Analysis of the IoT Framework for Sensor Data Connectivity

Anil Yadav
Amity University, Uttar Pradesh

Gaurav Pandey
JSS Academy of Technical Education, Uttar Pradesh

Sujata Pandey
Amity University, Uttar Pradesh

Vinay Kumar Pant
iNurture, Teerthanker Mahaveer University, Uttar Pradesh
pantvinay02@gmail.com

2022 International Mobile and Embedded Technology Conference (MECON) | 978-1-6654-2020-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/MECON53876.2022.9752025

***Abstract*— In this paper, major building blocks of IOTized ecosystem is discussed. The ecosystem is further divided into sub-ecosystem as IOT apps ranging from smart home, smart healthcare, smart transportation, smart retailer, agriculture and smart education system. This includes diversely connected devices which continuously communicate with each other and perform status update on localized and remote system. Further use cases have been developed and their framework have been proposed and compared to cater the requirements of the IOT ecosystem.**

Keywords—IOT, App, Security, Privacy, Sensor, Wireless

I. Introduction

Digital India initiative have opened a Pandora's box of opportunities to every entity on this earth to be part of this ambitious project to bridge the gap of digital divide within the country. One can be part of this ecosystem by building the infrastructure of digital India and someone else can be part of as a consumer of this infrastructure. However, big challenges are in pipeline for creation of such a complicated and heterogeneous ecosystem. Yes, this is Internet of Things (IOT) [1-10] which has brought a paradigm shift in the thought process of the societies in various segments; be it agriculture, education, transportation or health-care.

The most important part of IOT framework are wireless sensors. Numerous challenges have emerged due to rapid increase of wireless sensor devices. These sensor devices have dedicated roles assigned as part of the big IOT ecosystem to provide technological solutions to end user. Management of such diversified network of smart things need careful and systematic distinction of use case scenarios, design and implementation of services provided to every single object. Each ecosystem must ensure various pro-user facilities. These facilities require a framework which incorporates the heterogeneous infrastructure and provide a transparent service to ensure seamless connectivity, privacy, security of data.

Addressing the security issues over existing internet protocols for IOT apps are still evolving [4]. Authors in [5] have defined the specification for IPV6 protocols communication over IEEE 802.15.4.
This paper visualizes and portrays the major building blocks of an "IOTized" ecosystem. This ecosystem consists of basic requirement and a super-smart living experience through smart things. The big ecosystem constitutes further smaller ecosystems in this article named as IOT Apps. These sub-ecosystems range from Smart Home, Smart Health-care, Smart Transportation, Smart Retailer, Agriculture and Smart Education system [11-18].
Every sub-ecosystem of IOT Apps includes diversified connected devices that seamlessly communicate to each other. Additionally, devices can have sensors to capture data for respective roles. Devices may be restricted in their capability from processing power perspective but smart enough to execute their functional tasks. Furthermore, these smart objects continuously perform status update on localized system for observation or communicate the sensor data to remote sub-system through popular network. The information processed could be sensitive and confidential in nature, so their security and privacy should be ensured.

Also, in this paper few IOT applications scenarios are discussed with the possible use cases, and later existing frameworks and their features are proposed and compared to cater the needs of IOT ecosystem.

II. Real-Time IOT Apps

A. IOTized Health-care APP:

The Smart health-care system includes variety of sensors devices ranging from blood-pressure, ECG monitor, life support system, blood glucose meter, pulse and calorie meter etc. A smart-watch with pulse sensor is also a health-care device. As these devices generate data pertaining to the health condition of a patient, which requires availability, reliability, privacy, and real-time request & response between device sensors and the remote- monitor system. Such IOTized system falls under the category of sensitive & critical IOTized APP. Patient's health-care data can be referred to various health-care personnel, its privacy must be respected as per patient's wish [1].Categorically, such APP must be able to perform following operations -

- **Registration:** As the sensor devices are heterogeneous in nature and are compliant to different standards and specifications. Sensor devices must be able to subscribe with a common IOT Sensor Server (IOTS). The IOTS is analogous to a web server which is hoisted to perform client's request. Here clients are replaced with multiple sensor devices. IOTS provides reliable, secure and real-time services to the device sensors and communicates with a remote monitoring system. The protocol between

device sensor and IOTS must comply with the standards based on which heterogeneous devices are communicating to each other.

- **Seamless communication:** All the devices sensors and IOTS must be able to communicate seamlessly. To attain seamless communications, prioritization support must be available in IOTS.
- **Secure communication and data storage:** All communication among device sensors and IOTS must be carried out on secure channel. Provision of device authentication, authorization and optimum key exchange must be done by each IOTS prior to provide the services. Additionally, sensor data must be stored securely to prevent unauthorized access.
- **High bandwidth audio/video/image transmission:** Data transmitted to remotely monitored system, where human medical team (Doctors) analyzes the condition of patient based on the data received from remotely located IOTized APP. The remote monitoring team may provide recommendations. Additionally, remote setting of sensors must be available by the IOTized APP. Under such circumstances, real-time audio-visual data of IOTized APP must be available at remotely monitoring team with required QoS. Secure, reliable and lightweight coding techniques for resource constrained devices ensure enhanced throughput.
- **Real-time alarming and notification:** A real-time response is expected to mitigate the risk arises from critical health condition of the patient. IOTS must be able broadcast the notifications under such conditions.
- **Plug and Play:** Introduction of a new device in the home sensor network must be detected by the IOTS. The new device must be able to authenticate itself with the IOTS and start functioning according to its defining role. IOTS must provide the registration and authentication mechanism in home sensor network.

B. IOTized Home APP:

Figure 1 shows a use case of IOTized home environment in a wireless sensor network. Another building block of IOTized ecosystem is Smart home. A smart home also environment constitutes of smaller sensor devices with the ability to perform their assigned designated tasks. These devices ranges from smart-TV, smart-phone, Tablets, smart-watch, washing machine, coffee maker, air-conditioner, hair drier, refrigerator, home entertainment.

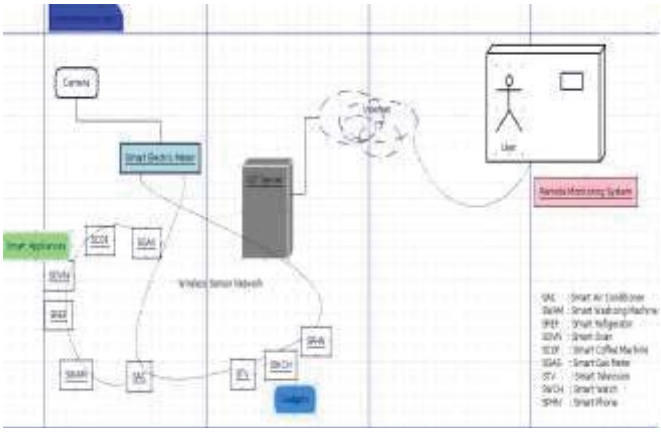

Figure 1. A use case of IOTized home environment in a wireless sensor network.

Any appliance which uses electricity is a vital entity of the smart home. The device sensors are connected to a common IOTS. It is important to analyze behavioral differences of the devices in a home sensor network environment. Each sensor is defined with different roles and accordingly their operations are monitored through the IOTS. Some of the use case scenarios of such an IOTized APP are depicted below –

- **Plug and Play:** Introduction of a new device in the home sensor network must be detected by the IOTS. The new device must be able to authenticate itself with the IOTS and start functioning according to its defining role. IOTS must provide the registration and authentication mechanism in home sensor network.
- **Status Update:** Sensor devices must be able to update the status of their operation through alert mechanism. A coffee machine raises the alarm after coffee preparation completion and eventually gets turn-off automatically. A smart electric meter must keep track of power consumption of each sensor devices across the home network and update the status with each associated device's data. A camera surveillance monitoring a toddler must raise the alarm whenever he crosses his predefined boundaries. An unauthorized attempt to access the vehicles parked in garage (or compound) must raise the alarm bell inside home. To accomplish all these notifications IOTS must implement the heterogeneous standards the sensor devices follow.
- **Seamless multimedia accessibility:** Home sensors devices specifically, smart-TV, smart-phone, tablets must playback the multimedia content seamlessly. A user in home watching the TV should be able to view the content on smart-phone or tablet or another smart-TV in a different room from where he left. The resumption of the content playback must be carried out with the context-awareness of home sensor network without user notices.
- **Remote Monitoring:** A user away from home wants to monitor the smooth functioning at home on his smart-phone or a display device. IOTS must be able to authenticate and authorize the remotely monitoring user.

C. Services offered by IOTized APP: Based on the use case scenarios discussed for IOTized APP, a common software

platform is desired to fulfil the requirements. A considerable amount of efforts have been spent to identify the idiosyncrasies of such heterogeneous and diversified network of things. The remaining part of this article discusses the start of the art technologies, systems and solutions to make such system a really secure, reliable and available to the user. The services offered by a common server to the sensor devices are mentioned below -

Smart TV: Authentication, Authorization, Multimedia, control & data.
Smart Washing machine: Authentication, control & data.
Camera: Authentication, control & data.
Smart Phone: Authentication, Authorization, Multimedia, control & data.
Smart Electricity Meter: Authentication, Authorization, Multimedia, control & data.

III. State of the art techniques

Based on the use-cases and the services discussed for IOTized APP, a common software platform is desired to fulfill the requirements. A considerable amount of efforts have been spent to identify idiosyncrasies of such heterogeneous and diversified network of things.

The remaining part of this article discusses the start of the art technologies, systems and possible solutions to make such system a really secure, reliable and available to the user.

One of the important aspects towards the solution of above mentioned problems is the technologies underneath. All the smart sensor objects lie on a wireless mesh network. RFID [15], ZigBee [2], ANT/ANT+ are some of the popular known standards to cater the physical infrastructure of the said ecosystem. Several communication protocols have been devised to meet the requirements of smart things. These are -

CoAP: Constrained Application Protocol is a light-weight version of HTTP. Things interact with each other in request/response format. [8]

MQTT: Simple and light-weight messaging protocol which works on subscription and notification model [11]. Optimization has been done for high-latency.

TLS & DTLS: Transport Layer Security uses TCP as its protocol underneath and Data-gram Transport Layer Security is designed to operate over UDP [9] [10]. DTLS is the communication protocol in sensor network to provide the security for the communication.

6LowPAN [3] [5] is a substitute name given for IPV6 Low Power Wireless Personal Area Network. The protocol is defines the specification for transmission of encapsulated message across the low power sensor network.

A comparative data is drawn below to depict the analogy between the full-fledged OSI Layer and the IOT layer.

HTTP/HTTPS (IPV4) ←→ (IPV6) CoAP/COAPS.
TCP/UDP, TLS (IPV4) ←→ (IPV6) UDP, DTLS.
IP (IPV4) ←→ (IPV6) 6LoWPAN, RPL.
Ethernet, WLAN (IPV4) ←→ (IPV6) RFID, NFC.

IETF formed working group CoRE [7] to provide a framework for resource constrained devices. CoAP, 6LowPAN are specified by this working group.

Above mentioned protocols are majorly related to transportation. However, a diverse set of communication protocols required for different applications to address the connectivity issues. These protocols address problems of following areas –

- Lighting/Home Automation
- High-value asset tracking
- Location tracking
- Proximity sensing
- Industrial Automation.

Various platforms are available which solves the connectivity issues as an ecosystem for smooth execution of applications of smart home appliances like televisions, air-conditioners, refrigerators, laptops, set-top boxes, smart-home based stations, vacuum cleaners etc. Unification of various communication frameworks will simplify the diverse applications' need. These are -

- Unified communication framework in os-platforms for addressing diverse applications where os-platform-powered devices are deployed.
- Organization based on connectivity-based paradigms
  - E.g. mesh-networking, ultra-low power sensing, etc.
- Identifying various application-based paradigms
  - E.g. smart-home, smart-office, industrial control, transportation, environmental monitoring, etc.

To build an ecosystem a two layered possible framework paradigm is depicted below and a comparative study across the protocols are enlisted.

ANT/ANT+:

- Proprietary, low-power, wireless sensor network technology operating in the ISM band (2.4 GHz).
- Low-power operation with long duty cycles, maximum data rate is 1 Mbps.
- Bi-directional communication channels; three types of messaging supported: broadcast, acknowledged, and burst.
- Current applications in fitness and cycling performance monitoring (Adidas, Garmin, Nike, etc.), future applications in health, home automation, and industrial sectors.

ZigBee:

- Technology based on low-powered mesh network.
- Mapped to IEEE 802.15 specification.
- Over-the-air data rate is 250 kbps; communication range from 10-100 meters.
- Applications in industrial controlled embedded sensing, home automation, security. [7]

Z-Wave:

- Low-power wireless communication protocol.
- Operates in 900 MHz frequency, with data rates up to 100 Kbps; communication range 30 meters.
- Z-wave network consists of controllers and slave devices; allows multi-hop communication in a mesh network topology.

- Primarily designed for home automation – remotely controlled applications in residential and light commercial environments. [12]

Bluetooth Low Energy (BLE):

- Operates in ISM band of 2.4 GHz.
- Communication range is 50m compared to 100m for traditional Bluetooth with an over-the-air rate of 1 Mbps.
- Use the star-bus network topology.
- Widely used, partly because of the popularity of Classic Bluetooth.
- Applications in sports and fitness, health-care, security & proximity, automotive, home electronics, automation. [16]

DASH7:

- Active RFID technology.
- Functions in 433 MHz ISM band which is unlicensed and with a maximum over-the-air rate of 200 Kbps.
- Capable of penetrating to concrete and water;
- Capable of transmission/receive over 1km, which is very long range;
- Packet size limited to 256 bytes;
- Advertised battery life of 10 years.
- Supports tag-to-tag communication; can emulate wireless mesh networks.
- Concept of Busty, Light, Asynchronous, Stealth, Transitive (BLAST).
- Applications in smart energy and building automation, location-based services and logistics, automotive. [17]

Wavenis:

- Ultra-low power and long range wireless communication technology supporting Machine-to-machine (M2M) applications.
- Operates in major ISM bands like 868 MHz, 915 MHz and 433 MHz; Typical over-the-air data rate is 19.2 kbps.
- Applications in smart metering, home automation, health-care, industrial automation. [18-21]

RuBee:

- Wireless technology using long-wave magnetic signals.
- IEEE standard 1902.1.
- Operates at 130 kHz; data packet size is 128 bytes; range of 1 to 30 meters.
- Not affected by presence of metal and water; can pass through almost anything.
- Applications in harsh environment visibility and security scenarios. [19]

EnOcean:

- Energy harvesting wireless technology.
- Enable wireless communication (ultra-low powered) between battery-less devices. Devices range from sensors, switches and gateways.
- Functions at various frequencies such as 902 MHz, 868.3 MHz and 315 MHz; communication range is 300 meters in open and 30 meters indoors.
- Radio packets are only 14 bytes long; over-the-air data rate is 125 kbps.
- Applications in industry, transportation, logistics and smart homes. E.g. wireless light switches, occupancy sensors, light sensors, temperature sensors, CO2 sensors. [20]

Wireless HART:

- This technology is based on Highway Addressable Remote Transducer Protocol.
- In short called as HART.
- Time synchronized, self-organizing, and self-healing mesh architecture.
- Operates in the ISM band of 2.4 GHz.
- Applications are primarily in industrial wireless sensing and automation. [21]

The protocols described above can be collectively arranged to form paradigms for connectivity & various applications running across the devices.
These paradigms are shown in figure 2 and Figure 3.

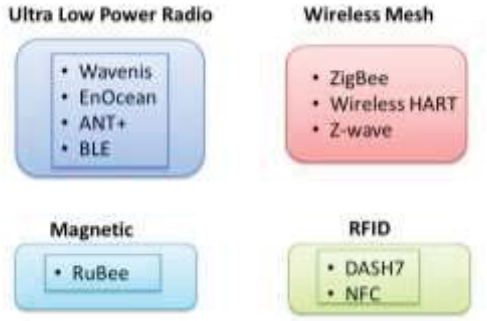

Figure 2: Connectivity paradigm depicting various hardware protocols.

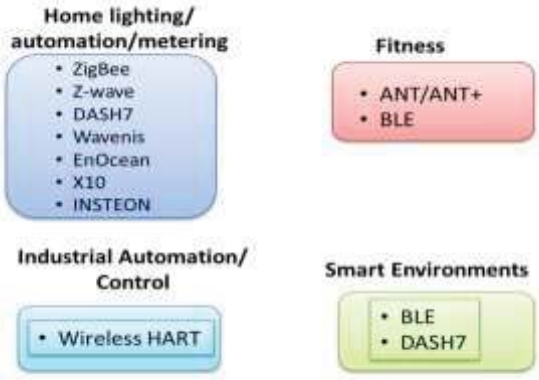

Figure 3: Application paradigm for various ecosystems.

A sample IOT framework in combination of connectivity and application paradigm is shown in Figure 4.

Figure 4: A sample IOT framework in combination of connectivity and application paradigm

Two use cases have been discussed: fitness application and home automation application. The various requirement specification and sample programming paradigm for the fitness application is shown in Figure 5.

(a)

Pseudo-code of Fitness Application

```
#include <os-platform/apps/fitness>
int main(){
    FitnessSensor s = new FitnessSensor ();
    //Connect to sensor (BLE/ANT+ driver interface)
    //When detecting running
   //Get heartbeat rate for every 30 sec
  //On detecting completion of run
   //Get number of steps
 //Upload data to user profile
}
```

(b)

Figure 5: Use case 1: (a) fitness application (b) Sample programming paradigm.

Similarly the various requirement specification and sample programming paradigm for the home automation application is shown in Figure 6.

(a)

Pseudo-code of Home Automation Application

```
#include <os-platform/apps/homeautomation>
int main ()
{
   HomeAutomationSensor s = new HomeAutomationSensor ();
   if (user1 enters the house gate in the evening)
       Switch the lighting of the living room, bedroom and kitchen to
profile1
    if (car monitoring system reports user1 is tired)
       Switch on lighting profile3 in living room
     if (user1 enters main door)
        Play genre 'relaxing' music on home audio
}
```

(b)

Figure 5: Use case 2: (a) Home automation application (b) Sample programming paradigm

The implementation of the above test cases using the existing IOT framework/technology is shown in Figure 7.

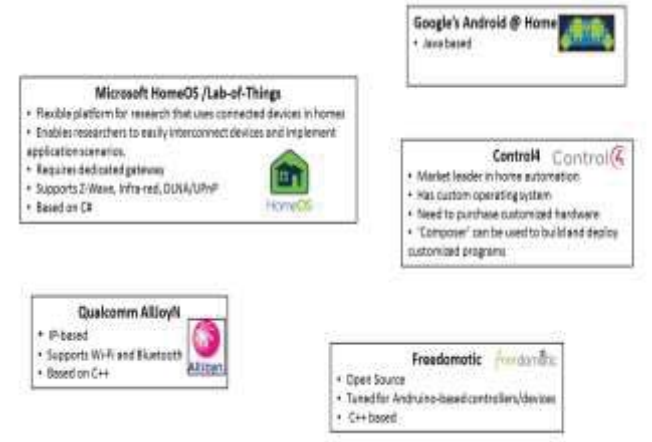

Figure 7: Depiction of IOT frameworks

IV. Limitations & Bottlenecks

Based on the captured requirements above, major bottlenecks to fulfill these requirements are described below -

Efficient bandwidth utilization for multimedia contents transmission. For effective utilization of available network

bandwidth to mitigate the high volume multimedia data exchange, a routing protocol need be explored. There are existing routing protocols available for audio-visual data in wireless sensor network, but this article does not cover those techniques.

Address security and privacy concern of sensor data. Different standards and specifications are being designed by multiple working groups. However, this article only covers the ITEF specific techniques and briefly discusses the protocols of IETF work groups.

VI. CONCLUSION & FUTURE WORK

This paper highlighted some of the many use cases of future network of things. It discusses the requirements of such heterogeneous networks and identified few application areas. Based on the application area, various possible connectivity, security & privacy services are depicted from user's point-of-view. Finally it highlights the state of the art techniques available which can be building blocks of thing's services in future. Study and exploration is further required to design the routing protocols for wireless sensor network of things.

VII. REFERENCES

[1] Tyrone Grandisona, Srivatsava Ranjit Gantab, Uri Braunc, James Kaufmana, "Protecting Privacy while Sharing Medical Data Between Regional Healthcare Entities", Online, last visited on 10 Nov, 2015.

[2] ZigBee. http://www.zigbee.org/. Online, last visited 20. April 2015.

[3] E.Kim, D. Kasper, N. Chevrollier, and JP. Vasseur. Design and Application Spaces for 6LoWPANs draft-ietf-6lowpan-usecases-09, January 2013.

[4] Tobias Heer, Oscar Garcia-Morchon, René Hummen, Sye Loong Keoh, Sandeep S. Kumar, Klaus Wehrle,"Security Challenges in the IP-based Internet of Things 2014", Wireless Personal Communications: An International Journal, Volume 61 Issue 3, December 2011 Pages 527-542 Kluwer Academic Publishers Hingham, MA, USA table of contents doi>10.1007/s11277-011-0385-5.

[5] IETF 6LoWPAN Working Group, http://tools.ietf.org/wg/6lowpan/

[6] G.Montenegro, N.Kushalnagar, J, Hui and D. Culler, " Transmission of IPv6 packets over IEEE 802.15.4 Networks, RFC 4944, September 2007.

[7] IETF Constrained RESTful Environment (CoRE) Working Group, https://datatracker.ietf.org/wg/core/charter/

[8] Z. Shelby, K.Hartke, C. Borman and B. Frank, " Constrained application Protocol (CoAP)," draft –ietf-core-coap-04(Internet draft), January, 2013.

[9] T. Dierks and E. Rescorla, " The transport layer security (TLS) Protocol Version 1.2. RFC 5246, Aug 2008, Updated RFC 5746,5878.

[10] T. Phelan. Datagram Transport Layer Security (DTLS) over the Datagram Congestion Control Protocol (DCCP). RFC 5238, May 2008.

[11] http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html#_Figure_2.1_-, "MQTT Version 3.1.1." Specification URIs. Online, last visited on 29. Sep 2015.

[12] Jesus J. Martínez, Teresa García-Valverde, Francisco Campuzano, Pablo Campillo-Sanchez, Alberto García-Sola, Juan A. Botía, "Multi-Agent Based Social Simulation Applied to Validation of Location Services", DOI: 10.3233/978-1-61499-050-5-91 In book: Ambient Intelligence and Smart Environments Volume 12: Agents and Ambient Intelligence, Publisher: IOS Press Books, Editors: Tibor Bosse, pp.91 – 118.

[13] https://en.wikipedia.org/wiki/Digital_India, Digital India, Online, last visited on 29. Sep 2015.

[14] Chaudhuri A., "Address Security and Privacy Concerns to Fully Tap into IoT's Potential", Online, last seen on 10 Nov, 2015.

[15] https://en.wikipedia.org/wiki/Radio-frequency_identification, Radio-frequency identification, Online, last seen on 10 Dec 2015.

[16] https://en.wikipedia.org/wiki/Bluetooth_low_energy, Bluetooth low energy, Online, last seen on 10 Dec 2015.

[17] https://en.wikipedia.org/wiki/DASH7, DASH7, Online, last seen on 10 Dec 2015.

[18] http://www.powershow.com/view/79956-NzBkY/WAVENIS_powerpoint_ppt_presentation, Ultra Low Power WSNs, Hype or ripe? Online, last seen on 10 Dec 2015.

[19] https://en.wikipedia.org/wiki/RuBee, RuBee, Online, last seen on 10 Dec 2015.

[20] https://en.wikipedia.org/wiki/EnOcean, EnOcean, Online, last seen on 10 Dec 2015.

[21] https://en.wikipedia.org/wiki/WirelessHART, WirelessHART, Online, last seen on 10 Dec 2015.

[22] A. Yadav, S. Pandey and R. K. Singh, "Lightweight capability-token for consent based authentication protocol for smart sensor nodes, " Journal of information security and application (Elsevier), Vol. 63, 103024, December 2021