RESEARCH ARTICLE OPEN ACCESS

Internet Of Things: Architecture,Issues and Applications

Mahesh Kalmeshwar[1], Assoc. Professor Dr. Nandini Prasad K S[2]
[1]*Dept of ISE, Dr. Ambedkar Institute of Technology Dr. Ambedkar Institute of Technology, Dr.AIT Bangalore, India*
[2]*Dept of ISE, Dr. Ambedkar Institute of Technology Dr. Ambedkar Institute of Technology, Dr.AIT Bangalore, India*

ABSTRACT
Recent past year's research on architecture standardization of IoT (Internet of thing) is going on, not yet concluded about standardization, It is still open and debatable how to make a standard platform. Thousands of researcher's and Engineers are concentrating on IoT architecture standardization. Few open source community have already started working on IoT architecture for standardization. Yet lot of improvement is needed. Even some organization are collaborating and coming up with standardization. This will give base IoT Architecture standardization or Initial architecture which can evolve one of the solutions for making standardization. Seminar report gives full-fledged and complete modularity for IoT architecture. Depending on user application any unwanted module can be removed and addition of any number of modules to the architecture can be done easily. Mainly concentrates on modularity and scalability of the software. It helps IoT SoC(system on Chip) manufacturer to make hardware platform in-order to fit IoT applications.
***Keywords*:** rchitecture,applications,Issues,Researchers,challenges.

I. INTRODUCTION

Kevin Ashton coined the IoT(Internet Of Things) term in 1999.He had used IoT for inventory system (RFID Devices). IoT is the collection of billions of end devices, from the tiniest of ultra-efficient connected end nodes or a high-performance gateway or cloud platform. IoT can be used for any kind of application, Like: Media, Environmental monitoring etc.

Today, IoT is used as a catchphrase by many sources. This expression encompasses a galaxy of solutions somehow related to the world of intercommunicating and smart objects. These solutions show little or no interoperability capabilities as usually they are developed for specific challenges in mind, following specific requirements. Moreover, as the IoT umbrella covers totally different application fields, development cycles and technologies used vary enormously. Thus implementing vertical solutions that can be labeled as "INTERnet of Things". For instance, in some fields such as manufacturing and logistics, communication and tagging solutions are well established as they provide a clear business benefit in terms of asset tracking and supply-chain. The same solutions do not apply for other fields such as domestics, where business synergies could provide services with clear added-value benefits.

What exactly IoT mean?

IoT is nothing but Internet of Everything or IoT is One Solution for all smart devices connecting to Internet and Monitoring, controlling or it is just NMS (Network Management System) There are lot of NMS's are available in the market like SNMP(Simple Network Management Protocol), TR69, organization like Newpoints and Datapath,HP,CISCO has there proprietary product. More than 100 NMS products are available in the market. The vision of the IoT has evolved due to a convergence of multiple technologies, ranging from wireless communication to the Internet and from embedded systems to micro-electromechanically that the traditional fields of embedded systems, wireless sensor network control systems, automation including home and building and other all contribute to enabling the IoT. Despite of a lot of research efforts in this area, architecture of IoT standardization still not up to the mark. Lot Existing architecture is messy and still needed to improvements to make standardization. Thousands of researchers and Engineers are making effort to finalize one standard solution for IoT architecture. Already open source people are putting more efforts to making standard solution. We are putting efforts to get required uninformative or making standard architecture for IoT.

Section II presents the proposal for standard architecture for IoT. Explains of different layers of IoT architecture and how these layers are interface each other. Deals with Modularity and scalable of the IoT architecture. Finally explain about Architecture on board side and its various software components interactions.

Section III Explores ecosystem of the IoT architecture and Deployment consideration. The use case examples explain in detail how the user can use. He/she is at

home, he/she on trip how he/she can monitor and controls the his/her home appliances.

Section IV IoT software explains about the use of IoT and its major work in design & development. Explains about development life cycle of IoT and other team names who are going to involved. Consideration of other issues like Security for data Base & access of it.
Section V Includes currently available platform in the market, example INTEL and ARM platform.
Section VI explains some known challenges. The challenges like its feature and how to replace existing NMS.
Section VII presents the researchers –organization researching and investing heavily on IoT platform development.
Conclusion is included in Section VIII.

II. ARCHITECTURE

The IoT Platform consists of Linux kernel (OS) and device driver (IoT peripheral Hardware). The Linux kernel must be fine tune for low power, low memory footprint, robust file system, and network subsystem.

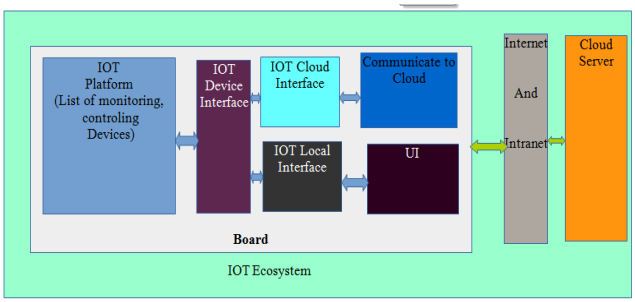

Fig. 2.1: Architecture

Iot Device Interface – it is called Hardware Abstract Layer (HAL) where all the device driver entry point given .HAL gives required abstraction to accessing for user application. Use of HAL is whenever you start porting to the other platform (Intel to ARM) only need to rewrite HAL, so the above layer middleware and application remains no change.

Middleware mainly contains controlling the device and read, write to device and security module and thin cloud interface. Middleware proved the uninformative access for user programs. Middleware can contain more module than what I mentioned. Middleware must be designed such a way that each module should be independent of each other. If two or more module dependency exist than it is required to write wrapper functions. Writing wrapper makes modularity and whenever changes required it is easily manageable to replace or addition of module.
Iot Local interface –is like on/off board display .The display is used for monitoring, Control and configuration of the IoT Devices. This local interface is with User Interface (UI).UI is GUI(Graphical User Interface).

Main software components IoT platform is, IoT Device interface IoT Cloud Interface(thin cloud client),Local Interface, GUI interface.If you want to communicate to the external word use cloud interface, Cloud interface must provide LAN,WAN and VPN configuration. Suppose we need to monitor or control from end device than we need to go through Cloud server or LAN through. It depends on application how you are accessing the IoT Basically architecture provide this feature along with security. According to the end user requirement software stack size varies.
Architecture is designed such that each module plug and play kind of role and easy to remove unwanted module. Removing unwanted module reduce the memory usage of secondary as well as main memory, and improvements in the performance.

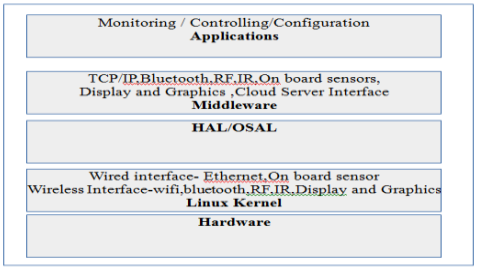

Fig2.2: Draft architecture on Board side

The base architecture on board side contains Application layer, Middleware, HAL (Hardware Abstract Layer) or OSAL (Operating system Abstract Layer), Linux Kernel, Hardware. The Linux Kernel or Linux operating system mainly contains device driver of Ethernet–wired connection, Wi-Fi, Bluetooth, RF, IR, Display and Graphics processor, secodray flash devices etc. On device side might more or less what is mentioned here. Hardware Abstract Layer (HAL) provide API(Application Programming Interface) user to access hardware and they should use this layer for accessing. This layer provides developer for fast development when changing the platform like

different board or SoC. Operating System Abstract Layer (OSAL) - Now question arises why this layer is needed when HAL is present in the architecture. This layer provides the OS independent layer example Linux, windows, iOS. Software above the OSAL layer can port easily without bothering of which OS or hardware.

Middleware – is used for interaction between application layer and down layer. This layer must be scalable and robust and reduced memory footprint.

Application Layer – Used for Developing the Applications. Application Developer has to use middleware API to communicate to the middleware stack. Looking at the above Fig.2.2 it is complete modularity, scalable and all modules are reusable components. Base version can be developed and later unknown modules can be added. This modularity makes sense while testing each component, layer wise testing and finally system test.

III. ECOSYSTEM

Ecosystem tells the scalability of the any software. The Ecosystem is gives complete insight of the IoT system.

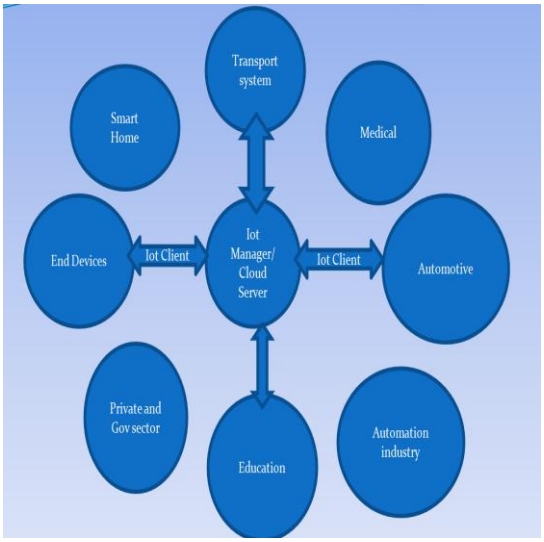

Fig3.1. IoT Ecosystem

To understand how the IoT system works,let us consider above ecosystem for only smart home and its communication to the IoT Manager or Cloud server. Smart home will have IoT board/hardware, IoT software is running on the board. The smart home has device such as washing machine, fridge, lights, window, Television, computer, Video surveillance camera. The entire smart home device connected to IoT board/hardware thorough wired or wireless.

IoT use case 1:

Suppose user is at home and want to control or monitor all his/her smart home device, which are connected to the IoT Hardware. From single IoT device, User can monitor their smart home(all the devices on fingertip).Smart phone is part of our lives. User can monitor or control their entire device which is present in their home using smart phone.

IoT Use case 2:

Suppose user at remote place in that sense user is holiday. Still they can monitor or control their home appliances. The IoT Hardware is communicating with IoT Manager or Cloud server as shown above figure 3.1. User will have access permission to the cloud. User has to login to cloud server than they can monitor or control their home appliance. If the architecture is scalable enough than it is very easy to extent to any application as motioned above figure 3.1 like Smart Home,Tarnsport system and Medical system(Monitoring patient health condition from anywhere in the world),Automotive industries, Automation Industry, Education system, Private and Government Offices, End Devices.

IV. SOFTWARE

IoT is just management software. Network management system (NMS) is one that executes network management applications (NMAs) such as hosts, gateways and terminal servers. These network elements use a management client or agent (MA) to perform the network management functions requested by the network management stations. IoT does not have Standard Software stack, Organization has their own stack. Most of the organization gets challenges to design software stack to easy and reusable component. Engineers and researchers collaborating to make IoT standard. If we look at current IoT middleware and platforms it clearly tells lot of improvement is required. Major work involves middleware and platform development to make IoT software standard across the industry. To maintain uninformative of IoT software like middleware, platforms and cloud interface is nothing but redefining the architecture. To build IoT, required collaboration from architects, developers such as application, middleware and platform and hardware developers. Finally all the data from device will send to Cloud server/IoT Manager. Cloud will have database for storing or analytics on data provided by IoT Device. Cloud has to provide data available round the clock and need to see how to handle the database failure and its security.

V. CHALLENGES

The recent data hack at SONY is a prime example of the kinds of damage that a company can sustain when its information systems get breached. It doesn't take much to extrapolate such an attack to a company with Internet connected devices. There have been many scenarios studied that project significant

harm and potential loss of life from such hacks. The technical challenge is to secure Internet-connected devices from cyber network attacks, as well as local physical attacks. Similar challenge exists for the cloud-hosted services, such as data analytics. The business challenge is to ensure that security is taken seriously and designed in by the equipment vendors, not looked at as a cost center and patched on after the fact. The challenge is substantial, and may require new industry practices be developed and adopted. Controls engineers today frequently 'air-gap' systems to completely isolate from the external threats. Before connecting operations systems to the IT system guarantees on security and stability are needed. Platforms have to 'learn' how to interact with a multitude of services and data/command streams often associated with different domains. Creates new requirements for security, privacy, identity management, and access control. In many cases such requirements have significant implications at the silicon level demanding novel architectural solutions in SoCs designed to drive IoT.

VI. RESEARCHERS

Many technical communities are vigorously pursuing research topics that contribute to the Internet of Things (IoT). Today, as sensing, actuation, communication, and control become ever more sophisticated and ubiquitous, there is significant overlap in these communities, sometimes from slightly different perspectives. More cooperation between communities is encouraged. To provide a basis for discussing open research problems in IoT, a vision for how IoT could change the world in the distant future. A fundamental problem that is pervasive in the Internet today that must be solved is dealing with security attacks. Security attacks are problematic for the IoT because of the minimal capacity “things” (devices) is used, the physical accessibility to sensors, actuators and objects, and the openness of the systems, including the fact that most devices will communicate wirelessly. The security problem is further exacerbated because transient and permanent random failures are commonplace and failures are vulnerabilities that can be exploited by attackers. It is likely that significant hardware support will be necessary for providing encryption, authentication, attestation, and tamper proof keys. Even if new devices are security-aware, dealing with legacy devices will prove difficult.

VII. CONCLUSION

Everyone has their own IoT software stack. It is difficult to make standard once the product shifted to market place, because everyone will have proprietary protocol in their IoT software. Using ropriety protocol it is difficult to communicate in the IoT Ecosystem. It makes sense to standardize when the technology is new. To make IoT standardization across the industries. To standardize we need to provide modularity, scalability, reusability and interoperability of software. Interoperability make all device can communicate within the IoT ecosystem.

REFERENCES

[1] Stefan Nastic, Sanjin Sehic, Duc-Hung Le, Hong-Linh Truong,SchahramDustdar ” Provisioning Software-defined IoT Cloud Systems”, 2014 Barcelona, International Conference on Future Internet of Things and Cloud

[2] Maurizio Giacobbe, Antonio Celesti, Maria Fazio, Massimo Villari and Antonio Puliafito, ”A Sustainable Energy-Aware Resource Management Strategy for IoT Cloud Federation” ,2015 Messina, Italy, IEEE International Symposium on

[3] Maryam Davoudpour , Alireza Sadeghian , Hossein Rahnama , “Synthesizing Social Context for Making Internet of Things Environments More Immersive” ,2015 Montreal, QC, 6th International Conference

[4] http://www.electronicsweekly.com/ - IoT Conference - 2014 and 2015

[5] Organization ARM and INTEL.

[6] https://www.arm.com/

[7] http://www.intel.in/content/www/in/en/internet-of-things/overview.html

[8] http://openiotivity.com/