International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-04, Issue-07, Oct 2018

Survey on Internet of Things Architecture: A Rehash of Old Ideas and New Ideas

M.R.Sheeba, Registration Number : 17221282162017,Research Scholar ,St.Xavier's College, Affiliated to Manonmaniam Sundaranar University , Abishekapatti ,Tirunelveli- 627 012,India.

sheebasjustus@gmail.com

G.Suganthi, Associate Professor, Women's Christian College , Nagercoil-629 801, India.

dr_suganthi_wcc@yahoo.co.in

Abstract-Internet of Things(IoT) is a collection of physical objects connected to the internet. There is tremendous growth in the number of smart devices connected in the network. Thus, to accommodate the large number of devices, scalable, flexible, interoperable, energy efficient and secure network architecture is required. This paper explores the various IoT architectures and proposed a new architecture based on the security and privacy considerations. IoT devices completely depends on network connection, which demands high speed, high reliability and availability. As IoT is highly heterogeneous ,security is a big challenge. The various heterogeneous objects connected through the internet, needs a flexible layered architecture. Thus scalable, flexible, interoperable lightweight, energy aware and secure network architecture will be required in the future of IoT.

Index Terms- flexible, Internet of Things(IoT), interoperable , privacy ,security, scalable

I. INTRODUCTION

The Internet of Things(IoT) represents the interconnection of several equipments such as devices and services. The cloud is an ideal component in an IoT architecture. Cloud provides on demand network access to a shared pool of computing resources. The smart objects communicate with the help of network. They will adopt heterogeneous technologies and standards and will have unequal capabilities in terms of processing, communication and energy availability.

II .LITERATURE REVIEW

The general IoT architecture consists of Clouds and Things.

ARCHITECTURE OVERVIEW: CLOUDS AND THINGS

In [3] Cloud computing, "the cloud," involves cloud service providers (providers): those offering the service, provisioning, and managing a set of technical resources; among tenants: those consuming the cloud services through direct relationships with providers. The providers' business model is generally to leverage economies of scale by sharing resources between tenants, while tenants gain from being able to pay only for the resources they require, thus removing a costly start-up base and being able to acquire service elasticity to rapidly scale up and/or scale down resources in response to fluctuations in demand and more generally, improving access to storage and computational services. The end-user of a system may interact with a cloud provider either directly or indirectly via tenant-provided services.

Cloud service offerings are generally divided into three main categories: 1) infrastructure as a service (*IaaS*); 2) platform as a service (*PaaS*); and 3) software as a service (*SaaS*) as shown in Figure 1 . In IaaS, the cloud service provider is responsible for the management of the network, hardware, and hypervisor. PaaS service providers offer, in addition, the managed OS and application environment. SaaS service providers manage everything on behalf of the tenants, including the application. There are other categories emerging, including network as a service, brokers as a service, sensors as a service, etc.

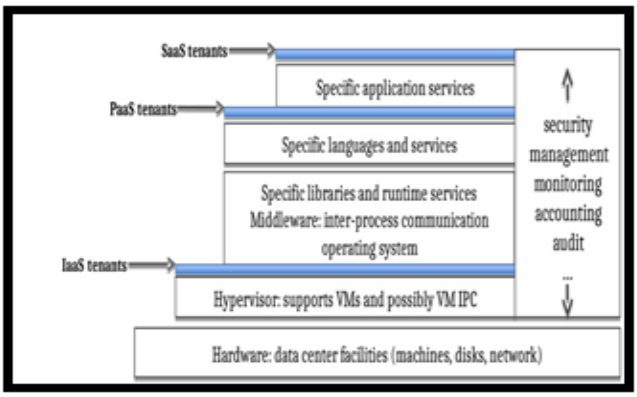

Figure 1 : Cloud Services

A. 7-Layer Architecture

In [1] Internet of Things can be viewed as a 7 layered architecture. The layers can be grouped into 4 groups: Fog

 DOI : 10.18231/2454-9150.2018.1027

Computing, Cloud Computing, Big Data, and Business Value as in Figure 2.

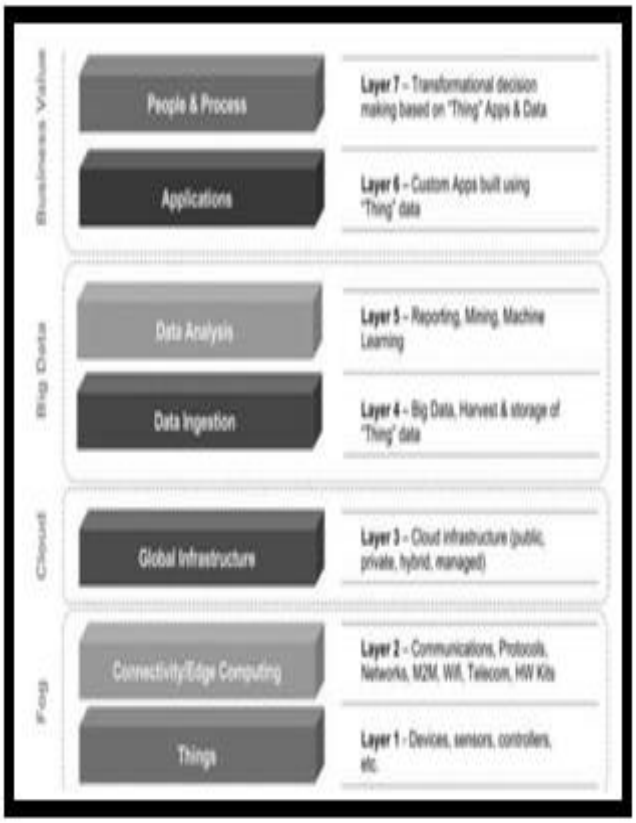

Figure 2 : 7-Layer Architecture

Fog Computing

It refers to the technologies and processes that occur outside the cloud and datacenters, and are distributed across the user base. The user base can be made up of humans, machines or objects with mobile devices, GPS technologies, sensors or other technologies that can process data at its source.

Global Infra Structure

Many IoT applications require multiple datacenters dispersed globally that can be able to scale on demand.

Big Data is a data collected in real time, near real time or batch and bought into the virtual or physical data centers.

Business Value

This layer increases revenue by optimizing business process, throughput and speed to market.

B. 6-Layer Architecture

In [2] based on the network hierarchical structure IoT architecture has six layers as in Figure 3.

Coding Layer

Coding layer is the foundation of IoT which provides identification to the objects of interest. In this layer, each object is assigned a unique ID which makes it easy to discern the objects .

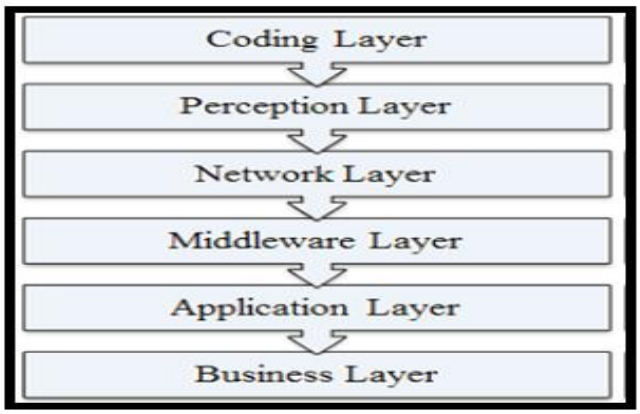

Figure 3 : 6-Layer Architecture

Perception Layer

This is the device layer of IoT which gives a physical meaning to each object. It consists of data sensors in different forms like RFID tags, IR sensors or other sensor networks which could sense the temperature, humidity, speed and location etc of the objects. This layer gathers the useful information of the objects from the sensor devices linked with them and converts the information into digital signals which is then passed onto the Network Layer for further action.

Network Layer

The purpose of this layer is receive the useful information in the form of digital signals from the Perception Layer and transmit it to the processing systems in the Middleware Layer through the transmission mediums like WiFi, Bluetooth,WiMaX, Zigbee, GSM, 3G etc with protocols like IPv4, IPv6, MQTT, DDS etc .

Middleware Layer

This layer processes the information received from the sensor devices. It includes the technologies like Cloud computing, Ubiquitous computing which ensures a direct access to the database to store all the necessary information in it. Using some Intelligent Processing Equipment, the information is processed and a fully automated action is taken based on the processed results of the information.

Application Layer

This layer realizes the applications of IoT for all kinds of industry, based on the processed data. Because applications promote the development of IoT so this layer is very helpful in the large scale development of IoT network. The IoT related applications could be smart homes, smart transportation, smart planet etc.

Business Layer

This layer manages the applications and services of IoT and is responsible for all the research related to IoT. It generates different business models for effective business strategies.

 DOI : 10.18231/2454-9150.2018.1027

C.5-Layer Architecture

In [4] the IoT can be capable of interconnecting various heterogeneous objects through the Internet, so there is a need for a flexible layered architecture. The Figure 4 is the 4-Layer Architecture performing all the functions.

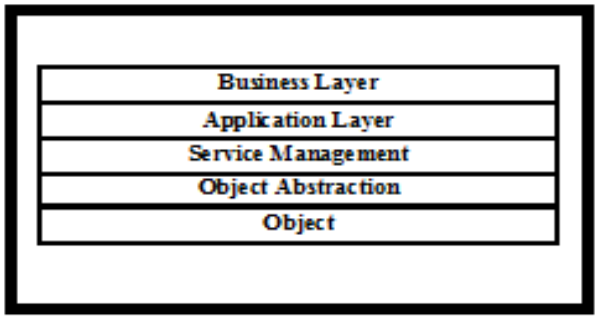

Figure 4 : 5- Layer Architecture

Objects Layer

The first layer is objects or perception layer, it represents the sensors used in IoT that collect and process information. The perception layer includes sensors and actuators. The sensors and actuators perform different functionalities such as identifying temperature, motion, location, weight, humidity, vibration, acceleration etc. This layer digitizes and transfers data to the Object Abstraction layer. The perception layer transfers data through secure channels. The perception layer initiates the big data created by IoT. This layer gives a physical meaning to each object. Object layer consists of data sensors in the form of RFID tags, IR sensors or other sensor networks which can be able to sense the temperature, speed, humidity, location and so on. Object layer gathers the useful information of objects from the sensor devices which is connected to those objects and converts the information into digital signals. Then the digital signal is passed to network layer .The Perception layer is nothing but collection of sensor, actuators which forms WSN

Object Abstraction Layer

The Object Abstraction layer transfers data to the Service Management layer produced by perception layer through secure channels. Data can be transferred through RFID, 3G, WiFi, GSM, ZigBee, Bluetooth etc. Cloud computing and data management processes are done by Object Abstraction Layer

Service Management Layer

The next layer is Service Management or Middleware layer. This layer pairs a service with its requester based on addresses and names. Service Management layer processes the data received, makes decisions and delivers the services required. The Service Management layer also allows the IoT application programmers to work with heterogeneous objects without any consideration to a specific hardware platform. Information received from the sensor devices is processed by Service Management Layer. The information is processed using some Intelligent Processing Equipment. Based on the processed results of the information fully automated action is taken.

Application Layer

This layer provides the services requested by customers. For example, it provides the temperature and air humidity measurements to customer. Application provides high quality smart services to meet customer needs. Application layer is very helpful in the large scale development of IoT network. Application related to IoT could be smart homes, smart transportation, smart planet and so on . It is a top most layer which consists of business logic, formulas and UI to user end.

Business Layer

This layer manages the overall IoT system services and activities. Business Layer builds a business model, graphs, flowcharts etc based on data received by Application Layer. The Business Layer also implements, design, monitor, analyze and develop the elements related to IoT. This layer supports decision making processes based on Big Data analysis. Business Layer also monitors and manages the underlying four layers. It also compares the output of each layer with expected output to enhance services . For effective business strategies it generates different business models.

D. 4-Layer Architecture

[10] The functionalities of the four layers in Figure 5 is given below

Real-world layer

It refers to the Real-World Objects (RWOs), i.e., the physical sensing devices that acquire the information that will be used by the IoT application.

Virtualization layer

It creates the Virtual Objects (VOs), which virtualizes the functionalities of the associated RWOs.

Aggregation layer

The different VOs can be combined in order to create Composite Virtual Objects (CVOs) capable of providing a determined service that a single VO cannot accomplish.

Application layer

It plans and understands what requested services are needed by the IoT application. It determines the strictly needed Service Level Agreement (SLA) that the platform is to execute by means of its CVO (and VO).

 DOI : 10.18231/2454-9150.2018.1027

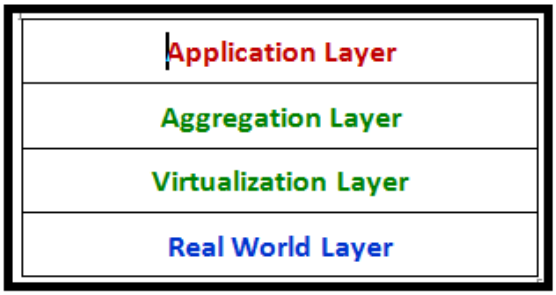

Figure 5 : 4-Layer Architecture

E. 3-Layer Architecture

The basic model is a 3-Layer Architecture consisting of the Application, Network and Perception Layers as in Figure 6.

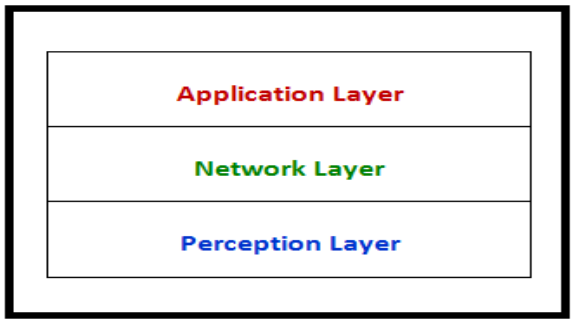

Figure 6 : 3-Layer Architecture

Application Layer

This layer is responsible for providing service requested by the customers.

Network Layer

The purpose of this layer is receive the useful information in the form of digital signals from the Perception Layer and transmit it to the Application Layer

Perception Layer

This layer gathers the useful information of the objects from the sensor devices linked with them and converts the information into digital signals which is then passed onto the Network Layer for further action.

III. PROPOSED ARCHITECTURE

The IoT paradigm comprises of a heterogeneous mix of connected devices in the internet. Our model comprises three major components, namely Perception layer ,Self organized Network layer, Self Organized Application layer .IoT will take care of the self management capabilities.

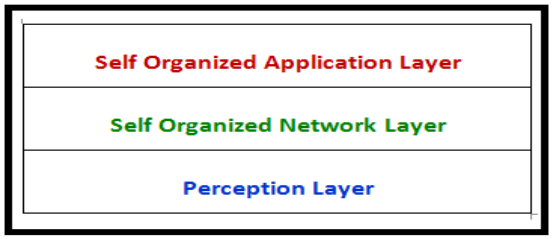

Figure 7 : Self Organized Multi tier Architecture

Perception Layer

Perception Layer forms the front end of the IoT devices. These are the so called “Things” of the system. Their main purpose is to collect data from its surrounding (sensors) or give out data to its surrounding (actuators).These have to be uniquely identifiable devices with a unique IP address so that they can be easily identifiable over a large network..These have to be active in nature which means that they should be able to collect real time data. These can either work on their own (autonomous in nature) or can be made to work by the user depending on their needs (user controlled).

Examples of Things: gas sensor, water quality sensor, moisture sensor ,RFID readers, Cameras etc.

Network Layer

Processors are the brain of the IoT system. Their main function is to process the data captured by the sensors and process them so as to extract the valuable data from the enormous amount of raw data collected.

Gateways are responsible for routing the processed data and send it to proper locations for its (data) proper utilization. In other words, we can say that gateway helps in to and fro communication of the data. It provides network connectivity to the data. Network connectivity is essential for any IoT system to communicate.

Example :LAN, WAN etc are of network gateways.

Application Layer:

Applications form a another end of an IoT system. Applications are essential for proper utilization of all the data collected. These cloud based applications which are responsible for rendering effective meaning to the data collected. Applications are controlled by users and are delivery point of particular services.

Examples : Home automation apps, Security systems, Industrial control hub etc.

Comparison of Architectures

The figure 8 shows the comparison of the various architectures that exists and the proposed one.

 DOI : 10.18231/2454-9150.2018.1027

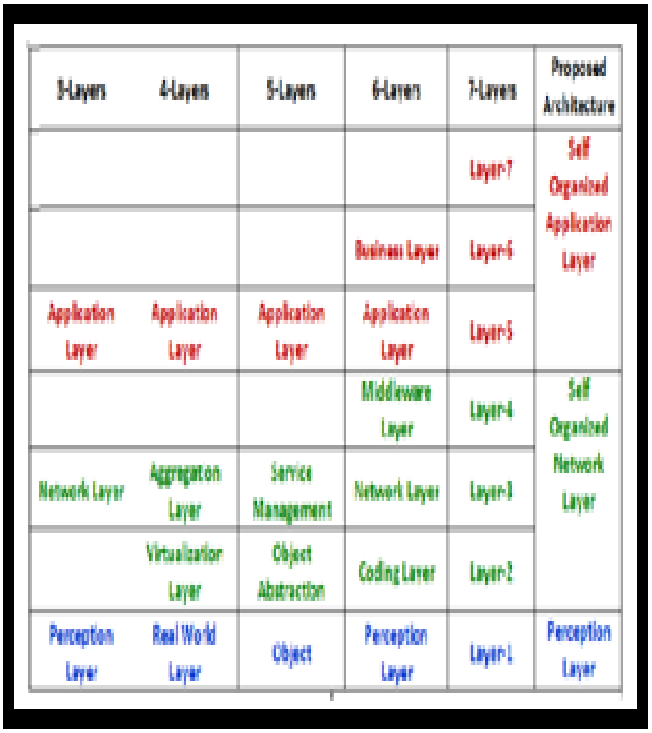

Figure 8 : Comparison of Architectures

IV.SECURITY ISSUES

A. Access

Cloud computing may increase the risk of access to confidential information. There can be increased risks due to government surveillance over data stored in the cloud, as the data may be stored in different countries.

B. Control over Data Lifecycle

Another major issue for cloud is to ensure that the customer has control over the lifecycle of their data, and in particular deletion, in the sense of how to be sure that data that should be deleted really are deleted and are not recoverable by a cloud service provider.

C. Availability and Backup

It is not easy to guarantee adequate availability and backup in the cloud. When data are hosted remotely in the cloud, backup is critical for businesses to recover in case of failure. But cloud providers enforcing resilience of their infrastructure might rely on seamless backups. This is a high security issue as these backups might be done without the customer's active informed consent and could lead to serious threats from an insider or external attacker.

D. Lack of Standardization

Cloud computing, as of today, lacks interoperability standards. There is no standardized communication between and within cloud providers and no standardized data export format which makes it difficult to leave a cloud provider. The lack of standards also makes it difficult to establish security frameworks for such heterogeneous environments and forces people for the moment to rely on common security best practice.

E. Multi-Tenancy

Multi-tenancy is an architectural feature whereby a single instance of software runs on a SaaS vendor's servers, serving multiple client organizations. The software is designed to virtually partition its data and

configuration so that each client organization works with a customized virtual application instance. This cloud service model affects security risks: in particular, in the SaaS model, customers are users of multi-tenant applications developed by CSPs, it is likely that personal data and even financial data are stored by CSP in the cloud, and it is the responsibility of the CSP to secure the data.

F. Audit

The provision of a full audit trail within the cloud, particularly in public cloud models, is still an unsolved issue.

V. PRIVACY ISSUES

[5] In the commercial, consumer context, privacy entails the protection and appropriate use of the personal information of customers, and the meeting of expectations of customers about its use. For organizations, privacy entails the application of laws, policies, standards and processes by which Personally Identifiable Information (PII) of individuals is managed. When considering privacy risks in the cloud, context is very important as privacy threats differ according to the type of cloud scenario.

A. Lack of User Control

When the SaaS environment is used, the service provider becomes responsible for storage of data, in a way in which visibility and control is limited. In cloud computing, consumers' data is processed in 'the cloud' on machines they do not own or control, and there is a threat of theft, misuse or unauthorized resale.

B. Unauthorized Secondary Usage

There is a risk that the data may be put to unauthorized uses. It is part of the standard business model of cloud computing that the service provider may gain revenue from authorized secondary uses of users' data, most commonly the targeting of advertisements.

C. Data Proliferation and Transponder Data Flow

The data's are replicated in multiple data centers. Movement of data onto the cloud and potentially across and between legal jurisdictions, including off shoring of data processing, increases risk factors and legal complexity.

D. Dynamic Provisioning

It is not clear to what extent cloud sub-contractors involved in processing can be properly identified, checked

 DOI : 10.18231/2454-9150.2018.1027

and ascertained as being trustworthy, particularly in a dynamic environment.

VI. CONCLUSION AND FUTURE WORK

With the emerging Internet of Things paradigm with a heterogeneous mix of connected devices and numerous distributed applications and services running over networks, we proposed the self organized multi-tier architecture. In addition we have discussed the various existing architectures and analyzed the various privacy and security issues in IoT. We described the research challenges in order to realize this self organized architecture that compromise our future work on this topic. A secure architecture for the cloud based IoT is to be designed with all the security and privacy features.

REFERENCES

[1] Anureet Kaur," Internet of Things (IoT):Security and privacy concerns", International Journal of Engineering Sciences & Research Technology, ISSN: 2277-9655

[2] M.U. Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi and Talha Kamal —"A Review on Internet of Things (IoT)", International Journal of Computer Applications (0975 8887) Volume 113 - No. 1, March 2015.

[3] Jatinder Singh, Thomas Pasquier, Jean Bacon, Hajoon Ko, and David Eyers, "Twenty Security Considerations for Cloud-Supported Internet of Things"IEEE Internet of Things Journal,Vol.3,No.,3,June 2016

[4] Suchitra.C, Vandana C.P, "Internet of Things and Security Issues", International Journal of Computer Science and Mobile Computing, Vol.5 Issue.1, January-2016, pg. 133-139

[5] Siani Pearson and Azzedine Benameur

"Cloud and Security Research Lab, Privacy, Security and Trust Issues Arising from Cloud Computing", 2nd IEEE International Conference on Cloud Computing Technology and Science

[6] Vandana Sharma, Ravi Tiwari, " A review paper on "IOT" & It"s Smart Applications, International Journal of Science, Engineering and Technology Research (IJSETR)", Volume 5, Issue 2, February 2016

[7]Ikuo Nakagawa, Shinji Shimojo,"IoT Agent Platform mechanism with Transparent Cloud Computing Framework for improving IoT Security", 2017 IEEE 41st Annual Computer Software and Applications Conference.

[8]Sarita Agrawal, Manik Lal Das —"Internet of Things", A Paradigm Shift of Future Internet Applications, Institute of technology", nirma university, ahmedabad – 382 481, 08-10 december, 2011.

[9] Z. Qin et al., "A Software Defined Networking Architecture for the Internet-of-Things," 2014 IEEE Network Operationsand Management Symp., May 2014, pp. 1–9.

[10] Alessandro Floris and Luingi Atzori,"Managing the Quality of Experience in the Multimedia Internet of Things" A Layered-Based Approach,Proceedings of the 2015 IEEE International Conference on Communication pp 1744-1752.

[11] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva, "Security for the Internet of Things: A Survey ofExisting Protocols and Open Research Issues", ieee communication surveys & tutorials, vol. 17, no. 3, third quarter 2015

[12] C.Medaglia and A. Serbanati, "An overview of privacy and security issues in the Internet of things," in *The Internet of Things*. New York, NY,USA: Springer-Verlag, 2010, pp. 389–395.

[13] R. Weber, "Internet of things-new security and privacy challenges,"*Comput. Law Security Rev.*, vol. 26, no. 1, pp. 23–30, Jan. 2010.

[13] Jun Zhou, Zhenfu Cao, Xiaolei Dong, and Athanasios V. Vasilakos," Security and Privacy for Cloud-Based IoT:Challenges, Countermeasures, and

Future Directions", IEEE Communications Magazine January 2017

[14] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things:A Survey," *Computer Networks*, vol. 54, no. 15, 2010, pp.2787–2805.

[15] C.-W. Tsai, C.-F. Lai, and A. V. Vasilakos, "Future Internet ofThings: Open Issues and Challenges," *Wireless Networks*,vol. 20, no. 8, 2014, pp. 2201–17.

 DOI : 10.18231/2454-9150.2018.1027