Print ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

Analysis of various issues in cloud of Things (COT)

K. Uma, N. Aafrin Parvin, A.R. Meaheesha Poorani*
Department of IT, VIT University, Vellore-632 014, India
***Corresponding author: E-Mail: meaheesha.rajesh@gmail.com**

ABSTRACT

Integration of cloud computing and Internet of Things is CoT. In 1980s, the world was moving towards convergence. The merging is accomplished when the information is shared by various devices. In many organizations, data is collected from various sources, which is stored in database and examined as reports. But in recent times, everything is an automated process. In 1999, Kevin Ashton, the father of "Internet of Things" defined that all things that are connected to the internet through sensing devices like RFID (Radio Frequency Identification) to attain intelligent identification and management. Various resources are gathered and abstracted conferring to tailored thing like semantics enables a thin as a service prototype, which is a way to build Cloud of Things. Cloud computing is a protracted from of distributed computing. It is a model to store data and for resource sharing. The Iot things are connected in active and universal network arrangement. Since IoT has the limited storage and handling capacity and issues like privacy, security, reliability and performance, it is considered by small world and small things. To understand the concept of efficiency of IoT, physical world of IoT should be mapped with virtual domain of cloud. Iot provides various opportunities to progress our daily lives, even though it has the disadvantages of leakage of security and privacy of personal information. Since data collected from IoT is overloaded to the cloud which increases security attacks and privacy issues are not controlled properly. Cloud based Internet of Things or cloud of things arose as a platform for intelligent use of applications, information in a cost effective manner. In this paper, we discussed the issues that are to be handled for using the cloud of things effectively and the solutions are described for the respective issues to make Cot error free.

KEY WORDS: COT (cloud of things), ICT (information communication technology), RFID (Radio Frequency Identification), IOT (Internet of Things), Resources, Security, Sensors, Service.

1. INTRODUCTION

In recent situation, huge number of devices such as smart phones, sensors, home appliances bonds the internet which sequentially leads to rise in global traffic issues. The quantity of devices linked to internet become more than the number of human beings from the year 2008. It has been estimated that more than 51 Billion devices having distinct IP address will be linked to Internet to enhance communication approximately in 2020. A rise in number of "Things" attain network abilities and further linked to global internet infrastructure. The machine to machine (M2M) interaction with business procedure empowers several new creative applications. Similar to cloud computing, its cyber physical systems direct its remuneration such as resource flexibility, scalability, etc. Internet technologies, like web services play a vital role in developing "Cloud of Things". Cloud computing is one of the successful paradigm to ensure cheap, and user friendly access to computing, networking resources. The drawback is that cloud solutions be deficient in interaction with the real time system. Cloud provisioning representation paves the approach for creative, value added service by interlinking the clouds with Internet of Things.

Smart Gateway Based Communication—when any information can link to internet and generate data, sometimes it is no longer essential to upload the data to the cloud. In such case, gateway device must make a decision when it is necessary to discontinue uploading the data and not to use resources of network and cloud. It is very useful in utilization of power in a efficient manner. The gateway device, linking IoT to the cloud, should perform additional functionality to do a little processing before sending it to the Internet and eventually to the cloud. The data gathered from wireless sensor networks and IoTs will be send via gateways to cloud. The expected data is then saved in the cloud and from there it is offer as a service to users. Machine to Machine (M2M) is a main area in the emerging Internet of Things where billions of devices will need to interact with each-other and exchange data in order to satisfy their purpose. There cross-layer communication and cooperation is followed. At M2M level where the machines assist with each other, a machine to business (M2B) where machines cooperate also with network-based services and business systems (business service focus). The main stimulus for device-dependent venture services is to take gain of the cloud uniqueness such as virtualization, scalability, multi-tenancy, performance, lifecycle management etc. A key motivator is the reduction of communication load with multiple designated points e.g. sending data to a single points in the network, and letting the cloud to do the load-balancing and supplementary mediation of communication. The below fig.1 is as COT architecture.

Architecture Design for COT: The architecture provides a scalable approach for IoT as it allows dynamic addition of number of "things".

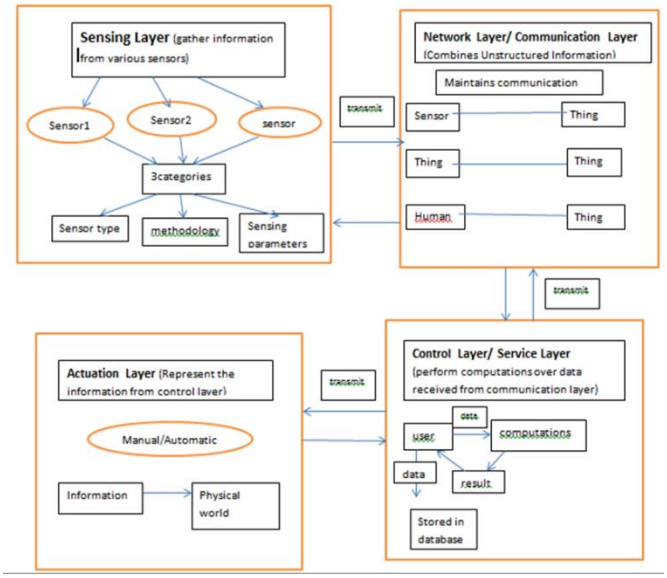

Figure.1. COT Architecture Design

Analysis of Issues in COT:

Protocol Support: Provision In homogenous objects, dissimilar protocols should be used for different things to connect to the Internet. For example, assume a sensor IoT, which will be working on different protocols like Wireless HART, ZigBee, and 6LoWPAN. In this, gateway device offers support for some protocols and it may not provide support for some other protocols. Many standards are not approved.so it depends on the sensor and the gateway that is used.

Energy Efficiency: For sensors and gateways, it as to interconnect the data to the internet and the cloud, so enormous amount of power and continuous communication with sensor nodes in needed. The key issue of cloud architecture is Energy Effectiveness, so it becomes an issue in Cloud of Things also. Data transfer between sensor networks and cloud uses more power. A wireless is composed of four components, they are sensing unit, processing unit, transceiver, and power unit. Power is a vital role when it comes to video sensing, video encoding, and decoding. Usually, as matched to decoding, video encoding is much problematic and the reason is effective compression. The encoder has to observe the redundancy in the video. For batteries it is not applicable and suitable. For huge number of sensors, an proficient usage of energy and lasting power supply is required. Since sensor networks is everywhere and it is connected with cloud will lead to increase of communication of data, in which it consumes more power.

Resource Allocation: Allocating resources is a main concern when different IoTs and things are requesting for resources in cloud. It is very difficult to identify what resources assigned to any particular IoTs. Resource allocation should be linked based on the sensor and the purpose for which sensor is used, their type, frequency of data generated, resource allocated has to be mapped.

Identity Management: When objects or things become portion on the intenert/Iot, they need to communication with one another and these objects must be recognized with unique identifier. It will be convenient to communication with object that are located in other networks. The Ipv6 address space supports universal networking. Nodes which are communicating on the internet are uniquely identified. In mobile devices, the mobile sensor nodes on vehicle and other objects need to have a link in the network if they are just entered.

IPV6 deployment: For identifying the objects that are communicating and IPv6 is used, then formal deployment of IPv6 is a problem.

Security Discovery: In Cot, cloud manager is responsible for discovering services for users in IoT. Any object can connect and disconnect to internet at any moment. Some nodes many be mobile nodes. Discovering new services, status and updating the service advertisement is becoming a problem in CoT. For tracking notes, managing the IoT node status, updating the existing nodes as well as new nodes, a constant approach is needed.

Quality of Service provisioning: When number of devices increases, the amount of data also increases. When the data is in abundance, unpredictability become the major issue, in which QoS would be an issue. Any amount of data and any type of data can be prompted. It might be the emergency data also. Based on the data and its importance, it should be sent to synchronization node. So QoS need to be supported in this case (Burak Kantarci, 2014).

Location of data storage: For data like critical, latency and jitter sensitive data, location is very important. In order to minimize the latency, it is essential to store the multimedia data close to the user. Time sensitive data like videos must also be stored in nearest physical location, so that the data is accessed in minimum time. Some storage server should be placed near to the user reducing the time for accessing big data.

Security and privacy: Ever since, cloud does not assure security and privacy, so PAN (Personal Area Network) data over IoT will be dealing with the same problem. With pervasive computing, small devices, might not be having enough security measures to protect data, becomes more susceptible. Data security is an issue on both IoT and cloud side.

Unnecessary communication of data: When cloud and IOT is integrated, huge amount of data is communicated over the network. Data is communicated with applications on cloud on one side and communicated or used by user on other side. Application satisfies the requirements of the user, as it provides service to the users. So at times, redundant data is transferred which consume much power, storage space, bandwidth, resources and processing. Sometimes, it is not necessary to synchronize device or upload the data to the cloud, when anything can be connected to internet and produce data.

Challenges in COT: Certain challenges in COT are consistency and accessibility of CoT services, diffident cryptography, data security and portability, internet needs. Observing the above listed security issues, CoT field is a big challenge. Security execution for CoT environment is elevated as a major concern because of its dispersed nature. Several inevitable challenges in security concerns are: Amount of objects or things interrelated in CoT is vast, Public Key Infrastructure (PKI) is incapable to handle the load of key management and storage. So, Public Key Cryptosystem might not be possible and not accessible for CoT agenda due to big number of interrelated devices. Even traditional cryptography algorithms with high rigorous calculations are not operative. PKI is centralized authority could not work accurately in dispenses CoT domain. Table.2, shows the issues and solution for the COT problem. In this paper, the major issues occurring in Cot are discussed, since it causes the integration to affect the Iot and cloud and the appropriate solutions for the respective issues are incorporated.

Table.2. COT issues and solutions

Name of the issue	Brief description	Solution
Protocol support	Different sensors may work on different protocols	Associating different protocols
Energy Efficiency	Requires more power and recurrent communication with sensor nodes	capable sleep mode and astute of solar system
Resource Allocation	Difficult to choose appropriate resources for IoT.	Transfer data packet from sensor node along with frequency of data.
Identity Management	Difficult to allocate unique ID for changing location of nodes.	setting IPv6 address to all the nodes
IPv6 Deployment	For recognition of object which are communicating, formal exploitation of Ipv6 is an issue.	Unique identification object is present.
Service Discovery	Difficult to discover and update service.	Unique representation of service advertisement.
Quality of Service Provisioning	Because of data abundance, Qos will be affected.	Proper transfer of data from Iot to cloud
Location of Data Storage	Multimedia data not stored in virtual storage	Allocating the time critical data
Security and Privacy	Not having enough privacy issues.	Prevent sensitive data from being damaged.
Communication of unnecessary data.	consuming a lot of power, bandwidth, storage space, and processing	Only required data should be distributed and communicated using smart communication.

2. CONCLUSION

Cloud of Things is virtual area to understand the theory of IoT applications. This is very much significant for connecting the real world with virtual world to hold huge amount of information contents as data. Trust and security are apprehension in CoT environment. Initially it required to be establishing between two parties. There are some trials to relate Identity based cryptography to cloud computing. The advantage of SCoT agenda relates wisely with the requirements of large-scale Cloud of Things. Clouds and IoT are among the most recent trends in ICT. Cloud of Things is a current trend of research topic to understand the competence of IoT. CoT provides distributed heterogeneous province to improve scalability and flexibility with reduced cost. However several challenges may need to consider realizing this concept proposed model will stimulate organizations for utilizing cloud services by reducing their expenditures. IoTs are gaining importance nowadays. It is not possible for standalone IoTs to handle large resources this paper contains a proper explanation about COT. Theories of cloud computing and IOT is discussed. Second and third section contains Security issues and challenges. With Cot, better security can be achieved and more meaningful services can be achieved. IoTs now going to become enlarge. Heterogeneous devices will generate different kind of information. Data amount and occurrence will slightly differ .This Cloud computing

services can be used to form better IoT services. Smart communication lowers the burden to large extent. Smart Network can be made component of this additional layer, to ensure the availability of provided services.

REFERENCES

Burak Kantarci, Hussein T, Mouftah, Trustworthy Sensing for Public Safety in Cloud-Centric Internet of Things, IEEE Internet of Things Journal, 1 (4), 2014.

Jiehan Zhou, Teemu Leppänen, Erkki Harjula, Chen Yu, Hai Jin, Laurence Tianruo Yang, Cloud Things, a Common Architecture for Integrating the Internet of Things with Cloud Computing, Proceedings of the 2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design, 2013.

Prashant Satpute, Omprakash Tembhurne, Review of, Cloud Centric IOT based Framework for Supply Chain Management in Precision Agriculture, International Journal of Advance Research in Computer Science and Management Studies, 2 (11), 2014, 175-180.

Sherif Abdelwahab, Bechir Hamdaoui, Mohsen Guizani, and Taieb Znati on, Cloud of Things for Sensing as a Service,Sensing Resource Discovery and Virtualization, IEEE, 2015.

Yen---Kuang Chen, Challenges and opportunities of Internet of Things, in the proceedings of 17th Asia and South Pacific Design Automation Conference, Santa Clara, CA, USA, 2012.