Otto-Friedrich-University of Bamberg

Professorship for Computer Science,
Communication Services, Telecommunication
Systems and Computer Networks

Seminar on

Fog computing in Next Generation Networks

Topic:

IoT Applications in Healthcare

Submitted by:
Likitha Purushotham

Supervisor: Prof. Dr. Udo Krieger

Bamberg, October 06,2020
Summer Term 2020

Contents

List of Figures

List of Abbreviations

eMR	Electronic medical record
eHR	Electronic health record
DTLS	Datagram Transport Layer security
IT	Information Technology
ID	Identification
IaaS	Infrastructure as a Service
IoT	Internet of Things
IoHT	Internet of Healthcare Things
IPSec	Internet Protocol Security
LS	Loss-sentitive
OS	Operating System
OTrP	OpenTrust Protocol
PaaS	Platform as a Service
QoS	Quality-of-Service
SDN	Software-Defined Networking
SDNC	Software-Defined Networking controller
SaaS	Software as a Service
SSL	Secure socket layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
WebRTC	Web Real time communication

I. Introduction

A. Motivation

The rapid growth in technology and information sector in recent years has resulted in a wide range of connectivity for various electronic and heterogeneous devices that can communicate effortlessly with each other over the internet.This is what is called as 'Internet of Things'[1].

Due to this growth in technology,we can experience a exponential growth in the usage of devices in upcoming years that can rule over the internet.

This technological improvement has made a gateway for various different industrial sectors including Healthcare inculcate IoT with varied applications leading to new possibilities.

According to the recent research in healthcare industries,the life expectancy is said to increase by 31% and the aged population is said to increase by 16% which can result in highly vulnerable population that are prone to chronic and other diseases resulting in a large percentage of deaths and global burden inturn leading to the shortage of healthcare workforce in upcoming years.

With this aim,several healthcare frameworks have been developed based on Internet of Healthcare Technology that can provide improved and reliable services with reduced cost,highly energy efficient and scalable solutions to meet the shortage of healthcare workforce and help in prevention of diseases,treatement and cure.

Nonetheless,the various healthcare devices generate a huge amount of heterogeneous data that require special consideration in terms of different data specific processing power,quick response time and huge storage of data which can be a challenging task.

In order overcome this challenge ,Taylor paper[1]proposes a 5-Layered IoHT framework that consist of Perception,Mist,Fog,Cloud and Application which is capable of handling different routing paths for different data types that consists of realtime and offline/batch mode data providing optimal resource utilization,balanced network load and allocate resources as required by making use of Software defined networks(SDN).

The results from the paper show that the proposed IoHT framework provide better QoS in terms of low power consumption,reduced latency and low packet drop rate leading to an efficient development for the existing & next generation e-Healthcare systems.

II. Background/Basics

A. Key Concepts

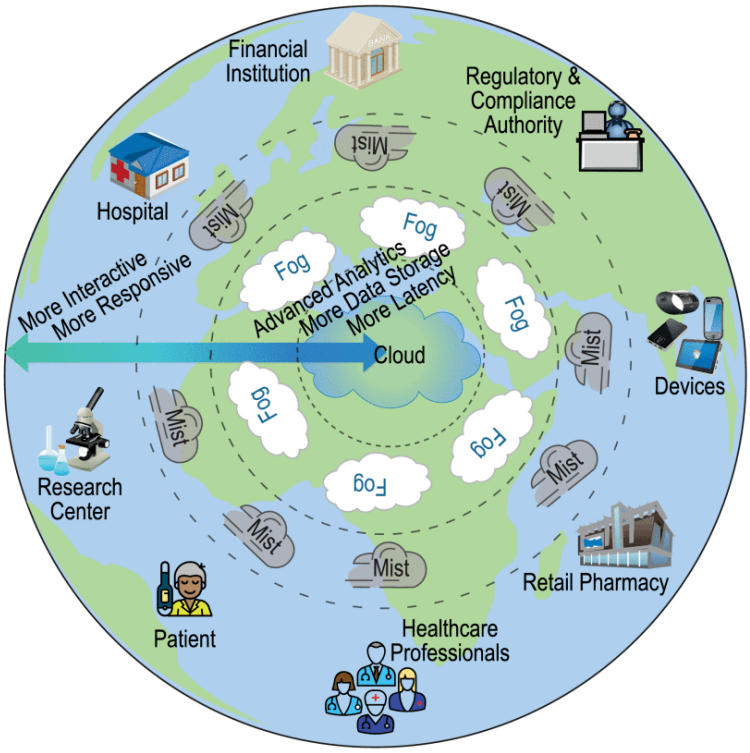

Figure 1: Proposed IoHT Framework with differet stalkholders

src:ASIF-UR-RAHMAN et al:[1]

1) CLOUD:

Cloud is a centralized mode of computing that can store and access the data and program on the remote servers that are hosted on the internet instead of on the local server or hard-disk.It is also called as Internet based computing because of its main functionalities such as storing,computing,control and communicating between servers on large data centers that are closer to the end user through the cloud-to-things continuum.

The main functionality of Cloud services is to help migrate from traditional environment to cloud computing to delivering the services over the internet that can ensure optimized performance,support,consistency and security to the maximum level.

The main technology for cloud computing is virtualization which seperates a physical computing device into more than one virtual devices,each performing and managing the computing tasks leading to the agility of increaseed IT operations and reduced cost by making maximum utilization of infrastucture resources.

The main aim of cloud computing is to make users utilize the technology and resources to an extent such that they stay focused on their business needs and cut down the cost instead of focusing on other IT related issues such as storage or performance or scalability and etc.

Cloud computing shares the same characteristics as like with Fog computing,Grid computing,Client-server model and Peer-to-peer[2].

Cloud consists of three layer of service models based on the services companies provide.

- Infrastructure as a service(IaaS):
  Provision of processing,storage,networks and other fundamental computing resources[3].

- Platform as a service(PaaS):
  Allows for the deployment of customer created applications and these application are restricted to the programming languages,libraries and services supported by the provider.

- Application/Software as a service(SaaS):
  Applications that are running on a cloud infrastructure.Here consumers can use the applications but have no control over the cloud resources such as network,servers,operating systems,storage, technologies or individual applications[3].

The key characteristics of Cloud Computing are:

- Scalability: Easy to scale up and scale down according to the business requirements and manage resource utilization instead of installing expensive upgrades.

- Maintenance and Performance: Maintaining is easy as it can be accessed from any where and ensures performance by frequent upgradation to recent trends leading to fast and efficient computing speed over the web services.

- Security:Monitoring is one of the main facilities of cloud computing and Data access and security is more efficient through cloud computing than other traditional systems.

- Resource pooling : Ability to serve multiple clients at a time using the resources that are pooled and this resource usage can be assigned or reassigned based on client needs any time.

- Broad network access: Enables the capablities of accessing the resources that are hosted in private cloud over the internet through standard mechanisms that promote use by heterogeneous applications such as mobile phones, tablets, laptops, and workstations.

2) FOG:

Fog Computing is an architecture that extends cloud computing to the edge of the network.It is the concept of a network infrastructure that distributes computation,communication,control and storage closer to the end users along the cloud-to-things continuum[4].

The devices at this layer is responsible for performing operations related to networking such as routers,gateways,bridges and hubs such that it is capable of performing both computational and networking operations simultaneaously.

Although the devices in fog layer when compared to cloud are resource constrained ,it ensures a reliable service with geological spread and decentralized nature over a wide area. When compared to the traditional cloud computing,fog computing ensures delay-sensitive service request from the end user with low energy consumption and less traffic congestion[5].

Above all,fog networks are considered as offloading to core computation and storage.Further,the nodes present in the fog network determine whether to process the service using the available resources or send to the cloud server.Hence fog computing helps to attain efficient resource utilization and greater performance concerning the delay,bandwidth and energy consumption[5].

The key characteristics of Fog computing are;

- Allocates the resources and services to the end users such as computation,communication,control,and storage.
- Can be fully distributed or mostly centralized or in between.
- Fog architecture and its applications can be virtualized but can also be implemented in dedicated hardware and software.
- Allows the same application to run anywhere with reduced need for specific applications just for the cloud,endpoints or edge devices.
- Allow applications to run on same physical platform without mutual interference from multiple suppliers.
- Enables the capacity of processing high number of nodes
- Fog often combines with cloud to allow end-to-end services impeccably.
- Determines the best way to carry out the computing,storage, and control functions based on the user requirements.
- Ensures efficiency and performance by pooling the resources anywhere between cloud and end-user systems.
- Enables a rapid innovation and afforadable scaling which can be much faster and cheaper to experiment with client and edge devices instead of waiting for the vendors

of large network and cloud boxes to initiate or adopt innovation.

- Enables data analytics at the network edge and can support time-sensitive functions for local cyber-physical systems.

3) MIST:

"Mist computing is an extreme edge of a network consisting of sensors and micro-controllers.Mist computing uses microcomputers and microcontrollers to send to the fog computing nodes and then onwards towards the centralized cloud computing servers.Main functionalities of Mist is to ensure resource collection by computation and communication capabilities to be available and to allow random computations to be provisioned,deployed,managed and monitored on sensors itself[6]".

The key characteristics of Mist Computing :

- In Mist computing the communication takes place at a high speed of computing in an embedded microcontroller which allows to send only relevant data to the gateway,router,or server by collecting the raw data at the edge of your network and then group them by filtering,anomaly identification mechanisms and pattern recognition which helps conserve the battery power as well as bandwidth[6].
- Due to the computing power on sensors,it consumes low power for data processing and optimizes the data before storing.
- All local analytics and decision making happen in mist layer with less overhead.
- It is highly robust for data and applications.
- Security is assured as the data is first being processed in the mist layer before sending it to the remote server.
- By adding mist layer to the existing fog-based architecture it helps in reducing the data volume to be transmitted through IoT devices using rule-based preprocessing of the data[1].
- The latency in processing,transmission and computational complexity is reduced by minimal usage of data volume which inturn reduces the power consumption in the framework.
- Mist facilitates time-critical data processing.
- Mist remains directly within the network fabric and operates on the extreme edge of the network using sensors and micro controllers[1].
- Mist is responsible for performing basic rule-based preprocessing of the the sensor data such as data aggregation,fusion and filtering[1].

B. SDN-Software Defined Networks

"Software-Defined Networking is an emerging approach that uses software-based controller or application programming interfaces(APIs) to reconfigure traffic on the network and communicate with the underlying hardware infrastructure[7]".

The main idea of SDN is to seperate physically the control plane and data plane[5].
Due to the increase in the interest of Internet of Things(IoT) and the huge heterogeneous data in the ubiquitous networks,it makes implementation very crucial in network.

To maintain these heterogeneous data efficiently by ensuring high QoS in terms of network scalability,privacy and security,the IoT framework relies on Software Defined Networking(SDN)[1] where the network resources are dynamically allocated and deployed on the IoHT technology framework in a centalized/distributed server.

SDN helps in fulfilling various requirements of applications and workloads through network virtualization by decoupling control plane from data plane in the IoHT framework to manage the resource demand of increasing IoT devices[1][8]
SDN consists of 3 parts :

- Application: Where the resources communicate or request over the internet
- Controller: Which is responsible for routing of data packet based on the information collected from application.
- Networking devices: Which is responsible for handling and moving of data,based on the request it recieves from the controller.

In general,allocating resources,scheduling,routing,flow control,packet-forwarding and other network functionality is handled by the SDN controller(SDNC).These SDN controllers communicate via TCP connection using switches which is responsible for defining fine-grained QoS provisioning based on the attributes and the state of data gathered from fog node[5].

Despite of the fact that Fog is a feasible way for latency-sensitive task[5],the available resources can differ based on the fog computing resources. Hence it is necessary to transfer some of the latency-aware fog tasks to cloud if there is no enough resource in the fog layer[5].However software defined QoS is provisioned by deploying dynamic QoS policy to handle fog services and SDN benefits from distrbuting latency-aware fog tasks using complete knowledge of network state.

SDN not only benefits the network infrastructure by optimizing the flow of data over the internet and prioritize applications availability based on the requirements by customizing the network services and allocating virtual resources in real-time using one centralized location but also ensures robust security by providing visibility to the entire network that can rectify the threat and act accordingly.Different levels of security can be applied at different zones for devices in a large network by the network administrator.

SDN plays a major role in edge computing and internet of things because of its speed and flexibility that require transferring of data quickly and easily between remote sites.

C. Cloud Features

"Cloud computing is a model for enabling ubiquitous,convenient,on demand network access to a shared pool of configurable computer resources that can be rapidly provisioned and released with minimal management effort or service provider interaction[3]"

Main objective is to compile,store,interconnect and manage on demand that supports various operating systems,programming languages,tools,databases and devices.[from Mobicom-KTR-Slides]

Which implies,

- Having scalability in distributed computing utilizing resource pools
- Storing large amount data(terabytes)
- Making a gateway for connections between applications to servers through IP networks
- Utlizing the scaling and multiplexing effects of resource usage

Example : Microsoft Azure studies

"Microsoft stands as one among the five Cloud market leaders that provide Infrastructure as a service [IaaS], Platform-as-a-Service[PaaS] and Software-as-a-Service [SaaS][9]"

Comman characteristics are,

- Application management:
  Easy to build,deploy and manage apps by customizing cloud software.

- Flexibility:
  Flexibile in choosing the functionalities according to the business infrastructure.

- Agility:
  Fast and up-to-date in terms of deploy,operation and scalability making infrastructure and applications agile.

- Compliance:
  Security and privacy demands ensured in maintaing the data stored.

- Storage:
  Faster and reliable delivery rate in terms of sharing data across the virtual machines by facilititaing optimal user experience and store heterogeneous data.

- Security:
  Security being highly ensured by having two-tier authentication protocol using hand biometric readers,proxy card access readers and etc.

III. IoHT-Framework

A. Layered Architecture

IoT implementation on large scale leads to challenges such as large number of connected devices and voluminous data having limited processing power and resources.Centralized cloud based IoT is a key that can handle huge data generated by heterogenous devices in an IoT Framework.
Although cloud is efficient enough on a large scale,it can cause some latency issues and consume more power which can make a solo cloud more critical at times.To handle the load on cloud,an introduction of Fog is an approach that ensures reliability,energy-efficiency and performance in IoT frameworks[10][1].

However there still exists QoS issues in order to deal with different kinds of data processing at each layers.The solution to this problem is the five layered fog-based architecture that is capable of handling different kinds of data processing based on the demands in different layers.The introduction of additional layer called "Mist Layer" to the Fog architecture reduces volume of the data that has to be transmitted to IoT devices using rule-based prepocessing which in turn reduces the power consumption,latency and computational complexity of the framework[1].

This 5 layered architecture is capable of reducing latency by selecting data transmission policies depending on the data source and ensure optimal resource utilization to deliver the processes to layers with reduced transmisssion delay using load balancing and guarantees the allocation of data sensitive resource based on the data transmission priorities.

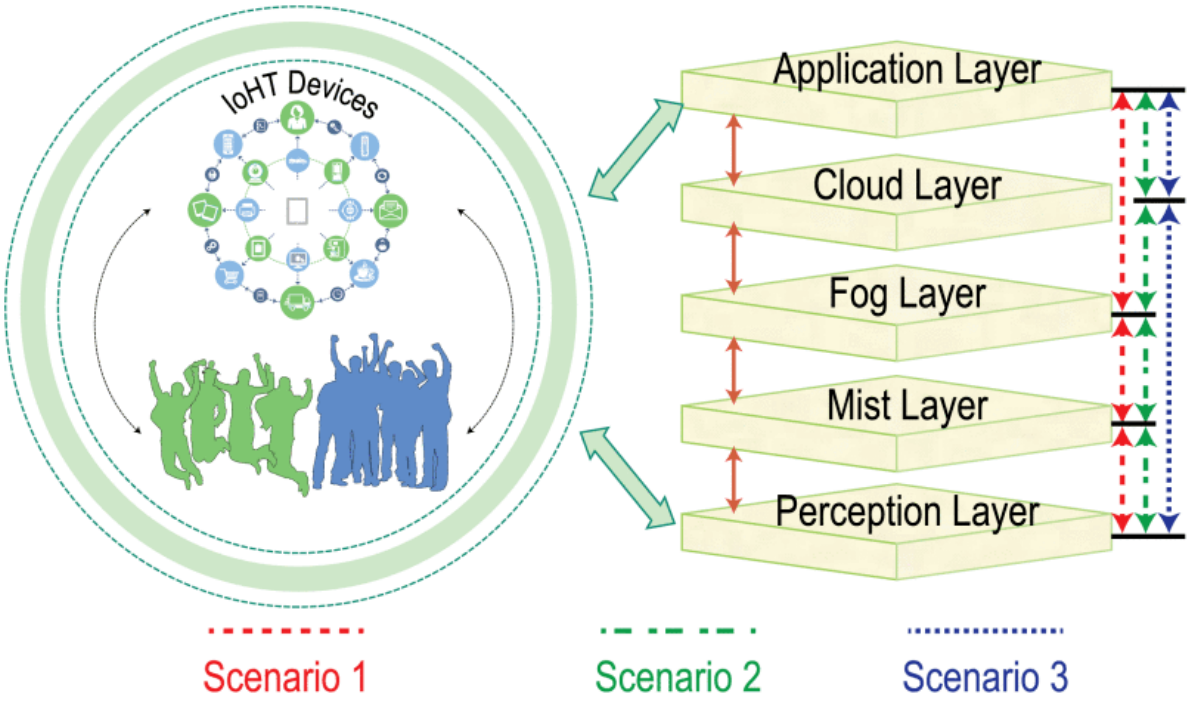

Figure 2: IoHT Framework

src:ASIF-UR-RAHMAN et al:[1]

B. The Components of 5-Layered Architecture

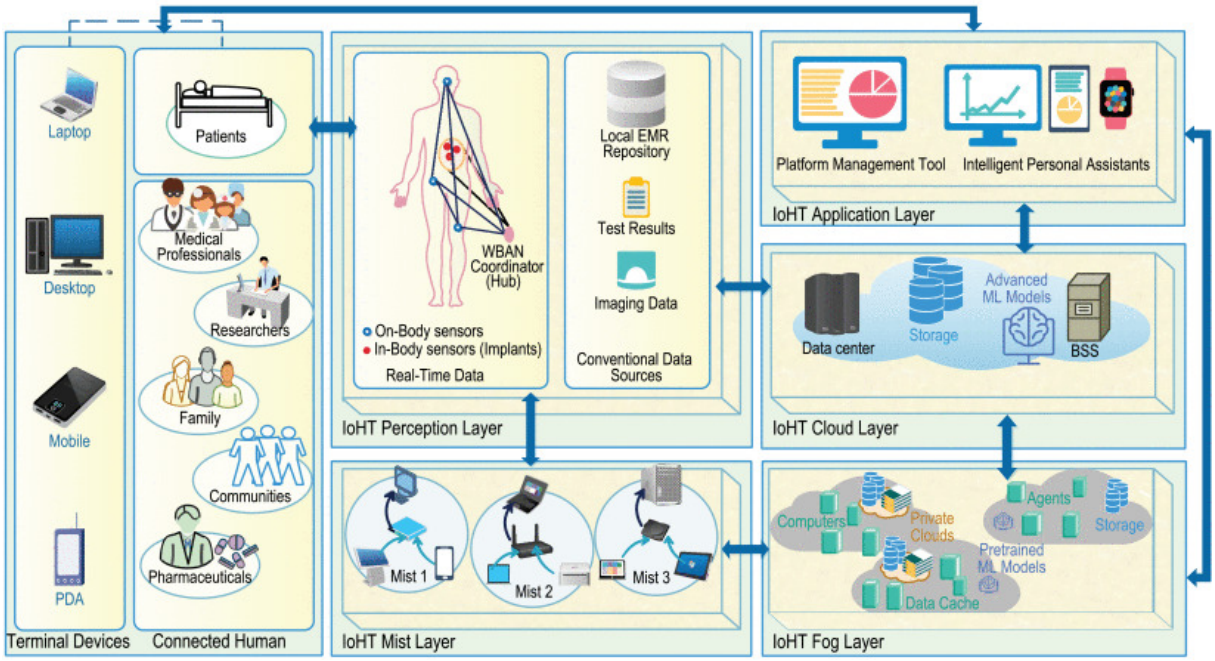

Figure 3: IoHT Framework Architecture

src:ASIF-UR-RAHMAN et al:[1]

Five Components of the framework are,

1) Perception Layer
2) Mist Layer
3) Fog Layer
4) Cloud Layer
5) Application Layer[1]

C. Layers and their Goals

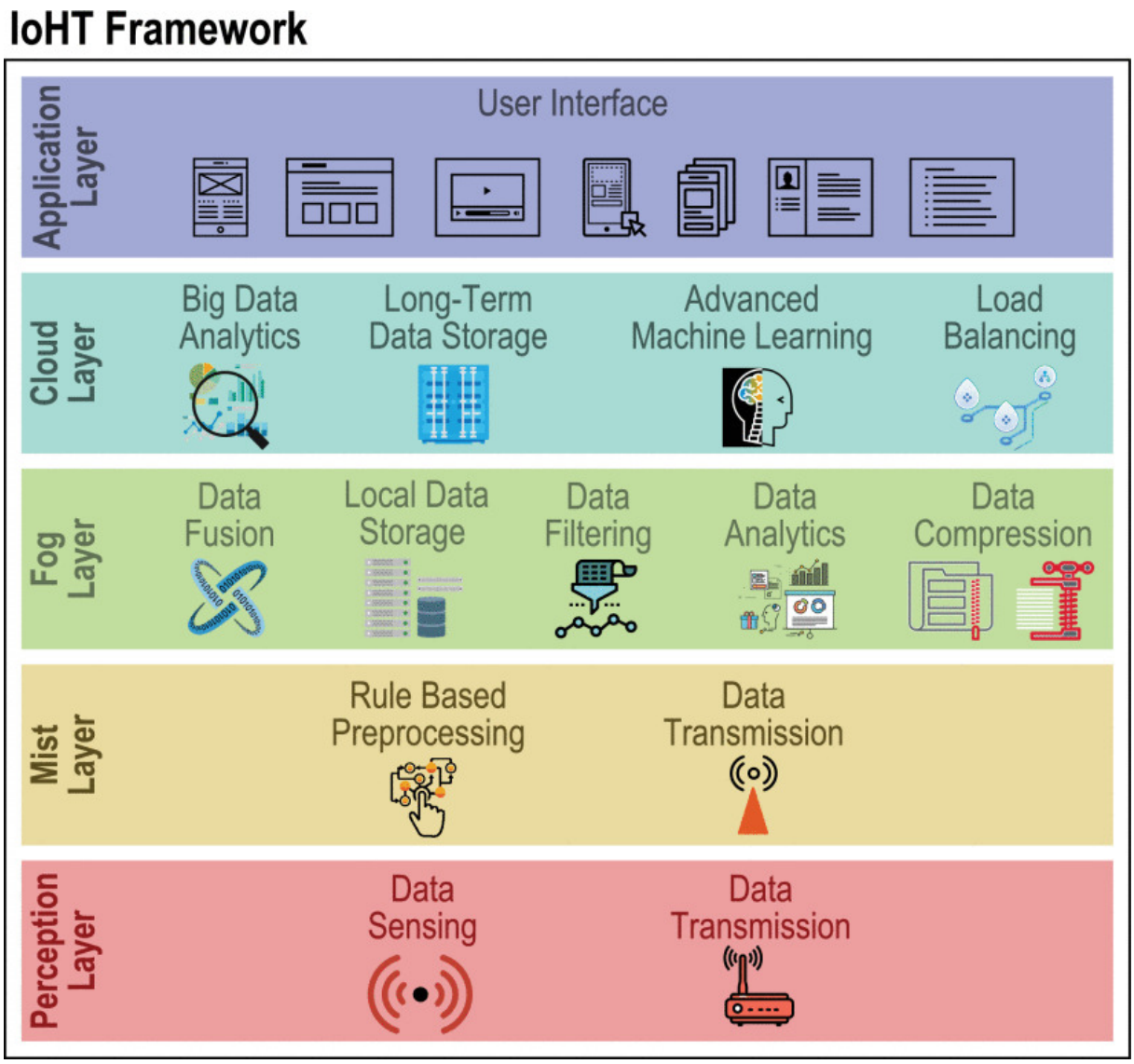

Figure 4: Functionaities of 5-Layered IoHT Framework

src:ASIF-UR-RAHMAN et al:[1]

1) Perception Layer:
It is the lowest layer in IoHT Framework which identifies the devices that is connected to transmission and data gathering devices such as sensors,RFID tags,readers,medical imaging devices,etc which is inturn connected to the network and collects the data which is real-time as well as non-real time data.Otherthan realtime data there exists healthcare Big data such as (non)medical imaging data,electronic medical record(eMR),unstructured clinical notes etc which requires special handling because of their requirement of advanced data analytics.Based on the data type and processing requirements ,both kinds of healthcare data is transmitted to the next layer either to the Mist or Fog or Cloud[1].

2) Mist Layer:
In order to deal with critical time data processing,Mist was introduced in the model which stays inside the network fabric and operates at the edge of the network using sensors and actuator controllers and performs prepocessing based on rule based

sensor data[1].Mist is responsible for optiml resource utilization of Things that have limited power,memory and communication bandwidth at the edge of IoT network.

3) Fog Layer:
In order to detect the anomalies(irregularities) and take immediate necessary actions by providing quick alarms at real time,Fog Layer was introduced.The fog layer is a decentralized architecture which ensures minimal latency and high responsiveness by bringing computing resources and application servers close together to the edge[1].This reduces latency and load on the cloud by local data storage,data compression,data filtering and intermediate data analytics that will improve QoS,System performance and save bandwidth.

4) Cloud Layer:
All healthcare data from fog layer and nonsensor sources such as eMR,eHR etc gets combined at Cloud layer for long-term storage, and big data and advanced analytics.The Cloud Layer is capable of connecting to Fog layer,Application layer and perception layer[1].It performs data analytics including machine learning,rule based processing,data mining and reasoning based algorithm to abstract meaningful data from healthcare data.

5) Application Layer:
It is the top most layer in IoHT framework that provides user interface between different stake holders and frameworks delivering many healthcare applications to the stakeholders and application developers by providing accesss according to the right and privilege from the cloud or fog layer directly[1].

D. Data processing & Storage

1) Data-centric perspective:

In order to ensure smooth connectivity of heterogeneous data,a data centric transmission scheme has been made use of in the five-layered architecture.

Depending on the availability of resource and data traffic,the processing load is assigned to either Mist or Fog or Cloud based on rule based Preprocessing, big data analytics,machine learning and etc in the 5-layered architecture.

The Below Flowchart describes the data transmission and processing that takes place at different layers of the IoHT Framework[1].

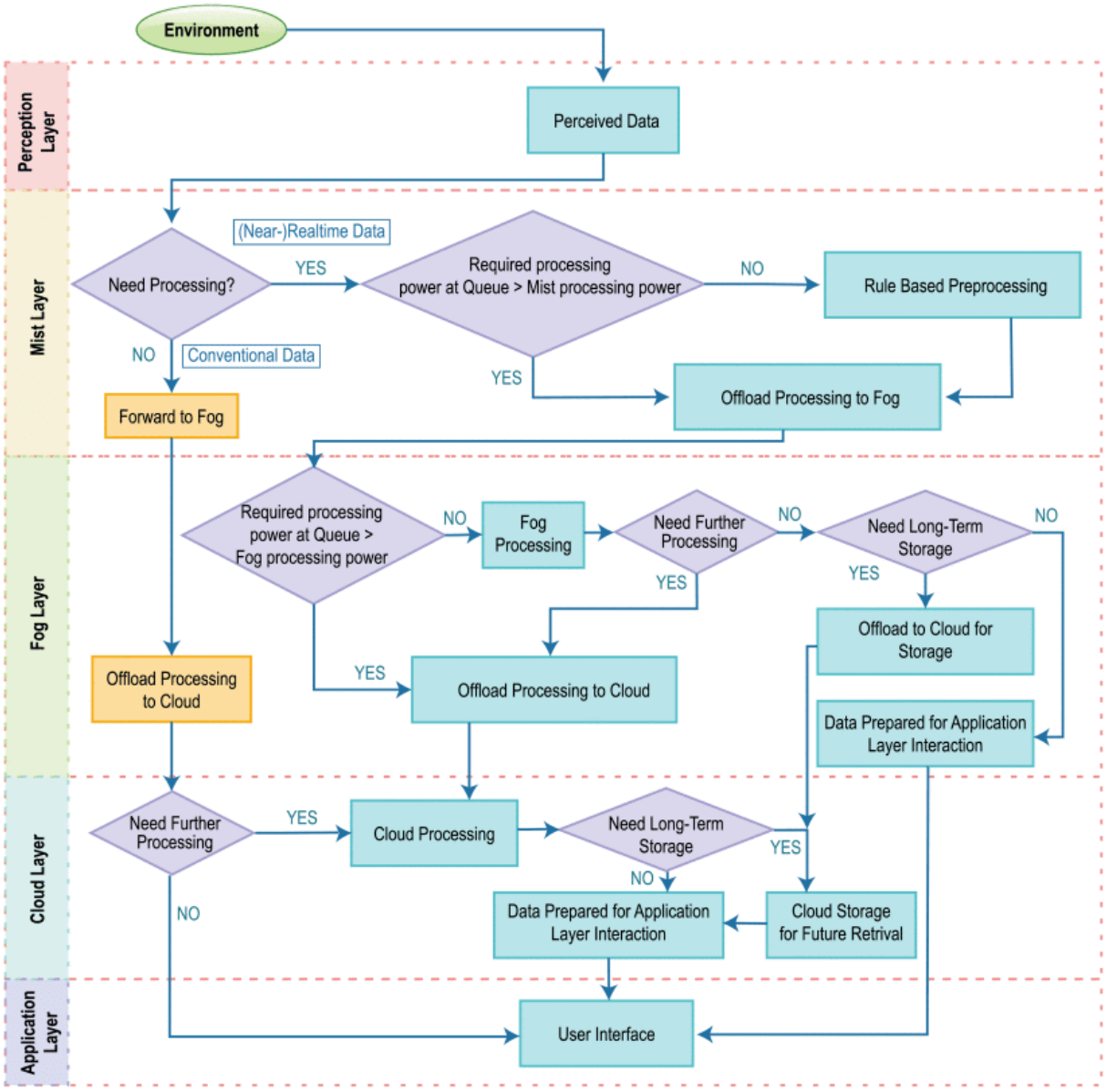

Figure 5: Flowchart of data transmission and processing

src:ASIF-UR-RAHMAN et al:[1]

In order to achieve consistent communication among the heterogeneous data that is generated from perception layer in the proposed IoHT Framework,a data centric transmission scheme was maintained in order to deal with different types of data that was generated such as real time,near real time and offline mode(batch mode/Big data).To processing this data,it takes place in two different paths based on the traffic of data and availability of resource to attain better QoS,reduced latency and optimized power consumption[1].

In case of real-time data,the data that is generated from the sensors that are located in the closest region and is first sent to Mist layer for processing and then forwarded to the next layer Fog which can deal with intermediate analytics and then the results are sent to application layer.

When the intermediate results sent by Fog layer is not sufficient,data is offloaded to

the cloud layer which is capable of handling big data analytics,advanced machine learning,massive data generated by advanced medical instruments and etc and the data get stored in cloud for long term data storage that can be used further for reference.

2) Networking: The heterogeneous data generated from perception layer that can be real-time and non real time is sent to the nearest IoT hubs for processing.According to the processing rules and data traffic,it is then forwarded to either Mist or Fog or Cloud for preprocessing.In this process,the most critical aspect is to maintain QoS and that is achieved by deploying SDN(Software Defined Network)a programmable network structure that works on IoHT framework as centralized or decentralized for resource allocation,scheduling,routing and flow control through SDNC that uses network virtualization by decoupling control plane from data plane[1].

To attain better QoS,the network traffic is prioritized based on the transmission rate and delay and is classified as Delay-sensitive(DS),loss-sensitive(LS) and both delay as mixed(M)[1].

A sample data of IoHT healthcare traffic classification is as shown below.

P	Traffic Type	Description		Service Type	Example
		C	tQ		
1	$\mathcal{DS}$	H	L	Critical Traffic	RT Patient Monitoring
				Video Traffic	VidStream EM & MC
				Multiconf.	Teleconf.
2	$\mathcal{LS}$	L	H	Images/Video	Medical Imaging
				Test Results	EMR
3	$\mathcal{M}$	M	M	NCMeasure	Regular PhyMeas

Legend: H–High; L–Low; M–Medium; RT– Real-time; VidStream EM & MC– Video streaming of elderly monitoring & motion control; Multiconf– Multimedia conferencing; Teleconf– Teleconferencing; PhyMeas–Patient physiological measurements; NCMeasure– Non-critical healthcare parameter measurement.

Figure 6: Flowchart of data transmission and processing

src:ASIF-UR-RAHMAN et al:[1]

E. Data Analytics & Machine Learning

With the evolution of IoHT in recent years,traditional databases cannot handle the huge data and there is a huge hype for Machine Learning methodologies and Data Analytics to be used to deal with the voluminous data generated by the sensors and IoHT devices in order to provide useful and innovative process to the industries for cost cutting and improved approaches helping their business models achieve a better experience by enabling a parallel execution and distribution of data on multiple servers.

The voluminous data generated by the IoHT devices require special methods and approach for handling and processing the structured and unstructured data.Machine learning plays an important role in IoHT Framework which is capable of handling the decisions based on certain Machine learning alogorithms where it can provide services with faster analysis and expert intervention for better treatment recommendations for the monitor of diseased person.By using machine learning methods in devices,it firstly works towards the goal irresppective of the factors that can impede and later decides the important input variables required to achieve the goal and predict the future events ensuring prevention before hand.[11]

Although data analytics could be made use of for measuring success overtime by providing smarter decision and generates report based on the data that was collected,it is not appropriate for IoT as data analytics is often static having limited-use in addressing fast-changing and unstructured data.[12]But Machine learning addresses the fast changing and unstructured data by focusing on the outcome fisrt and later decides automatically which variables is required and their interactions accordingly based on certain algorithm implementation.

Machine Learning is not just used for machines and devices where maintainence is automated but humans too,for calling an emergency support automatically when in need.

Example :
Diastolic/sistolic pressure alert event
High Blood pressure is one of the crucial factors that leads to stroke.Hence continous monitoring of blood pressure anytime anywhere is very essential in order to prevent and predict stroke before hand.[13] According to one of the research,a calibration method using machine learning algorithms was made use of in order to detect the variation of pulse transit time by detecting automatically the compensatory movements based on sensors and camera based devices around the patient.By continuously monitoring the patient,with an average of 0.5 ± 3.9mmHg for systolic and diastolic blood pressure[13],an aleart event will be sent when it reaches the above average blood pressure to the caretaker through the monitoring tool that can ensure high prevention and help well in hand.

IV. Case Study & Evaluation based on Taylor James paper

A. Weakness of the paper/Missing Elements

According to the research paper by Taylor,IoT is an emerging technology that supports global infrastructure for exchange of information between ubiquitous computing devices without any interaction of humans. This paper describes the importance of practical and intelligence of Iot applications majorly in healthcare sector using a 5-Layered Architecture that represents its functionalities in an effective way.However there are few other factors that must be take care of such that IoHT devices can work efficiently[14].

Few factors that require considerations are,

1) Implementing Classical Middleware approach - Publish & Subscribe method
2) Introduction to Docker/Kubernetes
3) Ensuring Privacy & Security

1) Classical Middleware Approach-Publish&Subscribe:

How can middleware approach of Publish & Subscribe method help IoT Platform to meet their requirements?

IoHT comprises of various ubiquitous devices and technologies that offers real time data transmission of the surrounding and provide triggers based on the changes in the physical world.This methods lead to the approach of smart Healthcare,smart city,smart application and etc where billions of devices are connected over the internet for seemless interoperability.

The classical sensor based devices deployed in IoT provide real time data but few devices have constraint where they can read the sensor data only once,which should be later distributed to several applications/services.To handle this challenge,a scalable cloud based messaging layer[15],Publish and Subscribe model is used,that can match the data stream to the interested applications and distribute data accordingly.

Pub/sub system mechanism ensures high performance processing and interoperability to allow devices to publish their presence(send data)to the node called as broker/router,which is responsible for traffic handling and distribution of data,and on the other side devices can subscribe to the broker for accessing the information based on their requirement.

Pub/Sub is an asynchronous messaging service that decouples services that produce events from services that process events.It ensures message storage and real-time message delivery with high availability and consistent performance at high scale[16].

Integrating publish/subscribe method in IoT platform is considered as the best approach for the interoperability and distributing various kinds of data over the network on different layers that acquires data from various other devices such as entities,devices,wireless sensors and etc.

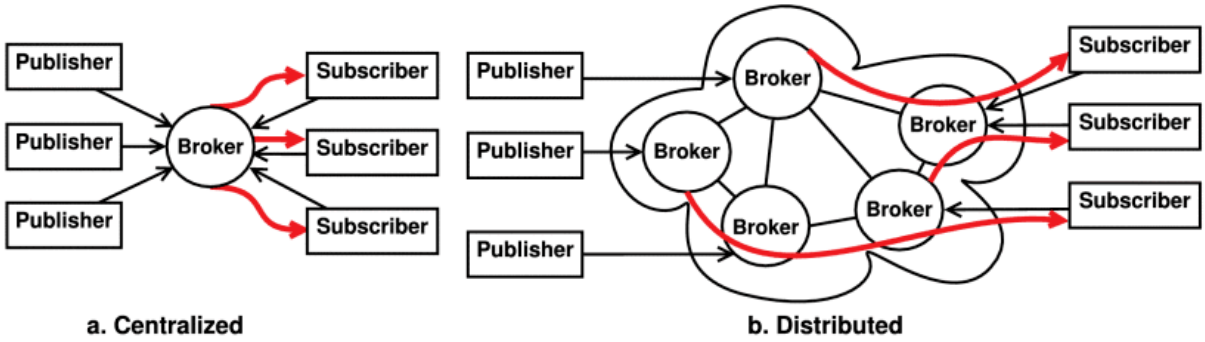

Figure 7: Publish-Subscribe System

src:ElHassan et al[17]

The usage of sensors and wireless technology for communication between the devices has lead to increased importance of wirless sensored networks in IoT.
Centralized pub/sub is more suitable for small network enterprise where as in case of large network consisting of many devices and heterogeneous data that uses topic-based filtering, Distributed pub/sub is very appropriate[17].

Example:
PubSub thermostat: Controlling the fan based on the temperature change in IoT system,where the devices in this system publish temperature data on their pubsub registry feeds and individual device IDs. A server python application, which can run from any machine, consumes the data from Cloud based on Pub/Sub topic and events. The server then decides whether to turn on or off the individual devices fans via a Cloud IoT Core configuration update[18].

2) Docker/Kubernetes:

Why is docker/kubernetes required in IoT Framework?

In recent years, cloud computing is an emerging field that deals with wide range of highly connected smart devices such as medical trackers,sensors,home appliances,and etc providing high computing power at low management effort.
As the developers deal with large number of devices,using containers can help them is many ways.

Containers are lightweight when compared to virtual machines that uses lightweight kernel namescapes and runs on Build,Ship and Run Paradigm and virtualize the operating system and not the hardware which can enable applications run in isolation without affecting other applications making easy to move,modify and deploy with high security and scalability.

The main idea of containers is to collect all the tools and libraries necessary to run a specific piece of software, and then isolating that software from the rest of the system. Because containers are not full-on virtual machines, they're efficient, and Docker which is lightweight,standalone, is a leader in making containers easy to work with and share with others by ensuring better security and easy development[19].

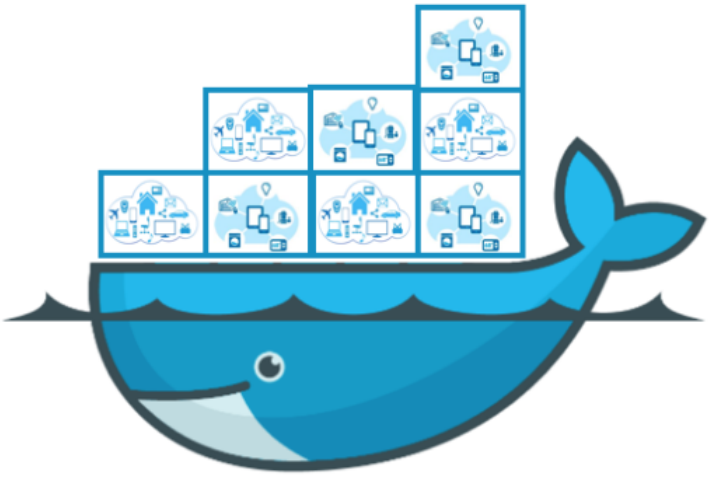

Figure 8: Docker Containers and IoT applications

src:[20]

Docker,"the worlds leading software container platform and a tool that helps to solve common problems like installing,removing,upgrading, distributing,trusting and managing software and provides a modern solution to tackle common software problems"[21].

It is easy to maintained and deployed upon the virtulization machines.In IoT Framework,Applications that run different services on many devices make it reasonable to utilize a technology providing easy deployment and high portability within a distributed system environment[21].

By using docker,the main challenges in IoT devices can be solved by enabling minimal hardware resources,highly scalable,distribution across the network, limited network access and heterogeneous device environments.

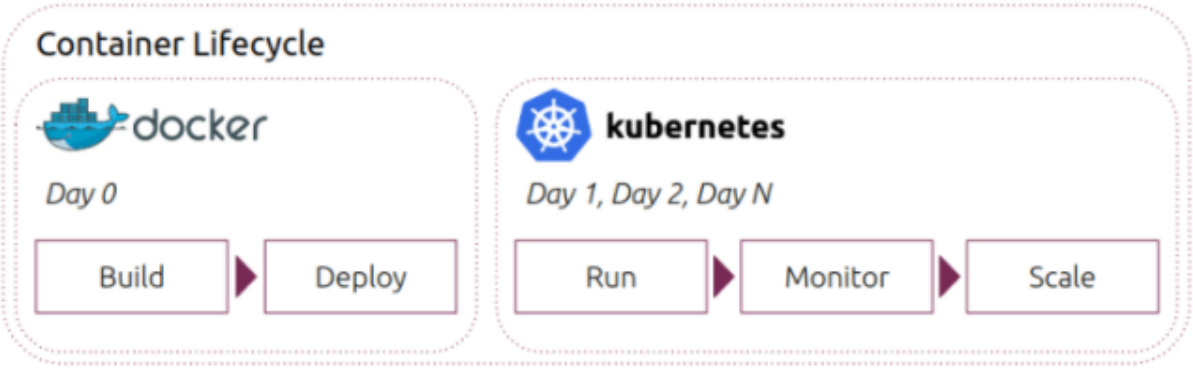

Figure 9: Docker and Kubernetes

src:[22]

To automate these functionalities on a large scale,Kubernetes,an open source platform is what is required which gives system admin more control on the containers for deploying,scaling,managing and automates the processes in containerized application.Kubernetes

benefits IoT as developers need not worry about the hardware or opeating system specifications and the property of self-healing makes the system more robust and reliable.With this ability,healthcare organizations in IoT platform implement both docker and kubernetes technology to reduce cost and time,provide high security,self-healing,quick deployment of application and highly scalable.

3) Privacy & Security:

Why privacy and security is important in IoT?

Privacy and security is one of the key challenges faced by IoT in order to ensure secure and encrypted communication among billions of devices collecting data through wireless network.Most of the security issues faced during communication are Malicious code injection,sniffing attack,Denial of service,proxy attack and etc.There are few other factors such as proxy attack and man-in-the-middle attack that occurs irrespective of the connectivity being encrypted or not[23].Hence it is necessary to ensure a secure and reliable communication protocols at all stack layers.

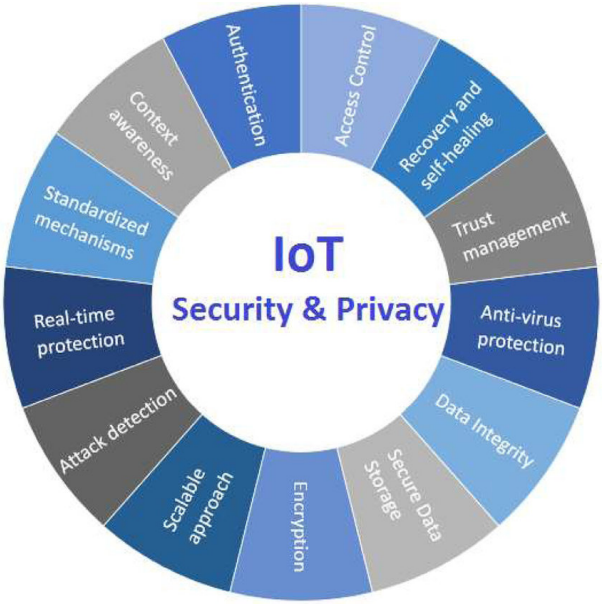

Figure 10: IoT security and privacy concerns

src:[23]

The new Fog computing framework allows storing and processing the data at edge/cloud-to-endpoint continuum by overcoming the limitation of IoT devices.In general distributed systems are more vulnerable to attacks when compared to centralized systems.
Cloud usually operates in heavily protected facilities and managed by cloud operators where as Fog needs to function in more vulnerable environments by meeting customers requirements.As fog has resources smaller when compared to cloud it may not protect itself because of limilited resources.
Hence there are many privacy and security issues in Fog architecture that has to be addressed such as authentication,secure communication,confidentiality and authorization.

Inspite of cloud-platform providing advanced cryptosystem to enhance security,it cannot be implemented on resource-constraint devices in Fog as many devices are located in various locations and the chances of malicious activities are high[24].
In order to deal with such problems,WebRTC(Web Real time communication) an open-source web-based application technology,is made use of which has the ability to deal with security issues in real-time communication by enabling and encouraging important security concepts at stack level.OpenTrust Protocol(OTrP) is used by applications to install,update,delete and manage security configurations.IPSec(Internet Protocol Security) is used in network layer which provides a end to end secure and transparent connection-oriented channel is used which is easier to run than TLS(Transport Layer security).Few applications rely on SSl(Secure socket layer) and DTLS(Datagram Transport Layer security) for secure data transmission.To deal with the Man-in-middle attack, media paths should be regularly monitored and should be coupled with encrypted signals for no spectical threat[23].

As the system grows large with enoromous data,it is always benificial to adapt lightweight protocols and encryption algorithms for better security in IoT environments and each object should check other's privacy policy for compatability before sharing data,as each system has its own privacy policies.Security and privacy is no longer an option but a must requirement in all fields.

V. Conclusion

The Rapid development in the field of internet and tehnology, IoT is changing our life by making things smarter and easier than ever before.According to Taylor[1],the proposed five-layered IoHT Framework consisting of perception,mist,fog,cloud and application layer provides an efficient,sustainable and evolved features by widening the boundries of internet for the interoperability between devices for anything,anytime and anywhere with advanced computing speed and scalability for usability in IoHT smart applications by enabling seperate routing paths to handle the real-time as well as conventional data generated by IoHT devices.This can help modern healthcare industries grow widely by providing services to the users through eHealthcare services inspite of reduced workforce.This also emphazises the importance of adapting modern technologies such as machine learning and data analytics to handle the increased complexity in computational analysis and ensure high QoS with low packet drop from the data generated by large heterogeneous medical devices and organizations. Also focuses on implementing few other factors such as privacy & security,usage on virtualization container technologies such as Docker & Kubernetes and making use of few middleware technologies such as Publish/subscribe system to the already existing famework that can help IoHT Framework work seemlessly with effective performance and scalable distribution of data for the IoHT based healthcare systems.

References

[1] M. Asif-Ur-Rahman, F. Afsana, M. Mahmud, M. S. Kaiser, M. R. Ahmed, O. Kaiwartya, and A. James-Taylor, "Toward a heterogeneous mist, fog, and cloud-based framework for the internet of healthcare things," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4049–4062, 2019.

[2] Wikipedia contributors, "Cloud computing — Wikipedia, the free encyclopedia," 2020, [Online; accessed 23-September-2020]. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Cloud_computing&oldid=979386752

[3] P. Mell, T. Grance *et al.*, "The nist definition of cloud computing," 2011.

[4] M. Chiang and T. Zhang, "Fog and iot: An overview of research opportunities," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 854–864, 2016.

[5] M. Mukherjee, L. Shu, and D. Wang, "Survey of fog computing: Fundamental, network applications, and research challenges," *IEEE Communications Surveys Tutorials*, vol. 20, no. 3, pp. 1826–1857, 2018.

[6] Radiocrafts. (2019) Cloud vs fog vs mist computing, which one should you use? [Online]. Available: https://radiocrafts.com/cloud-vs-fog-vs-mist-computing-which-one-should-you-use/

[7] I. VMware. (2020) Software-defined networking (sdn).

[8] I. T. Haque and N. Abu-Ghazaleh, "Wireless software defined networking: A survey and taxonomy," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 4, pp. 2713–2737, 2016.

[9] D. Pathak. (2018) Decoding the 11 business benefits of microsoft azure.

[10] A. M. Rahmani, T. N. Gia, B. Negash, A. Anzanpour, I. Azimi, M. Jiang, and P. Liljeberg, "Exploiting smart e-health gateways at the edge of healthcare internet-of-things: A fog computing approach," *Future Generation Computer Systems*, vol. 78, pp. 641–658, 2018.

[11] L. Syed, S. Jabeen, S. Manimala, and H. A. Elsayed, "Data science algorithms and techniques for smart healthcare using iot and big data analytics," in *Smart Techniques for a Smarter Planet*. Springer, 2019, pp. 211–241.

[12] C. McClelland. (2017) Applying machine learning to the internet of things. [Online]. Available: https://medium.com/iotforall/applying-machine-learning-to-the-internet-of-things-5bd0216d4cc3

[13] H. T. Ma, "A blood pressure monitoring method for stroke management," *BioMed research international*, vol. 2014, 2014.

[14] M. S. Virat, S. Bindu, B. Aishwarya, B. Dhanush, and M. R. Kounte, "Security and privacy challenges in internet of things," in *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*. IEEE, 2018, pp. 454–460.

[15] D. Happ, N. Karowski, T. Menzel, V. Handziski, and A. Wolisz, "Meeting iot platform requirements with open pub/sub solutions," *Annals of Telecommunications*, vol. 72, no. 1-2, pp. 41–52, 2017.

[16] G. cloud. (2020) What is pub/sub? [Online]. Available: https://cloud.google.com/pubsub/docs/overview

[17] F. T. El-Hassan and D. Ionescu, "Design and implementation of a hardware versatile publish-subscribe architecture for the internet of things," *IEEE Access*, vol. 6, pp. 31 872–31 890, 2018.

[18] M. DuPuy. (2017) Pubsub thermostat example. [Online]. Available: https://learn.adafruit.com/raspberry-pi-3-and-sensor-kit-for-google-cloud-iot-core/pubsub-thermostat-example

[19] J. Hans. (2017) Why putting the iot into docker containers will unlock it. [Online]. Available: https://www.rtinsights.com/docker-containers-for-the-iot/

[20] P. Singh. (2017) Docker containers and iot applications. [Online]. Available: https://iotbytes.wordpress.com/docker-containers-and-iot-applications/

[21] M. Großmann, S. Illig, and C. L. Matějka, "Sensiot: An extensible and general internet of things monitoring framework," *Wireless Communications and Mobile Computing*, vol. 2019, 2019.

[22] A. Chalkias. (2020) Kubernetes vs docker. [Online]. Available: https://ubuntu.com/blog/kubernetes-versus-docker

[23] A. Čolaković and M. Hadžialić, "Internet of things (iot): A review of enabling technologies, challenges, and open research issues," *Computer Networks*, vol. 144, pp. 17–39, 2018.

[24] K.-K. R. C. H. W. Ximeng Liu, Yang Yang, ""security and privacy challenges for internet-of-things and fog computing"," *Hindawi*, p. 3, 2018.