Volume 8, No. 3, March – April 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Design of Architecture for Efficient Integration of Internet of Things and Cloud Computing

T. Venkat Narayana Rao
Professor, Computer Science and Engineering
Sreenidhi Institute of Science and Technology
Hyderabad, India

Shaik Khasim Saheb
Assistant Professor, Computer Science and Engineering,
Sreenidhi Institute of Science and Technology
Hyderabad, India

A. Janiki Ram Reddy
Student, Computer Science and Engineering
Sreenidhi Institute of Science and Technology
Hyderabad, India

***Abstract*:** With a penchant of computing everywhere, everything is going to be connected to the Internet and its data will be used for various progressive purposes. All such required things are connected over the internet and communication is established between them. All the things which are connected may generate data, sometimes data may be used immediately and in some cases data has to be processed and stored for future use. So here comes the use of cloud, the data can be stored in cloud and can be used whenever required. The integration of cloud computing and Internet of Things (IoT) can enable the resource sharing more efficiently than before. From many surveys it is found that integration of IoT and cloud computing is in its initial phase and it has not extended to all application domains due to its inadequate security architecture. So, the paper discusses a secured architecture and the issues involved. The cloud services are integrated through a novel IP/MPLS (Internet Protocol/ Multiprotocol Label Switching) core. Elliptic Curve Cryptography (ECC) is used to ensure complete protection against the security risks. However, new challenges arise when cloud is integrated with IoT. The paper proposes an idea to integrate Internet of Things and Cloud Computing in order to increase the efficiency of computing environment and meet the challenges of speed and accuracy of the services extended by the providers.

***Keywords*:** IOT, cloud computing, Elliptic Curve Cryptography, IP/MPLS core, Architecture.

I. INTRODUCTION

Internet of Things IoT, the term first coined by Kevin Ashton in 1998. Internet of Things is a technology in which devices/objects are connected to one another, thus connecting things to each other form a network of things. Once the network is constructed, connected things can establish communication with the things in the current network [1].

Internet of Things mainly works with two components. First is the nodes and the other is data aggregator. Node is any communicating device which is present in the network. All the things or resources connected may create data or use data to be processed and stored it for further computations. Whenever the data is required to be stored, data aggregator can be used. Data aggregator is any device which is capable of collecting and storing data.

The Architecture of IOT consists of five layers-as shown in figure 1 i.e. Perception layer, Network layer, Middleware layer, Application layer, Business layer [6][7].

Perception layer, Network layer, Middleware layer are considered as hardware layers because these 3 layers deals with hardware mostly. The Application layer and Business layer are considered as software layers because these 2 layers mostly deal with software related issues.

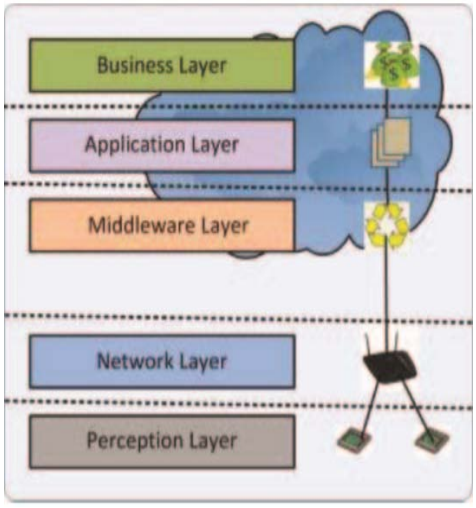

Fig 1 IOT LAYERS

Perception is the lowest layer. The purpose of Perception layer is to collect data from things that can be sensors or any other devices. This is the layer which deals with hardware part. The Network layer collects the data from perception layer and sends the collected data to the internet.

Middleware receives the data from the network/ internet. Middleware layer acts as the storage area. Stored data is also processed (if required) in this layer and necessary decisions can be taken based on the results.

Application layer collects the data from the Middleware layer and is used for presenting the data.

Business layer is all about business polices and making money. Data collected is moulded in to required form and services are provided.

Cloud computing is a technology for resource sharing. Start-ups are emerging in today's world. The major challenge for start-ups is lack of sufficient resources. So, cloud is a platform through which resource sharing can be done with efficacy. For example, if a company does not have a resource and if the required resource is too costly then the company can use the needed resource via internet with the help of cloud. Cloud provides resources to its clients on rental basis [7][8].

Figure 2 describes the services provided by cloud computing. Some of the services provided by cloud computing are:

Software as a Service (SaaS): If a user needs software which is very large in size, user can access the software from cloud via internet.

Platform as a Service (PaaS): PaaS provides a platform to build applications and services, with all the tools and resources required to do so.

I.

Infrastructure as a Service (IaaS): IaaS provides computation and storage services. Instead of purchasing expensive machines, servers, and storage devices, even for small tasks, user can outsource this task to the IaaS service provider. With storage in IaaS, not only the data is stored by the IaaS service, but also, it makes the data universally accessible over the Internet

Network as a Service (NaaS): Provides virtual network(s) to the users. Users can use the virtual network provided by the vendor.

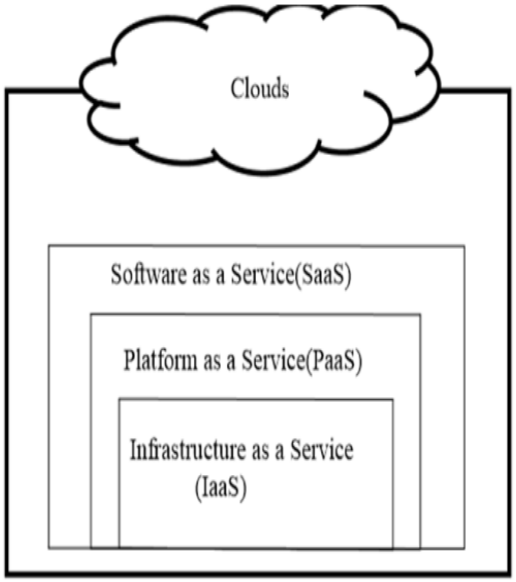

Fig.2 services of cloud computing

II. NEED FOR INTEGRATION

In utilizing IOT services, if the data is stored in data aggregator then the data can be accessed only within the network. So, accessing of data from remote places is restricted.

When internet of things gets integrated with cloud, the data gets centralized. So, the data can be stored in a cloud and can be accessed from anywhere through internet. This is one of the major requirements for integration.

IoT is generally characterized by real world and small things with limited storage, processing power, performance, security, and privacy. When we integrate IOT with cloud storage, processing power, performance and security can be enhanced. Alternatively cloud can also be implemented in real world scenarios.

Since 2011, number of connected devices has already exceeded the number of people on Earth. The connected devices have reached 9 billion and are expected to grow more rapidly and reach 24 billion by 2020. Since, number of connected devices is rapidly increasing, so there is going to be a lot of data as well. Storing that data locally is difficult hence, cloud is required.

III. INTEGRATION OF CLOUD COMPUTING AND INTERNET OF THINGS

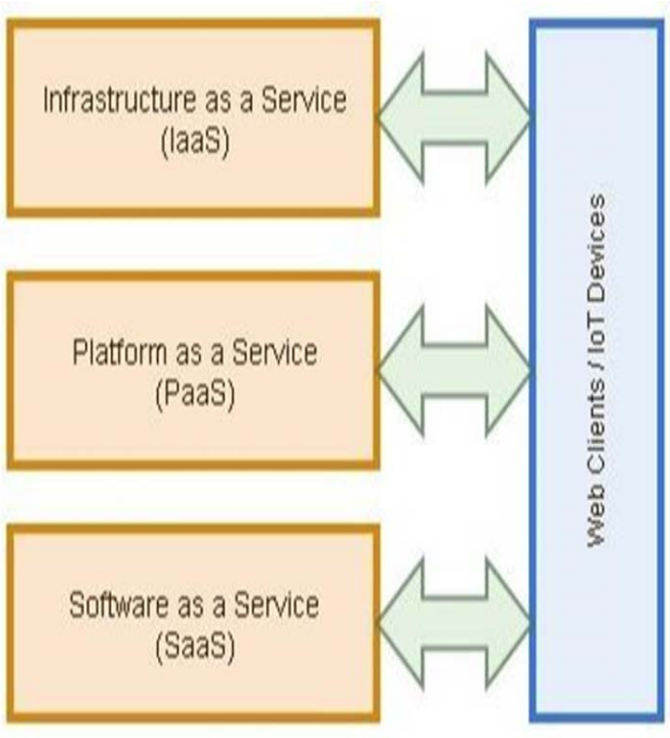

Fig 3 cloud services integrated with cloud

The integration of IOT and Cloud computing enables new services as shown in figure 3 and some other services are:

- SaaS (Sensing as a Service)
- SAaaS (Sensing and Actuation as a Service)
- SEaaS (Sensor Event as a Service)
- DBaaS (Data-Base as a Service)

- EaaS (Ethernet as a Service) / NaaS (Network as a Service)
- IPMaaS (Identity and Policy Management as a Service)
- Data as a Service (DaaS)

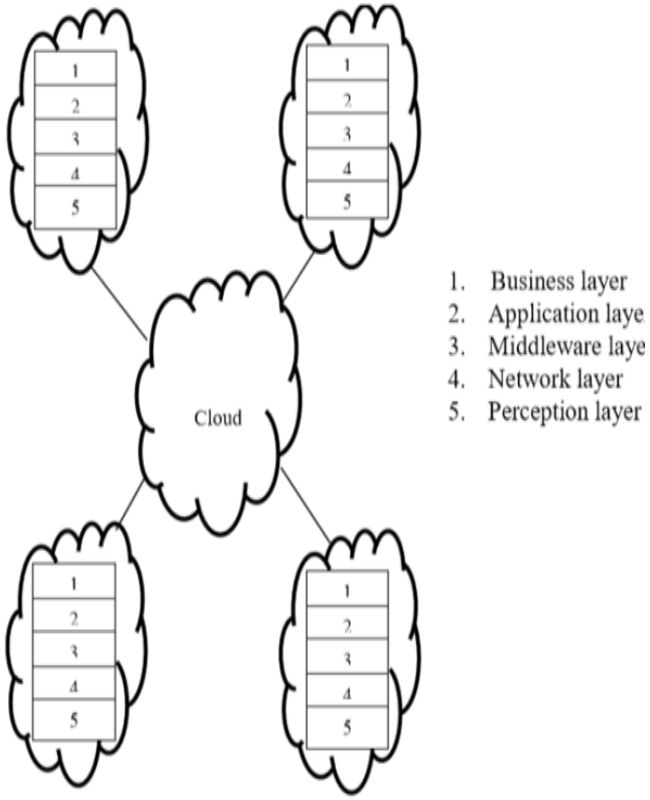

Fig 4. IoT layers integrated with Cloud

Various layers of IoT are integrated to get mutual benefits as shown in figure 4.

IV. PROPOSED ARCHITECTURE

Why secured Architecture?

This paper introduces a secured architecture which uses Elliptic curve cryptography.

Elliptic curve cryptography is a cryptographic technique which uses ellipses to encrypt and decrypt the data[8].

Though the IoT integration with cloud creates more advantages, there are equally larger threats from the attackers. As the information is not encrypted and the privacy of the information is not ensured and the senders and the receivers are not authenticated via secure connections[5].

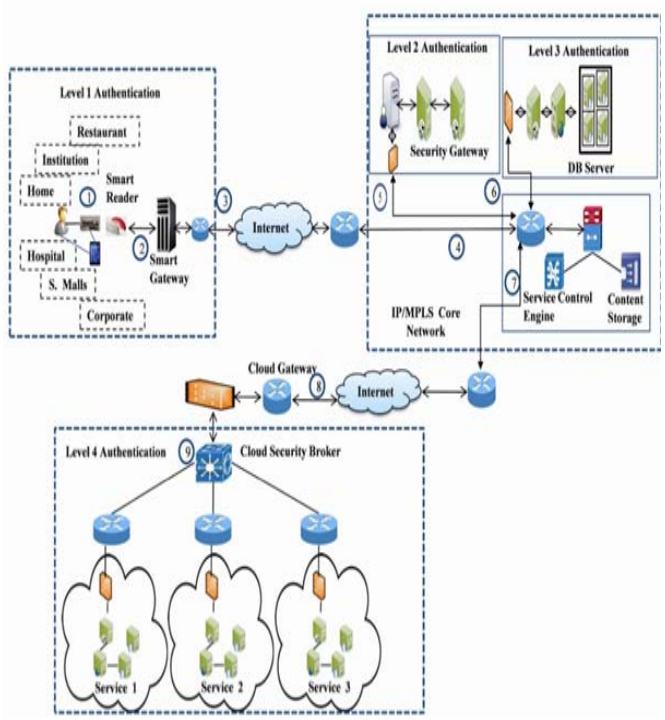

Fig **5.** proposed architecture

In this proposed architecture, user must install Intelligent Smart Card (ISC) in all the things present in the network. This ISC is capable of encrypting the MAC address of the device and will send the encrypted MAC along with the data every time.ISC also generates a UID for every user.

The proposed architecture is end to end encrypted and the cloud vendor decrypt the encrypted message and recognises the device.

Firstly, the data from the device is sent to the smart reader. The mutual authentication is done between ISC and smart reader using Elliptic curve cryptography.

Smart reader receives the data from the device and sends it to the nearest smart gateway. It collects the data, stores the data temporarily, performs pre-processing, filters the data, reconstructs the data into a more useful form and uploads only the necessary data to the cloud through IP-MPLS core.

Now data is sent from smart gateway to the nearest data centre, from their data is sent via internet to data centre where authentication of data will take place.

The cloud vendor authenticates the user using UID sent along with the data. Secondly the device from which the data is sent is authenticated by decrypting the encrypted MAC which is received along with data.

If the data received is authenticated successfully, the data will be sent to cloud gateway where one more authentication phase is initiated. Based on the above phases of authentication the data will be stored in the cloud [1][6].

V. IMPLEMENTATION

Based upon the architecture mentioned in section IV, following are the steps involved, to store the data in cloud in secured and efficient manner.

Step 1: User registeration with cloud vendor.

Step 2: Cloud vendor installs Intelligent Smart Card (ISC) and required equipment on all the required devices. Eery device to have a uniquely identified by unique id (UID).

Step 3: Data from the device/ thing is sent to the smart reader with the help of Intelligent Smart Card if the device is authenticated successfully.

Step 4: Smart Reader transmits the data to the smart gateway which is capable of taking the data from smart readers.

Step 5: Smart gateway will send the data to the nearest data centre available as shown in figure 5.

Step 6: Now data from data centre is moved to the data centre of cloud manager via internet.

Step 7: Cloud manager does two levels of authentication as explained in section IV. If the user and device is authenticated successfully data will be moved to cloud security broker.

Step 8: Cloud security broker does one more level of authentication as explained in section IV , if the data is authenticated successfully data will be stored successfully in cloud.

Retrieval of data from cloud to device is done in same manner but in reverse order.

VI. ISSUES INVOLVED WHEN CLOUD INTEGRATED WITH IOT

When a technology is integrated with another technology it is not going to be easy to handle the things. Lot of connectivity issues may arise. Some of the key issues which arise when IOT is integrated with cloud are[2]:

Energy efficiency:

It is evident that sensor networks are available everywhere and connectivity with the cloud will lead to lot of data communication, which consumes a huge quantity of power. The wastage of energy may arise when IOT is integrated with cloud. One possible solution could be is by means for sensors to generate power from the environment such as solar energy, vibration or through air. It is also advised to incorporate sleep mode option for saving energy.

Resource allocation:

When dealing with real world things, unexpected processes would demand for resources on a cloud, in such situations resource allocation will be a challenge. It would be very difficult to decide how much a particular resource may be required by an entity or a particular device/thing. Depending upon the sensor and the purpose for which sensor is being used, the type, amount, and frequency of data generation the resource allocation has to be mapped.

Device management:

In IoT, as per the user requirements anything may enter the network or leave the network at any point of time. It will be difficult for the cloud manager to maintain the status in such cases and in proposed architecture each and every device must be installed with ISC, making the process further complex.

Unnecessary Communication of data:

In some cases, the cloud has to retrieve the data from a device or any sensor and has to store that data for exploratory analysis on a daily basis (or after some specified time of period). In these cases cloud manager will automate the retrieval of data. In case of failure of device, the device will not work but cloud tries to fetch the data which is not possible. So, here lot of unnecessary communication of data creep in.

VII.APPLICATIONS

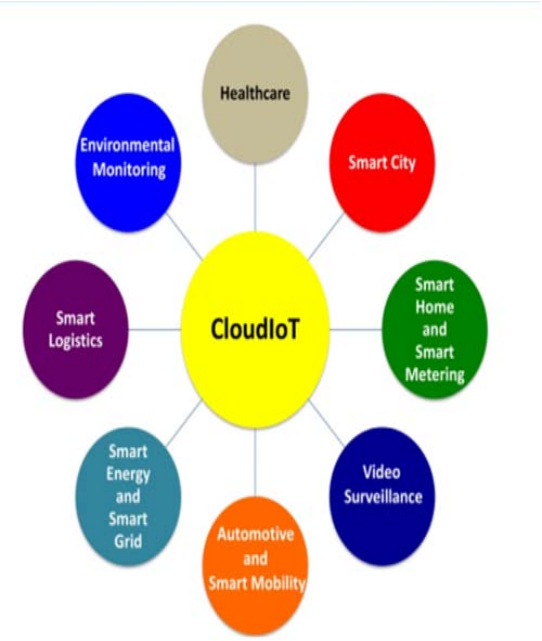

Fig 6 Applications

When the internet of things gets integrated with cloud, the data gets centralized. The centralization of data by the virtue of IOT and cloud computing integration many applications can be employed shown in figure 6 i.e. The applications include HealthCare , Smart Cities, Home Automation Systems ,Video Surveillance , Autonomous, Smart mobility , Smart Energy Smart Grid , Smart Logistic, Environmental monitoring and many more services [3][4].

VIII. CONCLUSION

The paper discusses about the integration of IoT's and cloud computing, for extending enhanced and more effective services to the user and which include efficient utilization of resources. The paper proposes an architecture which does four levels of authentication. This secured architecture of integration discusses how IoT and cloud architectures communicate with each other in an efficient manner and how security protocols are used in integration.
This paper further focus on some important issues ensuing Integration of IOT and Cloud computing. Adapting standardized solutions for those issues is a future and potential scope of this paper.

REFERENCES

[1] 2015 3rd International Conference on Future Internet of Thing and Cloud: Design and Development of Integrated, Secured and Intelligent Architecture for Internet of Things and Cloud Computing.

[2] Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th – 18th January, 2014: Cloud of Things: Integrating Internet of Things and Cloud Computing and the Issues Involved.

[3] International Journal of Hybrid Information Technology Vol.8, No.12 (2015), pp. 367-376 http://dx.doi.org/10.14257/ijhit.2015.8.12.28 : Combination of Cloud Computing and Internet of Things (IOT) in Medical Monitoring Systems

[4] International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 3, March 2016: Integration of Internet of Things (Iot) and Cloud Computing For Smart Cities

[5] International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-4, Issue-5): Integration of Cloud Computing for IoT

[6] http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

[7] http://www.webopedia.com/TERM/C/cloud_computing.html.

[8] Lobna Yehia, , Ayman Khedr, Ashraf Darwish, Hybrid Security Techniques for Internet of Things Healthcare Applications, Advances in Internet of Things, , 2015, 5, 21-25.