ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)

Security Improvement in Social IOT

[I]Priyadharshini.P, [II]Ramya.J
[I,II]Assistant Professor/CSE

Abstract
In the Social Internet of Things, objects are establishing their social relationships in an independent way. The main problem is to understand that how the objects in Social IoT can interact in order to build the trusted System. Hence focus on the trustworthiness models namely objective and subjective models. These models provide peer to peer (P2P) communication in social networks. Distributed Hash Table (DHT) also constructed in order to provide security. Transaction Factors are assigned based on the importance of transactions in the network. Finally, trustworthiness of every node can be calculated based on the transaction factors assigned and their trust values. This will identify the malicious node which gives us more security in the social network.

Keywords
Social Internet of Things (SIoT), Distributed Hash Table (DHT), Social Networks, Peer to Peer (P2P), Trustworthiness Management.

I. Introduction

In SIoT, separating the level of people and things are possible. It allows objects to have their own social networks and allow humans to protect their privacy. When the objects interact with other objects in the network in an autonomous way, billions of traffic exists in the IoT environment. This will lead to malicious behaviour in the environment. Hence trustworthiness management plays an important role. Without this management, it will not provide the trusted network. SIoT provides many benefits like navigability, scalability and trustworthiness.

The main objectives of this work are to improve the security by trustworthiness management of social IoT and to build a trusted system on the basis of behaviour of objects.

II. Literature Survey

A. Integrating RFIDs and Smart Objects into a Unified Internet of Things Architecture

The main goal of the middleware solution[5] is the abstraction of device functionalities and communication capabilities by providing a common set of services and an environment enabling service composition. The merits includes proposed IoT architectural model introduces a more generic IoT architecture by integrating both the RFID and smart object-based infrastructures. The limitations includes that it doesn't give solution based on scalability, adaptability and there is a less performance.

B. Relationship-Based Access Control: Protection Model and Policy Language

ReBAC model to capture the essence of the paradigm, that is, authorization decisions are based on the relationship between the resource owner and the resource accessor in a social network maintained by the protection system. The merits includes that our model can be generalized to incorporate relations of higher-arity. The demerits are that the context hierarchy assumes a tree shape: that is only single inheritance is permitted.

C. Securing the Internet of Things

Its main aim is to provide lightweight cryptography for constrained devices, including block and stream ciphers and asymmetric mechanisms. The merits are the delegation mechanism is one privacy preservation proposal. An unauthorized RFID reader will retrieve only a random value, so it will not be able to track the user. The demerits are that there is performance degradation in the security techniques.

D. The Clustering of Internet, Internet of Things and Social Network

The clustering will promote the developing of the Internet of Things and social network. It is easy for scientists to analyse the behaviors of objects and people as data. It doesn't deal with human social networks and entity social networks relationships.

E. TRM-IoT: A Trust Management Model Based on Fuzzy Reputation for Internet of Things

The main aim of this system to help a sensor node requesting a specific service to find the most trustworthy route leading to another sensor node providing the corresponding service. The proposed model TRM-IoT has better performance. Proposed model doesn't provide information about updating the global trust and local trust changes.

F. A reputation-based trust management system for P2P networks

Proposed a reputation based, distributed trust architecture for P2P networks to identify malicious peers and to prevent the spreading of malicious content. The protocol is based on the query-response architecture of the first generation P2P networks. It reduces the number of query and response messages. Being a reputation-based protocol, our system in the end relies on the judgement of its users. Therefore, it can be effective only against attacks that are discernible by the user.

III. Proposed Methodology

Our proposed method based on both subjective and objective trustworthiness models. i.e peer to peer communication in social networks. Objective model based on peer to peer communication and the subjective model based on social networks. Subjective model defines that every friend has its own opinion about the other nodes based on its personal experiences. This opinion is identified from the feedback about the past transactions. Introduce weights for the opinions received from the friends. In the objective model, the construction of distributed hash table takes place. Chord Algorithm is used for distributed hash table construction. A distributed hash table stores the key value pairs by assigning keys to different nodes, a node will store the values for all the keys.

Here trustworthiness value can be evaluated using the following equations:

$$T_j = (1-\alpha-\beta)R_j + \alpha O_j^{lon} + \beta O_j^{rec} \quad (1)$$

T_j represents the trustworthiness.

α , β represents the weights of long and short term opinion.

O_j^{lon} is the long term opinion and

O_j^{rec} is the short term opinion.

R_j is the centrality.

To obtain the trustworthiness value, the following equations are needed.

$$R_j = \frac{(A_j + H_j)}{(Q_j + A_j + H_j)} \quad (2)$$

The above equation is used for calculating centrality.

A_j represents number of times p_j acts as an intermediate node.

H_j represents how many times p_j provider of service. Q_j represents number of times p_j requested a service.
The equations used for calculating long and short term opinion are given below.

$$O_j^{lon} = \frac{\sum_{i=1}^{M}\sum_{l=1}^{L} C_{ij}^{l} w_{ij} f_{ij}^{l}}{\sum_{i=1}^{M}\sum_{l=1}^{L} C_{ij}^{l} w_{ij}} \quad (3)$$

$$O_j^{rec} = \frac{\sum_{i=1}^{M}\sum_{l=1}^{L} C_{ij}^{l} w_{ij} f_{ij}^{l}}{\sum_{i=1}^{M}\sum_{l=1}^{L} C_{ij}^{l} w_{ij}} \quad (4)$$

Here, w_{ij} represents transaction weight factor .

C_{ij} represents credibility and

f_{ij} represents feedback.
The following equation is used for calculating credibility value

$$C_{ij} = \frac{(1-\gamma-\delta)T_i + (\gamma * 1) + (\delta * 1)}{1 + \log(N_j + 1)} \quad (5)$$

δ , γ represents the weights and N_{ij} defines number of transactions.

A. System Design

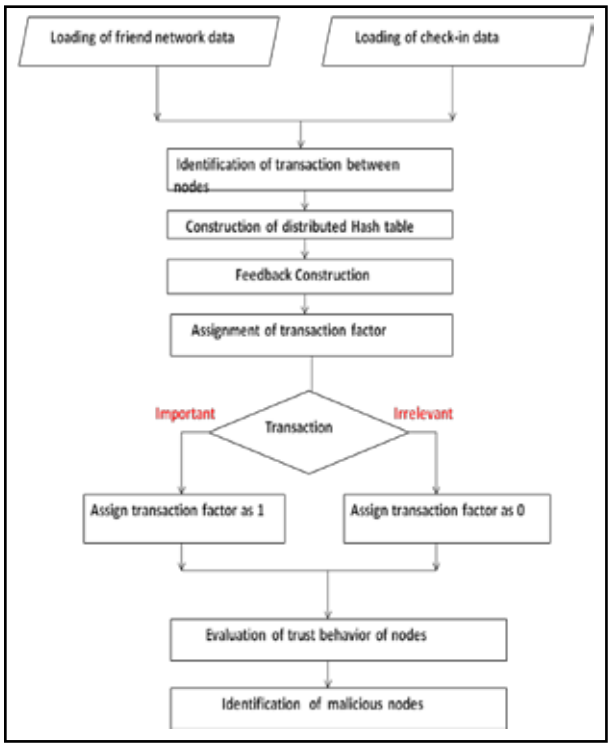

Fig.1 System Flow Diagram

B. Modules

The proposed method includes the following modules: Loading and processing of Dataset, Construction of Hash Table, Evaluation of Transaction Factor and Performance Evaluation.

C. Processing of Dataset

Processing of two types of dataset was done. First one is edges dataset. It consists of node communication i.e. Source node and destination node. The second dataset is check-ins dataset. It consists of node, check in time, latitude, longitude, location id. These datasets were taken from the real dataset of the location-based online social network Brightkite from the Stanford Large Network Dataset Collection. Here we can view the data. This will be used as the input for further processing.

D. Construction of Distributed Hash Table

In the construction of hash table, we are going to use chord algorithm.The chord algorithm consists of the parameter identifier, the identifier is the hash of the node id, where node represents the person. A distributed hash table stores the key value pairs by assigning keys to different nodes, a node will store the values for all the keys. Distributed hash table helps to identify the node and their communication. If any node needs any other nodes keys and values, it will search it in DHT only. This will be only maintained or managed by Pre-Trusted Objects. Here, key is generated for corresponding node i.e value. This key, values provides more security in information sharing. These keys are stored in the database. While processing the system, these keys and values can be retrieved from the database. Source Hash Key and Destination Hash Key are used as the input in order to find the corresponding node or value belongs to that particular key.

E. Chord Algorithm

The Chord system is an efficient distributed lookup service

ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)

based on the Chord protocol. The Chord system supports five operations: the addition and departure of Chord server nodes, and insert, update, and lookup of unstructured key/value pairs. All operations use the lookup primitive offered by the Chord protocol. The Chord protocol supports just one operation: given a key, it will determine the node responsible for storing the key's value. The Chord protocol uses a variant of consistent hashing to assign keys to Chord server nodes. Chord allows updates to a key/value binding, but currently only by the originator of the key. The Chord system does not provide an explicit delete operation an application that requires this feature may implement it using update (key, value) with a value corresponding to the "delete-operation" that is interpreted by the application.

Advantages:

- This chord algorithm is used for distributed hash table construction.
- The chord algorithm is a simple and common approach.
- User will get reply with in a log (n) time.
- Lack of redundant overhead.
- DHT algorithms store their data references in an organized way, they will always beat flooding algorithms

F. Identification of Transaction Information

After identifying the node communication, we should identify the transactions among the nodes. In this module, we identify the transactions among the nodes. Based on the services involved in the transactions, the feedbacks are provided. After that, view the transaction information with the node information.

G. Evaluation of Transaction Factor

In this module we are going to evaluate the transaction factor. The transaction factor is evaluated based on its importance of transactions. If the transaction between the nodes is important then the transaction factor is fixed as 1.If the transaction between the nodes is irrelevant then the transaction factor is fixed as 0. This information is used as a weight of the feedback. The following are the some examples of services that provided in the proposed system. They are:

- Placement
- Exam
- Entertainment
- Birthday
- Bank
- Food
- Password
- Medicines
- Movies

Based on the services, weight factors are assigned and also feedbacks are provided. If the weight factor is 1, then we will give the feedback above 0.5 and if it is 0, then will give feedback below 0.5.

H. Performance Evaluation

After assigning weights and feedbacks to the transactions, trustworthiness value will be calculated. Based on that value, malicious node and its path will be detected. The node or path which has highest value will be considered as trusted node or path and lowest value node or path considered as an un trusted node. After this, performance will be evaluated in the form of graph.

IV. Experimental Results

The experimental result shows that the security is much improved in the Social Internet of Things. The highest trust values for transaction are achieved in our proposed system.

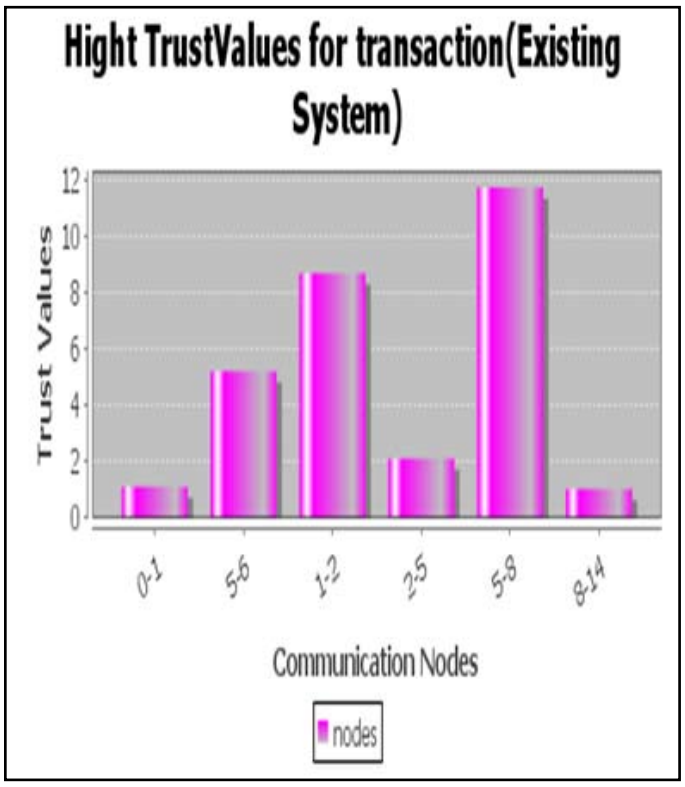

Fig. 2 : High Trust Values for Transactions (Existing System)

The above figure illustrates that the high trust values obtained for each node in the existing system.

Table I : Trust Value For Node

Source	Destination	Trust Value
0	1	8.189738485263987
5	6	8.109738483426575
1	2	16.70217825913127
2	5	4.093338188813542
5	8	16.702178259131266
8	14	5.774987370106874

The above table I shows the trust values calculation and the figure 3 illustrates that the high trust values obtained for our transactions based on the table. This gives us the path which has the highest trust value.

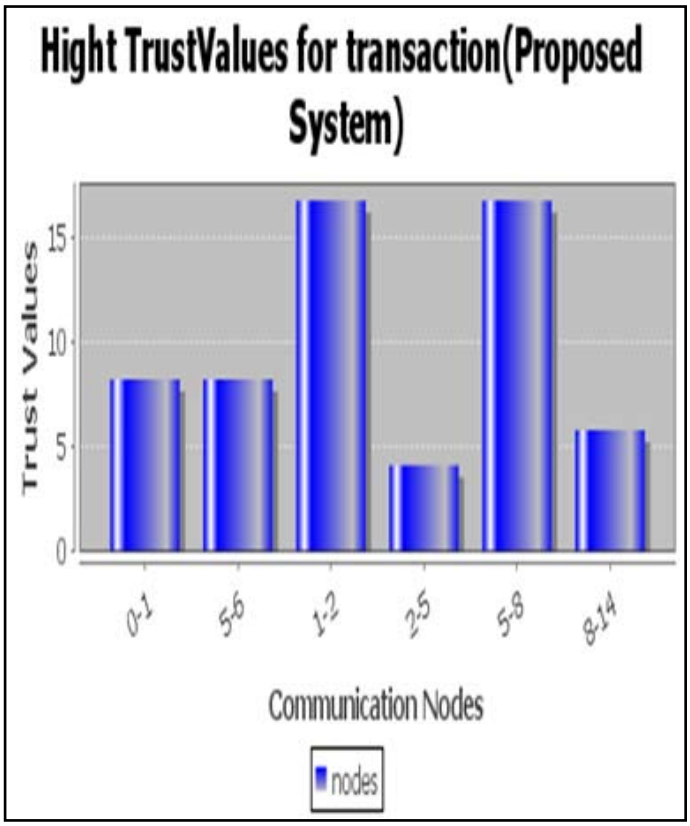

Fig. 3 High Trust Values for Transactions

The path which has highest trust value is considered to be the trusted path. The path which has lowest trust value is considered to be an untrusted path and that path contains the malicious node.

V. Conclusion And Future Scope

A. Conclusion

We have proposed the trusted network using subjective and objective trustworthiness models. In the existing system, they used only the subjective approach to find trusted node and path. But our proposed method provides more security by combining both the models. This will increase the performance. This will be more applicable in social networks like twitter, Facebook, LinkedIn etc.

B. Future Scope

This work can be further enhanced by identifying the shortest path to broadcast the information in a less execution time.

References

[1] *L. Atzori, A. Iera, and G. Morabito, "The Internet of things:A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, 2010.*

[2] *P. Mendes, "Social-driven Internet of connected objects," inProc. Interconn. Smart Objects with the Internet Workshop, Lisbon,Portugal, 2011.*

[3] *L. Ding, P. Shi, and B. Liu, "The clustering of Internet, Internet ofthings and social network," in Proc. 3rd Int. Symp. KAM, Wuhan,China, 2010.*

[4] *D. Guinard, M. Fischer, and V. Trifa, "Sharing using social networks in a composable web of things," in Proc. 8th IEEE Int. Conf. PERCOM Workshops, Mannheim, Germany, 2010.*

[5] *E. A. K. amd, N. D. Tselikas, and A. C. Boucouvalas, "Integrating RFIDs and smart objects into a unified Internet of things architecture,"Adv. Internet Things, vol. 1, no. 1, pp. 5–12, 2011.*

[6] *L. Atzori, A. Iera, and G. Morabito, "SIoT: Giving a social structure to the Internet of things," IEEE Commun. Lett., vol. 15, no.11, pp. 1193–1195, Nov. 2011.*

[7] *J. Surowiecki, The Wisdom of Crowds, New York, NY, USA: Doubleday, 2004.*

[8] *R. Roman, P. Najera, and J. Lopez, "Securing the Internet of things," Computer, vol. 44, no. 9, pp. 51–58, 2011.*

[9] *M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito, "A subjective model for trustworthiness evaluation in the social Internet of things," in Proc.IEEE 23rd Int. Symp. PIMRC, Sydney, NSW, Australia, 2012, pp. 18–23.*

[10] *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, Comput.Netw" vol. 56, no. 16, pp. 3594–3608, Nov. 2012.*

[11] *D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, "TRM-IoT: A trust management model based on fuzzy reputation for Internet of things." Comput. Sci. Inf. Syst., vol. 8, no. 4, pp. 1207–1228, 2011.*

[12] *T. DuBois, J. Golbeck, and A. Srinivasan, "Predicting trust and distrust in social networks," in Proc. IEEE 3rd Int. Conf. PASSAT and IEEE 3rd Int. Conf. Socialcom, 2011, pp. 418–424.*

[13] *M. Nitti, R. Girau, and L. Atzori. Trustworthiness Management in the Social Internet of Things: first theorital analysis [Online]. Available: http://social-iot.org*

[14] *B. Carminati, E. Ferrari, and M. Viviani, "A multi-dimensional and event-based model for trust computation in the social web," in Social Informatics, Berlin, Germany: Springer, 2012,pp. 323–336.*

[15] *J. A. Golbeck, "Computing and applying trust in web-based social networks," Ph.D. dissertation, Univ. Maryland, College Park, MD, USA, 2005.*

[16] *J. Golbeck and J. Hendler, "Inferring binary trust relationships in web-based social networks," ACM Trans. Internet Technol., vol. 6, no. 4, pp. 497–529, Nov. 2006.*

[17] *A. Jøsang, R. Hayward, and S. Pope, "Trust network analysis with subjective logic," in Proc. 29th Australasian Computer Science Conference, Hobart, TAS, Australia, 2006, pp. 85–94.*

[18] *A. Jøsang and S. Pope, "Semantic constraints for trust transitivity," in Proc. 2nd Asia-Pacific Conf. Conceptual Modelling, Newcastle, NSW, Australia, 2005, pp. 59–68.*

[19] *B. Christianson and W. S. Harbison, "Why isn't trust transitive?"in Proc. Int. Workshop Security Protocols, Cambridge, UK, 1997, pp. 171–176.*