Indian Journal of Science and Technology, *Vol 12(17), DOI: 10.17485/ijst/2019/v12i17/143128, May 2019*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A Novel Trust Establishment Model in SIoT Network based on Sociological Aspects of Users in Social Networking Services

Chanchal Sharma*, M. Afshar Alam and Aqeel Khalique

Department of Computer Science and Engineering, Jamia Hamdard, New Delhi – 110062, Delhi, India;
chanchal.kaushik25@gmail.com, aalam@jamiahamdard.ac.in, aqeelkhalique@jamiahamdard.ac.in

Abstract

Objective: The proliferation of internet results in exponential increase of the connected devices across the globe. These devices are continuously communicating with each other for several computational and information exchange tasks. These connected devices belong to IoT network and are also known as devices everywhere, anywhere. **Methods:** These IoT devices establish connection with each other for performing the desired computational tasks. Though, IoT devices are ubiquitous in nature, however, security and privacy remains a concern while establishing communication. To overcome these concerns, trust management is required before initiating communication among these devices. Trust management is domain where privacy of IoT devices is preserved and simultaneously ensuring security objectives in the IoT network. Research authors have proposed numerous models on trust management based on fuzzy logic. **Findings:** Our research scope is to propose a trust management model based on sociological aspects of users. In this paper, we have inclusively considered SIoT network for developing a deterministic model which can explicitly mention the trustworthiness of guest devices as determined by the host device. The determination is supported by the logical expression and is based on social attributes of the SIoT device, severity of the computational task and computational incentive of the task. **Application:** We present the model including the flowchart and algorithm supported by truth table. Our model is light weight and deterministic in nature which can be implemented by digital logic in the devices.

Keywords: Internet of Things, Privacy, Security, Trust Establishment, Trust Model, Trust Management Model, SIoT

1. Introduction

In today's digital era of communication and technology, computer, mobile and other connecting devices are becoming ubiquitous in nature. According to a study, total number of connecting devices present on the planet exceeds multiple times the total population of humans making it more than 4 devices per person on the planet. By 2021, more than 20 billion devices will be connected to internet and communicating to each other as and when required making it pervasive in nature[1]. This pervasive nature of these devices makes communication very obvious in nature and hence these devices are also known as Internet of Things (IoT) devices. The primitive nature of IoT devices is that they are anywhere, everywhere making communication and computation ubiquitous in the ICT domain. IoT network is the inter-networking of physical devices, smart devices, electronic appliances, automobile vehicles and other electronic devices having software, sensors, actuators, and network connectivity which enable these components to collect and exchange data over a network. IoT devices are transforming our ICT spectrum completely. Application areas of IoT network includes automation, healthcare, sustainable ICT, smart cities, traffic monitoring, logistics, retail industry, interactive and haptic computing etc.

**Author for correspondence*

In communication over IoT, there is vulnerability in the messages being communicated among the devices due to high level of heterogeneity. This vulnerability includes lack of trustworthiness of the heterogeneous devices, integrity and reliability of these devices. IoT network uses diversified devices, multiple communication channels and lack of standards and enabling protocols result in multiple security threats. In a diversified distributed environment such as IoT network authentication, authorization, access control and non-repudiation are important to ensure secure communication. Before initiating communication, these devices are required to establish a secure channel for communication. These secure channels are established after establishing trust among the communicating devices. Trust establishment is necessary to ensure that the vulnerabilities present in these devices should be resolved and ongoing communication is secure. These vulnerabilities are resolved by fulfilling security requirements by employing designated security mechanisms. Figure 1 shows security concerns in IoT network. Among these security concerns, privacy remains a challenge in IoT network as it solely depends on nature and characteristics of the devices. Due to heterogeneity in the devices, privacy cannot be controlled once the communication is started. That is one of the reasons to establish trust among the communicating devices before starting the communication. This method of establishing trust among the communicating devices is an aspect of Trust Management in IoT devices. Figure 2 shows the relation between Trust Management and communication among the devices. Trust can also be established among the communicating devices by negotiating on certain aspects which is called Trust Negotiation. Trust Negotiation and Trust Establishment together comes under Trust Management.

Though, continuous efforts have been made for establishing trust in the untrusted IoT network. It is important that mutual trust among devices is essential to initiate communication or to perform any computational activity in the IoT network. One of the challenges in IoT communication is establishing trust among the guest devices with the host device. A number of algorithms and models were proposed for trust establishment among devices in IoT network. These trust management models were based on several attributes for trust computation. In[2] presented a classification tree for Trust Computation. The trust computation can be based on QoS, social trust, distributed, centralized belief theory, Bayesian system, fuzzy logic, weighted sum, regression analysis, event/time driven, and single/multi trust. One of the approaches towards establishing trust among IoT devices is by treating these IoT devices as social IoT (SIoT) devices. The social aspect of human behaviour in Social Networking Services (SNS) becomes analogous in the SIoT network. We study this aspect and deduce a trust model based on human behaviour in SNS for SIoT network. Our trust model is novel and deterministic in nature where we have analysed the social characteristics of these devices in SIoT network. We have elaborated our work and propose a trust management model in this study. The structure of this paper is as follows: Section 2 discusses available literature but not limited in context of trust management model in SIoT network. Section 3 discusses the proposed model in light of social trust in SIoT network. Section 4 present the future work and we conclude our paper in Section 5.

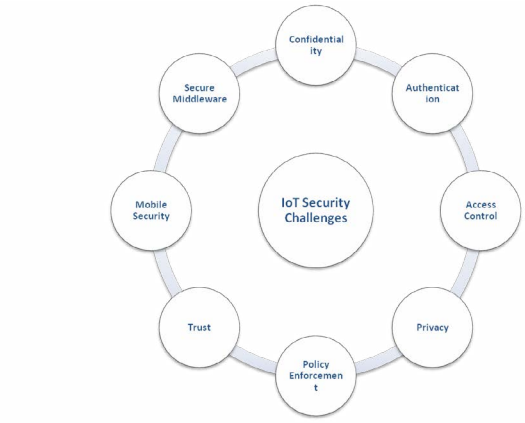

Figure 1. Security Concerns in IoT.

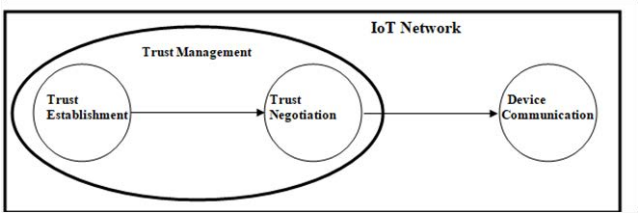

Figure 2. Trust Management in IoT.

2. SNS in Social IoT

In SIoT, social network and IoT give a new paradigm to IoT devices and hence the IoT network becomes SIoT network which includes humans and IoT devices. In SIoT network, devices have their own social networks which offer humans to impose rules on these devices to protect their privacy, security and also lead to secure communi-

cation after establishing trust. Companies such as eBay, Amazon and Google[3,4] use social relationship models to provide secure and reliable services by using the reputation and trust metrics with reference to SIoT devices. In SIoT network, trustworthiness of IoT devices are measured using several trust management models as discussed later in literature review section. However, trust management is a major challenge in SIoT to ensure reliable data analysis and enhanced device security.

With evolution of social network across the digital globe, people across the world have developed social behaviour over the digital platform. Users are connected to each other using their social profile through direct, mutual or indirect connections. Social network mainly builds upon users having similar personal or career interests, activities, backgrounds or real-life connections. Growth of SIoT is also depending upon interaction paradigm of the IoT devices to adopt a social approach. In SIoT network, the devices are capable of establishing social relationships with others. The interactions among devices occur in their social network. In SIoT network, IoT devices start communication with each other after establishing trust using a trust management model. In next section, we present trust management model which is derived from human social network or primarily SNS. We have utilized the human social behaviour in SNS into our SIoT network. This analogy is validated on the basis of the obvious nature of SIoT network as shown by several authors in literature survey. This validation can also be seen here[5].

We have studied and investigated the potential of combining social paradigm of human behaviour and ubiquitous nature of IoT devices.

2.1 Role of Trust in IoT Devices

Trust in IoT communication plays an important role as the communication take place among multiple devices. Trust in human sociology refers to a degree of extent at which information can be shared explicitly without any constraint of privacy preservation. Degree of trust is inversely proportional to the degree of privacy as shown in Figure 3. Degree of trust is much required while initiating communication and the satisfaction of trust requirements are strictly related to the identity management and access control issues among IoT devices[6]. A relation between trust and privacy specifies that it is the ability of an entity to determine whether, when, and to whom information about itself is to be released or disclosed with other device[7].

In IoT devices, communication among devices is initiated after establishing trust between the devices. We cannot require pre-existing trust relationships between devices as IoT network is very dynamic and pervasive in nature. It is important to establish trust among the device at runtime before initiating communication. Trust establishment is also important as it takes care of data or information sharing/ privacy preservation based on the trustworthiness of the device. The data or information being shared with other devices is private information and it must not be misused by the other device.

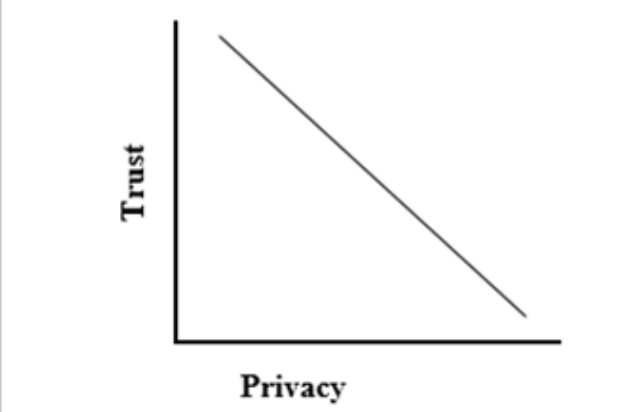

Figure 3. Relation between trust and privacy in social networking.

2.2 Literature Survey: Trust Model based on SIoT

In this section, we have reviewed several trust model based on SIoT:

In[8] proposed a model for SIoT objects with reference to social connections. The model uses a distributed approach which is based on advanced scalability and improved feedback. The approaches were based on the following criterion:

- Involvement of the devices rather than owner.
- Ease of discovering services and resources and provide an effective distributed solution based on human connection.
- SNSs platform that includes devices instead of human beings.

The architecture of the proposed SIoT model includes different layers on server and client side. In their model, Base layer, Component Layer and Application Layer are present on server side. Object Layer, Object abstraction layer and Social agent layer are present on client side.

In[9] proposed a system architecture that were based on to incorporate things for an implementation of social network. They also defined some policies to administrate the social relationships among objects to get the subsequent safe social network. They have also simulated the attributes of SIoT network by using SWIM mobility simulator. Their simulation result is based on type of relationship and it also gives probability distribution of the distance among those relationships.

In[10] proposed a subjective trust model to construct a management system for the objects trustworthiness which should derive the consumption of the services and the information delivery towards trusted nodes. The model defines how each device computes the trustworthiness of its neighbouring friend devices on the basis of its own experience and on the opinion of the friends in common with the potential service provider. Each device computes the trust of its friends on the basis of its own experience and the opinion of common friends with potential service providers. A feedback system is employed and the credibility and centrality of the IoT devices are applied to evaluate the trust level.

In[11] focus on to build a reliable system based on the nature of devices provided by the SIoT users. They defined their model into two models namely subjective model and objective model. In the subjective model, each device computes the trustworthiness of its adjacent devices by own experience or by the opinion of common device. In the objective model, information about every device is stored in a distributed hash table. The model was based on different type of relationship named as parental object relationship, co-location object relationship and co-work object relationship, ownership object relationship and social object relationship. The architecture proposed in the model was based on four components namely Relationship management, Service discovery, Service composition and Trustworthiness management.

In[12] proposed a trust model that uses recommendation, reputation and knowledge to calculate trust metric of every device. Their model computes reputation properties (Recommendation and Reputation trust metrics) as well as knowledge property (Knowledge trust metric).

The approach we propose differs from the literature for several major reasons.

- All the approaches proposed earlier were majorly focussed upon social aspects of humans in SNS
- Complex algorithm based on fuzzy logic or soft computing
- Our approach is light weight in terms of complexity and deterministic in nature.

The research study reviewed in this work are not limited though we have included the most relevant and related work based on SIoT with respect to our proposed model. Our proposed model is different from existing trust model/algorithms because our novelty lies in a very new paradigm of SIoT which we have validated through existing work in the similar domain. We have incorporated human sociological behaviour in social networking and override the similar behaviour in IoT devices operating in a SIoT network. Although, the behaviour may seem obvious in nature but we have taken the exemplary scenario for trust establishment before starting communication or any kind of collaborative computing performed in the ubiquitous environment of SIoT devices. In next section, we present our model and the flow diagram. We have also performed the truth table analysis for determining the deterministic value of the trust metric based on the parameters. These parameters discussed in detail in next section.

3. Proposed Trust Model Based on Sociological Aspects of Users in SNS

In social network, users are connected through each other over social connections including known contacts, acquaintance, friends, relatives etc. These connections need not ensure that the users know each other personally and having greater friendship affinity, trustworthiness, reputation etc. For example, if a user is required to catch up for a meeting with another user, it is important that there must be trust, reputation, mutual benefit and purpose of meeting. Narrowing down these constraint, there are 3 parameters which are required if the users want to catch up for a meeting. These parameters are:

- Trustworthiness: Degree of trust between the user based on reputation or recommendation. It can be historic or current.
- Severity: Degree of criticality of the situation. It can be high or low.
- Incentive: Benefit or reward as a resultant of the meeting/communication.

Considering these parameters in social network, any user will be ready for catch up for a meeting/communication with a friend (guest) of his/her if that guest user will be having trustworthiness (historic or current) based on reputation or recommendation and the catch up for a meeting/communication will also depend on severity (purpose) of the meeting/communication, incentive (reward) for the friend (guest) user. The possibility of successful meeting/communication depends on the sociological aspect of the user based on the parameters.

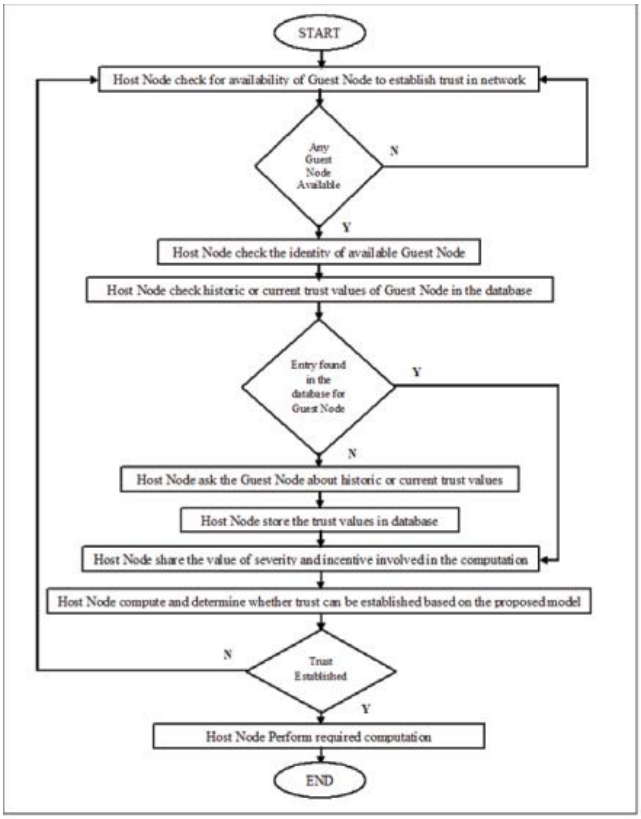

Figure 4. Flow model of proposed trust establishment model.

In our proposed model, we use sociological aspect of user in social network and implemented in SIoT network for multiple devices. A device (host) in SIoT network will initiate communication or undergo transaction/computation with another device (guest) after successfully establishing trust. We use social networking behaviour of users as a basis to establish trust and propose a deterministic expression based on the truth table. The host device will check for trustworthiness (historic or current) of the guest device and share the severity of the transaction/computation along with incentive involved (if any, on successful completion of transaction/computation). It is not necessary that a user will be ready for performing any transaction/computation with another in his friend list. We formulated all these possibility of transaction/computation being performed through truth table. Figure 4 show the flowchart of the proposed model. Figure 5 show the model architecture of the proposed model. In the model architecture, we have shown the host device and the guest devices. Figure 5 further shows the communication being passed among the host and guest devices before establishing trust to start the transaction/computation.

1: Host Broadcast (Availability)→Guest Devices
2: Host (Verify Guest ID)→Database
3: Database (Current/Historic Value)→Host
4: Host Broadcast (Severity, Incentive)→Guest Devices
5: Available Guest Devices (Acknowledgement)→Host Device
6: Host (Trust Established, 0|1)→Acknowledged Guest Device

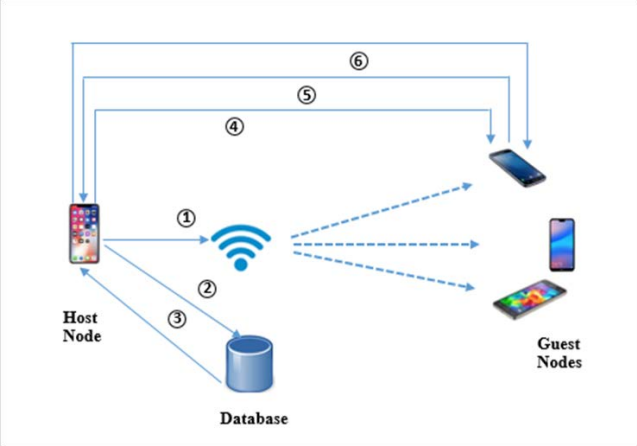

Figure 5. Trust establishment between host device and guest devices.

Based on the flowchart and model architecture, the trust metric will be calculated by the host device. The host device will be having access to the current/historic trust value of the available guest devices. The severity and incentive parameters are shared among the communicating devices. The host device acting as a SIoT device will be having social aspect of human behaviour in SNS and therefore will determine the trust metric to establish trust on the above decided constraints i.e. current/historic, severity and incentive of the transaction/computation. In current/historic trust metric, the value can be either

historic present (HI=1), historic absent (HI=0), current present (CU=1) or current absent (CU=0). In severity of the transaction/computation, the value can be either high severity (SE=1) or low severity (SE=0). In incentive of the transaction/computation, the value can be either incentive present (IN=1) or incentive absent (IN=0). Considering these 4 parameters (historic trust metric, current trust metric, severity and incentive), there will be 24 (=16) possible case scenarios which can lead to a deterministic response of establishing trust based on the calculated trust value among the communicating devices. These possible case scenarios will result into deterministic response of trust establishment (TE), the values can be 0 or 1 (0 stands for TE is not possible based on the proposed algorithm among the host and guest device, 1 stands for TE is possible based on the proposed algorithm among the host and guest device. The trust established among the communicating devices wills either true (1) orfalse (0) and hence the proposed algorithm is deterministic in nature. TE will be 1 i.e., trust will be established among communicating devices if these conditions are met:

{(HI OR CU)=1} & {(SE OR IN)=1}
(HI AND CU)=1
where, OR= Logical OR operator
AND=Logical AND operator

Otherwise TE=0 because, in the proposed algorithm, the social communication among the devices in SIoT network will be generally based on the social aspects of human behaviour in social networking services. In all other cases, where TE=0, both of HI and CU parameters are 0 implying that the devices are unknown to the host device which also signifies that their identity information is not available to the host device. Hence, it is analogically equivalent to the social communication of users in SNS where it is highly unlikely that a user interact/communicate with any other user whose identity information is not available (i.e. being unknown to the user).

There are 2 algorithms namely *HostAgent* and *DatabaseRecord* which are used to implement the proposed model. These algorithms as shown in Figures 6(a), 6(b) run on host device and database respectively.

We present a truth table, Figure 7, showing whether trust can be established among host and guest devices or not based on our model. Further, a Boolean expression is formulated using Karnaugh Map, as shown in Figure 9, based on the input parameters and conditions on which trust can be established in SIoT network (when the possibility of performing transaction/communication is true). The Boolean expression, hence, make our model deterministic in nature.

```
Algorithm 1: HostAgent

function isDiscoverable( )
  {
    check for guest devices available for communication;
    return guest_devices_id;
  }

function isRecordPresent( )
  {
    Check from database for guest_devices_id whether historic_trust_value or
current_trust_value present;
    If (historic_trust_value||current_trust_value = isPresent)
                return historic_trust_value, current_trust_value;
  }

function calculate_new_trust_metric( )
  {
      transmit severity, incentive to available devices;
      calculate new_trust_metric;                    //based on the parameters
```

Figure 6a. Algorithm for the proposed model.

```
Algorithm 2: DatabaseRecord

function updateRecord( )
  {
      update current_trust_value for corresponding guest_devices_id;
      return acknowledgement;
  }
```

Figure 6b. Algorithm for the proposed model.

TRUST		SEVERITY	INCENTIVE	TE
Current	Historic	High/Low	Yes/No	Yes/No
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	1
0	1	1	1	1
1	0	0	0	0
1	0	0	1	1
1	0	1	0	1
1	0	1	1	1
1	1	0	0	1
1	1	0	1	1
1	1	1	0	1
1	1	1	1	1

Figure 7. Truth table for computing trust establishment metric.

	SE'.IN	SE'.IN	SE.IN	SE.IN '
CU'.HI'	0	0	0	0
CU'.HI	0	0	1	1
CU.HI	1	1	1	1
CU.HI'	0	1	1	1

Cell Index	Variables	Color Marking
(6,7,14,15)	HI.SE	BLUE
(9,11,13,15)	CU.IN	GREEN
(10,11,14,15)	CU.SE	PURPLE
(12,13,14,15)	CU.HI	RED

Figure 8. K-map for reducing expression.

$$F(CU,HI,SE,IN)=HI.SE + CU.(IN + SE + HI) \quad \text{(eq. 1)}$$

Based on the above K-Map, the reduced expression is shown Equation 1. This logical equation can be represented using logic gates with input parameters CU, HI, SE and IN. The logical diagram of the deterministic equation is shown in Figure 9.

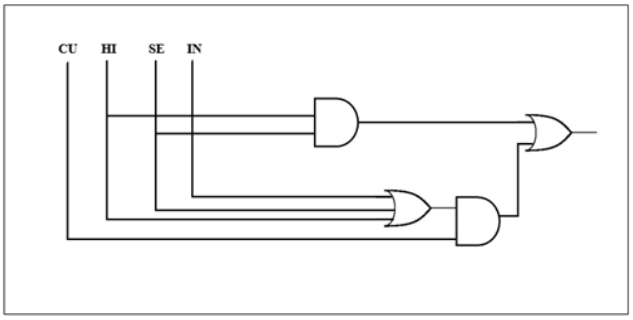

Figure 9. Logic diagram based on equation.

4. Future Work

As shown in earlier section, we have presented a novel trust establishment model in IoT devices based on sociological aspects of users in social network. Our model gives deterministic result in binary form (0/1) whether trust can be established among host and guest device or not. Our Boolean expression can be further used in electronic circuits and ready to be embed in sensor nodes or IoT devices. Future work is not only limited into deployment and fabrication of our Boolean expression in IoT devices, sensor nodes etc. to establish trust but can be extended and used in scalable distributed environment including heterogeneous devices undergoing trust establishment.

5. Conclusion

In this study, we present a model for calculating Trust Establishment metric for IoT devices in SIoT network. Our model is primarily based on sociological aspects of user's behaviour in social networking services. In SIoT network, devices have their own social networks which offer humans to impose rules on these devices to protect their privacy and security. It also leads to secure communication after establishing trust, where trustworthiness of IoT devices are measured using reputation and trust metrics with reference to the devices. Our model is lightweight and deterministic in nature. Furthermore, it can be deployed using digital logic within the circuit of the devices or can be implemented using coding. We present the truth table based on our validation and rules of social connections among users for any computation/transaction. Our model is best utilized in current environment where devices are ubiquitously present for connection and computation. Industrial applicability of the model can be in several segments such as Smart Automation, Smart Home/Cities, Smart Agriculture, Smart Retail, Smart Cities, Healthcare, Wearable Computing, Sustainable ICT communication. For instance, in traffic management, connected cars can exchange real time traffic data among each other. If a car wants to exchange the traffic data with cars ahead/behind it, the car first get the parameters required to establish trust and it can determine the trust establish metric. If the nearby cars are trustworthy and trust can be established, then the car will exchange the traffic data with other cars. Other possible scenario in different application domains can also be considered.

6. References

1. Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated [Internet]. [cited 2016 Aug 18]. Available from: https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated.
2. Guo J, Chen IR, Tsai JP, A survey of trust computation models for service management in internet of things systems. Computer Communications. 2017; 97:1–14. https://doi.org/10.1016/j.comcom.2016.10.012
3. Josang A, Ismail R, Boyd C. A survey of trust and reputation systems for online service provision. Decision Support Systems. 2007; 43:644–81. https://doi.org/10.1016/j.dss.2005.05.019
4. Page L, Brin S, Motwani R, Winograd T. The PageRank citation ranking: Bringing order to the Web L. Page. Proceedings of the 7th International World Wide Web Conference. 1998; 7:161–72.
5. Lin Z, Dong L. Clarifying trust in social Internet of Things. Transactions on Knowledge and Data Engineering. 2018; 30(2):161-72. https://doi.org/10.1109/TKDE.2017.2762678

6. Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead. Computer Networks. 2015; 76:1–62. https://doi.org/10.1016/j.comnet.2014.11.008
7. Yan Z, Zhang P, Vasilakos A. A survey on trust management for Internet of Things. Journal of Network and Computer Applications. 2014; 42:120–34. https://doi.org/10.1016/j.jnca.2014.01.014
8. Atzori L, Iera A, Morabito G. SIoT: Giving a social structure to the Internet of Things. IEEE Communications Letters. 2011; 15:1193–5. https://doi.org/10.1109/LCOMM.2011.090911.111340
9. Atzori L, Iera A, Morabito G, Nitti M. The social Internet of Things (SIoT) - When social networks meet the Internet of Things: Concept, architecture and network characterization. Computer Networks. 2012; 56:3594–608. https://doi.org/10.1016/j.comnet.2012.07.010
10. Nitti M, Girau R, Atzori L, Iera A, Morabito G. A subjective model for trustworthiness evaluationin the social Internet of Things. IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications; 2012. p. 18–23. https://doi.org/10.1109/PIMRC.2012.6362662
11. Nitti M, Girau R, Atzori L. Trustworthiness management in the social Internet of Things. IEEE Transactions on Knowledge and Data Engineering. 2014; 26:1253–66. https://doi.org/10.1109/TKDE.2013.105
12. B.Truong, N., Um, T.W., Lee, G.M, A reputation and knowledge based trust service platform for trustworthy social Internet of Things [Internet]. [cited 2016]. Available from: https://www.semanticscholar.org/paper/A-Reputation-and-Knowledge-Based-Trust-Service-for-Truong/6960e855b20262c49d492b32d31f0fd6c20a46f5.