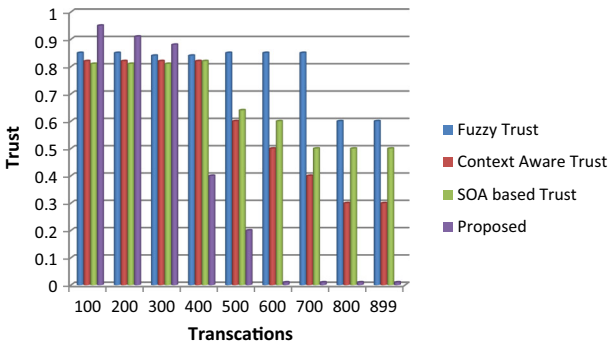

Fig. 7 Proposed scheme detected the presence of On Off selective forwarding attack at 400th transaction and isolated the node from the network at 600th transaction

transaction. Saied et al. [17] detected the attack at the 800th transaction and the node performing the attack was still giving chances to be active in the network.

5 Conclusion

The Social Internet of Things (SIoT) is a new paradigm that integrates two giant technologies namely Internet of Things (IoT) and Social Networking. Due to the increased pervasiveness, the want for smarter objects and services has significantly increased. This paper proposes a dynamic trust management model that computes trust based on direct observation, indirect recommendation, centrality, energy and service score of the object. The proposed trust model is also reliable against On Off selective forwarding attacks and results in better application performance. The proposed trust model outperforms the fuzzy trust, Context aware trust and SOA based trust in terms of detecting accuracy. The proposed trust management scheme identified untrustworthy nodes and isolated the nodes very quickly. This might in turn be considered as a drawback. Giving more chances for low trust value nodes, all types of attacks and attackers can be identified. In the future, we plan to extend the trust management scheme by giving more opportunities to the low trust value nodes to perform in the network. This helps in learning the attacker's pattern and detect variety of attacks.

References

1. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks Elsevier, 54*(15), 2787–2805.
2. Nitti, M., Girau, R., & Atzori, L. (2014). Trustworthiness management in the social internet of things. *IEEE Transactions on Knowledge and Data Management, 26*(5), 1–11.
3. Atzori, L., Iera, A., & Morabito, G. (2011). SIoT: Giving a social structure to the internet of things. *IEEE Communication Letters, 15*(11), 1193–1195.
4. Kleinberg, J. (2000). The small-world phenomenon: An algorithmic perspective. In *Proceedings of the thirty-second annual ACM symposium on theory of computing* (pp. 163–170).
5. Atzori, L., Iera, A., Morabito, G., & Nitti, M. (2012). The social internet of things (SIoT): When social networks meet the internet of things: Concepts architecture and network characterization. *Computer Networks, 56*(14), 3594–3608.
6. Adali, S., Escriva, R., Goldberg, M. K., Hayvanovych, M., Magdon Ismail, M., Szymanski, B. K., Wallace, W. A., & Williams, G. T. (2010). Measuring behavioral trust in social networks. In *International Conference on Intelligence and Security Informatics (ISI)*. 150–152).
7. Saied, Y. B., Olivereau, A., Zeghlache, D., & Laurent, M. (2013). Trust management system design for the internet of things: A context-aware and multi-service approach. *Computers and Security, 39,* 351–365.
8. Wang, J. P., Bin, S., Yu, Y., & Niu, X. X. (2013). Distributed trust management mechanism for the internet of things. *Applied Mechanics and Materials, 347,* 2463–2467.
9. Bao, F., & Ing-Ray, C. (2012). *Dynamic trust management for the internet of things applications*. San Jose, CA: International Workshop on Self Aware IoT.
10. Bao, F., Ing-Ray, C., & Guo, J. (2013). Scalable, adaptive and survivable trust management for community of interest based internet of things systems. *Eleventh International Symposium on Autonomous Decentralized Systems (ISADS),* 1–7.
11. Mahalle, P. N., Thakre, P. A., Prasad, N. R., Prasad, R. (2013). A fuzzy approach to trust based access control in internet of things. In *3rd International conference on wireless communications, vehicular technology, information theory and aerospace and electronic systems*.
12. Bachi, G., Coscia, M., Monreale, A., & Giannotti, F. (2012). Classifying trust/distrust relationships in online social networks. privacy, security, risk and trust (PASSAT). In *International Conference on Social Computing (SocialCom)* (pp. 552–557).

13. Meena Kowshalya, A., & Valarmathi, M. L. (2015). Improved network navigability and service search in social internet of things (SIoT). *International Journal of Research and Scientific Innovation, 2*(9), 75–77.
14. Anna–Kaisa, P., & Christophe D., (2012). CRAWDAD dataset thlab/sigcomm2009 (v.2012–07–15), traceset: mobiclique. doi:10.15783/C70P42.
15. Chen, D., Chang, G., Sun, D., Li, J., Jia, J., & Wang, X. (2011). TRM-IoT: A trust management model based on fuzzy reputation for internet of things. *Computer Science and Information Systems, 8*(4), 1207–1228.
16. Chen, I. R., Guo, J., & Bao, F. (2014). Trust management for SOA-based IoT and its application to service composition. *IEEE Transactions on Services Computing, 9*(3), 482–495.
17. Saied, Y. B., Olivereau, A., Zeghlache, D., et al. (2013). Trust management system design for the internet of things: A context-aware and multi-service approach. *Computers & Security, 39,* 351–365.

A. Meena Kowshalya obtained her Bachelors in Information Technology from Bharathiar University and Masters in Computer Science and Engineering from Anna University. She is the gold medal winner for the academic year 2011. She is now Assistant Professor, Department of Computer Science and Engineering, Government College of Technology, Coimbatore, Tamil Nadu, India. She has a total of 10 years of teaching experiences. Her area of research interests includes Information Retrieval, Social Internet of Things, Social Networks and Wireless networks.

Dr. M. L. Valarmathi graduated from Madurai Kamaraj University in the year 1983. She completed her Masters in Computer Science and Engineering and Doctorate in Computer Science and Engineering from Anna University. She, currently is the Professor of Department of Electrical and Electronics Engineering, Alagappa Chettiar College of Engineering and Technology, Karaikudi, Tamil Nadu, India. Her main area of interest includes Image Processing, Internet of Things, Optimization Techniques, Big Data Analytics and Wireless Networks. She has published more than 90 journal papers and conference proceedings.