A study on development issues over IOT platforms, protocols and operating system

M. Sruthi
SCOPE
VIT University
Vellore, India
Sruthi.m0611@gmail.com

R.RAJKUMAR
SCOPE
VIT University
Vellore, India
vitrajkumar@gmail.com

Abstract— **Internet of things(IOT) is a network of things given access to the internet. The application of IOT is in various field as agriculture, healthcare, banking, logistics etc. The user can have a customized IOT system according to their constrained for the system. There are various application protocols such as MQTT,COAP,XMPP,REST with their own advantage and that can be used as application protocol for the system that suits their constrains of the system. The data that are sensed by the system is stored in a cloud platform. There are various platforms that provides services such as data analytics, notification, generating the action and take control over system. To implement the IOT system there are various operating system such as contiki os, tiny os, RTos, google BRILLO. Each has characteristics of such as running on low memory space, supporting platform, and connectivity to some cloud providers. This paper aims to provide a survey of platforms, protocols, operating system on IOT. Followed by the challenges in IOT deployment, and various applications of the IOT.**

***Keywords* — IOT platforms, protocols, Operating system**

I. INTRODUCTION

Internet of things is a network of object that is given access to the internet. The object is physical object that can be a vehicle parking field, any machines, even light can be controlled. By giving things access to the internet, the environment is monitored, gets notified and taken action to control the environment. The application of the IOT is in many field including home automation, logistics and transportation, agriculture, healthcare, banking, energy management system, smart city, smart parking system, smart traffic control system. The IOT was first coined by the Kevin Ashton in 1999 and establish a laboratory in MIT for connecting the objects through RFID. In 2005 the IOT is mentioned by ITU. In 2010 Google developed a car that is fully connected to the internet and access the map and accordingly it is self-automated. This a important project in the field of IOT.In 2010 the Bluetooth low energy protocol was developed that enables the objects to be connected with low power consumption. In 2011 IPV6 is launched that support the large number of objects to be connected to internet is 3.4×10^{38}. The technologies that enable the connectivity and the communication over the network of objects are Bluetooth, zigbee, Wi-Fi, 4G LTE. Each of this technology differs in their range of transmission, power consumption, and speed. Based on the application the technology that are used to provide connectivity, and power constrain the technology chosen may vary.

Technologies	Range	Power
Wi-Fi	50-100 meters	high
Bluetooth	10 meters	Low
zigbee	10-100 meters	Very low

Table 1 list of technologies provide connectivity between objects

II. STATE OF ART

A. IOT PLATFORMS

Xively: this platform provides a platform as a service for building an IOT APP. The things are connected to the xively platform by protocols such as REST, HTTP, and MQTT [1]. It ensures security by having a secure server with device and user authentication by their API key which is assigned to them while registering as a new user [2]. It provides a SDK for Arduino, android, python, java, PHP, RUBY. It provide three services such as directory as a service by provide storage space to store data, data as a service in which we can make a data analysis and business as a service for a connected business and product. The xively also provides a unique API for the data visualization that is being stored in cloud [3]. Xively has also has been won many awards as an IOT technology innovator in 2015 and also many awards in year 2013.[11]

Axeda: is a platform that provide the storage space to store the data of the things, analyses the data and get notified. The axeda supports the MQTT protocol for the communication with the axeda cloud. It has a middleware called IOT connectivity to easy integrate and connect the things to cloud. It also has SDK to build the APP and to access the data through web app. The axeda cloud providers has also obtained an ISO 27001:2013 certificate for ensuring security in axeda cloud. The axeda cloud also works with protocol such as SOAP, REST [3].The grovey scripting engine is there to support the application development. The axeda provide connectivity between things and cloud by axeda wireless protocol [3], [4].

Thingworx: it is an IOT APP development platform that allow the user to developers to develop them own application. The data communication and device control in turn is through REST protocol, MQTT [3], [4]. There is a codeless mashup builder that allows the user to create their own APP without any need to code. It also allows the social networks to collaborate with users such as twitter, LinkedIn, google + [4]. SQUEAL is a search engine that is used to data analysis, search and query the data repository stored in cloud [2].

Thingsquare: is a platform each connected object runs a wireless thingsquare mist os. It ensures the secure connectivity by the AES protocol. Thingsquare IDE is a web based IDE to build online mist APP [3]. This thingsquare mist is a gateway through which the things are connected in the form of mesh. The visibility of the device is within the mesh [4].

Platform	**Integration To cloud**	**SUPPORTIN G PROTOCOL S**	**SECURITY**	**TYPE OF ANALYTIC S**
XIVELY	Rest API	HTTP/HTTPS MQTT	SSL/TSL	Data analytics, business analytics
AXEDA	Axeda wireless protocol	MQTT,SOAP, REST	ISO 27001:2013 For ensuring security	Data analytics
THING WORX	Rest API	MQTT,XMPP, COAP,DDS,	LDAP authenticatio n	SQUEAL analytics
THING SQUAR E	Thingsquare mist	IPV6,RPL,6lo wPAN	AES protocol SSL	Data analytics

Table 2 list of platform that provide PaaS as a service

B. IOT PROTOCOLS

MQTT: Message QueuingTtelemetry Transport

The MQTT is messaging protocol that is applied in the application layer. It works like the things will be publishing the messages in the broker. From the broker the user can subscribe the data of the things published in the broker. The MQTT runs on the top of TCP/IP. The security can be applied by authentication. The MQTT is not applicable to the system that has passive sensors, as the sensors/device may be in sleep state during the communication [6]. The Message from the brokers can be subscribed the interested group [6],[7].The MQTT can be used in many application such as healthcare, smart metering and the Facebook uses the MQTT protocol [6],[7],[8].

COAP: Constrained Application Protocol

The COAP is a web based protocol like REST, which runs on the top of the HTTP [6]. The COAP runs on the top of UDP. The COAP ensures the security by the messaging sublayer that detects the duplicate packets. The COAP is a protocol that is designed to operate in low power and in noisy links [7]. The COAP has a session based connection. It uses the HTTP GET, PUT and POST, DELETE [6], [7], [8], [9]. The messages send are acknowledged by sending a confirmable message type.

XMPP: Extensible Messaging and Presence Protocol

The XMPP is a messaging protocol for chatting that allows to implement the security on it [6]. It is a decentralized protocol that runs on all internet platform.it ensures the secure communication. The XML stanza is used to provide connection between the client and the server [7]. The XMMPP supports publish/subscribe architecture and has a build in TLS/SSL. It also support the request response approach. It is extensible. It runs over the TCP/IP. It supports small message and low latency message exchange [9].

AMQP: Advance Message Queuing Protocol

It is an open standard messaging application protocol. It runs on the TCP layer. It is suitable to use in an environment where the control is needed. This is a more appropriate IOT protocol [6]. The AMQP requires a more reliable communication so it supports TCP. The publish/subscribe is also supported by the AMQP [7]. The AMQP can send more message than the XML. The AMQP is used by JP Morgan Company that send 1 million messages per day [9]. The AMQP provides reliability by storing and forwarding method [8].

PROT OCOLS	**TYPE**	**SECURITY**	**RUNS ON**
MQTT	Publish/subscribe	Explicit implementation	TCP/IP
COAP	REST based	Inbuilt to detect duplicate packet	UDP
XMPP	messaging	Inbuilt security by SSL/TSL	TCP/IP
AMQP	Open standard, publish/subscribe	Reliable by store and forward	TCP/IP

Table 4 list of protocols in IOT

C. IOT Operating system

Contiki

The contiki is an OS that is design to run in low memory space. It is portable. The contiki supports both event driven and multi-threading. The contiki OS runs on the linux platform. It supports various microcontrollers such as Atmel ARM, Atmel AVR, STM32w TI MSP430, TI CC2430, TI CC2538, TI CC2630, TI CC2650, LPC2103, Freescale MC1322 4, Microchip dsPIC, Microchip PIC32.It also supports various protocols such as 6lowPAN, IPV6, COAP. The latest version of contiki is 1.6. It provides security by implementing contikisec, TLS/DTLS. It contains a rime stack that contains a list of light weight protocol. [12], [13].

Tiny os:

It is mainly designed for the implementation of WSN. It is made secure by implementing tinysec. It contains three IDE for the SDK app development such as TINYDT, TinyOS Eclipse Plugin ―YETI 2‖, TinyOS Eclipse Editor Plugin. The protocol supported by tiny OS include Broadcast based Routing, Probabilistic Routing, Multi-Path Routing, Geographical Routing, Reliability based Routing, and TDMA based Routing, Directed Diffusion [12]. THE

PROTOCOL SUPPORTED BY TINY OS TCP, UDP, ICMPv6 and IPv6, 6LoWPAN, RPL and CoAP. Hydrogen routing protocol is used for reliable communication [13].

RIOT

It is based on microkernel architecture. It is able to run on 8 bit, 16 bit and 32 bit processor. It is partly portable. The protocols 6LoWPAN and RPL are provided with support to TCP, UDP and IPv6. The SDK's support programming in C,C++.

os	**Memory space**	**Multithreading**	**Languages support**	**Portable**
Contiki	<2 KB	yes	C	Highly portable
Tiny OS	< 1 KB	partial	C	Partly
RIOT OS	1.5 KB	yes	C,C++	Partly

Table 4 list of operating system in IOT

III. Key issues in IOT development

A. Security

The security is the main key issues in the internet of things when the system becomes vulnerable to attacks the effects is more drastic such that the control over the environment or monitoring goes wrong and the effect range depend up on the system scenario. For example there is difference between the light automated systems and healthcare system when become vulnerable to attacks. So the security must applied in system both in hardware and during the data transmission.

B. Interoperability/ Standardization

Interoperability is the key feature In the IOT system. Many technologies, protocols there should be interoperability to provide the services that may vary from each system and to serve the customized need of the user. The IOT doesn't have a standard that is agreed up on all. This standardization has a major role in the brand of the product. Along with the existing standards in future open standards are needed for new business model.

C. Privacy

The IOT system should ensure that the individual user privacy is maintained. Both the system and the data transmission should enable the privacy.it should gain the confidence from the user that both the connected devices, services provided by the system, and the data analytics services provided by the iot platform that their personal information are not know to any other third party.

IV DISCUSSION AND CONCLUSION

IOT is a paradigm that involves concepts such as sensor networks, cloud computing. There are various cloud platform. Among which xively is the top among the cloud service providers. The main part of the cloud computing in IOT is to provide storage. But most of the cloud providers provide platform as a service to create the IOT app. Then on moving to security part the cloud providers such as axeda concentrate more on the security and won the ISO certificate for ensuring security. But each cloud providers have their own architecture for security. The users should analysis the security concern in the cloud providers before they choose their cloud platform. This is an important decision has to been taken by the user in choosing their cloud provider as this many chance of data in security and privacy issues.

There are many application level protocols the protocols used to implement depend up on the architecture of the system. If the system is based on a master slave then the MQTT protocol can be used in the application layer protocol. But security is to be implemented by any security protocol for the MQTT protocol. But whereas the security is considered then COAP or XMPP is preferred that has some inbuilt security features. When the speed is considered as a main key then the AMQP protocol is preferred. Then the choice of protocol in application layer also depends up on the underlying transport layer. The MQTT, XMPP, AMQP runs on TCP/IP whereas the COAP runs on the UDP. The COAP is a session based and also ensures the packet delivery. The XMPP has an inbuilt SSL/TSL security feature.

The OS that is chosen also depends up on many factor such as multithreading, portability of OS, protocols supported and the memory space taken to run. When the memory is consider then the RIOT runs on low memory that requires less than i.5 kb. When the portability is considered the contiki OS is considered. The contiki also support many protocols such as COAP, IPV6, and MQTT.

But on the hole the RIOT OS is preferred that runs on low memory space, allows both multithreading, and partly portable and supports protocols 6LoWPAN, RPL are provided with support to TCP, UDP and IPv6.

Thus in this paper various cloud platforms, protocols, operating system on IOT is discussed. The detailed pros and cons of each platforms, protocols, and operating system are said and comparison table is also given. Various key issues in developing an IOT system is also discussed. . But the choice of protocol, platforms, OS depends up on the system scenario. This paper gives an overall view of some existing platforms, protocols, operating system and prefer a set of protocol, platforms, OS in terms of security, services, memory

REFERENCE

[1] Diaz, M., Martín, C., & Rubio, B. (2016). State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. Journal of Network and Computer Applications.

[2] Balamuralidhara, P., Misra, P., & Pal, A. (2013). Software platforms for internet of things and M2M. *Journal of the Indian Institute of Science*, *93*(3), 487-498.

[3] Köhler, M., Wörner, D., & Wortmann, F. (2014). Platforms for the internet of things–an analysis of existing solutions. In *5th Bosch Conference on Systems and Software Engineering (BoCSE)*.

[4] Mineraud, J., Mazhelis, O., Su, X., & Tarkoma, S. (2015). Contemporary Internet of Things platforms. *arXiv preprint arXiv:1501.07438*.

[5] Masek, P., Hosek, J., Zeman, K., Stusek, M., Kovac, D., Cika, P., ... & Kröpfl, F. Implementation of True IoT Vision: Survey on Enabling Protocols and Hands-on Experience.

[6] Al-Fuqaha, A., Khreishah, A., Guizani, M., Rayes, A., & Mohammadi, M. (2015). Toward better horizontal integration among IoT services.*Communications Magazine, IEEE*, *53*(9), 72-79.

[7] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *Communications Surveys & Tutorials, IEEE*, *17*(4), 2347-2376.

[8] Colitti, W., Steenhaut, K., De Caro, N., Buta, B., & Dobrota, V. (2011, October). Evaluation of constrained application protocol for wireless sensor networks. In *Local & Metropolitan Area Networks (LANMAN), 2011 18th IEEE Workshop on* (pp. 1-6). IEEE.

[9] Karagiannis, V., Chatzimisios, P., Vazquez-Gallego, F., & Alonso-Zarate, J. (2015). A survey on application layer protocols for the internet of things.*Transaction on IoT and Cloud Computing*, *3*(1), 11-17.

[10] Asensio, Á., Marco, Á., Blasco, R., & Casas, R. (2014). Protocol and architecture to bring things into internet of things. *International Journal of Distributed Sensor Networks*, *2014*.

[11] Heo, Y. J., Oh, S. M., Chin, W. S., & Jang, J. W. (2015, August). A Lightweight Platform Implementation for Internet of Things. In *Future Internet of Things and Cloud (FiCloud), 2015 3rd International Conference on* (pp. 526-531). IEEE.

[12] Borgohain, T., Kumar, U., & Sanyal, S. (2015). Survey of Operating Systems for the IoT Environment. *arXiv preprint arXiv:1504.02517*.

[13] Gaur, P., & Tahiliani, M. P. (2015, May). Operating Systems for IoT Devices: A Critical Survey. In *Region 10 Symposium (TENSYMP), 2015 IEEE* (pp. 33-36). IEEE.

[14] Glaropoulos, I., Vukadinovic, V., & Mangold, S. (2014, August). Contiki80211: An IEEE 802.11 Radio Link Layer for the Contiki OS. In *High Performance Computing and Communications, 2014 IEEE 6th Intl Symp on Cyberspace Safety and Security, 2014 IEEE 11th Intl Conf on Embedded Software and Syst (HPCC, CSS, ICESS), 2014 IEEE Intl Conf on* (pp. 621-624). IEEE.

[15] Bjelica, M. Z., Golan, G., Radovanovic, S., Papp, I., & Velikic, G. (2014, April). Adaptive device cloud for Internet of Things applications. In *Consumer Electronics-China, 2014 IEEE International Conference on* (pp. 1-3). IEEE.

[16] Bjelica, M. Z., Ignjatov, N., Papp, I., & Teslic, N. (2014, May). Device cloud platform with script based agents for "anywhere access" applications development. In *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014 37th International Convention on* (pp. 1061-1065). IEEE.

[17] Mazhelis, O., & Tyrvainen, P. (2014, March). A framework for evaluating Internet-of-Things platforms: Application provider viewpoint. In *Internet of Things (WF-IoT), 2014 IEEE World Forum on* (pp. 147-152). IEEE.