Volume 7, Issue 1, January 2017 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Survey on Trust Management Models in Internet of Things Systems

Thamburu T. R.[*], Asst. Professor Vinitha A.V.
Department of CSE, Thejus Engineering College, Vellarakkad,
Kerala, India

DOI:: 10.23956/ijarcsse/V7I1/0115

Abstract— The Internet of Things (IoT) is an emerging technology that has started gaining new momentums in recent years and trust of IoT entities is an inevitable aspect to be ensured when different entities have to collaborate and communicate. IoT creates a smart environment by providing advanced intelligent services for human beings, which helps people to overcome perceptions of risk and uncertainty. A wide variety of services and applications for IoT have emerged in to various areas such as banking, healthcare, transportation shopping etc. There is a chance that the large sensitive data could be exposed while applying these applications and hence it is necessary to consider trust related aspects and other security problems which can threaten confidential data and personal privacy. Thus trust is a very complicated concept to be achieved in terms of security, reliability, integrity and confidentiality. An efficient trust management model is to be employed in every IoT system to protect the system against malicious attacks and thereby ensuring reliable and secure data transmission. To achieve this objective, various trust management models are used to enforce different security measures in a social IoT system. Three different trust management models namely reputation model, subjective model and dynamic model are explained and pros and cons of each model are stated and thus the advantage of one model over the other is understood. Accordingly in this paper, a detailed study of each model is done with other pinpoints thus leading to a thorough study of three different trust management models.

Keywords— Internet of Things, Trust management model, Social IoT, Trust, Security, Reputation

I. INTRODUCTION

Internet of things is a concept that enables entities to sense and collect required information from the physical world and share this collected information through internet which can be processed and used for various purpose. In IoT, a thing can be a person, location, time information or a condition. Thus we can say that an IoT is nothing but an internetworking of devices to share data across internet. Since the devices are built with chips and sensors, each device becomes locatable.

The IoT is a novel paradigm that is of considerable interest in modern world since it enables us to create a smart environment using this technology. The goal of the IoT's development is to connect the environment and physical world to the wireless networks; this would enable machines, objects and work environment interactive. By using IoT sensors, objects will be capable of interchanging the data with other machines without the help of human interference. However, the security risk is increasing rapidly due to its openness. So making sure whether the communicating entities are legitimate or not is an important concern. To solve this issue a trust management system is introduced in to the IoT network. Trust management models aid this process of ensuring legitimacy of entities in an IoT system.

Trust management aiming at solving distributed security related issues become a researching spot in recent years. Trust management is a useful technology to provide security service and its consequence has been used in many applications. Trust management plays a very important role in IoT for reliable data fusion and mining. So with the help of a trust management system IoT can provide the proper trust service according to the request.

The establishment of trust management for IoT remains an open issue. There are rare researches on the trust management in the context of the IoT . While the existing techniques make the concept of IoT feasible, a large number of challenges lie ahead for making the large scale real world deployment of IoT applications.

The rest of the paper is organized as follows: section 2 explains the challenges of IoT trust management and gives a brief idea about the need of implementing a trust management model. Section 3 surveys three different trust management models namely peerTrust model, subjective model and dynamic model. Also the detailed procedure of how trust computation is performed in each model is clearly discussed. Section 4 conducts a comparative study of the three trust management modes followed by the conclusion in section 5.

II. BACKGROUND

In this section, the main features of the Social IoT such as the challenges posed by an IoT system and need of incorporating a trust management model is clearly discussed.

A. Challenges of IoT Trust Management

The IoT trust management must have strong security assurance for all IoT nodes at all circumstances. But achieving this is a tedious task since IoT trust management possesses different challenges as follows:

- Heterogeneity: The communicating entities will only have an interface in common, their protocols, computational power, energy consumption, storage capacity will vary from one another
- Scalability: The number of things joining an IoT system can increase rapidly, so the trust management system should be able to handle such rapid increase in data transaction using carious load balancing algorithms.
- Data and privacy: In an IoT, millions of data can flow in to this system, so ensuring data privacy is an important concern.
- Identity: It is possible that a node hide its true identity, so identity management is an important aspect of the IoT which must be handled by various trust and reputation systems.
- Trust and governance: An entity must be able to select the most legitimate node from the network to accomplish the required task.

B. Need of implementing trust mechanism in IoT

Incorporating an efficient trust management model to the IoT system can lead to various benefits which are discussed below:

- Excellent flexibility: Nodes or users can define their own personalized policies to judge whether an object is trusted or not.
- Improved efficiency: Trust management system must be able to make decision according to the required criteria in such a way as to provide a good performance.
- Cross-domain platform: Trust management model can provide uniform decision making for heterogeneous nodes and sub-networks in IoT.
- Compatibility: a trust management system can assist or take advantage of other security protocols and mechanisms.
- Solve problem of uncertainty: With trust management, it is possible for the nodes to choose a suitable course of action when making operational decisions.

III. SURVEY

A. PeerTrust Model

In peerTrust model, trust evaluation is performed at each peer in a dynamic and decentralized fashion. And thus this model requires no central database to store all global data, instead each peer maintains a trust data which is a small database to store a portion of global trust data. Also, the trust data which is needed to compute the trustworthiness of peers is stored in a distributed manner across the network.

Each peer has a trust manager which mainly performs two functions, feedback submission and trust evaluation. Each peer also has a data locator for the appropriate placement of trust data over the network. The operation is performed in 2 steps. First the trust manager submits the feedback about a particular peer to the network and data locator will reroute this trust data to appropriate peers for storage. Second it is the duty of the trust manager to compute the trustworthiness of a target peer. The data locator helps to collect the trust data about the target peer from the network and then computes the trust value.

1) Challenges in P2P Networks:

This model being implemented over a structured p2p network, it lacks a centralized authority and hence incurs many challenges [4] [5] [6] as follows:

- Most existing reputation systems does not have mechanisms to differentiate honest feedback from dishonest ones and so the process of trust assessment becomes inaccurate if a peer submits dishonest feedback
- It is not compulsory that each peer have to provide feedback and so most existing systems suffers from insufficient feedback to make decisions about the status of a peer
- Most peers behave differently at different context and so the process of trust computation becomes inaccurate. For e.g. a peer remains honest for small transactions and behaves maliciously for larger transactions to make more profit
- Most existing systems lacks mechanisms to handle strategic dynamic personality of peers

2) Security Threats in P2P Networks:

The p2p networking environment suffers from many security threats as follows:

- Distribution of tampered data:
  An attacker peer x provides a fake resource with the same name of the real resource that peer y is searching for. This fake resource could be a virus program or a Trojan horse.
- Man in the middle attack:
  The malicious peer intercepts and modifies the message send from provider peer to the requester peer with its own IP address.
- Peers are easily compromised:
  Peers in a p2p networking environment are more easily compromised.

3) Trust Parameters:

P2p reputation model have 5 trust parameters defined as follows:

- Feedback (S):
  P2p model are feedback based systems i.e. decision about a particular peer is taken based on the feedback collected from other peers [11]. Feedback is the amount of satisfaction a peer receives during a transaction.
- Number of transaction (I):
  Some peer may try to improve its trust value by increasing the number of transaction to hide some of its misbehaving transaction. So the feedback metric alone is not sufficiently enough to compute the trust value since just taking the summation of feedback would result in inaccurate trust computation. An enhanced metric is computed as the ratio of total amount of satisfaction peer u receives to the total number of transactions peer u has.
- Credibility factor (CR):
  A peer may submit false statements about other peers due to jealousy or other motives. And so a trustworthy peer obtains many false statements against it even though it provides required service for every transaction. To avoid this, the model introduces a parameter called credibility factor. The feedback from higher credibility peer is weighed more than those with lower credibility.
- Transaction context factor (TF):
  Transaction context factor is an important trust parameter to differentiate transactions because transactions may differ from one another. This metric is used to differentiate critical transactions from non-critical ones.
- Community context factor (CF):
  This trust metric is used to solve community-specific issues and vulnerabilities. One method to solve feedback incentive problem is to award peers with a community context to enhance the participation of peers. Incorporating this metric make this model more robust against several malicious activities of peers.

4) Trust Computation:

The above defined parameters can be combined and a formula to compute the trustworthiness of peers is introduced. The trust value of peer u denoted by T (u) is defined as

$$\text{T (u)} = \alpha * \sum_{i=1}^{I(u)} S(u,i) * \text{Cr (p(u, i))} * \text{TF (u, i)} + \beta * \text{CF (u)}$$

where α and β denote normalized weight factors for collective evaluation and community context factor. I(u) denote the total number of transactions performed by peer u with all other peers. P(u, i) denote other participating peer in peer u's i^{th} transaction.

Unlike other trust management models, the p2p model lacks a central controlling authority to compute the trust value of all peers. Instead in this model, each peer collects the trust value of the target peer from other peers and then performs trust computation of target peer on the fly.

B. Subjective Trust Management Model

In this model, the social networking concepts are incorporated in to the IoT system that has led to so called Social Internet of Things (SIoT). The process of information discovery becomes easy even if the SIoT is made up of large number of nodes i.e., it supports scalability to a great extent. This model consists of many objects which belong to an owner and each object is capable of establishing social relationships in an autonomous way. This model enables to build a reliable system on the basis of the behaviour of objects.

1) The Social Internet of Things:

The main objective of adopting SIoT paradigm is to enhance the service discovery and thereby building a reliable system. In this model, each node will compute the trust value of its friends on the basis of its own experience and on the opinion put forward by the common friends. This social-oriented approach identifies different relationships that can occur between objects.

The process of identifying such relationships among objects will help to obtain required information from the most trusted object, thereby eliminating other malicious attacks. Ownership object relationship exists among objects that belong to a same user. Co-location object relationship and Co-work objet relationship exist among domestic objects and objects of same workplace respectively. Social object relationship is established among objects who interact occasionally and Parental object relationship is defined on similar objects of same brand.

2) Trust Parameters:

In this model each node p_i in the network computes the trust value T_{ij} of its N_i friends on the basis of its own experience and on the opinion put forward by its K_{ij} common friends. T_{ij} is the trustworthiness of node p_j seen by p_i. If p_i and p_j are not friends, they will not have any interaction experiences and so the trustworthiness is calculated by the suggestion put forward by the common friends. The basic trust parameters used for calculating trust value is as follows:

- Feedback system:
  A node p_i will submit a feedback to the service provider p_j denoting the satisfaction level of the service it has received. The feedback from node p_i to node p_j for a transaction l is denoted by f_{ij}^{l}. The value of f_{ij}^{l} varies

between 0 and 1. f_{ij}^{l}=1, if the node is fully satisfied by the service and f_{ij}^{l}=0 if it is not satisfied with the service.

- Total number of transactions:
  This metric identifies the occurrence of abnormal high number of transaction between two nodes i and j and is denoted by N_{ij} .
- Credibility:
  This metric is a key factor to evaluate the feedback and trust level provided by the nodes. It is denoted by C_{ij} and have values in the range [0,1].
- Transaction factor:
  It represents the relevance of a transaction l between nodes p_i *and* p_j and is denoted by ω_{ij}^{l}. It differentiates critical transactions from non-critical ones and has values 0 and 1. This metric can also be used as a weight for the feedback.
- Relationship factor:
  This metric represents the type of relationships that exist between communicating entities. Accordingly, in this trust management model, 5 types of relationships are introduced as follows:
  1. Ownership Object Relationship (OOR) -- 0.9
  2. Co-Location Object Relationship (CLOR) – 0.8
  3. Co-Work Object Relationship (CWOR) – 0.8
  4. Social Object Relationship (SOR) – 0.6
  5. Parental Object Relationship (POR) – 0.5

  Relationships between two objects belonging to a same owner are categorized as OOR. Since the chance of malicious activity of such nodes is less, it is assigned a highest factor value. Similarly, CLOR and CWOR relationships are established among domestic objects and objects of same work place respectively. Objects that are encountered occasionally is categorized under SOR and hence it is assigned a small factor value. POR are established between objects of same brand but that are never met and so POR are the most risky and thus it has the lowest factor value. It is clear that higher values indicate higher trustworthiness. If two objects are linked by two or are relationships, the strongest relation with the highest value is considered.
- Centrality (R_{ij}):
  This metric identifies the role played by a node in a network. If a node is invoked in a huge number of transactions or if node maintains numerous relationships with other node, such nodes plays a central role in the network [10].
- Computation capability (I_j):
  The malicious behaviour of an object depends on the computational capability possessed by an object. It is clear that a smart object has more capabilities to cheat compared to a dummy object. So while computing trust of a particular node, the intelligence it possess should also be a key factor in consideration. Accordingly, four classes of objects are introduced and each class is defined on the basis of computation capability and assign a different value to each class as follows:
  1. Class 1 : smart phone, tablet – 0.8
  2. Class 2 : setup box – 0.6
  3. Class 3 : sensor – 0.4
  4. Class 4 : RFID – 0.2

  Mobile objects with great communicational and computational capabilities such as smartphones, vehicle control unit are categorized as class 1. Static objects with some computational capabilities such as displays, smart video cameras belong to class 2. Objects with only sensing capability falls under class 3 and class 4 is assigned to RFID-tagged objects. This metric represents a static characteristic of the object since it does not change over time and hence this parameter is also included in trustworthiness computation.

3) Subjective Trustworthiness:

Based on its own experience and on the opinion of its common friends each node computes the trust value of its friends. To calculate the trustworthiness of a particular node, each node stores the feedback it receives. This helps to avoid single point of failures as $T_{ij}$and is defined as follows:

$$T_{ij} = \alpha R_{ij} + \beta I_j + \gamma O_{ij}^{dir} + \delta O_{ij}^{indir}$$

This trust computation depends on centrality, Intelligence, of its own direct experience O_{ij}^{dir} and on the opinion of its K_{ij} common friendsO_{ij}^{indir}. The terms α, β ,γ and δ are used to give different weight to the different terms in the above sum. To maintain the trustworthiness value between 0 and 1 keep α+β+γ+δ = 1.

If the nodes that request the service and the node that provides service are not close, then the trustworthiness value is obtained by multiplying the trustworthiness values of adjacent nodes in the route from the requester to the provider. At the end of every transaction, the node that received service will submit a feedback about the received service. If p_i and p_j are adjacent to each other p_i can directly assign feedback to p_j and also to its common friends that have contributed to the calculation of the trust value. If p_i and p_j are not adjacent, then it is the duty of intermediate nodes to propagate the feedback up to the provider, only if the previous node have credibility greater than a threshold.

C. Dynamic Trust Management Model

In dynamic trust management mode, routing is performed in an environment containing both malicious and selfish nodes along with trustworthy nodes. The trust management protocol computes the trust value of each node in the network and thus secure routing path is selected based on this computed trust value. Once a node registers to a network, the trust related information needed to calculate the trust value is collected from the respective nodes. Based on the computed trust value, the protocol detects malicious and selfish nodes and re-route the packets accordingly. This increases the message delivery ratio and performance of the network. Thus if a node is a trusted node, it gets access to the network and can perform data transfer to other nodes by choosing secure path based on the trust value computed by trust management protocol.

In this dynamic approach, the routing model used is the double-copy routing mechanism. The main idea behind this double-copy routing mechanism is that a node is capable of forwarding a data packet to multiple nodes at a time rather than to a single node. The assumption is that each mobile node will have a finite communication range. If a data receiver is not within the communication range of a data sender, the packetized data can only be transmitted through a sequence of intermediate nodes.

1) Metrics In Trust Computation:

The dynamic trust management model maintain three trust properties for each node namely honesty, cooperativeness and community-interest defined as follows:

- Honesty
  Honesty trust metric represent whether a node is honest or not. To compute the honesty value of node j, node I will keep track a count of suspicious dishonest interaction experiences performed by node j which node I has observed during a time interval [0,t]. This is done with the help of a set of anomaly detection rules such as high discrepancy in recommendation, great difference in retransmission interval, delay etc. A node is treated as a dishonest node if this count exceeds a system-defined threshold and thus the value of honesty metric of node j will be equal to 0.
- Cooperativeness
  Cooperativeness trust metric represents the willingness of a node to provide the required service or trust recommendation [8] [9]. This metric is computed by measuring the degree of co-operative nature of node j as evaluated by node i based on direct observations over a time interval [0, t]. The social relationship existing among each node is used to characterize the cooperativeness. Each node maintains a friend-list denoting the friends it has. The cooperativeness trust value of node i towards node j is computed as the ratio of number of common friends over total number of nodes that i and j have. The assumption is that friends are likely to be cooperative towards each other and thus nodes within its friend-list are more trustworthy compared to other nodes.
- Community-Interest
  In community-interest trust metric, nodes with similar capability or common interest are organized in to a specific community. Each node maintains a community-list denoting the communities to which it belongs. The community-interest trust of node i towards node j is computed as the ratio of the number of common communities participated by node i and node j to the total communities of node i and node j based on the direct observation of node i of node j over [0, t]. A node with high community-interest value denotes an active node.

2) Trust Management Scheme:

In this trust management model, the IoT environment does not have a centralized trusted authority. Each node can perform autonomously and independently with other nodes. Every device (node) in the IoT environment has an owner and an owner can have multiple devices. Each owner maintains a friend-list containing the friends of that particular owner. Nodes within a friend-list have more interaction experiences with each other.

Similarly, each owner also maintains a community-list denoting the communities to which it belongs. A device can be operated by its owner in certain communities or working environments and so the nodes belonging to a particular community have similar interests or capabilities. The scheme differentiates uncooperative nodes from malicious nodes. Uncooperative nodes are those nodes which does not provide the requested service if the service provider does not have a strong social tie with the service requester. A malicious node on the other hand tries to break the basic functionality of IoT system by providing wrong recommendations and information.

3) Trust Computation:

The trust value is a real number which varies between 0 and 1 where 1 denotes complete trust, 0.5 denotes ignorance and 0 denotes distrust. When computing the trust value, the following notations are used: node i is the trustor, node j is the trustee and node k is the recommender to provide its feedback about node j to node i.

When a node i directly interact with another node k at time t, node i will update its trust value as follows:

$$T_{ij}^{X}(t) = (1 - \alpha)\, T_{ij}^{X}(t - \Delta t) + \alpha\, D_{ij}^{X}(t) \quad ; \text{if } j == k$$

and

$$T_{ij}^{X}(t) = (1 - \gamma)\, T_{ij}^{X}(t - \Delta t) + \gamma\, R_{Kj}^{X}(t) \quad ; \text{if } j \neq k$$

Here, Δt is the time interval between two consecutive interaction and X denote honesty, cooperativeness or community-interest. $D_{ij}^{X}(t)$ denotes direct trust of node i towards node j in X at time t. $R_{Kj}^{X}(t)$ denotes recommendation from k towards j in X at time t. α is the weight on direct trust with respect to experience. The value of α varies between 0 and 1 and higher α means that trust evaluation relies more on direct observation.

If a node i does not have direct interaction experience with node j, node k can act as a recommender of node j if node k has interaction experiences with node j. To avoid bad-mouthing and ballot-stuffing attacks from a recommender k, node i uses its direct trust towards node k, $D_{ij}^{X}(t)$. Hence another parameter β is introduced as follows:

$$\gamma = \beta D_{ik}^{X}(t) \,/\, 1+ \beta D_{ik}^{X}(t)$$

This model introduces the concept of social relationships in to the IoT environment and enhance it assures enhanced trust assessment efficiency and are free from misbehaving attacks.

IV. COMPARATIVE STUDY

The comparative study of the three trust management models are shown in table 1

Table I Comparitive Study of Three Trust Management Models

Trust management models	Metrics	Consider social relationships	Consider intelligence of device	Network strain	Response to changes	Handling misbehaving attacks
PeerTrust model	• Feedback • Credibility • Transaction context factor • Community context factor	No	No	High network strain	Very slow	Suffer from attacks
Subjective model	• Feedback system • Relationship factor • Centrality • Computational capability	Yes	Yes	Less strain	Slow	Resilient to attacks
Dynamic model	• Honesty • Cooperativeness • Community-interest	Yes	No	Less strain	Fast	Resilient to attacks

V. CONCLUSIONS

The IoT is a new paradigm in modern technological world that allows devices to share information among each other and so the trust of IoT entities participating in the communication process is a crucial factor to be considered. A social IoT is a mix of traditional P2P networks and social networks, where social relationships are established autonomously according to the owners social network and thus can obtain the required service from trusted entities easily. Trust in an IoT system is a major concept to be handled properly in order to achieve secure and reliable data transfer. The trust management in an IoT environment can be modelled using various models such as reputation approach, subjective approach, dynamic approach, objective approach etc. The motivation behind this paper is to introduce different trust management models which are inevitable in an IoT system. In this paper, three trust management models are being surveyed namely PeerTrust model, subjective model and dynamic model. Also the different trust metrics that are used for evaluating trust and insights on how a trust metric can be customized to meet the requirements and goals of target system are also analysed. This paper also gives an overview of IoT, security attacks in IoT, need of trust management in an IoT system and thus conducts an in-depth comparative study of three trust management models for IoT describing the pros and cons of each trust management model.

ACKNOWLEDGMENT

I am extremely thankful to my Principal Dr. Satheesh Kumar for giving me his consent for this seminar. I am thankful to Prof Saju P John, Head of the Department of Computer Science, for his valuable suggestions and support. I am indebted to my project Coordinators Prof Saju P John, Mrs. Sheena K. S and my guide Mrs. Vinitha A V, Asst. Professors, Dept. of Computer Science and Engineering for their constant help and support throughout the presentation of the project by providing timely advices and guidance. I also thank God almighty for all the blessing received during this endeavour. Last, but not least I thank all my friends for the support and encouragement they have given me during the course of my work.

REFERENCES

[1] Li Xiong and Ling Liu, "PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities", IEEE Transactions on Knowledge and Data Engineering, Vol.16, No. 7, July 2004

[2] Michele Nitti, Roberto Girau, Luigi Atzori, Antonio Iera and Giacomo Morabito, "A Subjective Model for Trustworthiness Evaluation in the Social Internet of Things", 23rd Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 2012

[3] 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

[4] R.A. Malaga, "Web-Based Reputation Management Systems: Problems and Suggested Solutions," Electronic Commerce Research, vol. 1, no. 4, 2001.

[5] C. Dellarocas, "The Digitization of Word-of-Mouth: Promise and Challenges of Online Reputation Mechanism," Management Science, vol. 49, no. 10, 2003.

[6] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara, "Reputation Systems," Comm. ACM, vol. 43, no. 12, 2000.

[7] C. Dellarocas, "Analyzing the Economic Efficiency of Ebay-Like Online Reputation Reporting Mechanisms," Proc. Third ACM Conf. Electronic Commerce, 2001.

[8] Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay Tolerant Networks," in *IEEE Conference on Computer Communications*, San Diego, CA, March 2010, pp. 1-9.

[9] L. Atzori, A. Iera, and G. Morabito, "SIoT: Giving a Social Structure to the Internet of Things," *IEEE Communication Letters*, vol. 15, no. 11, Nov. 2011, pp. 1193-1195.

[10] L. Freeman, "Centrality in social networks conceptual clarification," *Social networks*, vol. 1, no. 3, pp. 215–239, 1979.