International Journal of Advance Research in Science and Engineering
Vol. No.5, Special Issue No. (01), February 2016
www.ijarse.com
IJARSE
ISSN 2319 - 8354

SECURING INTERNET OF THINGS WITH DISTRIBUTED INTELLIGENCE FRAMEWORK

N. N. V. V. Praveen Kumar[1] P. C. S. Dileep[2]

[1,2]*Computer Science and Engineering, Pragati Engineering College (India)*

ABSTRACT

IoT is an ingenious coaction of sensors and devices bulging up new challenges to security and privacy in end to end communication of smart objects. Considerations for managing the huge data injected by smart objects is a crucial part. This paper gives an overview and analysis of distributed intelligence framework, especially in the area of IoT, through an IoT Manager. Together with the applied security solutions, the paper highlights the need to provide a secure manager for the smart devices to provide a flexible infrastructure for fault detection, fault tolerance and fault-repair mechanism. Finally, this paper proposes a distributed intelligence security framework for all the smart IoT devices.

Keywords: Distributed Intelligence, Fault Detection, Huge Data, IoT Manager, Sensor.

I. INTRODUCTION

The term, Internet of Things (IoT) that refers to uniquely identifiable objects, things, and their virtual representations in an internet-like structure, was first proposed in 1998. IoT will consist of a huge number of smart devices, sensors, electronic chips, services, people and other physical objects which have potential to interconnect, interact and exchange information about themselves and the surrounding environment. Now a Days IoT has been using for regular services in day to day life. A comprehensive management framework of data that is generated by the objects should store and interactively managed by a manager. By using different networks and devices we depend a lot on the smart devices, and we should be very careful about the data that is being generated by the IoT devices should be accurate and legitimate.

II. PRESENT IOT ARCHITECTURE

The present IoT Architecture is shown in the below figure [1].

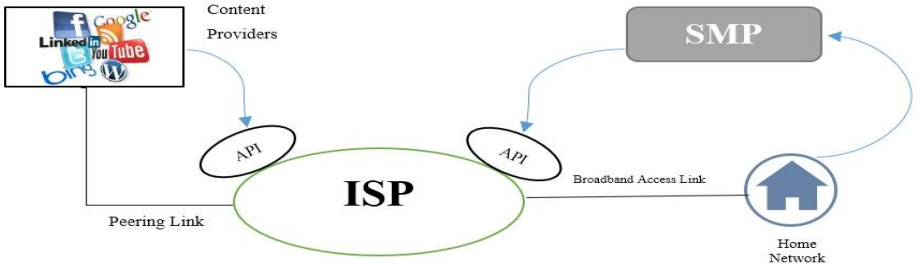

Fig.1

As illustrated in figure, the main challenge for IoT researchers is developing the API's which interact with sensors for providing smart services. Programming Languages like java,.NET are providing IoT services with their supporting frameworks. Upon these frameworks services of IoT can be developed rapidly. But designing smart services involves multiple factors and always a tradeoff exists between one design option with other. Balancing each design issue may affect the architecture also. Sometimes if security issues are weighed in the flexibility of the architecture.

III. LOOP HOLES IN PRESENT ARCHITECTURE

Till now the considerations for managing the huge data injected by the smart objects is neglected in IoT Research. There is no scheduling of tasks as per priority basis.

3.1 Issues and Challenges

Following are the some of the issues and challenges related to security for IoT

1.Security can be resource consuming and if you are using low power embedded device, this can be a big challenge.

2.The computation power available in IoT is limited and may be insufficient for the processing of security algorithms.

3.The battery capacity is also limited and their life duration is strongly connected to the quantity of computations executed in the embedded processor.

4.Storing limitations also are hurdles for embedded security features.

IV. PROPOSED DECENTRALIZED INTELLIGENCE FRAMEWORK FUNCTIONS OF IOT MANAGER

1.Handling communications among the Smart Devices will be the main functionality.

2.All the sensors in smart environment will not directly communicate with each other.

3.The IoT manager will have the responsibility of taking a proper decision to forward a sensor message to another smart object.

4.Till now, the considerations for managing the huge data injected by the smart objects is neglected in IoT Research.

5.We propose a scheme to filter out the sensor messages which are insignificant considering some pre-specified priority levels for message transmission.

6.The IoT manager also has a fault detection, fault tolerance & fault repair mechanism.

4.1 Proposed Architecture for IoT Manager

Figure 2 shows the architecture design for the IoT Manager

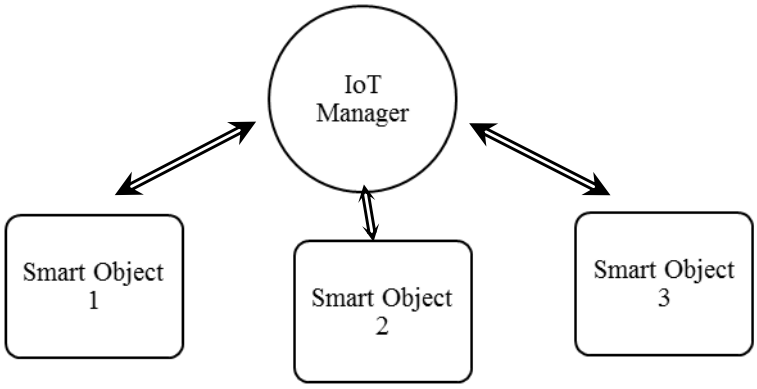

Fig.2 Architectural Design for the IoT Manager

The IoT Manager will manage the data send by various smart objects. The data will be communicated through the layers as proposed before. IoT manager might be a website or an application which acts as a background framework which will manage the sensor messages which are insignificant considering some pre specified priority levels for message transmission. Consider a Smart Fire Extinguisher in a lobby which is connected through internet to the owner, works on the sensor built in it. As the temperature in the lobby increases to a certain extent the smart object will respond to it by sending information to the owner that there is a rise in temperature in the lobby and it automatically activates the fire extinguisher. What if the data send is not accurate i.e. if there is a bug in the sensor or it is hacked by the hackers, there should be an intermediate layer where the data is checked and sent to the respected owner.

4.2 Proposed Design for the Intelligence Framework

In general, the framework can be divided into 3 layers. Fig [3] shows the layered architecture for the framework.

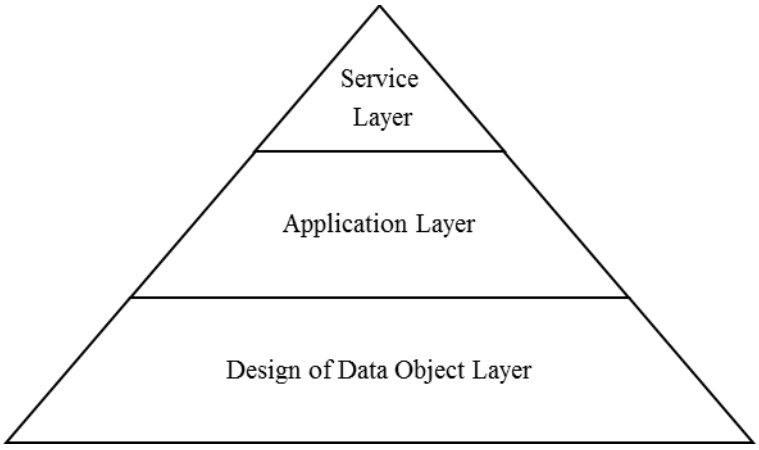

Fig 3. Distributed Intelligence Framework Architecture

As of now IoT has been significantly being increased at rapid speed. For every progress there will be a problem in any aspect regarding it. So we can overcome them with this architecture.

The first layer or the basic layer is the Design of Data Objects, where the smart objects or the IoT devices are designed in the proposed format using a data manager called IoT Manager.

The Second layer is the Application Layer where the data is managed or interpreted using the IoT Application Manager which is handled by the providers.

The Third Layer is Service Layer where the data and the corresponding information is sent through the Manager.

4.3 Advantages of the Proposed Architecture

1.Inherent cost effective due to separation of control, managing entity with the smart environment.

2.The IoT Manager will have ability to synchronize the tasks of the objects.

3.Scheduling of tasks as per priority-basis can be done at IoT Manager-Level.

4.As in ubiquitous, pervasive networks, autonomy of functionalities is not a concern in our distributed intelligence-framework but the IoT Manager acts as an intelligent negotiator between the smart objects.

4.4 Threats to Proposed Framework

The main threat to our proposed framework is the IoT manager can be compromised by false positives. The reason can be a faulty sensor or a sensor sending out signals for service even when service is not warranted. In that case the design of the application layer has to be tuned so that possibility of false positives reduces without adversely effecting the mechanism of the service layer.

V. FUTURE WORK

The distributed intelligence framework we have proposed does have fair degree of transparency, security but in future we propose to make it more robust. We did not develop a robust security framework and we have limited the framework with mechanisms to avoid false positives while sensors are activated. Its design principle is challenging in nature which has forced us not to consider such aspects in depth in this paper.

5.1 Possible Application Areas of Proposed Framework

The framework we propose is having enough potential for deployment in various commercial sectors like housing, healthcare, transport etc. where smart services are becoming indispensable day by day. In housing sector, a real estate group can plan smart home ventures with help of our proposed framework. In healthcare sector our distributed intelligence framework can reduce the load on patient maintenance system by taking off some load of the system by managing data in distributed smart environments. In military operations imagine rapid and smart communication between troops our framework may connect the distributed troops and even sensors can make it possible to communicate between air force, navy, army personnel during warfare.

VI. CONCLUSION

This paper presents a novel scheme of distributed intelligence for securing IoT which involves an IoT manager which is responsible for central functionality of providing a medium of communication for the smart objects. These smart objects may reside in different environments. Our framework reduces the risk involved while working with sensors which behave in irrational way.

REFERENCES

[1]. Hui Suo, Jiafu Wan, Caifeng Zou, Jianqi Liu, Security in the Internet of Things: A Review, 2012 International Conference on Computer Science and Electronics Engineering, 648 – 651, 978-1-4673-0689-8, INSPEC 12695467.

[2]. Vijay Sivaramany, Hassan Habibi Gharakheiliy, Arun Vishwanath_, Roksana Boreli, Olivier Mehani, Network-Level Security and Privacy Control for Smart-Home IoT Devices, 2015 Eight International Workshop on Selected Topics in Mobile and Wireless Computing, 163 – 167, INSPEC 15651329.

[3]. Sachin Babar, Antonietta Stango, Neeli Prasadn, Jaydip Sen, Ramjee Prasad, Proposed Embedded Security Framework for Internet of Things (IoT), 978-1-4577-0787-2/11/$26.00 ©2011 IEEE.

[4]. Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, Imrich Chlamtac, Internet of things: Vision, applications and research challenges, Ad Hoc Networks 10 (2012) 1497–1516.

[5]. Sachin Babar, Parikshit Mahalle, Antonietta Stango, Neeli Prasad, Ramjee Prasad, Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT), pp 420-429, ISSN 1865-0929, 978-3-642-14478-3.

[6]. Frederick J.Riggins, Samuel Fosso Wamba, Research Directions on the Adoption, Usage and Impact of

[7]. the Internet of Things through the Use of Big Data Analytics, ISSN 1531 – 1540, 15301605,

[8]. DOI10.1109/HICSS.2015.186