
Ms. Thamburu T.R\textsuperscript{1} & Mrs. Vinitha A.V\textsuperscript{2}
\textsuperscript{1} M.Tech student, Dept. Of CSE
Thejus Engineering College, Vellarakkad, Kerala, India
\textsuperscript{2} Asst. Professor, Dept. Of CSE
Thejus Engineering College, Vellarakkad, Kerala, India

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. 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 preserve the security and privacy of IoT systems, a trusted architecture for service management is introduced. A technique to detect and prevent the occurrence of SQL injection attack is also incorporated which greatly improved the network security and efficiency of the IoT system. The model makes the IoT system resilient to several types of attacks like bad mouthing attack, ballot stuffing attack, white washing attack discriminatory attack and self-promoting attack. Also the model aims to ensure a trustworthy system by removing the untrustworthy IoT devices from the social IoT system.

Keywords— Internet of things, trust management model, SQL injection attack, network security, efficiency

1. 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 should be 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 becomes 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. 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.

2. Background

In this section, the main features of the Social IoT such as the challenges posed by the IoT system, the need of incorporating a trust management model and possible attacks in IoT are discussed:

2.1. 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 various 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.

2.2. 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.

2.3. Attacks In Social IoT

A malicious node can perform a variety of trust-related attacks in an IoT environment as follows:

- Self-promoting attack: A malicious node can promote its own capabilities by providing good recommendations for itself so as to increase its chance of being selected as a service provider and then it provides dishonest service.
- Bad-mouthing attack: In order to reduce the chance of a good node being selected as a service provider, a malicious node provides bad recommendation’s about a good node so as to reduce the reputation of a well-behaved node.
- Ballot-stuffing attack: In order to increase the chance of a bad node to be selected as a service provider, a malicious node provides good recommendation’s about a bad node so as to boost the reputation of another bad node.
- Discriminatory attack: A malicious node tries to attack the nodes with which it does not have strong social ties or its non-friends in a social IoT system.
- White washing attack: A malicious node tries to wash away its bad reputation by disappearing and then rejoining an application.
- SQL injection attack: SQL injection attack is the process of insertion of SQL queries via input data to access the database.

2.4. SQL Injection Attack

SQL injection attack is a code injection attack in which an attacker inserts SQL code to a website to gain access to the resources or to modify the data. The SQL code is nothing but a request for some action to be performed on the database. Actions include commands to add, delete or modify the records in a database, affecting data integrity. Thus SQL injection allow attackers to spoof their identity, modifying or tampering the existing data, destroying data or making it unavailable, perform repudiation issues such as violating transactions or changing balances, gain access to complete disclosure of data and thus becoming administrators of the database server.

Figure 1: SQL injection attack

Figure 1 show how an SQLI attack is performed on a website. Instead of typing the exact username or password, the attacker can use special SQL commands such as ‘OR 1=1’ which equates to true at all times. Thus an attacker could gain unauthorized access to a website.
3. Literature Survey

The security risk is increasing rapidly day by day due to the openness nature of IoT. Traditional strategies such as access control are not sufficient to resolve the security issues of distributed system because of poor scalability. And so trust management models aiming at solving such security related issues becomes a top researching spot in last few years [1]. It is from social science that the concept of trust originated [2]. Furthermore, Trust is an abstract concept that can provide uniform decision making for heterogeneous and multi-domain IoT. Therefore an efficient trust management model is essential to solve such IoT related issues.

The term Trust management was first introduced by Blaze et sl. [3]. He designated trust management as a separate component of security services. He also described trust management as a potential approach for specifying security policies. The paper presents a prototype implementation of a new trust management system called policymaker that is capable of developing several security features. Yosra Ben Saieda, Alexis Olivereaua, Djamal Zeghlacheb, Maryline Laurentb in 2013 proposed a context aware and multiservice approach for the Internet of Things [4]. Most existing models compute the trustworthiness score based on a single factor. Also they do not take past experience of node in to consideration. This model takes this factor in to account by regrouping all past experiences in to a single metric. Simulation results show that this model show good performance and is able to withstand a class of common attacks.

S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini in 2014 proposed an efficient method to achieve security, privacy and trust in Internet of Things: The road ahead discusses the main challenges faced in the field of IoT security, the existing solutions and suggests some hints for future research. The solutions put forward by this paper if deployed, will help to achieve confidentiality, privacy for users, access control, trustworthiness among devices and users, comply with security and privacy policies [5].

Chen et al. [6] proposed a model for trust management based on fuzzy reputation for IoT. The model is applicable to an environment populated with wireless sensors only and hence QoS trust metrics like packet forwarding ratio, packet delivery ratio etc. are considered.

Bao and Chen et al. [7] proposed a trust management model which considers both QoS trust metrics and social trust metrics. Trust is calculated by taking both direct observations and indirect recommendations. But the drawback is that the model is unable to adaptively adjust the trust parameter upon varying conditions and hence is vulnerable to misbehaving attacks and results in poor performance.

4. Proposed System

In trusted architecture model, 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.

Figure 2 shows the system architecture for the trusted architecture model which mainly consist of two sections- SQLI attack prevention and trust formation. If a user tries to perform SQL injection to access a website, the request is first forwarded to a secure shell. The secure shell decides whether to grant permission for accessing the database with the help of a validation checker. The user entered details during login is passed to the validation checker,
which consists of a bunch of methods to filter all input data from users.

The result is passed back on to the secure shell and if the login is valid, then access to the database is granted. If the login is invalid, then access to the database is denied and thus the SQL injection attack is prevented. If the user is valid, he can perform information discovery by posting a query. The other users could view the posted queries and can give appropriate replies. A user obtains multiple replies for a single posted query. So it is a tedious task to decide the accuracy of the given reply. So here the accuracy of the reply is estimated by computing the trust of that IoT device.

There are three trust metrics- morality trust, supportive trust and civic trust which are defined as follows:

- **Morality trust**: Morality trust metric represents whether a node is moral or not. Morality trust is computed as the ratio of number of positive experiences over the total experiences. To compute the morality trust 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.

- **Supportive trust**: Supportive trust metric represents the willingness of a node to provide the required service or trust recommendation. Supportive trust is computed as the ratio of common friends between the users. When two users are the only friends and if the value of other two metrics is zero, then friendship bond between them is removed i.e. the two users remain no longer as friends. The social relationship existing among each node is used to characterize the supportiveness.

- **Civic trust**: In civic trust metric, nodes with similar capability or common interest are organized in to a specific community. Civic trust is computed as the ratio of common communities of posted query and replied user. A user can update his profile by adding communities in which he is aware of. Each node maintains a community-list denoting the communities to which it belongs. The idea is based on the concept that a user can belong to 1 or more community and also the posted query can also belong to 1 or more community. And if both are same, then the percentage of civic trust increases.

The overall trust value of each IoT device is obtained by performing summation of these three individual trust metrics. The IoT device with the highest trust value is selected among all replied devices. A positive feedback is send to most trustworthy IoT devices for the process of trust updation.

The steps can be summarized as follows:

1. Collect basic details during registration along with MAC address and stored encrypted with password
2. Community owner can allow or block the entry of a user to the social IoT system
3. Perform validation of user entered details using validation checker to prevent the occurrence of SQL injection attack
4. Performs information discovery by posting a query
5. Compute morality trust as the number of positive experiences over total experiences
6. Compute supportive trust as the number of common friends
7. Compute civic trust as the number of common communities in posted query and replied user
8. Calculate the overall trustworthiness value by aggregating morality, supportive and civic trust
9. Provide feedback for the process of trust updation

### 4.1. Advantages:

- **The trusted architecture for social IoT environment to detect and prevent the occurrence of SQL injection attack**
- **Once an SQL injection attack is encountered, that particular IoT device becomes blocked and is unable to remain active in the social IoT network**
- **Faster information discovery since the trust assessment is accurate**
- **The proposed model integrates social relationships among IoT device for trust computation**
- **The blocking of untrustworthy IoT devices from social IoT environments leads to an incredible increase in network security**
- **The trusted architecture model detects the occurrence of self-promoting attack, bad-mouthing attack and ballot-stuffing attack by considering morality as a trust property**
- **The model also detects discriminatory attacks by considering supportive and civic metrics as trust property**
- **The protocol remembers the trust information of each identity which detects the occurrence of white washing attack. Once a node disappears from the IoT system, trust value is decayed over time to indicate the node inactivity period.**
- **Reduced server load**
Compared to existing trust management models, the required storage cost and communication cost is significantly reduced.

5. Results and Discussions

To analyse the performance of the entire system, five metrics are used. They are:
1. SQLI attack detection rate
2. Network security
3. Server load
4. Storage cost and communication cost
5. Resiliency

5.1. SQLI Attack Detection Rate

The figure 6.1 clearly explains the SQLI attack detection rate versus time in both existing system and proposed system. Since all the prevailing existing systems possesses no mechanisms to detect the occurrence of SQLI attack, the SQLI attack detection rate of all existing system is nearly zero. The proposed system detects the SQLI attack that is performed hourly and hence there is a steep increase in SQLI attack detection rate.

5.2. Network Security

The figure 6.2 depicts the relation between SQLI attack detection rate and security of the proposed system. The proposed trusted architecture model eliminates the untrustworthy IoT devices when SQLI attack is performed. Hence the number of untrusted IoT devices in a social IoT system decreases, which leads to an increase in network security level of the social IoT system.

5.3. Server Load

The figure 6.3 depicts the server load versus SQLI attack detection rate graph. The proposed trust model eliminates the untrustworthy IoT devices. Hence the total number of IoT devices that is to be handled by the social IoT system decreases, which leads to a decrease in the server load.

5.4. Storage Cost And Communication Cost

When two nodes directly interact with each other, they can directly observe each other’s activity and can update their trust assessments. The storage cost per node is $0(N_T N_X)$, where $N_T$ is the number of IoT devices and $N_X$ is the number of trust properties (morality, supportive and civic trust). The communication overhead per node from node i’s perspective is $0(N_X \sum_{j=1}^{N_T} \pi_{ij})$, where $\pi_{ij}$ is the encountering rate or interaction pattern of node i with node j.

5.5. Resiliency

The proposed trusted architecture model makes the social IoT system resilient to several attacks such as SQL injection attack, bad-mouthing attack, ballot-stuffing attack, white-washing attack, self-promoting attack and discriminatory attack.
6. Conclusion

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. Trust in an IoT system is a major concept to be handled properly in order to achieve secure and reliable data transfer. To preserve the security and privacy of IoT systems, a trusted architecture for service management is introduced. A technique to detect and prevent the occurrence of SQL injection attack is also incorporated which greatly improved the network security and efficiency of the IoT system. The model makes the IoT system resilient to several types of attacks like bad mouthing attack, ballot stuffing attack, white washing attack discriminatory attack and self-promoting attack. Also the model aims to ensure a trustworthy system by removing the untrustworthy IoT devices from the social IoT system.

There are several future research areas. The trusted architecture model does not considered the intelligence capabilities possessed by an IoT device. The malicious behavior 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 possesses should also be a key factor in consideration.

7. References


