Architectural Based Security Mechanism in Internet of Things

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

***Abstract*- The Internet of things required the intercommunication between machine to machine without involvement of human commands. As there is no involvement of human being, only machines has to communicate with each other, the security concerns are the major concern in the field of IoT. To minimize the security concerns, the proposed work is to implementation of architectural based security mechanism like encryption techniques, secure protocol, various security certificates and authentication such as password protection, in the architecture of the Internet of things IoT. The different security mechanism is implemented on each layer of IoT architecture according to the property and characteristic of the layer.**

***Keywords: IoT, Security, encryption, protocol, authentication*.**

I. INTRODUCTION

The internet of Things can be defined as “the capability of machine to interact with another machine without human assistance and are embedded with artificial intelligence enough to make self decision irrespective of human involvement”. The intercommunication between the machines has no human involvement during the process, the security and the privacy of the data travelling to and from the machine is the biggest challenge for achieving the broadly acceptance of the Internet of Things technology.

The present work is in the field of application of security mechanism during data travel from IoT device to microcontroller or microcontroller to storage server it can be cloud server or REST server and vice versa during uploading and retrieving of the data to complete the desired task of the machine. At present scenario security has often a low priority for vendors of IoT device which affects the trust building factor which will impact the acceptance of emerging technology, Internet of Things.

The five layered architecture [1] of IoT and the security mechanism are implemented on each layer in the five layered architecture as per the property of each layer like implementation of encryption techniques[2]. Like AES 128 bit in the layer where the actual communication held in the architecture, likewise authentication mechanism such as password protection etc are implemented on the layer associated with the controlling in the architecture, security of transport layer can be provided by various techniques such as Transport layer security and Datagram Transport Layer Security which act as service layer in IoT architecture[2]. Here in this paper we have described the key elements to enable the intercommunication in IoT architecture like Internet Protocol (IPv6), reason behind the choosing IPv6 over IPv4 is the limited availability of address in IPv4[5]. As per latest research done in the field of IoT it is concluded that now the IoT is not only limited with the use of sensor technologies rather now it uses the information network where technology integrates both the smart device as well as the information network associate that device with the intelligent network to survive in the IoT environment. Rest of paper are organized in following manner: In section II Study of architecture is discussed where the various architectures of IoT and adopted architecture of the IoT are described. In section III Essential element to enable intercommunication in IoT architecture. In section IV Issues related to IoT is mentioned. Section VI proposed work and at last section VII is the conclusion.

II. LITRATURE REVIEW

A. *Architectural based reviews:*

There are two types of architecture mostly popular. First three layered architecture[3] and secondly five layered architecture [1].

1) Earlier there was only three layer[3] in the IoT architecture i.e; perception layer, network layer and application layer but there was a drawback in this three layer architecture that this architecture was unable to describe the characteristic and connotation of the IoT. Recent research activities going on in the field of IOT, the finer aspects of each and every process takes place during interaction of machine to other machine were become need and necessity too.
2) The adopted the architecture[1], 5 layer architecture where the 5 layers are presentation layer, application support layer, network transmission layer, network access layer and perception layers describes the finer aspects of each and every process takes place during interaction of machine to other machine and we can precisely identify which layer is performing which task.
3) Other architecture are studied from the IOT academic architecture [4]. The IOT technology is practically adopted by several countries such as USA, Japan, Egypt and UK in the field of classroom and education process. In this architecture it has nine layer namely application layer, IoT service layer, management layer, communication layer, security layer, IoT process layer, virtual entity layer. Service organisation layer and device layer. Basically IoT Academia has nine layer

architecture but in this paper's research work there is one more layer assed service layer agreement (SLA Layer).

Trends in the IoT popularity needs a proper architecture to meet the need of requirement of IoT environment.

B. Enabling Intercommunication

To enable intercommunication in the IoT architecture there are some elements[1] which are essential for the successful communication between machines and create IoT environment:

Selection of Operating System: We know that operating system provides interface between platform and connectivity which enables intercommunication between machines. Linux and Window are two popular operating system.Other than that there are some RTOS also(real Time Operating System) like free RTOS and contiki.

IoT Platform: IoT platform is the interface between the Iot device sensor and data network because there is information sharing mechanism during the machine to machine Intercommunication. IoT is nothing but a suite of component that enable developer to deploy app, remote data collection, secure connectivity, device and sensor management. IoT platform has two types data storage first cloud based and second rest server based.

Connectivity: In IoT, the connectivity is the key element because without connectivity there is no possibility of exchange of data, information flow and machine to machine intercommunication. There are various types of connectivity technology in IoT they are TCP/IP, WIFI, BLUETOOTH/BLUETOOTH SMART, LPWAN(Low Power Wide Area Network: LoRaWAN, Sigfox, LTE-M) and the latest is 6LoWPAN(IPv6 Low-power wireless Personal Area Network: Thread).

C. Issues related to IoT

There are various issues related to IoT for the world wide acceptance of IoT

With the increase in the acceptance of IoT world wide the various issues related to security and privacy are also increased. As the IoT device assembled many more component to build IoT environment the connectivity of those componemts is also an issue for IoT[5][6][7].

Major security concern in IoT are interoperability and connectivity[6]. In interoperability the exchange of data or information and that data or information is used for some process. Security concerns in interoperability are the middle man attack or eavesdropping. Connectivity Issue is related to the physical connection or connection technology used in IoT architecture to enable the communication between Network access layer and application support layer to initiate the data transmission among the IoT architecture.

In present scenario the most of the internet paradigm used host to host communication this is the major drawback for I in the IoT.

Address related issue will also be encountered in future in the field of IoT because there is prediction that by year 2020, 30 millions IoT device are to be installed worldwide which will work on IoT environment or more than 30 millions. The address conflict problem may occur in future as the exponential increase in IoT device will encountered in future. This is the major reason behind the use of IPV6 over IPV4.As IPV6 is capable of automatic randoming the suffix of IPV6 address for providing more privacy.

There are various source of vulneralities which occurs due to intentionally and unintentionally system failure and can be occur due to radio frequency interference, there are more vulneralities like database relater, loopholes in privacy related protection.

To build the trust and for acceptance of IoT technology the security and privacy challenges are to be focused. There is no human assistance in the IoT system, only machine to machine interaction is there and the data travelled to or from the machine to another machine with the use of networking mechanism but there are the problems like the unauthorised access of of the network or third party who is not authentic element to take part in communication between machines in IoT environment. This unauthenticated element can be hackers, snoofers, or by spoofing, or by eavesdropping, or by unauthorized data modification or middle man attack, or denial of service attack.

Example of network security attack: Eavesdropping, If smart device is designed to automatically switching on or off of the switches to conserve energy but if in the network security attack eavesdropping manages to recover the information in between controlling and networking layer or between smart device and and the channel through which it flows the information or data. It can be prove to be disastrous attack for any network. This kind of problems are present in th field of IoT, but the solution of this kind of problems are also in a trend in the field of research and develop[ment in the field of IoT.

III. PROPOSED WORK

After the analysis of architecture related and security related works accomplished in the field IoT, based on that we proposed the following work:

We propose the security and privacy enforced are must be architectural based. Security mechanism or technology are imposed on each layer of layer on the basis of property and characteristic of that layer.Like in perception layer, there should be filter for the different levels of professionals like developer level personnel's are eligible to access the code of IoT device and can be any time read or write permission or has a right to execute, modify the coding of IoT device.

In network access layer and network transmission layer as the data is transferred in this layer only the data passed from this layer should not at all accessible to everyone in the network, it should be intelligible only to the designated or targeted person. For this we can imposed various encryption techniques like AES, Hash Functions, MD5,SH1, DES etc. In further layer, application support layer is associated with the database or data storage management, so in this layer we should provide a authentication mechanism to access data and information from the data storage either cloud based or REST server based or multi server based.

Lastly presentation layer, security technologies should be implemented coupled with the software technologies because there should be an interface which plays an important role to decide the desired application for showing the result to the end user. Here in IoT end users are machines only because there is no human involvement in between the process in IoT. For this we can apply various protocols like TLS and DTLS to the presentation

PRESENTATION LAYER	SERVICE LAYER
APPLICATION SUPPORT	CONTROL LAYER
NETWORK TRANSMISSION	COMMUNICATION LAYER
NETWORK ACCESS LAYER	
PERCEPTION LAYER	EXECUTION LAYER

ADOPTED ARCHITECTURE ⟺ EARLIER ARCHITECTURE

Fig 1 Adopted architecture merged with earlier architecture

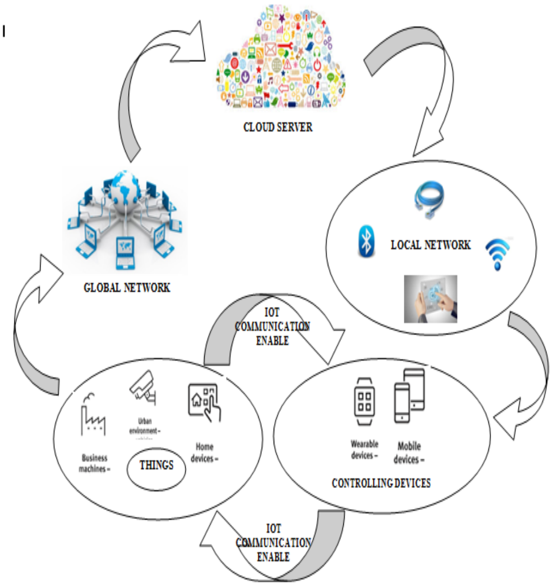

Fig 2 Intercommunication enabled IoT

The above figure is the blueprint of proposed method of enabling intercommunication in IoT evnviroment.

The proposed mechanism initiated with the controlling devices which are connected to the local network either wifi or 3G/2G/4G/Ethernet or Bluetooth because the controlling device also needs the internet connection to communicate with the things in IoT.Here in the proposed network the data or instructions are stored in the cloud server which can be accessible to both Controling Device and T of IoT. The Things like smart homes or smart surveillance cameras or business unit. The Things are also connected to the global network for accessing the data or information or instructions stored at cloud server.

We proposed the java as the most suitable language for IoT programming because of platform independency feature of java. Java does not depend upon the hardware platform as it needs only java runtime environment which includes java virtual machine to run the code which makes java portable. In C and C++, the programmer has to code for the hardware control which may differ from machine to machine or which is different for every hardware, which prove the java as superior language for IoT programming.

The adoption of AES 256 bit encryption technique for encryption and decryption of the data in network access layer before data transferred for one machine to another machine is proposed.

IPv6 is used as protocol adopted in the network layer. The reason behind use of IPv6 over IPv4 is the address space limit. One major reason behind IPv6 use is the constrained devices are used in IoT example 6LowPAN, COAP, DTLS. IPv6 also provides the in built network security.

IV. CONCLUSION

The following conclusion can be drawn on the basis of study that the security and privacy policies are prove

to be a challenging task for the IoT environment as in future there will be a widely acceptance of the IoT system are predicted. So more focus are important to provide security of IoT system. In this paper we have proposed the architectural based security in which the security and privacy are imposed based on the property of each layer in the architecture.

V. REFRENCES

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

[2] 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.

[3] Juan R. Pimentel Electrical and Computer Engineering Department Kettering University Flint, Michigan, USA"AEffective and Easy to Use IoT Architecture" in 2014 IEEE

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

[5] Hiro Gabriel Cerqueira Ferreira, Rafael Timóteo de Sousa Júnior, Flávio Elias Gomes de Deus, Edna Dias Canedo "Proposal of a Secure, Deployable and Transparent Middleware for Internet of Thing"in IEEE journal.

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

[7] Soumya Kanti Datta, Christian Bonnet Communication Systems Department, EURECOM, Biot, France" Interworking of NDN with IoT Architecture Elements: Challenges and Solutions" in 2016 IEEE 5th Global Conference on Consumer Electronic