ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal) | Impact Factor: 7.089|

Visit: www.ijirset.com

Vol. 6, Issue 9, September 2017

Enhancing Internet of Things Security Using a Trust-Based Framework

Prabal Kumar Joshi

Assistant Professor, PG Department of Computer Science and Applications, Guru Nanak National College, Nakodar Distt. Jalandhar, India

ABSTRACT: The internet of things, or IoT, is a global framework for the information age that connects virtual and physical objects using information technology and adaptable communication that is available throughout the evolution process to give advanced services. IoT is only being used to address safety-related issues. Users' private information may be impacted by information sharing between several devices. Therefore, to reduce the possibility of malicious and vulnerable failures, an appropriate approach mechanism is needed. Multiple services IoT is susceptible to numerous harmful attack kinds. One possible remedy for distributed network security concerns is trust management. The algorithm used to compute trust in this article only computes the trust for suspicious neighbours that are listed among the suspicious nodes; it does not compute the trust for all neighbours. As a result, energy consumption has significantly decreased when compared to the basis article technique.

KEYWORDS: internet of things, trust management, safety, energy.

I. INTRODUCTION

The Internet of Things is a network made up of diverse devices with varying process capabilities that can interact and communicate in a smart setting. In the future, we anticipate that one million gadgets will be connected to the Internet of Things. This global network allows real-time communication and information sharing between smart devices like computers, smartphones, sensors, drivers, and other commonplace gadgets (Mendoza & Kleinschmidt, 2018). Smart cities, smart networks, and—above all—electronic health are only a few of the innovative and practical applications that have been brought about by new IoT samples. The goal of all these applications is to enhance the quality of life. However, a robust and secure mechanism for safeguarding this billion IoT devices is necessary to achieve all of these devices (Awan, 2019).

By endangering this tool's dependability through phony services, cooperation denial, and other harmful actions, malevolent partners can pose a major threat to optimal network performance. As a result, organizations that function in such a transparent and hazardous setting must make the right choices regarding the level of trust they should have in a particular partner; this is an essential task, but it is not without difficulties (Kravari & Bassiliades, 2017). In IoT, trust management is a crucial topic. This problem enables a lot of gadgets and objects to express their thoughts on their partners' trust. This regulation aims to stop the negative consequences of services rendered by incompatible or self-centred nodes. To ensure that data is moved and kept to a minimum device should have faith in one another notwithstanding the unpredictability of services offered in IoT applications. It is extremely challenging to achieve reliability among heterogeneous groups managing many services in an IoT framework (Altaf, Abbas, Iqbal, & Derhab, 2019). In recent years, research has focused on trust management as a means of resolving disparate safety-related challenges (Wang, Bin, Yu, & Niu, 2013). Research on trust management in the context of IoT is scarce.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal) | Impact Factor: 7.089|

Visit: www.ijirset.com

Vol. 6, Issue 9, September 2017

II. THE IMPORTANCE OF TRUST

IoT has been regarded as a service provider (SP) among the various features of services. Trust management's goal is to offer a beneficial service that presents skilled services for service requester (SR), with IoT assistance. Figure 1 illustrates this relationship. Because trust echanisms impact both RS (for privacy protection) and PS, there is a reciprocal relationship here (Wang et al., 2013).

Trust management

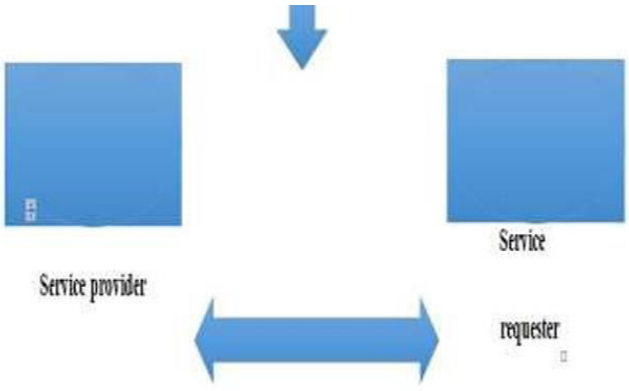

Figure 1. The services model

Conventional scales are used for availability control, coding, and IoT information protection. However, with the complex and heterogeneous Internet of Things, coding alone cannot resolve this issue since internal vulnerabilities can provide false information, which is confirmed by a system using trustworthy coding. The phrase for joining the network in the availability control field is that its identification will be given in the list of availability control. In any case, the system that controls the availability of variable behaviours is not secure, especially when it comes to malicious behaviour, and traditional availability control is not suitable for distributed environments because it is centralized. Trust management, however, can get around those problems. The foundation of this management is a single, adaptable system that can display all trust relationships, localize trust relationship control, and separate mechanism derived from the policy. Every component of the network is the outcome of the trust management issue. The most widely used trust management software has the ability to assess trust and make decisions based on trust that have a strong connection to the Internet of Things. Researched solutions regarding trust can yield some of the components and attributes of trust management:

Services: The function of trust management is assigned by this feature. The fundamental tenet of trust management is that in order to make a safe choice, one must have faith in the additional immunity information provided by a third party that can be trusted. In a network system, trust as a third party readily offers services to both service providers and service requesters.

Decision-making –the purpose of managing trust. The dependability of nodes, which collaborate with one another and select a dependable navigation and data transfer method based on their decision to provide a service, is what determines trust.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal) | Impact Factor: 7.089|

Visit: www.ijirset.com

Vol. 6, Issue 9, September 2017

Decision-making – the purpose of managing trust. The dependability of nodes, which collaborate with one another and select a dependable navigation and data transfer method based on their decision to provide a service, is what determines trust.

Self-organization. This feature displays the management of trust. Certain nodes or even subnetworks can be selected and self-organized based on trust management for a specific task (such as package delivery or data analysis) in terms of collaboration with one another in the network scene (i.e., IoT). Three crucial components are self-organization, decision-making, and services. We provide various definitions of trust mechanisms based on these characteristics.

Definition 1 (trust mechanism T). A self-organized collection of items based on their trust condition for deliberate decision-making is called trust management.

III. RELATED WORKS

Numerous scholars have examined trust in the context of the Internet of Things. Based on textual data, authors have suggested trust-centered personal services in (Otebolaku & Lee, 2018). This method illustrates how a person's text data can be utilized for the feedback process. They offer the computations, model, and architecture needed to showcase their own personal services. The authors of (Li, Song, & Zeng, 2017) have defined a policy-based system, assessed and provided the performance of their solutions, and suggested a dependable internet and policy-based that has solutions for smart cities.

The authors of (Sharma, Pilli, Mazumdar, & Govil, 2016) have put out a framework for managing trust. Various calculable trust models have been offered by authors, including flow models, graphical conceptual models, fuzzy models, probabilistic models, simple statistical models, learning machine models, and distance models. Using both direct and indirect data, authors have put forth a distributed trust model for the Internet of Things' multiple services in Mendoza & Kleinschmidt (2018). Through direct interactions between groups (services requests) and neighbor advice (exchange of trust tables), MT design allocates positive scores for legitimate nodes and negative scores for malevolent nodes.

To evaluate the efficacy of the model, authors created malicious nodes with weak assaults. The obtained findings demonstrate that the suggested MT model detects harmful network behaviours, with a particular emphasis on regions with 10% to 30% of malicious nodes. This methodology could be used to identify other prevalent IoT attacks, as allocated and On-Off attacks. The authors of (Maddar, Kammoun, & Youssef, 2018) have put out a novel intrusion detection model for the Internet of Things, specifically for WSNs. To ensure that nodes connect with the appropriate nodes for every transaction, this architecture tracks the nodes' geographic locations. Next, authors have put up guidelines for identifying attacks. In order to update trust nodes and eliminate malicious nodes, a mathematical model for calculating trust was presented.

According to Mendoza and Kleinschmidt (2018), trust is computed in a way that uses a lot of energy. Since node energy consumption in IoT networks is crucial, this should be taken into account in the suggested method. Certain studies that compute trust solely for suspicious nodes can be utilized to reduce bandwidth and energy expenditure due to trust calculation. Numerous techniques can be used to identify suspicious nodes, including those with unusual traffic. Therefore, the suggested approach modifies the trust computation methods to reduce energy consumption.

IV. PROPOSED METHOD

Our suggested approach involves assessing each network node's level of trust, which is done by neighbor nodes in a semi-centralized and semi-distributed fashion. Malicious nodes are identified and added to the blacklist, after which

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal) | Impact Factor: 7.089|

Visit: www.ijirset.com

Vol. 6, Issue 9, September 2017

they are either served or blocked. Additionally, in the last step's approach, a mechanism has been created for the first time to remove nodes from the blacklist in the event that they are mistakenly added or change their behavior, obtain the required services from their neighbor, and serve them (block out). As a result, we have created five distinct stages for our suggested approach, each of which we will discuss in detail below.

First phase: definition of the server's blacklist and initialization of trust values for the remaining nearby nodes in each node.

Setting the starting value of trust to zero means that, at the start of the algorithm, each node does not know enough about its neighbors; hence, it considers zero to mean that it does not know anything about the other neighbors. A list known as the "blacklist" will be defined on the trust server since the suggested approach leverages it for centralized trust management. Sabotage nodes that have reported different suspicions of nearby nodes are included in this list. This black list is defined at this level, and it contains no nodes.

Second phase: computation of trust values for each node's surrounding nodes

Every node at this level determines the trust values for adjacent nodes (the nodes to which they are connected and the information transmitted to them via these nodes). Algorithm 1 (the trust calculation algorithm in the basis article) is used to calculate trust for every node.

Third phase: submit a report on the discovery of malicious nodes.At this point, each node will compare these data with predetermined threshold values after determining the trust value.

Since trust values range from 1 to -1 and a value of 0 indicates that each node is not recognized, the threshold is equivalent to (-0.5). It notifies the trust management server of the nearby node as the suspicious node if it was less than the specified value.

Fourth phase The trust management server provides service management and receives services based on trust values Reports that certain nodes are suspected of being their neighbors are sent to the trust management server at this point. Right now. if the threshold (n/2 of the number of neighbors) is exceeded by the quantity of these reports. The node in question will be added to the list of sabotage nodes, which will minimize receiving service from the node, try to block it, and diminish giving service to it.

Fifth phase: extract harmless nodes from the blacklist. At this stage, after a predetermined amount of time (t), the server will recalculate the trust for every node that joins the blacklist. This procedure is necessary because the node can think that the issue needs to be fixed due to a mistake, a computational or network fault (such as latency and assaults, etc.). However, it could be feasible for a node to exhibit malevolent behavior for a number of causes (such an unforeseen error, programming issues, or any other cause), but after that time, it resumes its typical and typical function. Because of this, the blacklist must be removed. In order to accomplish this, the server requests that neighbors of malicious nodes compute new trust values for the malicious node and transmit them to the server via a trust recalculation message. If these numbers are less than the threshold value, the server will also retain the node in the list; if they are greater, the node will be removed from the black list.

Our method with the method of article (Mendoza & Kleinschmidt, 2018) has some special differences that we briefly describe each of them:

1. Our suggested approach calculates trust values only in certain cases and at particular times, as opposed to having neighbors calculate trust continuously, send these trust value tables for other neighbors, and update data for each

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal) | Impact Factor: 7.089|

Visit: www.ijirset.com

Vol. 6, Issue 9, September 2017

other. This is very helpful for network nodes, which are typically devices with a lot of energy, memory, and processing power.

2. Our approach sends simply the nearby nodes' identifiers rather than tables of trust values for neighbors that generate a lot of traffic over the networks. that is suspected is transmitted to the trust management server, which substantially lowers network traffic and energy usage.

3. To maximize the advantages of utilizing both approaches, a semi-centralized semi- distributed structure has been employed in the suggested approach. The nodes' actions by their adjacent nodes, which are close to one another, is examined, and a high-power server that manages the monitoring process by taking into account all factors makes the final decision.

4. The suggested approach uses the last step, restoring nodes from the black list, for the first time among related articles that also accomplish the aforementioned advantages. Nodes that have been placed on the blacklist in an incorrect manner or due to temporary maladministration should have their associated behavior reviewed after a while. If necessary, they should be taken off the blacklist and allowed to resume their regular sending and receiving services.

Algorithm 1 shows how to calculate the trust of each node by the neighbors of that node. In this algorithm, all neighbors of a node compute the trust value of that node based on the algorithm 1 in the base article (line 3), and if this value is lower than the trust threshold (line 4), this node as a the malicious node will be sent to the server (line 5).

Algorithm 1- Neighbour trust computing algorithm in each node.

1. T neighbors=0;
2. for (Node n: Neighbors)
3. 3-Tn =compute Trust (n);
4. if Tn< Trust_Thresh then
5. Send To Server As Malicious Node (n)
6. end if
7. end for

Algorithm 2. shows how the central server detects the malicious nodes. In this algorithm, all network nodes are first asked to calculate the trust of their neighbors and submit suspicious cases according to algorithm 1 for the server (lines 5 and 6). If the node identifies one or more of its neighbors as suspicious nodes and sends to the server, the server increases the amount of reports received for malicious activity of those nodes for one unit (lines 7 to 11). Then, if the number of received reports exceeds the threshold, the server will add this node to its blacklist (lines 13 to 17).

Algorithm 2- the algorithm for recognizing blacklist by server

1. Black List=∅;
2. for (Node n: Network Nodes)
3. Num Of Reporti=0;
4. end for
5. for (Node n: Network Nodes)
6. Receive Reports(n);
7. If it sends some Nodes as malicious sNodes then
8. for(Node i: malicious Nodes)
9. Num Of Report i++;
10. end for
11. end if
12. end for

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal) | Impact Factor: 7.089|

Visit: www.ijirset.com

Vol. 6, Issue 9, September 2017

13. for (Node i: Network Nodes)
14. if num Of Reporti> Report_Thresh then
15. Add i to Black List;
16. end if
17. end for

Algorithm 3. shows the way node leaving the blacklist. In this algorithm, the server first sends a request for reassessment of trust to all neighbors of the nodes that are in blacklist, and if these nodes redirect the node to the server as a malicious node, the server again adds one unit to the number of incoming reports (lines 4 to 11). If the number of reports is less than the threshold of the sent reports, it means that the node is getting out of the malicious state and is a normal node (lines 12 to 16). Of course, this limit of threshold can be stricter than the threshold set in Algorithm 2, since in recalculating the nodes' trust; the node must secure the server's credibility. This algorithm should be repeated at specific intervals, which varies depending on the network application and the type of node.

Algorithm 3- Algorithm for leaving node from blacklist server

1. for (Node n: Black List)
2. Num Of Reporti=0;
3. end for
4. for (Node n: Black List)
5. for (Node i: n.Neighbours)
6. Request Recalculating Trust(n);
7. If it sends n as malicious Node then
8. Num Of Reportn++;
9. end if
10. end for
11. end for
12. for (Node i: Black List)
13. if num Of Reporti<Report_Thresh 2 then
14. remove i from Black List;
15. end if
16. end for

V. SIMULATION AND EVALUATION OF RESULTS

The Helios eclipse ide simulation environment must be downloaded and launched before you can create a trust management simulation environment based on the JADE library (Hanoosh, 2021). The suggested approach is then put into practice utilizing the provided battery life model and the base paper algorithm (Mendoza & Kleinschmidt, 2018) for an Internet of Things network, and the outcomes are compared.

In the first experiment, the time needed to locate the malicious nodes is determined by the number of harmful nodes in the network (the ratio of malicious nodes to total nodes), as illustrated in Figure 2. As you can see, this time increases in tandem with the number of rogue nodes. Table 1 displays the findings of this comparison.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal) | Impact Factor: 7.089|

Visit: www.ijirset.com

Vol. 6, Issue 9, September 2017

Table 1. Comparison results of the mean time for detecting malicious nodes in the proposed algorithm with article [1].

Proposed algorithm	Basic article[l]	percentage
27	40	10
30	48	20
32	52	30

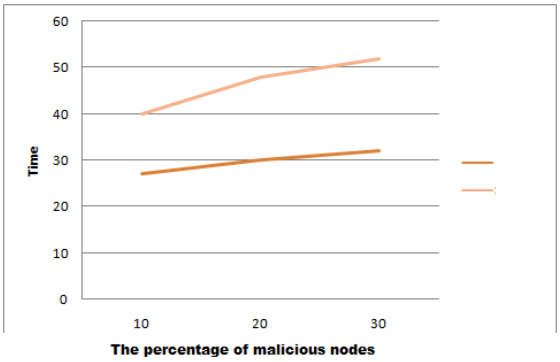

Figure 2. Comparison of the mean time for detecting malicious nodes in proposed algorithm and paper [1]

The second experiment uses the number of packets delivered in its frame size and the number of packets sent in its frame size to determine how much energy is used. As you can see in Fig. 3, our approach uses a lot less energy because trust is not determined sequentially. Additionally, our algorithm generates less traffic because it only determines trust by looking for suspicious activity.

There is a notable decrease in the time required to identify questionable nodes inside the network. Table 2 displays the relative energy consumption outcomes of the suggested method and article (Mendoza & Kleinschmidt, 2018).
Energy consumption comparison results of the proposed algorithm with article (Mendoza & Kleinschmidt, 2018)

Proposed algorithm	Basis article[1]
3017	1534

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal) | Impact Factor: 7.089|

Visit: www.ijirset.com

Vol. 6, Issue 9, September 2017

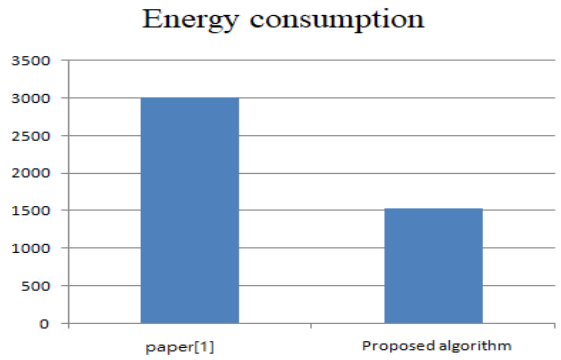

Figure 3. Energy Consumption Comparison with article [1]

VI. CONCLUSION

(Mendoza & Kleinschmidt, 2018) calculates confidence in a way that uses a lot of energy, and since energy-consuming node objects in IoT networks have significant relevance; this should be taken into account in the suggested approach. Limiting the calculation of trust to suspected nodes is one method to cut down on energy usage and network traffic brought on by trust calculations. A node with anomalous traffic is one of the many ways to identify a suspicious node. In order to reduce energy usage, the suggested approach in this study is to modify the trust calculation. The suggested approach was created in five stages. Rather than determining trust for every neighbor, the suggested method just determines the amount of trust for the suspicious neighbours, who are included in the list of suspicious nodes, will be calculated. Since determining the trust requires energy, energy consumption will be decreased in this method. Only when nodes exhibit aberrant behaviour can this procedure be used. An algorithm based on the volume of input and output traffic from each node will be developed in order to identify these suspicious and unusual nodes. In this sense, a node may be seen as suspicious if the volume of input traffic it receives exceeds the volume of outbound traffic. The results show that the suggested approach uses less energy than the one described in the article (Mendoza & Kleinschmidt, 2018).

REFERENCES

1. Altaf, A., Abbas, H., Iqbal, F., & Derhab, A. (2019). Trust models of internet of smart things: A survey, open issues, and future directions. Journal of Network and Computer Applications, 137, 93-111.
2. Awan, K. A., Ikram Ud Din, Ahmad Almogren, Mohsen Guizani, Ayman Altameem, and Sultan Ullah Jadoon. (2019). uted Trust Management Mechanism for Internet of Things.". RobustTrust–A Pro-Privacy Robust Distrib IEEE Access7.
3. Hanoosh, Z. (2021). A New Approach for Trust Calculation in Internet of Things. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(11), 6325-6332. Kravari, K., & Bassiliades, N. (2017). Social principles in agent-based trust management for the Internet of Things. Paper presented at the 2017 19th International Symposium on
4. Symbolic and Numeric Algorithms for Scientific Computing (SYNASC).
5. Li, W., Song, H., & Zeng, F. (2017). Policy-based secure and trustworthy sensing for inter internet of things in smart cities. IEEE Internet of Things Journal, 5(2), 716-723.
6. Maddar, H., Kammoun, W., & Youssef, H. (2018). Effective distributed trust management model for Internet of Things. Procedia Computer Science, 126, 321-334.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal) | Impact Factor: 7.089|

Visit: www.ijirset.com

Vol. 6, Issue 9, September 2017

7. Mendoza, C. V. L., & Kleinschmidt, J. H. (2018). A distributed trust management mechanism for the Internet of things using a multi-service approach. Wireless Personal Communications, 103(3), 2501-2513.
8. Otebolaku, A., & Lee, G. M. (2018). A framework for exploiting Internet of Things for context- aware trust based personalized services. Mobile Information Systems, 2018.
9. Sharma, A., Pilli, E. S., Mazumdar, A. P., & Govil, M. (2016). A framework to manage trust in internet of things. Paper presented at the 2016 International Conference on Emerging Trends in Communication Technologies (ETCT).
10. Wang, J. P., Bin, S., Yu, Y., & Niu, X. X. (2013). Distributed trust management mechanism for the internet of things. Paper presented at the Applied Mechanics and Materials.