INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact Factor: 6.078

(Volume 8, Issue 3 - V8I3-1373)

Available online at: https://www.ijariit.com

Analysis of a Fuzzy Based Security Approach for SIoT based Large-Scale Smart Environment

Gayatry
gayatrymisra@gmail.com
DAV Institute of Engineering and Technology, Jalandhar, Punjab

Harpreet Kaur
harpreet_daviet@yahoo.in
DAV Institute of Engineering and Technology, Jalandhar, Punjab

ABSTRACT

Large-scale smart environments (LSEs) are distributed systems that covers wide geographical area characterized by a large number of possibly heterogeneous, interacting Internet of Things (IoT) devices. Their deployment aims to provide enhanced cyber-physical services to its users, IoT allows the physical objects in daily life connect to internet and by creating an environment where these object can identify and communicate with each other through different communication methods including Wi-Fi and sensor technologies. But with LSEs there is new concept included which is Social Internet of Things (SIoT), SIoT moderates the challenges of IoT like trust,entity discovery and management by developing" social-like" relationships between the objects that search only those nodes with mutual social relations then the complexity and the time duration of the search could be drastically reduced. Now due to less approaches to develop a efficient LSEs and issues like Security and Trustworthiness are still to conquer incase of SIoT. The system includes implementation of a security system that is user friendly and can be used commercially which comprises of LSE Sensor, LSE End User, LSE Edge, where LSE Gateway(Server) acting as mediator .This paper proposed to resolve the security issues and reduction of maliciousness resulting in the increasing trustworthiness. In Proposed system there is usage of Fuzzy Logic rather than Crisp Logic that provide the user with better results and overcome the related issues by improving parameters like latency, trustworthiness factor and no of nodes detection in the system ,by addition of Fuzzy Logic and Artificial Intelligence(AI) there is analysis of sound(alerts)coming from a particular sensor thereby increasing the reliability and removing congestion.

Keywords *- IoT, Smart Environment, Security, Cloud Computing, Edge Computing, LSEs, SIoT, Fuzzy Logic, AI.*

1. INTRODUCTION

IoT is a new concept that gained huge attention from miscellaneous sectors, which improves automotive, infrastructure, telecommunications, and intelligent environmental applications [1,2]. Sensor information provides essential data in smart environment applications. The data should be accurate for better results. But as with any IoT device, data reliability can be erratic, because of sensors behavior, hardware failures, minimized nodes ,untrue positives, unusual values.. While taking into account the context of critical applications such as health care [3]. Security approaches are difficult to be implemented; security and privacy policies must be incorporated in smart environment applications that process sensitive data without effecting quality.

LSEs are distributed systems that cover a wide geographical area characterized by interacting IoT devices.They provide enhanced cyber-physical services to users. LSEs are recognized as highly dynamic systems. They should add, update, and remove functionalities depending on the available devices and services. Within an LSE, native objects, that are directly deployed, owned, and managed by LSE, other two kinds of entities are considered, namely foreign and external objects which are following, first are objects that enter and exit an LSE and don't belong to the LSE itself private mobile devices are examples of this type of objects. The other ones are located outside the LSE, that provide exploitable functionalities. In the considered open and dynamic scenario, issues like trustworthiness, Data processing, entity discovery and management need to be addressed. Furthermore, it is necessary to have methodological guidelines and tools to foster the development of LSEs By dealing with their complexity.

© 2022, www.IJARIIT.com All Rights Reserved

Edge computing was developed due to growth of IoT devices,that connect to the internet, many IoT devices generate enormous amounts of data during the course of their operations. Edge Computing is a distributed computing that brings data storage closer to location, Where it is require to improve response times and save bandwidth. In this nodes dynamically enter in the system then in the gateway (server). In the remaining parts of the paper, the proposed platform is discussed. the related work is described in section 2 while section 3 discuss the proposed framework, Secure IoT Framework for SIoT.

2. RELATED WORK

In the past few years studies shows that there were lots of research in development of Large Scale Smart Environment and its related issues

Y. Oh et al.(2010) [1] proposed architecture that integrated large-scale contexts from multiple sensors, and made a decision by reasoning about the collected contexts. The discussion was made about designed architecture that directed communities between large information entities and enhances intelligence abilities. L.Atzori et al. (201) [] paper identified scheme for establishing and management of social relationships between objects that resulted in safe social network, that describes a possible architecture for the IoT that included the functionalities required to integrate things into a social network and analyzed the characteristics of the SIoT network structure by means of simulations.

M.nitti et al. (2014) presented trustworthiness management in the SIoT that proposed subjective and objective approach. The big difference between the methods is the subjective approach has a slow transitory response while dealing with nodes with dynamic behaviors, a malicious person modifies her actions based on the relationships contradictory to this, the objective approach suffers from this kind of behavior, since a node's trustworthiness is global for the entire network and it includes both malicious nodes and liberal nodes

G. Fortino et al. (2015)This paper proposed a large-scale complex networked cyber physical system in which the Smart Objects (SOs) were fundamental building blocks. A novel software engineering approach aims to support a systematic development of SOs-based systems. The effectiveness of the proposed approach was demonstrated through a simple yet effective case study that showed the development of a smart office SO from the high-level design to its agent-based implementation. M. Diaz et al. (2016) This paper observed many connected technologies like RFID (Radio Frequency Identification) and WSAN (Wireless Sensor and Actor Networks) in order to exchange information. The requirement for better control, monitoring and management in many areas and the ongoing research in this field, had originated the appearance and creation of multiple systems like smart-home, smart-city and smart-grid. There are limitations of associated devices in the IoT in terms of storage, network and computing, and the requirement of complex analysis, scalability, and data access, require a technology like Cloud Computing to supplement this field. The IoT generates large amounts of diverse data quickly when there are millions of things feeding data to Cloud Computing.

F. Cicirelli et al (2017) discussed that in this paper Large-scale Smart Environments (LSEs) are open and dynamic systems where issues related to scalability and interoperability are addressed, aspects concerning services and objects discovery and reputation assessment require being managed. L Atzori, et al. (2017) proposed stages, generations characterized the development of IoT, along with the motivations of their triggering. Besides, it analyzed the role that IoT can play in addressing the main societal challenges and the set of features expected from the relevant solutions. Youqing Fan et al (2020) observed that fashion industry operates in a fast moving and dynamic environment which required fashion designers to respond to market trends continuously. It made potential for application IoT in fashion retail. Customer in-store behaviors reflected their hidden preferences. It was based on use of IoT as a framework of data collection tools to capture customer behaviors in-store.AI such Fuzzy logic and Adaptive Neuro-Fuzzy Inference System (ANFIS) were used to analyze customer purchasing intentions and simulation as well. This showed us that IoT can derive the required data of customer behaviors and uses AI to analyze the preferences. Its used to help salespersons to revert customer needs fast and with accuracy. However from above literature it can be seen there is still lack of developing an efficient and secure SIoT LSEs.

3. METHODOLOGY

This section describes SIoT as secure digital platform. Considering that SIoT networks are mostly suited. This methodology includes the scenario of making a security system in a shop, that works smartly without creating any hindrance to the shopkeeper, to make it safe and secure from burglars in an LSE environment, by addition of Fuzzy Logic. It contains different modules like LSE End User, LSE Gateway (Server), LSE Sensor (Noise sensor) and LSE Edge(Dynamic sensors). The working of these modules is merely based on simulation and all these modules work as sockets thereby covering concept of Socket Programming. There are unlimited static sensors installed in the shop The sensor nodes are sending alerts that consist of both true and false alerts. Due to addition of fuzziness in the system there can be seen great improvement in the results and its functionality.

3.1 Fuzzy Logic

Fuzzy logic is based on "degrees of truth" rather than the usual "true or false" (1 or 0) Boolean logic.

It has the capability of recognizing, representing, manipulating, interpreting, and utilizing data and information that are vague and lack certainty; Fuzzy logic has been applied to many fields, from control theory to AI. AI is the ability of a computer program or a machine to think and learn its a way to make machines behave and work like humans. It is also a field of study that makes computers "smart". Many factors have been improved by using this technology like there is generation of infinite alerts and nodes entering in the system which leads to congestion, only true alerts by gateway (server) are allowed pass to shopkeeper(LSE End user).

3.2 Tools Required

In this paper java socket programming is used to implement the technique

1. Java Socket Programming:

Java Socket programming is used for communication between the applications running on different JRE Java Socket programming can be connection-oriented or connection-less.

There are two classes used Socket and Server Socket for connection-oriented socket programming and for connection-less socket programming the below is used

Datagram Socket and Datagram Packet

The client should have the following: -

© 2022, www.IJARIIT.com All Rights Reserved

IP Address of Server
Port Number

2. Core Java :
Java has a runtime environment (JRE) and API called a platform. Java is a **programming language** and a **platform**. Its robust, object-oriented and secure programming language.
Database Connectivity - **DBC (Java Database Connectivity)**
JDBC **J**ava **D**ata**b**ase **C**onnectivity is a standard set of API (**A**pplication **P**rogramming **I**nterface)
It interacts with different database from Java application.
DBC Core Components are:

- Driver Manager
- Driver
- Connection
- Statement and Result Set

3.3 Implementation
Listed Below are the steps of proposed algorithm:
1. Start the gateway where the signal latency to be checked using a threshold value. Sense the signals from the sensors and send alerts to end users.
2. Start the end users who will receive alerts from gateway.
3. Start the node sensor that detects various sound noise levels from the environment.
4. Start the dynamic sensors using edge Computing.
5. All sensors send signals to gateway that includes both category of static and dynamic Sensors.
6. Gateway reads the different noise value and calculates the latency as per the following
Equation. :

$$Lcur = (Tcur - Tpre) – Lprev ,$$

Where Lcur = Current Latency in ms Tcur = Current Timestamp in ms Tpre = Previous Timestamp in ms Lpre = Previous Latency in ms.
7. Calculate the threshold value for the alert detection using the following equation at Fuzzy Gateway :

$$TWF = (Tat / (Tat + Taf)) * 100 ,$$

Where TWF = Trust Worthiness Factor, Tat = Total True Alerts,Taf = Total False Alerts, TV = (Lcur * Lprev) / TWF,Where Tv = Threshold Value Lcur = Current Latency in ms Lpre = Previous Latency in ms.
8. Analysis is done by gateway whether the latency calculated is greater than the calculated fuzzy threshold value.
9. If detected latency is greater than the given fuzzy threshold value then gateway sends the alert to the end user otherwise the counter update will be done for false alerts whose latency value is less than the given fuzzy threshold value.

$$At = At + 1 \text{ (if the signal fuzzy threshold value is greater)}$$

where At is True Alert, Af = Af + 1 (if the signal fuzzy threshold value is lesser) where Af is False Alert.

10. End user receives the alert from the gateway and total alerts stored in the backend.

4. RESULT ANALYSIS

4.1 Simulation:
Simulation is used which makes the use of static and dynamic sensors that work exactly as real time sensors thereby reducing the cost and manpower for establishing them.

4.2 Parameters
The proposed approach is compared on the basis of parameters as, Latency, No of nodes detections and Trustworthiness factor.

1. Latency
Latency generally means measure of delay in any two alerts. The delay it takes for alerts to go from server to end user. The formula to calculate Latency of the alert:

$$Lcurrent = (Tcurrent – Tprevious) – Lprevious$$

Where Lcurrent is the present latency of the alert given to end user and L previous is the last latency, Tcur – Tprevious is the latency time which indicates current time and previous time. **Figure 1** below shows the Latency in Gateway Crisp is less as the compared to Gateway Fuzzy, while using Fuzzy logic, there is more delay in alerts that increases latency which contributes to less no of fake alerts that makes the Gateway Fuzzy more efficient.

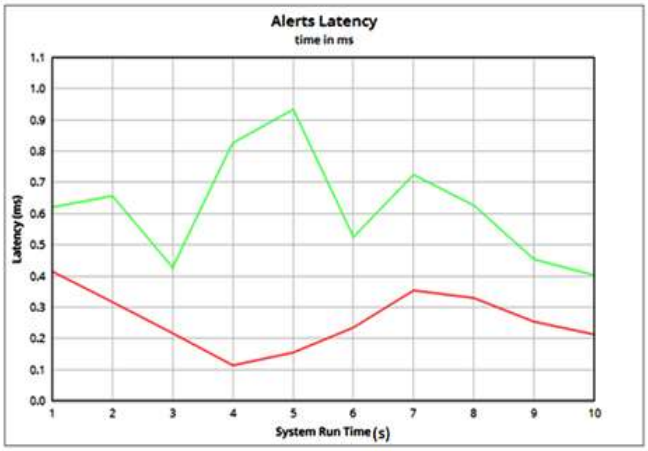

Figure 1 Comparison of latency parameter on the basis of Gateway Crisp and Gateway Fuzzy

Table 1

S No	Gateway (Crisp) ms	Gateway (Fuzzy) ms
1.	0.413	0.619
2.	0.315	0.655
3.	0.215	0.425
4.	0.112	0.825
5.	0.153	0.932
6.	0.233	0.523
7.	0.352	0.723
8.	0.328	0.625
9.	0.252	0.452
10.	0.211	0.401

2. **No of Nodes Detection**
It means no of nodes being detected over the communication network.
The formula for no of Node Detections :

$$Dn = Sum(Dnt)/count(Dnt) – Sum(Dnf)/count(Dnf)$$

Where Dn is no of nodes detected, Dnt means detected true nodes and Dnf means false nodes.

Figure 2 shows Nodes Detection in Gateway Crisp is less as the compared to Gateway Fuzzy, while using Fuzzy logic ,there are more nodes detected for false alerts which means higher communication efficiency on Fuzzy Gateway, If there is less

© 2022, www.IJARIIT.com All Rights Reserved

detection that generally indicates gateway not capable of detecting true alerts that less efficiency.

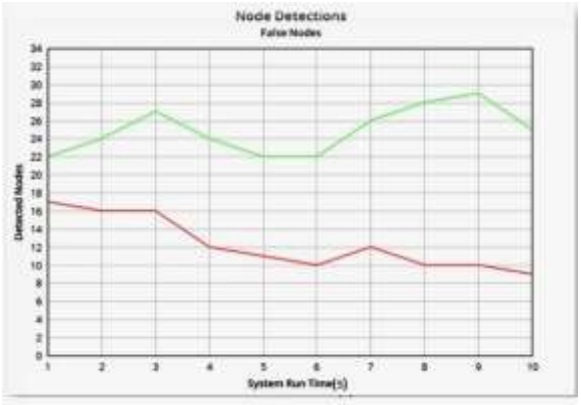

Figure 2 Comparison of No of Nodes Detection parameter on the basis of Gateway Crisp and Gateway Fuzzy

Table 2

S No	Gateway (Crisp)	Gateway (Fuzzy)
1.	17	22
2.	16	24
3.	16	27
4.	12	24
5.	11	22
6.	10	22
7.	12	26
8.	10	28
9.	10	29
10.	9	25

3. Trustworthiness Factor

The alerts entering in the system are true or false, trustworthiness factor is calculated by true alerts and false alerts . The formula is below:

$$TWF = (Tat / (Tat + Taf)) * 100$$

where Tat is total true alerts and Taf is total false alerts, by using fuzzy logic the TWF increases thereby work is faster.

Figure3 shows that Trustworthiness Factor in Gateway Crisp is less as the compared to Gateway Fuzzy, while using Fuzzy logic, the TWF increases.

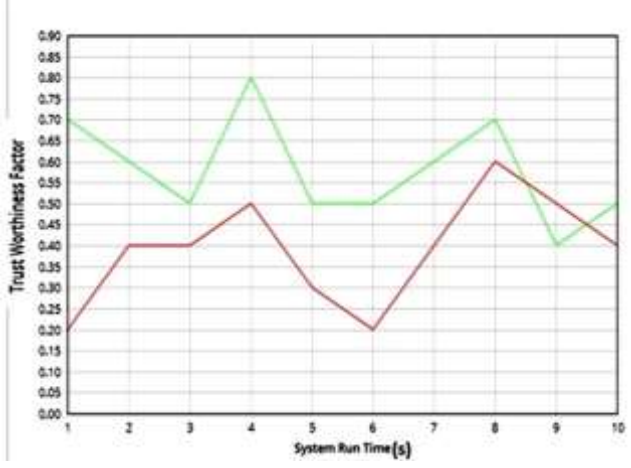

Figure 3 Comparison of Trustworthiness Factor parameter on the basis of Gateway Crisp and Gateway Fuzzy

Table 3

S No	Gateway (Crisp)	Gateway (Fuzzy)
1.	0.2	0.7
2.	0.4	0.6
3.	0.4	0.5
4.	0.5	0.8
5.	0.3	0.5
6.	0.2	0.5
7.	0.4	0.6
8.	0.6	0.7
9.	0.4	0.5
10.	0.4	0.5

5. CONCLUSION AND SCOPE

This approach allows removing any malicious device in a network. It can be see there is significant improvement by using fuzzy logic in the results. By using fuzzification the results are better and enhanced as there is analysis of alerts(sound) that is coming from a particular sensor thereby increasing the reliability and removing congestion. This paper proposed to resolve the security and reduction of malicious nodes. The improved results shows that Latency is increased by 25.84% to 61.8%,also No of Nodes Detection also varies from 12% to 24% And TWF shows significant increase from 39% to 58%.Future aspects can be using security algorithms for detecting false nodes who generate false alerts along with trustworthiness factor. There can be addition of public and private key mechanism where a node can be detected with its passed public key to Gateway (Server) and authenticate it with private key.

6. REFERENCES

[1] Y.Oh, J.Hanetal.“context management architecture for large-scale smart environments,”*IEEE* IEEE Communications*Mag.*, vol. 48, no. 3,pp. 118–126, mar. 2010.

[2] F. Cicirelli*et al.*, “An edge-based approach to develop large-scale smart environments by Leveraging SIOT,” in *Proc. 14th IEEE Int. Conf. Network Sens. Control (ICNSC)*, Calabria, Italy, May 2017, pp. 738–743.

[3] B. Rubio et al., “state-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing,” *j .network Computer Appl.*, vol. 67, pp. 99-117, may 2016.

[4] N. R. Jennings, “on agent-based software engineering,” *artificial Intelligence*, vol. 117, no.2, pp. 277–296, 2000.

[5] A. Vinci, “an edge-based platform for dynamic smart city applications,” *future generation Computer Syst.*, vol. 76, pp. 106–118, Nov. 2017.

[6] M. Zorzi et al.“Understanding the internet of things: definition, potentials, and societal role of a fast evolving Paradigm,” *Ad Hoc Network.*, vol. 56, pp. 122–140, mar. 2017.

[7] S. Das, *smart environments: technology, protocols, and Applications*. Hoboken, NJ, USA: Wiley, 2004.

[8] F. Cicirelli*et al.*, “on the design of smart homes: a framework for activity recognition in home environment,” *J. Med. Syst.*, vol. 40, no. 9,P. 200, 2016.

[9] A. Zanella, et al. “IoT for smart cities,” *IEEE Internet Things J.*, vol. 1, no. 1,pp. 22–32, Feb. 2014.

[10] Z. Khan, et al “Towards cloud based big data analytics for smart future cities,” *J. Cloud Comput.*, vol 4, no. 1,p. 2, 2015.

[11] Y. Sun, et al. “Internet of Things and big data analytics for smart and connected communities,” *IEEE Access*, vol. 4, pp.766–773, 2016.

© 2022, www.IJARIIT.com All Rights Reserved

[12] C. Savaglio et al. “Towards a development methodology for smart object-oriented IoT systems: A metamodel approach,” in *Proc. IEEE Int. Conf. Syst. Man Cybern. (SMC)*, Oct. 2015, pp. 1297–1302.

[13] L. Atzori, et al. “Trustworthiness management in the Social Internet of Things,” *IEEE Trans. Knowledge Data Eng.*, vol. 26, no. 5, pp. 1253–1266, May 2014.

[14] M. Bain. (2014). *Sentilo—Sensor and Actuator Platform for Smart Cities*. Accessed: Apr. 21, 2017.

[15] M. Roman*ist al.*, “A middleware infrastructure for active spaces,”*IEEE Pervasive Comput.*, vol. 1, no. 4, pp. 74–83, Oct./Dec. 2002,doi: 10.1109/MPRV.2002.1158281.

[16] G. Lehmann, A. Rieger, M. Blumendorf, and S. Albayrak,“A 3-layer architecture for smart environment models,” in *Proc. 8th IEEE Int.Conf. Pervasive Comput. Commun. Workshops (PERCOM Workshops)*, Mannheim, Germany, 2010, pp. 636–641.

[17] Chan, Chi On, Henry CW Lau, and Youqing Fan. "Implementing IoT-adaptive fuzzy neural network model enabling service for supporting fashion retail." *Proceedings of the 4th International Conference on Machine Learning and Soft Computing*. 2020.

© 2022, www.IJARIIT.com All Rights Reserved