Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

Implementation of Security Mechanism in Iot Platform

Madhavi Shrivastava#1, Shajid Ansari#2, Somesh Deewangan#3
#Department of Computer Science
G.D.Rungta College of Engineering and Technology,
[2]R.S.R.Rungta College of Engineering and Technology
Kohka, Bhilai, Chhattisgarh, India.

***Abstract* - The security is the major key element for the acceptance of IoT as IoT is the network of smart objects, capable enough to automate the Things of Internet of Things. Here in this paper we have successfully implemented the security mechanism in the network access layer, where basically the data encryption and decryption process is implemented. The platform used for IoT is thingworx and user interface which act as client who communicates with the IoT platform is a web application. This web application fetch the data from the sensor and send the encrypted data to the thingworx and thingworx will decrypt that data and sets a status or make a decision on received data and again encrypt the data and send it back to user interface in encrypted form.**

Keywords: IoT, web application, encryption, decryption, user iterface, sensor.

INTRODUCTION

Internet of thing is basically the network of things; things can be home appliances, various machines in a factory, or other devices. Here in this system, there is no human assistance to guide or control the things in Internet of Thing. The IoT system is designed to be so intelligible that it can take the decision by its own or it can provide the alert message to the user. The IoT is basically the network of physical object, these object can be hardware or software. These objects are connected to the internet and exchange the data and values over internet. This impact of sending the values or exchanging the values are making the IoT highly automated platform and highly smart. To provide the security and privacy to the IoT platform should have proper security mechanism including cryptography operations[6].

The things in thingworx are the object to measure, To achieve the challenge of initializing 50 billion devices by the year 2020, wide range of acceptance is needed. For widely acceptance of the IoT there are various types of attributes which affect the acceptance of IoT are security, portability, and compatibility. [2] Security mechanism used in the present work, to encrypt and decrypt the data is AES. Before choosing AES a vast [3]comparatively study is done to compare the various encryption techniques like RSA, DES, AES, Diffie-Hellman, Aria, Clefia, and we conclude to go with the AES because we can control key size, block size and no. of rounds as well in AES and it is more secure and faster as compare to other security techniques.

The thingworx is used as IoT platform where we can send data over the internet by the external client or agent like postman client etc. and it will communicate with thingworx and perform the desired action to the value passed to the thingworx by the external client. Thingworx has the capabilities of allowing the external client which in terms of thingworx called as EDGE via various connection protocol like TCP/IP or HTTP or HTTPS. As we know that the HTTP is the connection protocol which allows us to initiate the communication over the internet. [7]Our architecture adopts the web services interaction by the means of http request and responses carrying the data to the thingworx platform. In our work there is necessity of HTTP protocol because our web application is the outside client and there will be need of HTTP protocol to communicate with the Thingworx Platform.

The web application is designed in javascript and with the use of jsp for designing and inserting the widgets and design the user interface. JavaScript is scripting language used for the initialization of dynamic behaviour we can call as it works on the event occur like onclick or ondoubleclick.

Rest of the paper is organized as section II Alogrithm to solve the security issues which describes the way to move forward in the present work, section III describes how thingworx works, section IV describes the working of present work and then last one is section V Conclusion which describes the result and the scope of work in future.

ALGORITHM TO SOLVE THE SECURITY ISSUES

Before describing the algorithm let us focus on motive of the work [2]. The desired result of our project is to match the future work which to make IoT board or a black box which would receive the plain text as input and gives the encrypted output which can be used for many IoT application[2]. IoT is totally based on the network of devices or machines or network of different clouds, there are various security issues occur during the data travel to and from device to server and vice versa, like eavesdropping, sniffing, spoofing, middle-man-attack and denial of service.

Present work provides a mechanism of securing the data while travelling over the network by sending encrypted data over network and receiving encrypted as a response. This mechanism prevents the data to be intelligible to the middle man or security attack like eavesdropping.

The processes of implementation of security mechanism of the present work is visualized in working section of this paper. The whole algorithm depends on the analysis of the data travelled to the thingworx and from the thingworx and to and from the user interface. In IoT the end devices or things or smart devices are connected to the global network and controlling devices are also connected to their internet it may be wifi, broadband, or other cellular data 2G or 3G or 4G. These network may or may not be followed the secure enough to restrict the network attacks, so this will be the reason for the data security becomes necessity.

This scenario will prevent data which is travelling over the internet in the architecture adopted from the previous work[1] and implement the cryptography in network access layer where data to be unintelligible to the attackers like eavesdropping, middle man attack. The encrypted data is travelling over internet which ensures the security of data travelling to or from the thingworx platform as well as to or from the user interface. This is the algorithm to be implemented to provide the security in the Thingworx IoT platform and initiate a secure transmission of the data over the connection.

THINGWORX

The thingworx is the IoT platform which provides the capabilities to bind the automation, optimization, control and monitoring into a single framework.[5] The thingworx provide us the tool to convert our imagination into a working model where the automation of works done manually, optimization of the work to make it so efficient. Controlling the IoT enabled device globally irrespective of distance, and monitoring is to keep the track record of the data for the monitoring purposes.

The thingworx has five component in its development process which starts from the initiate the thinking process of automation of anything to build the project. The five components of developing process are:

EXPERIENCE: In this component the thingworx allows us to think of any real time scenario which needs to get automated. Example in our work we think of the automation of temperature maintenance unit to get automated of our factory unit located at Bhilai, Raipur and Jagdalpur from a single place our from anywhere from the globe. We think of placing temperature sensor at temperature maintenance unit which sends the data to web application in a regular interval. This reading of temperature is then send to the thingwrox and as per the temperature received the thingworx will decide the factory unit should be in a running state or shutdown state. There is condition coded under thingworx that if temperature exceeds from 50 then sutdown the unit and if below 50 then the unit will be in a running state.

MODEL: Model is basically a collection of data. Data, what data is to be collected, The Data is the, RAW data does not have any meaningful outcome through which we can make decision to go further. In our project we get collected the raw data as temperature , name of factory unit, status of the factory unit which changes as per change in temperature of the factory unit. Model includes objects and collection of all sort of objects is known as things[5].

ANALYZE: In analyze, the name itself contains the term analysis of what kind of operation is to be applied raw data collected from the model stage into a meaningful data, what all are the properties of that data and what event will perform on that data to get the desired outcome. Like in our project we collect the raw data temperature, Name of Unit. Now the analysis is done that what will be the temperature limits to avoid the danger and we analyzed that the if temperature exceeds to the 50 then the unit will be in danger and the thingworx will automatically takes the decision to shut down the unit and it will change the status in the user interface as DANGER and SHUTDOWN and again when temperature cool down below 50 then the thingworx will restart the factory unit and sets the status in the user interface as ACCEPTABLE and RUNNING. The thingworx will receive the temperature at regular interval of time to monitor the temperature.

CONNECT: This stage is associated with the connectivity of sensor to thingworx and thingworx to user interface. The connects takes care of the communication protocol also which connects the thingworx and user interface. In our project the HTTP protocol is used as communication protocol. The connect uses various method to retrieve the data from the sensor and feed those dat in to the user interface and lastly sends that data to thingworx and repeats the process opposite for response. Connects assign the internet protocol to that thing which is collected at the model[5]. In connect stage we uses the http protocol GET, DELETE, POST, PUT method to send and retrieve data to or from toe thingworx to web application and vice versa[8].

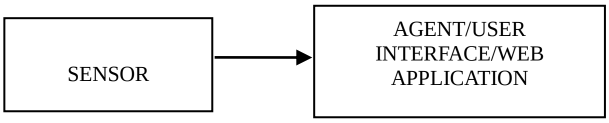
BUILD: Build is the designing of user interface or the designing of external component to communicate with the thingworx like adding of widgets like buttons, textbox etc. In our project we have designed a web application using javascript and jsp. This web application connects with thingworx by the http protocol and passes the data to the thingworx and receives the data from the thingworx as response with the help of GET, PUT, and POST method to retrieve the data, feed the data into the thingworx and send the updated data to the thingworx respectively and then show shows the status of our factory unit as running or shutdown as per the condition check in the thingworx .

WORKING

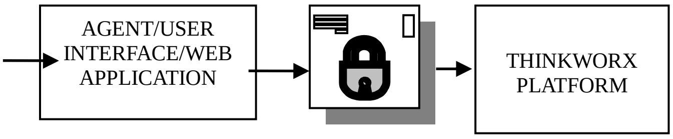
The working of our project start with the user interface which is capable of connecting and sending data to the thingworx, and thingworx receives that data perform operation accordingly and resends the data as response to the user interface.[1]In our previous work we have proposed the architectural based security mechanism, where we proposed to imposed the security mechanism to the different layer in the IoT architecture.In our present work we have implemented the AES encryption technique to encrypt and decrypt the data.

There are following scenario which shows the transmission of data and can be visualize like as follows :

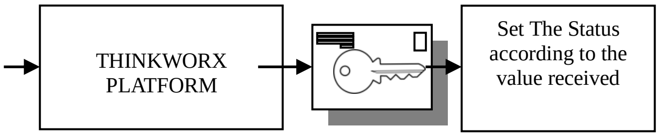
Step 1. Sensor will sense the data from the factory unit and sends it to the user interface/agent which in our project is a web application designed using java script and jsp.



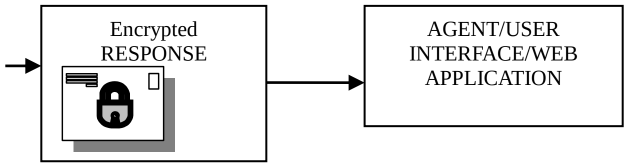
Step 2. Our WEB APPLICATION receives the data from the sensor in regular interval and encrypt that data and send this encrypted data to THINGWORX platform



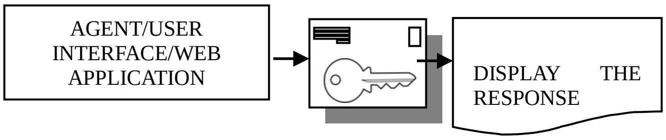
Step 3. Thingworx receives encrypted data and thingworx will decrypt that data with the key initialized once at the time of coding in thingworx after making the successful connection between thingworx and user interface.



Step 4. Thingworx sets the status according to the data and encrypt the response and send back to user interface.



Step 5. The encrypted response is received by WEB APPLICATION and then decryption mechanism is applied to it and read by UI and display the status as sent by the thingworx in a plain text.



Above is the visualization of working of our project which shows the implementation of AES encryption decryption technique in both in the client as well as in the thingworx IoT platform.

CONCLUSION

Our previous work proposed the implementation of security mechanism in IoT. In that paper the architecture of IoT is analyzed layer wise to determine the possible security that should be applied in each layer as per their role.In the present work we have worked on the network access layer where to secure the data by data encryption technique AES. From the result, it is shown that the successfully implementation of the AES encryption technique in the thingworx platform. Thingworx is considered as the blackbox, which receives the encrypted input, decrypt it and then sends the encrypted response to the user interface and we have designed a REST client a web application to simulate the working of the present work. In terms of our previous work we can say that we have successfully implemented the security mechanism in network access layer. We have adopted the future work of the research paper on security of internet of things as challenge and have completed the work. present work is the simulation of the challenge. Future scope is to work on the implementation of security mechanism in network transmission layer which is implementation of IPv6 protocol whose implementation is under research, but for our project we have adopted 8080 protocol.

REFERENCES

[1] Madhavi Shrivastava,Shajid Ansari, Somesh Deewangan,"Architectural base security mechanism in IOT" in 2017 IJERTInternational journal of engineering and researchand technology,vol.6 Issue 6, June-2017

[2] Shivaji Kulkarni, shrihari Durg, Nalini Iyer,"Internet of Things(IoT) Security", 2016, 3rd International Conference on Computing for Sustainable Global Development (INDIACom), Pages: 821 – 824

[3] K.B. Priya Iyer, R. Anusha , R. Shakthi Priya, "Comparative Study on Various Cryptographic Techniques",2014, International Journal of Computer Applications (0975 – 8887) International Conference on Communication, Computing and Information Technology (ICCCMIT-2014)

[4] K.Sekar, and M.Padmavathamma "Comparative Study of Encryption Algorithm over Big Data in Cloud Systems" in 2016 IEEE

[5] Juan R. Pimentel "An Effective and Easy to Use IoT Architecture", 2014, 10th IEEE Workshop on Factory Communication Systems (WFCS 2014), Pages: 1 – 4

[6] Premnath and Zygmunt J. Haas "Security and Privacy in the Internet-of-Things Under Time-and-Budget-Limited Adversary Model", 2015, IEEE WIRELESS COMMUNICATIONS LETTERS, VOL. 4, NO. 3,JUNE 2015 277Sriram

[7] Moreno Dissegna, Riccardo Manfrin, Marco Rotoloni, Lorenzo Vangelista, and Michele Zorzi, "RAL: a RESTful M2M communications framework for IoT", 2015, International Wireless Communications and Mobile Computing Conference (IWCMC) Pages: 1096 – 1101.

[8] Christian Prehofer, "Models at REST or Modelling RESTful Interfaces for the Internet of Things", 2015, IEEE 2nd World Forum on Internet of Things (WF-IoT), Pages: 251 – 255.

[9] Chang-le Zhong, Zhen Zhu, Ren-gen Huang Foshan University Fosha*n," Study on the IOT Architecture and Gateway Technology*" in 2015 14th International Symposium on Distributed Computing and Applications for Business Engineering and Science.

[10] Hiro Gabriel Cerqueira Ferreira, Edna Dias Canedo, Rafael Timóteo de Sousa Junior Electrical Engineering Department, University of Brasília – UnB – Campus Darcy Ribeiro – Asa Norte – Brasília – DF, Brazil, 70910-900*" IoT Architecture to Enable Intercommunication Through REST API and UPnP Using IP, ZigBee and Arduino*"in 1st International Workshop on Internet of Things Communications and Technologies.

[11] Hany F. Elyamany, and Amer H. AlKhairi *"IoT-Academia Architecture: A profound approach*" in IEEE 2015, June 1-3 2015, Takamatsu, Japan.

[12] Soumya Kanti Datta, Christian Bonnet Communication Systems Department, EURECOM Sophia Antipolis, France" *Securing DataTweet IoT Architecture Elements*" in IEEE journal