IETE Technical Review

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/titr20

Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies

Sahshanu Razdan & Sachin Sharma

To cite this article: Sahshanu Razdan & Sachin Sharma (2022) Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies, IETE Technical Review, 39:4, 775-788, DOI: 10.1080/02564602.2021.1927863

To link to this article: https://doi.org/10.1080/02564602.2021.1927863

Published online: 23 May 2021.

IETE TECHNICAL REVIEW
2022, VOL. 39, NO. 4, 775–788
https://doi.org/10.1080/02564602.2021.1927863

REVIEW ARTICLE

OPEN ACCESS

Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies

Sahshanu Razdan[1] and Sachin Sharma[2]

[1]School of Computing, National College of Ireland, Dublin, Ireland; [2]School of Electrical and Electronic Engineering, Technological University Dublin, Dublin, Ireland

ABSTRACT

In the Internet of Medical Things (IoMT), the Internet of Things (IoT) is integrated with medical devices, enabling improved patient comfort, cost-effective medical solutions, quick hospital treatments, and even more personalized healthcare. The paper first provides the introduction of IoMTs and then introduces an architecture of IoMTs. Later, it provides the current operations of the healthcare system and discusses the mapping of these operations into the architectural diagram. Further, several emerging technologies such as Physically Unclonable Functions (PUF), Blockchain, Artificial Intelligence (AI), and Software-Defined Networking (SDN) are envisioned as important technologies to overcome several challenges in e-healthcare such as security, privacy, accuracy, and performance. Finally, we provide three case studies for IoMT based on – (1) PUF-based Authentication, (2) AI-enabled SDN Assisted e-healthcare, and (3) Blockchain Assisted Patient Centric System. The solutions presented in this paper may have a huge impact on the speed at which IoMT infrastructure can efficiently evolve with market evolution.

KEYWORDS

Healthcare; Internet of Medical Things (IoMT); Internet of Things (IoT); Network architecture

1. INTRODUCTION

The Internet of Medical Things (IoMT) is the blend of medical devices with the Internet of Things (IoT). IoMTs are the future of current healthcare systems where every medical device will be connected and monitored over the Internet via healthcare professionals. This offers a faster and lower cost of health care as it evolves. Figure 1 shows an example of IoMTs where patient vitals are collected via sensor devices and sent to the IoMT applications through the Internet. The information then flows to the healthcare expert and medical staff and then a response is sent back to the needed patients.

During COVID-19 pandemic, there is currently a rise in telehealth practices due to physical distance guidelines which are compelling healthcare professionals to operate patients remotely through IoMT devices [1]. Further, Sustainable Development Goals (SDG) by 2030 was approved by the United Nations (UN) in 2015 [2]. Good health and well-being is an important goal in SDG. Currently, IoMT has the ability to fulfil the goal of good health and well-being. This paper is about providing an overview of IoMT, listing and presenting important emerging technologies such as PhysicallyUnclonable Functions (PUF), blockchain, Artificial Intelligence (AI) and Software-Defined Networking (SDN) in IoMT, and providing case studies of IoMTs. The contributions of this paper are as follows:

(1) Introducing a Cloud-Fog architecture to IoMT.
(2) Presenting review work on PUF, blockchain, AI, and SDN for e-healthcare.
(3) Proposing PUF, blockchain, AI, and SDN-based mapping for e-healthcare.
(4) Providing an experimental study to the case studies considering the above mapping in IoMT.

The paper is organized as follows: Section 2 provides introductory background to IoMT where the Internet of Things (IoT) and smart hospitals are discussed, Section 3 provides an architecture for IoMTs by having things, fog, and cloud layers. Section 4 introduces PUF, blockchain, AI, and SDN technologies for e-healthcare and maps these technologies with the architecture introduced for IoMT, Section 5 reviews the existing work in e-healthcare related to the considered technologies, Section 6 provides an overview and experimental studies of the case studies presented, finally, Section 7 concludes and provides ideas for future work.

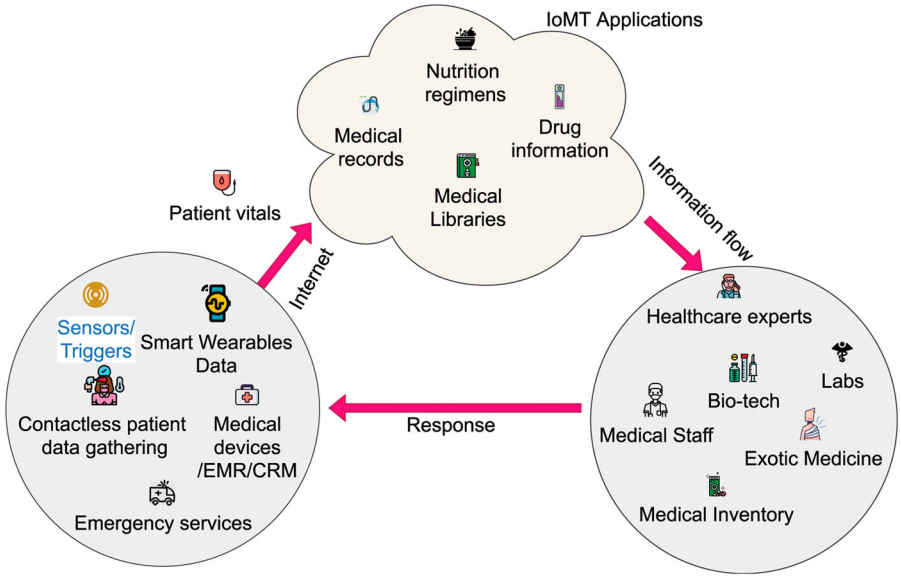


Figure 1: Internet of medical things (IoMT)

2. IOMT AND SMART E-HEALTHCARE

2.1 IoMT and Enabling Wireless Technologies

IoT systems consist of sensors and devices connected via a network of cloud ecosystems over high-speed connectivity between each module. The raw data collected at these devices/sensors is sent directly to the vast storage offered by cloud services. This data is further cleaned and then analysed to gain further insights into it. This requires additional software, tools, and applications which will further assist in visualization, analysis, processing, and management of the data.

Figure 2 shows several wireless technologies such as RFID (Radio Frequency Identification), NFC (Near Field Communications), Bluetooth, LTE (Long Term Evolution) and 5G/6G (and beyond) inter-linked with several

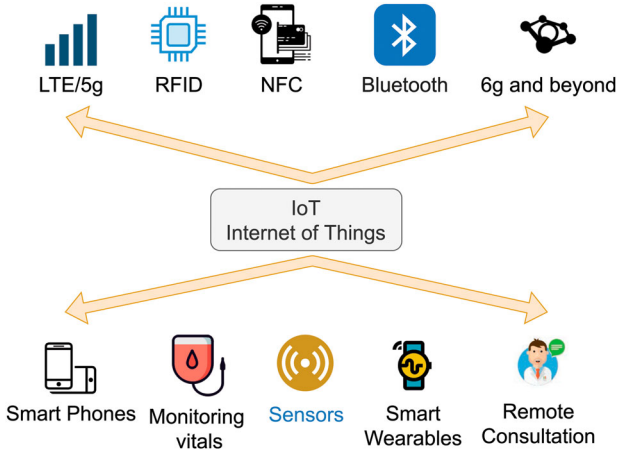


Figure 2: Internet of things, enabling technologies and devices

devices such as smartphones, monitoring devices, sensors, smart wearable, and other medical devices. Currently, the use of 5G/6G or beyond is prevalent in IoMT due to their high bandwidth and ultra-low latency benefits.

2.2 Smart E-healthcare

Smart hospitals are the hospitals that are built on intelligent automated and optimized modules (maybe based on AI/ML) on the ICT infrastructure to improve patient care procedures and to add new capabilities. There are several applications of smart hospitals such as telemedicine, telehealth, remote robot surgery. Telemedicine is to provide clinical care at a distant location, while telehealth is to provide non-clinical care at a distance. In remote robot surgery, medical robots perform surgery through instruction from the doctor sitting far away.

Figure 3 shows an example of a smart healthcare system in which the inbound data from various sources is first collected (*e.g.* through remote gathering or physical gathering) and sent to EHR (Electronic Health records systems). Data could be classified as unstructured if it is collected offline on paper as medical notes by the personnel. If the data is collected in a structured form from the devices and sensors by using predefined data fields for users to enter, then it becomes easy to process in further systems such as CRM (Customer Relational Management) System. The CRM brings to use the tools for analysing data and then assigning it to its predefined target in the ecosystem. The essential data and information from EHR systems is sent to the CRM system

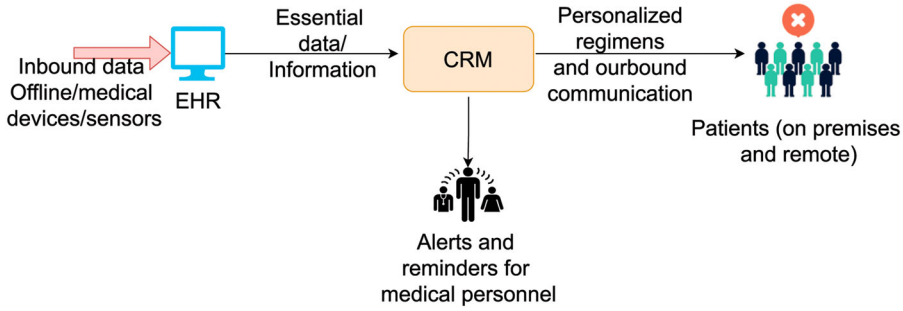


Figure 3: Example of smart e-healthcare system

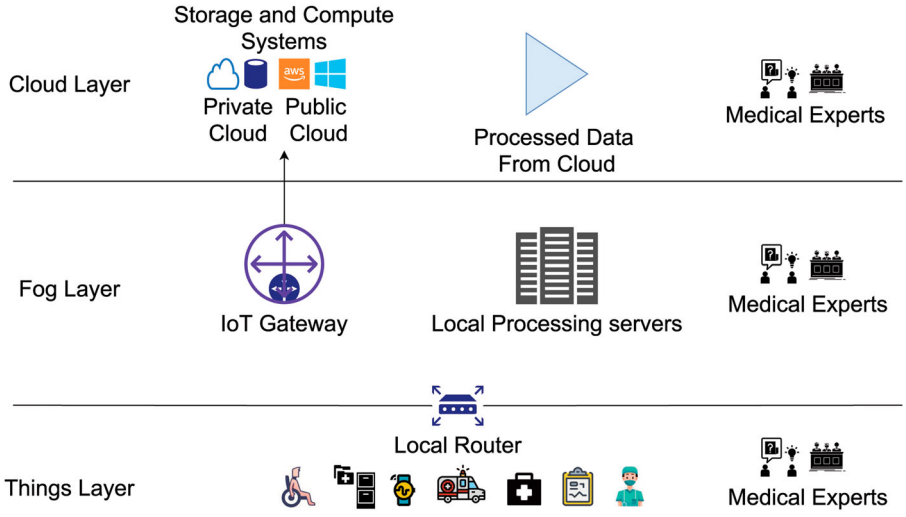


Figure 4: Operations within layers in IoMT

and it processes this patient data. This processed data generates further triggers to patients and medical personnel in the ecosystem. The patients receive outbound communication from hospitals and health experts in the form of personalised health regimens. The doctors and other medical staff get notified about the reminders and other alerts from the same CRM software in the ecosystem.

3. ARCHITECTURE FOR IOMT

The architecture for IoMTs consists of three layers (Figure 4). There are three layers: (1) things layer, (2) fog layer, and (3) cloud layer. This is a modified version of the architecture present in [3]. In this architecture, healthcare experts can also communicate directly through the router between the Thing layer and Fog layer and through the local processing servers at the fog layer. Each layer is described below:

(1) The things layer consists of patient monitoring devices, sensors, actuators, medical records, pharmacy controls, nutrition regimen generator, *etc*. This layer is directly in contact with the users of the ecosystem. The data from elements such as wearables, patient-monitoring data, remote care data is collected at this layer. The devices used at this should be securely placed to ensure integrity in the data collected. The local routers in the ecosystem are responsible for connecting these devices to the fog layer. The data is further processed at the fog and at the cloud layer to generate meaningful information. Further, in order to reduce the delay, the healthcare experts can get the patient data through this router.

(2) The fog layer operates between the cloud and the things layer. This layer consists of local servers and gateway devices for a sparsely distributed fog networking framework. The local processing power is harnessed by the lower layer devices for real-time response to their users. These servers are also used

to manage and administer the security and integrity of the system. The gateway devices at this layer are responsible for redirecting this data from these servers to the cloud layer for further processing. Further, in order to reduce the delay, the healthcare experts can get the patient data through this router.

(3) The cloud layer consists of data storage and computation resources for the data to be analysed and derive decision-making systems based on it. The cloud also offers a vast reach to incorporate huge medical and healthcare systems to handle their day-to-day operations with ease. This layer consists of cloud resources where the data generated from the medical infrastructure will be stored and analytical work could be performed as deemed necessary in the future.

4. EMERGING TECHNOLOGIES IN IOMTS

In this section, we discuss various technologies such as blockchain, PUF, AI, and SDN and their role in IoMT.

4.1 Blockchain Technology

Blockchain is a decentralized ledger recording transactions of computing nodes in the network. The IoMT has raised growth in distributed computing markets and blockchain offers a solution to many issues arising in the security of participating entities in the healthcare system built around it. The blockchain consists of blocks or nodes that are connected over a network wherein the information exchanged between any of the nodes in the networking is recorded and can further be used for cross-references. These blocks contain the information from previous blocks and this methodology helps in identifying the exact source of miscreants in the network. The blocks that are not identified in the network are thus discarded and thereby paving the way for blockchain being considered for use as a trusting strategy in information exchange systems such as IoMT [4].

Blockchain enables entities to interact with each other without the presence of a centralized authority in the network. The data entries in blockchain are stored as blocks of data. These blocks as stated earlier contain information about its nearest blocks in the chain with cryptography protocols to bundle them as used securely. These blocks and their data can be read by other users but the data in these blocks remain tamper-proof. Blockchain also enables smooth processing of smart contracts that do not need any central authority to trigger them [5]. These contracts are self-executable in design and thus require no supervision. A prevalent "smart contract" company is Ethereum facilitating their service on blockchain platforms [6].

A visual representation of various healthcare elements on the blockchain platform is shown in Figure 5. The role

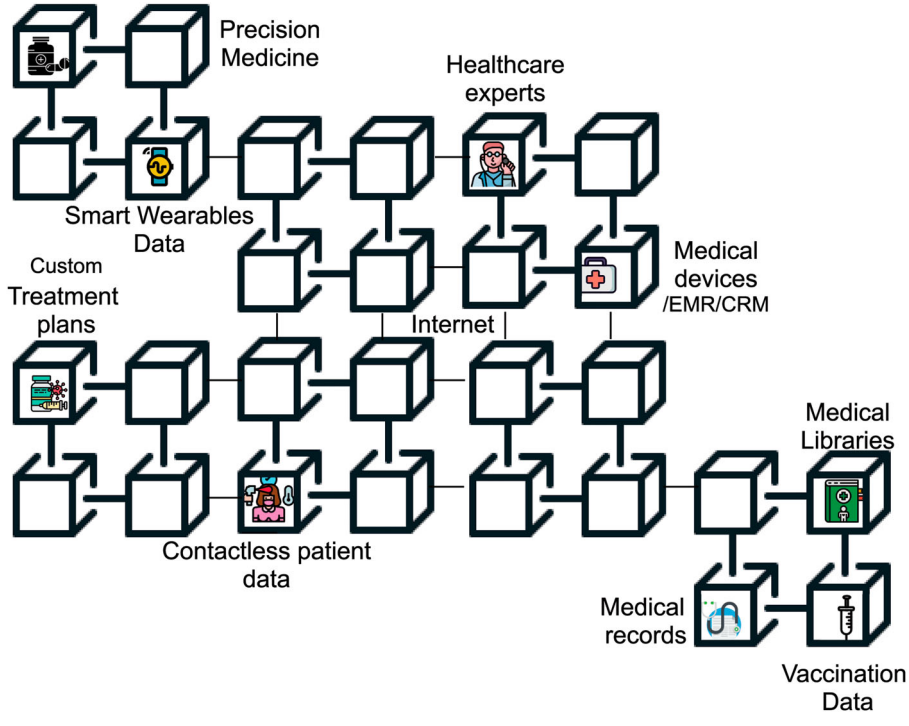


Figure 5: Use of blockchain in IoMTs

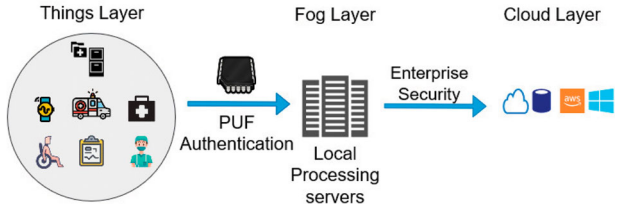


Figure 6: PUF devices enabled IoMTs

of blockchain in the healthcare sector to adopt solutions built around it requires infrastructure to be divided into smaller modules. These modules can then be integrated with the appropriate devices in the IoMT framework. The resultant system is going to be distributed in nature and would allow decentralization of power in the network. The benefit of deploying blockchain systems comes with a trust factor while the influx of data in the healthcare ecosystem is ever-growing. The blockchain promises to satisfy the ever-increasing demand for data-exchanges over the healthcare infrastructure. The use of blockchain is currently being tested for EHR systems in the hospitals followed by some clinical use trials around the world [7].

4.2 Physically Unclonable Function (PUF) Devices

PUF devices generate a unique fingerprint for the vulnerable elements in the IoMT ecosystem. These unique fingerprints/signatures arise from the variation in the fabrication of these devices. These fingerprints can be used for secret key generation (cryptography keys) to secure the devices and their data in the IoMT ecosystem where the end devices (sensors) are at risk of hardware tampering attacks [8]. Figure 6 encompasses mapping of PUF devices with the architecture introduced in the previous subsection. The PUF devices reside in the thing layer in our mapping. These devices play an important role when it comes to the authentication of IoMT devices in the ecosystem. As shown in Figure 6, after the fog layer, security is ensured by more specialized enterprise security solutions offered by service providers in the architecture (such as AI/ML-based).

4.3 AI in IoMT

Figure 7 shows several IoMT applications of AI, including Machine Learning (ML) and Natural Language Processing (NLP) in e-healthcare. Precision medicine requires advanced diagnostics and tailored regimens with quick delivery time. AI makes a compelling case for this by offering real-time solutions in determining new pathways for treating certain conditions based on historic and real-time data. The various features in the healthcare ecosystem can be modified by using AI-based solutions. These will include AI techniques for the creation of classifiers such as automatic capturing of patient information, scheduling patient appointments, determining lab tests, treatment plans, medications, surgical treatment, *etc*. These classifiers could further be trained and support decision-making processes. For other classifiers that cannot be recorded digitally, NLP offers methods to extract information from such unstructured data points in the infrastructure. These could come in the form of lab reports, physical examination notes, operative notes, and other discharge related information of the patients [9]. Further, machine learning predicts future conditions based on historical data. It applies supervised, unsupervised or reinforced learning to predict future conditions.

4.4 SDN in IoMT

The network part in IoMTs can be divided into two parts: (1) data plane and (2) control plane. The data plane forwards traffic towards its destination, while the control plane performs the necessary tasks that allow the data plane to make forwarding decisions. Software-Defined Networking (SDN) provides a standard way to communicate between the data plane and control plane. The examples of standard SDN protocols are OpenFlow, Open vSwitch Database Management protocol, and OpenFlow

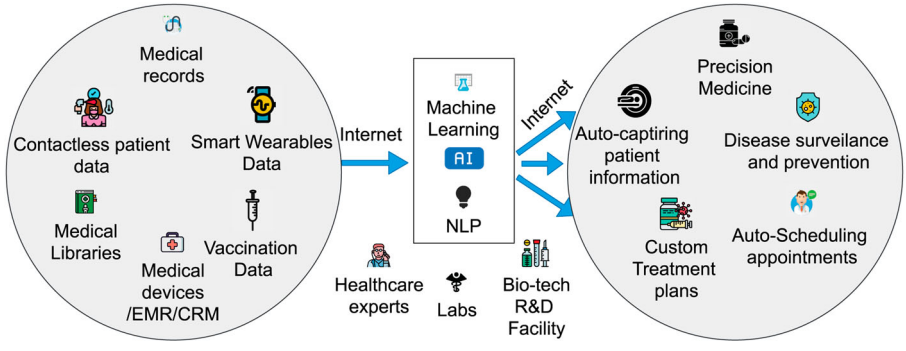


Figure 7: AI, machine learning and NLP enabled IoMTs

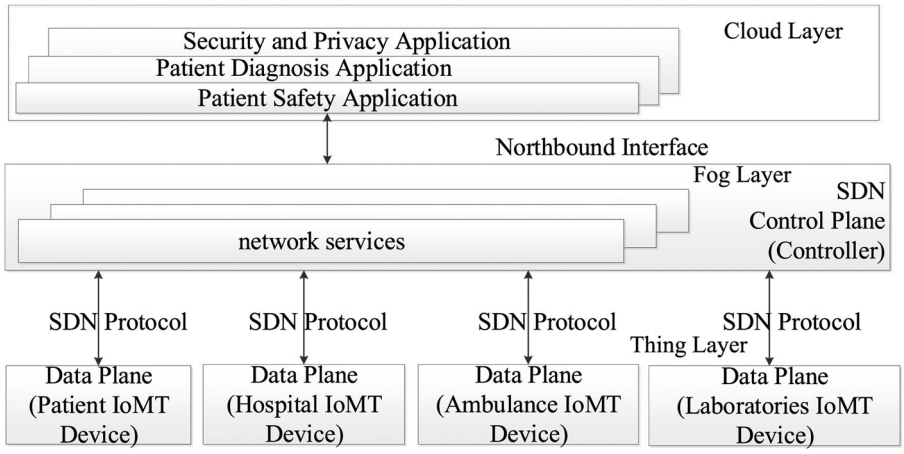


Figure 8: SDN enabled IoMTs

Configuration protocol (OF-CONFIG) [10]. As the interface between the data plane and control plane can be made standard using a standard SDN protocol, lots of different data of the data plane can be collected from an external server (may be located at the cloud) using the standard OpenFlow protocol. This enables the development of the different e-healthcare application, as they can reside on the cloud layer.

Figure 8 shows our proposed SDN enabled IoMTs, where IoMT devices are connected with e-healthcare applications, which may be located in the cloud, through the SDN control plane (it can be at fog layer). The SDN control plane collects the data from IoMT devices and provides it to an e-healthcare application. The e-healthcare application could be a security and privacy application, a patient diagnosis application or a patient safety application. Figure 8 also shows the northbound interface for the communication between the SDN control plane and an AI application. This interface is important for the collection of data from the control plane and the insertion of commands from the AI application to the IoMT device. The proposed architecture is a modified version of the architecture proposed for the Internet of Vehicles enabled with SDN [11].

5. RELATED WORKS

The use of sensors for the collection of data from parameters like temperature, ECG, blood pressure, pulse, and heartbeat has transformed the accuracy of the data and has eventually led to patients getting better service than before [12]. Patient monitoring systems have improved the response from healthcare experts as well. Table 1 provides an overview of the related work in the e-healthcare domain. The first column provides the reference number, the second column provides the enabling technologies used, the third column shows the features considered and the last column depicts the IoMT applications considered.

Table 1: Related work. HCC is Hepatocellular Carcinom

Ref.	Technologies	Feature	Applications
[12]	AI/ML	Analysis	Diagnosis
[13]	AI	Accuracy	COVID Screening
[14]	L-RNN	Missing Data	HCC
[15]	ML	Precision	Brain Tumor
[16]	AI, ML	Accuracy	Cardiovascular
[17]	AI	Selection NN	Spectrum Sharing
[18]	ML, blockchain	Accuracy, Security	Stress Level
[19]	Blockchain	Authentication	All
[20]	Blockchain	Security, Privacy	EHR/EMR/PHR
[21]	Blockchain	Security	EHR
[22]	Cryptography	Security	Medical Data
[23]	PUF	Privacy, Tracing	Host Tracing
[24]	PUF	Security, Sensing	Secure Sensing
[25]	PUF	Authentication	Telehealth
[26]	SDN, AI	Accuracy, Security	All
[27]	SDN	VR haptic behavior	Surgical Training
[28]	SDN, Scheduling	Performance	Health monitoring
[29]	SDN	Traffic flow	All

L-RNN is layered recurrent neural networks and EHR is electronic health record.

Reference works [12–17] show the applications of AI/ML for the e-healthcare domain. In [12], ML and AI solutions are used to augment the diagnosis and screening process of the identified COVID-19 patients with the help of "radio imaging" technology which works on similar methodology as "computed tomography (CT)", X-Ray, and blood sample data. Using deep convolutions neural networks, the diagnosis process of the coronavirus disease was sped up by many folds. This helped the experts designing customized solutions for treatment and control the spread in the early days. The vaccination studies are being carried out on such models to come up with an appropriate drug to fight against this virus. Further, in [13], deep learning-based methods were used to screen

COVID-19 patients through X-Rays and CT scans. The method has shown 100% accuracy in screening COVID-19 patients.

In [14], Layered Recurrent Neural Networks (L-RNN) are applied to predict the missing data in the Hepatocellular Carcinoma data. The problem with this research is that only two data sets were used to measure the accuracy of the method. In [15], several ML algorithms, association rule mining, *i.e.* Partial Tree (PART), Random Forest, Naive Bayes, and Random Tree are compared to detect brain tumour from the Magnetic resonance (MR) images. It is shown that PART outperforms other considered ML techniques in predicting brain tumours. In [16], several AI/ML methods are reviewed to monitor cardiovascular diseases. It was argued that most AI methods follow the black-box approach. Therefore, it is hard to know what is the reason for a specific outcome? The same concern is mentioned at [30, 31]. In [17], deep reinforcement learning and neural networks-based approaches were used to use the spectrum access, thereby meeting performance requirements in terms of latency, error rate, *etc*. Further, the need for big data analytics in overcoming other issues such as green and sustainable ICT has highlighted at [32, 33]. AI and ML solutions are also used to provide security and privacy in networks. For example, in [34], AI/machine learning-based method was proposed to detect DDoS and some privacy attacks.

In [18–21], the application of blockchain in attaining security is applied. In [18], ML-assisted blockchain-enabled architecture is proposed to detect and prevent stress in a secure manner. It is highlighted that the use of blockchain can enable security. The problem is that it is difficult to have blockchain-based solutions at IoMT end devices due to their resource overheads. Further, in [19], a blockchain-based authentication method is proposed for medical devices. The benefits of blockchain in the form of decentralization, reliability and security are highlighted in this work. Moreover, in [20, 21], the secure management of EHR (Electronic Health Record), EMR (Electronic Medical Records), and PHR (Personal Health Records) using blockchain is explored. This work shows its concern on how blockchain storage can cope with the practical needs of EHR/PHR/EMR. Further, in [22], cryptography methods (symmetric and asymmetric) are enhanced to meet the security requirements of medical data.

In [23–25], PUF-based devices are used to ensure security or privacy in the e-healthcare system. In [23], PUF-based host tracking system is proposed for contact tracing in the crowded area taking into account the privacy of COVID patients. In [24], PUF-based sensors are used to secure physical measurements. Further, [25], PUF-based sensor devices are used to securely monitor for COVID-19 patients.

Reference works [26–29] show the application SDN in IoMT in providing slicing and network management. In [26], an AI-enabled SDN application is implemented to detect malware botnets. Moreover, in [27], an SDN-based surgical training framework is proposed for IoMT. This framework will be useful in several telehealth services such as telemedicine, telesurgery, and surgical planning. In [28], an SDN-based Non-Orthogonal Multiple Access (NOMA)-based scheduling method is proposed. This considers the channel state, energy consumption, and delay. The results show advantages in terms of energy consumption, network delay, and effective throughput. Furthermore, in [29], an SDN-based e-healthcare management system is proposed with which different QoS requirements could be met using SDN based on different traffic requirements.

In [35], we come across various applications of IoMT in the context of COVID-19. The review offers an associated architecture and various other technologies that are deployed to mitigate the virus threat. The paper also highlights the development of new IoMT technologies merged with AI, Big data, and blockchain. Security and Privacy are shown as a major concern for IoMT.

Further, in [36], the authors have discussed the challenges faced by data-intensive ecosystems in the cyber-physical systems such as mobile healthcare environmental monitoring. The paper focuses on the security vulnerabilities and solutions for big data systems that will enable these future smart storage systems.

Our paper is different from the related work and other survey paper such as [35], as it reviews the previous work, implements the case studies (presented in the next section), and shows the applicability of these technologies in IoMT.

6. CASE STUDIES

This section presents case studies and analysis based on the experimental studies on PUF, AI-enabled SDN, and blockchain.

6.1 PUF-based Authentication for E-healthcare

Figure 9 presents an overview of our proposed PUF-based authentication framework where the e-health

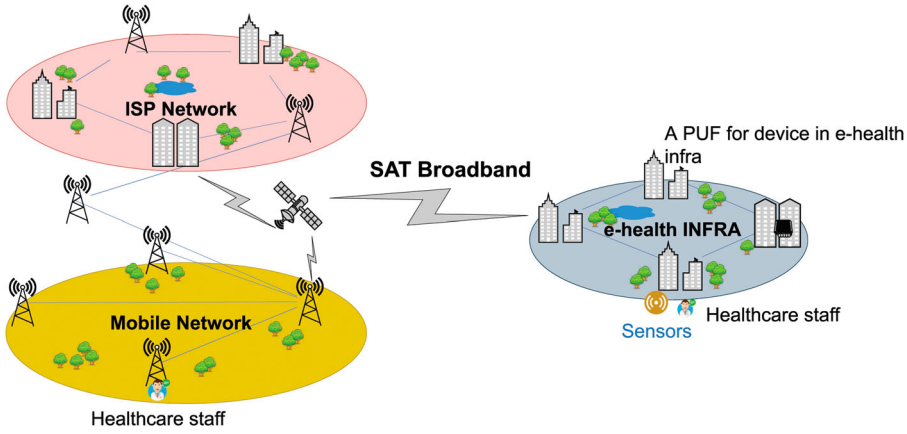


Figure 9: PUF-based authentication overview

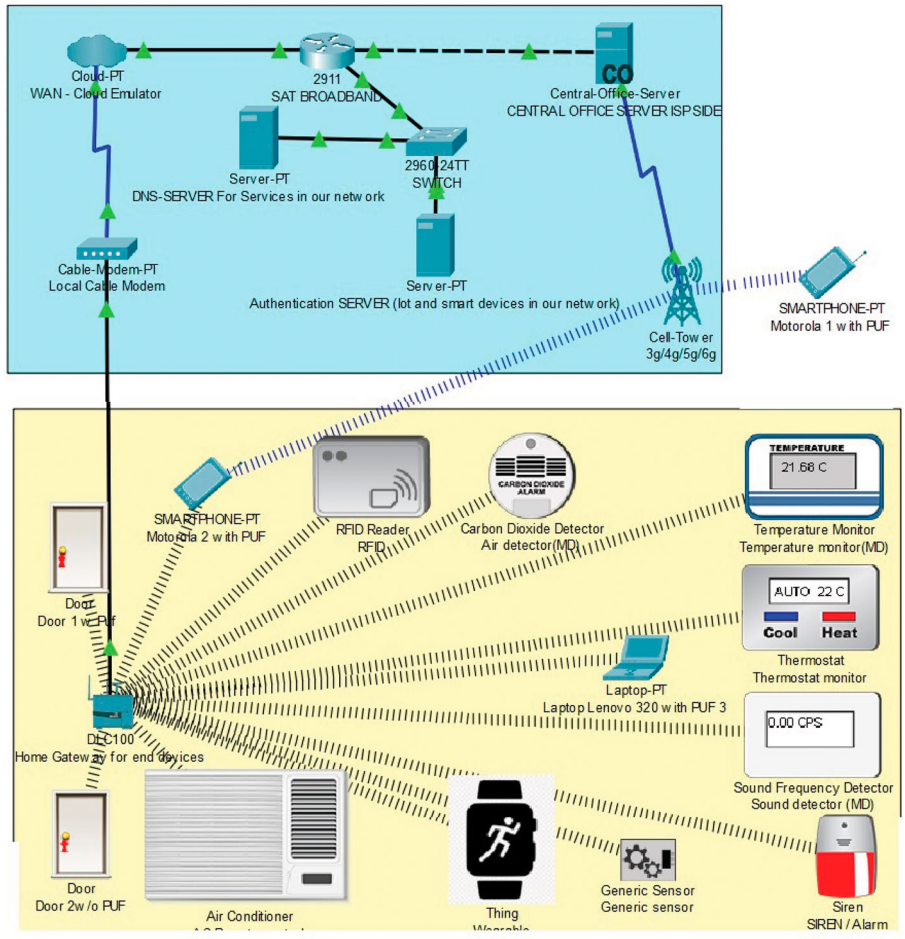


Figure 10: Detailed simulated topology over Cisco packet tracer

infrastructure containing IoMT PUF devices are connected over a satellite broadband network with ISP (Internet Service Provider) and mobile networks. Using this framework, we show that IoMT devices can be remotely authenticated and accessed by healthcare professionals on a remote device through a PUF-based mechanism. A detailed view of connected devices can be seen in Figure 10. In this case study, we use the Cisco packet tracer (a simulation tool) to simulate the framework.

Figure 10 shows all the IoMT devices located in the e-healthcare infrastructure. The topology is created by configuring a Satellite broadband router (SAT), which acts as

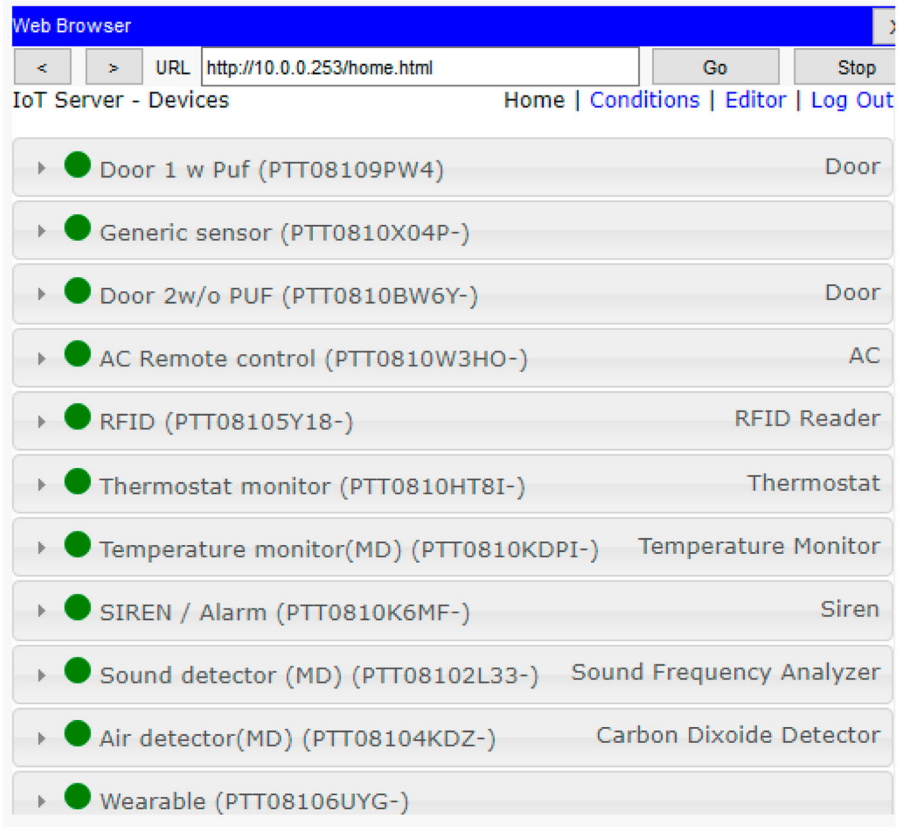


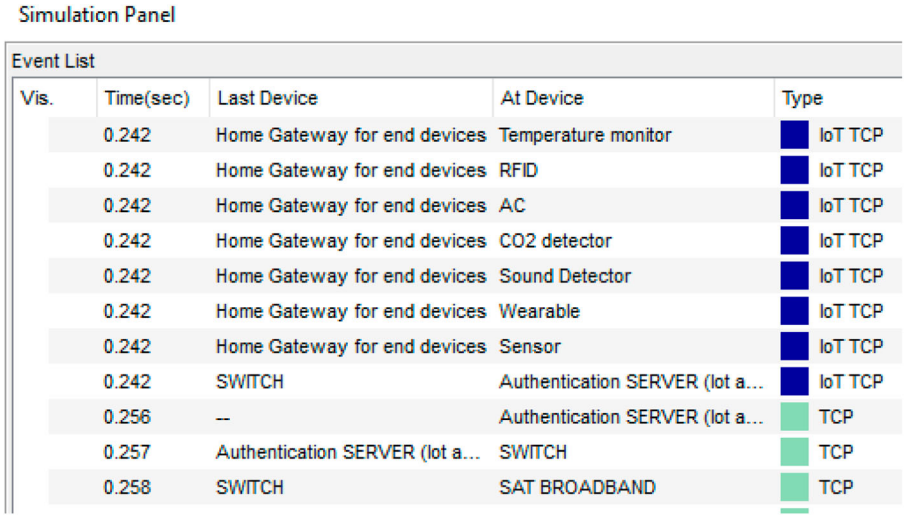
Figure 11: Remote server authentication

a pivot point for authentication of devices trying to connect in a fog-cloud architecture. We have added a WAN (Wide Area Network) Cloud Emulator for connecting the end devices to the services controlled from a far away simulated device in the network. A DLC100 Home Gateway is added in our topology for connecting end devices with our ISP over a Cable Modem-PT, which serves as a cable modem for redirecting traffic back and forth. The elements from the street network can be seen in the form of a Cell tower which serves as a 3G/4G/5G point for connecting smartphones.

For the representation of the authentication process, we have simulated 13 end devices that reside in an e-health ecosystem. To configure the end devices, we used DHCP IP configurations. The simulation aims at connecting the IoT device including IoMT devices in our environment to various other end devices based on a decentralized authentication server mechanism. We have thus established the topology that can be used to securely connect devices over a discrete channel such as a satellite broadband channel. For this purpose, we based our DNS servers and IoT authentication server on a satellite broadband channel which could discretely serve as an authentication channel.

For this case study, we based our IoMT authentication server on 10.0.0.253. This is where every device in our e-health infrastructure will get authenticated based on its credentials and associated PUF signature. An administrator account has been created for registration and remote operation of the devices. For the device, Motorola 1 with PUF the IPv4 Address, its DNS server (10.0.0.254), and the default gateway for packet transmission are configured and represented in 10. Similarly, for other end devices in our ecosystem like SmartPhone-PT Motorola 2 with PUF, Laptop-PT Lenovo 320 with PUF, IoT device DOOR with PUF, Wearable device, siren, temperature, and sound monitor, an RFID reader and an air detector, we have used similar configurations for IP generation. The state of these devices framework can be controlled remotely using other end devices like SmartPhone-PT Motorola 2 with PUF, Laptop-PT Lenovo 320 with PUF, SmartPhone-PT Motorola 1 with PUF.

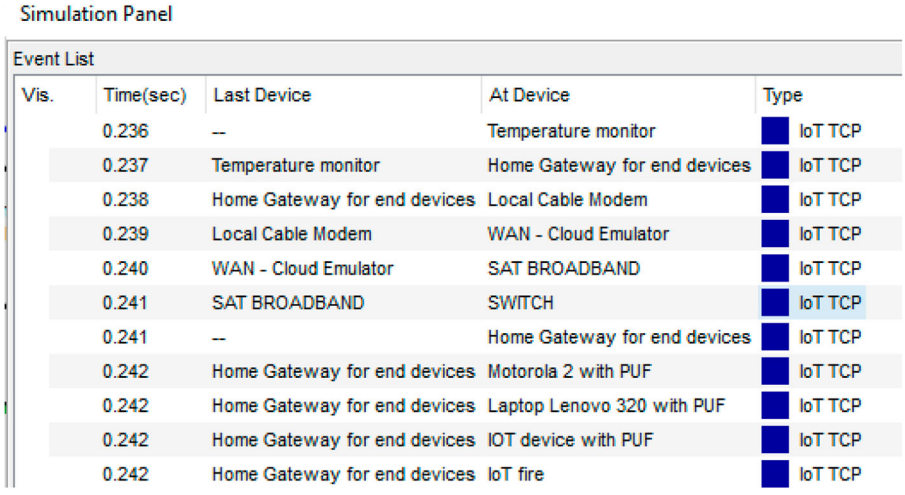
Figure 11 depicts the connection to a remote authentication server at IP address 10.0.0.253 hosting the registration server for our IoT devices in the e-health infrastructure. This can be seen clearly as we have connected all the other end devices in the same network. We have thus established the framework that can be used to securely


Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.242	Home Gateway for end devices	Temperature monitor	IoT TCP
	0.242	Home Gateway for end devices	RFID	IoT TCP
	0.242	Home Gateway for end devices	AC	IoT TCP
	0.242	Home Gateway for end devices	CO2 detector	IoT TCP
	0.242	Home Gateway for end devices	Sound Detector	IoT TCP
	0.242	Home Gateway for end devices	Wearable	IoT TCP
	0.242	Home Gateway for end devices	Sensor	IoT TCP
	0.242	SWITCH	Authentication SERVER (Iot a...	IoT TCP
	0.256	--	Authentication SERVER (Iot a...	TCP
	0.257	Authentication SERVER (Iot a...	SWITCH	TCP
	0.258	SWITCH	SAT BROADBAND	TCP

Figure 12: Authentication initiation time


Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.236	--	Temperature monitor	IoT TCP
	0.237	Temperature monitor	Home Gateway for end devices	IoT TCP
	0.238	Home Gateway for end devices	Local Cable Modem	IoT TCP
	0.239	Local Cable Modem	WAN - Cloud Emulator	IoT TCP
	0.240	WAN - Cloud Emulator	SAT BROADBAND	IoT TCP
	0.241	SAT BROADBAND	SWITCH	IoT TCP
	0.241	--	Home Gateway for end devices	IoT TCP
	0.242	Home Gateway for end devices	Motorola 2 with PUF	IoT TCP
	0.242	Home Gateway for end devices	Laptop Lenovo 320 with PUF	IoT TCP
	0.242	Home Gateway for end devices	IOT device with PUF	IoT TCP
	0.242	Home Gateway for end devices	IoT fire	IoT TCP

Figure 13: Authentication completion time

connect devices over a discrete satellite broadband channel. For authentication in an IoMT simulated environment, we have the "IoT TCP" event filtered out from the list of simulated events on our presented framework. We captured this event in simulation for 0.5 seconds and have presented the case study for authentication processing time in Figures 12 and 13. In Figure 12, we find the initiation of the authentication process at the 0.236th second for the event "IoT TCP" and in Figure 13 we find the same request for the device "temperature monitor" getting served at the 0.242th second. The device "temperature monitor" got captured in the simulation panel first requesting the server at 0.236th seconds and at 0.242th and the request was fulfilled. The time captured for this event is around 0.006 seconds for all other considered devices in the e-health infrastructure framework.

6.2 SDN Enabled E-healthcare

In this subsection, we provide a case study on SDN enabled E-healthcare where SDN is enabled in the IoMT devices and an SDN controller is placed at the cloud, as shown in Figure 8. In this case study, not all the IoMT devices have the Internet connectivity to connect with the controller. Therefore, those devices have not communicated with the controller through the other IoMT devices in the network. In [37], we provided an algorithm to automatically establish an SDN session between a wireless SDN connected network with the controller where only a few wireless devices can reach the controller directly. In this work, a standard OpenFlow protocol is used as an SDN protocol to connect with the controller. We applied the same algorithm to connect IoMT wireless devices with the controller. In this algorithm, hybrid SDN

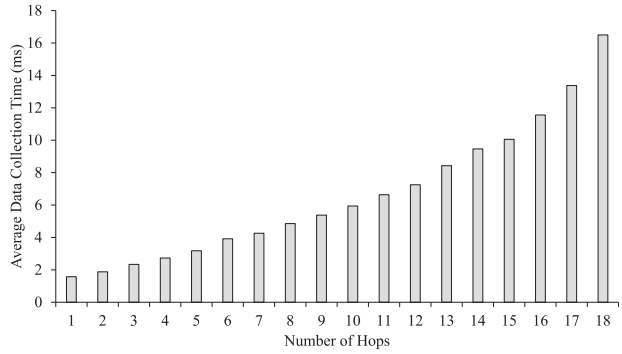


Figure 14: Data collection time (ms)

wireless IoMT devices are used where IoMT wireless devices can run traditional protocols as well as OpenFlow protocol. Traditional routing protocols such as OLSR (Optimized Link State Routing Protocol) is used as a protocol to find the path to the controller. The control paths are established on the path decided by traditional routing protocols and data paths are decided by the application running on the controller (see Figure 8).

We performed the emulations using Mininet-Wifi (an emulator for wireless SDN emulations). We created three different IoMT device topologies using 20 different IoMT sensor devices: (1) linear, (2) sparse, and (3) dense and the SDN session creation time is calculated. It is shown that as the number of hops between an IoMT device and the controller increases, the SDN session establishment time increases. Further, we calculated the data collection time in SDN. Figure 14 shows the data collection time. It is shown that data collection time is as short as 16 ms for an IoMT device which 18 hops away from the controller. It shows the short time of SDN in collecting data from wireless IoMT devices even though the device is far away. The future work is to apply AI solutions for issues *e.g.* security issues of IoMT devices.

6.3 Blockchain Assisted Patient-Centric System

In this case study, our goal is to show how blockchain could be used to ensure the security and privacy of EHR (Electronic Health Records) in the e-healthcare industry. In this subsection, we briefly describe our implemented blockchain assisted patient-centric system. Additional detail of this case study can be found at [38].

Figure 15 shows a blockchain assisted patient-centric system. The case study makes use of a smart contract on an Ethereum consortium blockchain to shift patient's health records being managed and controlled by the healthcare industry to a patient-centric application. Using this system, patients are in control of their health data. Figure 15 shows the administrator entity in the user-end in addition to patients and hospitals. This entity is responsible for the registration of the hospital entities in the blockchain framework. Hospitals registered with the blockchain framework could securely share patient data with the proposed patient-centric system using the web application in the front end. Once the data is shared with the system, patients are in charge of the data and can share it with any other doctors or hospital entities registered with the Ethereum blockchain patient-centric system. This data is stored on the distributed ledger. In [38], we measured the performance and security of this system. It was shown that using the Ethereum blockchain, security could be ensured and performance could be maintained. The delay in accessing such data was less than 1 second.

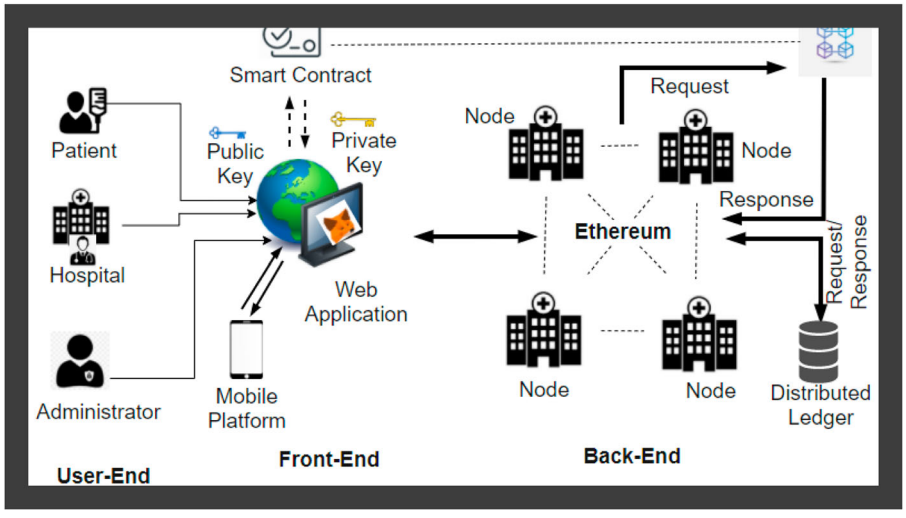


Figure 15: Blockchain assisted patient centric system [38].

7. CONCLUSION

In this paper, we provided details about the Internet of Medical Things (IoMT) and presented an architecture for IoMTs. Further, emerging technologies – PUF, Blockchain, Artificial Intelligence and Software-Defined Networking – are investigated for different aspects of IoMTs such as security, privacy, diagnosis, and treatment. Finally, we provided three case studies of IoMTs considering these technologies. The experimental results show the applicability of these technologies in the e-healthcare system for authentication, security, performance, or data collection time.

Health systems currently face challenges related to shortages of critical medical professionals, long waiting times, rising demand for services, and financial constraints. IoMT could help in easing some constraints by shortening the time healthcare experts invest in repetitive activities (using AI methods), thus allowing them to focus on other activities, such as seeing more patients.

In the PUF authentication case study where we established a framework for authentication of IoT devices in the e-health ecosystem, we found that authentication bottlenecks at satellite broadband pivot point. So in the future, we will divide the authentication process into three stages. In the first stage, we will define the authentication process on the credentials-based PUF signature and then continue the authenticating from there onwards. In the second stage, we will focus upon the actual pivoting point in our framework and use a distributed network topology. In the final stage, we will compare the actual computation costs of the authentication process and deploy such a mechanism wherever possible in the ecosystem.

In the case of the blockchain assisted patient-centric system, scalability is the problem. The system can saturate with the number of patients and hospital devices registered with the considered blockchain framework. The problem with SDN solutions will be that each device cannot be made SDN enabled. This means that the gathering of important data will be a challenge. Further, current AI-based solutions follow the black-box approach. These solutions need to be explained so that patients and doctors can understand why decisions are made and why they are important. Currently, researchers are applying methods to make AI accountable [30, 31]. However, the work is in the initial stage currently. Future work could be focused on making AI accountable for IoMTs. Further, there is concern related to the performance efficiency of AI applications.

DISCLOSURE STATEMENT

No potential conflict of interest was reported by the author(s).

ORCID

Sachin Sharma http://orcid.org/0000-0002-8358-2258

REFERENCES

1. Koonin L. M. *et al.*, "Trends in the use of telehealth during the emergence of the covid-19 pandemic – united states, January-March 2020," *Morb. Mortal. Wkly. Rep.*, Vol. 69, pp. 1595–1599, 2020.

2. Wu J., Guo S., Huang H., Liu W. and Xiang Y., "Information and communications technologies for sustainable development goals: State-of-the-art, needs and perspectives," *IEEE Commun. Surv. Tutor.*, Vol. 20, no. 3, pp. 2389–2406, 2018.

3. Naresh V. S., Pericherla S. S., Rama Murty P. S. and Reddi S., "Internet of things in healthcare: Architecture, applications, challenges, and solutions," *Comput. Syst. Sci. Eng.*, Vol. 35, no. 6, pp. 411–421, 2020.

4. Wang Q., Zhu X., Ni Y., Gu L. and Zhu H., "Blockchain for the IoT and industrial IoT: A review," *Internet Things*, Vol. 10, pp. 100081, 2020. Special Issue of the Elsevier IoT Journal on Blockchain Applications in IoT Environments.

5. Taylor P. J., Dargahi T., Dehghantanha A., Parizi R. M. and Raymond Choo K.-K., "A systematic literature review of blockchain cyber security," *Digit. Commun. Netw.*, Vol. 6, no. 2, pp. 147–156, 2020.

6. Singh A., Parizi R. M., Zhang Q., Choo K.-K. R. and Dehghantanha A., "Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities," *Comput. Security*, Vol. 88, p. 101654, 2020.

7. Dilawar N., Rizwan M., Ahmad F. and Akram S., "Blockchain: Securing internet of medical things (IoMT)," *Int. J. Adv. Comput. Sci. Appl.*, Vol. 10, p. 1, 2019.

8. Shamsoshoara A., Korenda A., Afghah F. and Zeadally S., "A survey on physical unclonable function (PUF)-based security solutions for internet of things," 183, p. 107593, 2020.

9. Ahmed Z., Mohamed K., Zeeshan S. and Dong X., "Artificial intelligence with multi-functional machine learning platform development for better healthcare and precision medicine," *Database*, Vol. 2020, p. baaa010, 2020.

10. S. Sharma. "Towards high quality and flexible future internet architectures," Ghent: Ghent University, Faculty of Engineering and Architecture, 2016.

11. Sharma S., "Towards artificial intelligence assisted software defined networking for internet of vehicles," in *Intelligent Technologies for Internet of Vehicles, Internet of Things*, N. Magaia *et al.*, Eds. Springer Nature Switzerland AG, 2021.

12. Lalmuanawma S., Hussain J. and Chhakchhuak L., "Applications of machine learning and artificial intelligence for Covid-19 (SARS-CoV-2) pandemic: A review," *Chaos Solitons Fractals*, Vol. 139, p. 110059, 2020.

13. Sedik A., Hammad M., Abd El-Samie F. E., Gupta B. B. and Abd El-Latif A. A., "Efficient deep learning approach for augmented detection of coronavirus disease," *Neural Comput. Appl.*, Vol. 2021, pp. 1–18, 2021.

14. Turabieh H., Abu Salem A. and Abu-El-Rub N., "Dynamic L-RNN recovery of missing data in IoMT applications," *Future Gener. Comput. Syst.*, Vol. 89, pp. 575–583, 2018.

15. Khan S. R., Sikandar M., Almogren A., Ud Din I., Guerrieri A. and Fortino G., "IoMT-based computational approach for detecting brain tumor," *Future Gener. Comput. Syst.*, Vol. 109, pp. 360–367, 2020.

16. Kilic A., "Artificial intelligence and machine learning in cardiovascular health care," *Ann. Thorac. Surg.*, Vol. 109, no. 5, pp. 1323–1329, 2020.

17. Song H., Bai J., Yi Y., Wu J. and Liu L., "Artificial intelligence enabled internet of things: Network architecture and spectrum access," *IEEE Comput. Intell. Mag.*, Vol. 15, no. 1, pp. 44–51, 2020.

18. Rachakonda L., Bapatla A. K., Mohanty S. P. and Kougianos E., Sayopillow: A blockchain-enabled, privacy-assured framework for stress detection, prediction and control considering sleeping habits in the IoMT, 2020. Available: arXiv:abs/2007.07377.

19. F. Fotopoulos, V. Malamas, T. K. Dasaklis, P. Kotzanikolaou, and C. Douligeris. "A blockchain-enabled architecture for IoMT device authentication," in 2020 IEEE Eurasia Conference on IoT, Communication and Engineering (ECICE), Yunlin, Taiwan, 2020, pp. 89–92.

20. Esposito C., De Santis A., Tortora G., Chang H. and Choo K.-K. R., "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Comput.*, Vol. 5, no. 1, pp. 31–37, 2018.

21. Girardi F., De Gennaro G., Colizzi L. and Convertini N., "Improving the healthcare effectiveness: The possible role of EHR, IoMT and blockchain," *Electronics*, Vol. 9, no. 6, pp. 884, 2020.

22. Noura M., "Efficient and secure cryptographic solutions for medical data," Theses, Univ. Bourgogne Franche-Comté, July 2019.

23. Yanambaka V. P., Abdelgawad A. and Yelamarthi K., "PIM: A PUF based host tracking protocol for privacy aware contact tracing in crowded areas," *IEEE Consum. Electron. Mag.*, pp. 1–1, 2021.

24. Ma H., Gao Y., Kavehei O. and Ranasinghe D. C., "A PUF sensor: Securing physical measurements," in *IEEE PerCom Workshops*, 2017, pp. 648–653.

25. Masud M., Singh Gaba G., Alqahtani S., Muhammad G., Gupta B. B., Kumar P. and Ghoneim A., "A lightweight and robust secure key establishment protocol for internet of medical things in COVID-19 patients care," *IEEE Internet Things J.*, pp. 1–1, 2020.

26. Liaqat S., Akhunzada A., Shaikh F. S., Giannetsos A. and Jan M. A., "SDN orchestration to combat evolving cyber threats in internet of medical things (IoMT)," *Comput. Commun.*, Vol. 160, pp. 697–705, 2020.

27. Cecil J., Gupta A., Pirela-Cruz M. and Ramanathan P., "An IoMT based cyber training framework for orthopedic surgery using next generation internet technologies," *Inform. Med. Unlocked*, Vol. 12, pp. 128–137, 2018.

28. Askari Z., Abouei J., Jaseemuddin M. and Anpalagan A., "Energy efficient and real-time NOMA scheduling in IoMT-based three-tier WBANs," *IEEE Internet Things J.*, pp. 1–1, 2021.

29. S. Badotra, D. Nagpal, S. Narayan Panda, S. Tanwar, and S. Bajaj. "IoT-enabled healthcare network with SDN," in 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2020, pp. 38–42.

30. Sharma S., Nag A., Cordeiro L., Ayoub O., Tornatore M. and Nekovee M., "Towards explainable artificial intelligence for network function virtualization," in *Proceedings of the 16th International Conference on Emerging Networking EXperiments and Technologies*. New York, NY: Association for Computing Machinery, 2020, pp. 558–559.

31. W. Guo. "Partially explainable big data driven deep reinforcement learning for green 5G UAV," in *ICC 2020 – 2020 IEEE International Conference on Communications (ICC)*, Dublin, Ireland, 2020, pp. 1–7.

32. Wu J., Guo S., Li J. and Zeng D., "Big data meet green challenges: Big data toward green applications," *IEEE Syst. J.*, Vol. 10, no. 3, pp. 888–900, 2016.

33. Wu J., Guo S., Li J. and Zeng D., "Big data meet green challenges: Greening big data," *IEEE Syst. J.*, Vol. 10, no. 3, pp. 873–887, 2016.

34. A. Abdelkefi, Y. Jiang, and S. Sharma. "SENATUS: An approach to joint traffic anomaly detection and root cause analysis," in *2018 2nd Cyber Security in Networking Conference (CSNet)*, Paris, France, 2018, pp. 1–8.

35. Mohd Aman A. H., Hassan W. H., Sameen S., Attarbashi Z. S., Alizadeh M. and Latiff L. A., "IoMT amid COVID-19 pandemic: Application, architecture, technology, and security," *J. Netw. Comput. Appl.*, Vol. 174, p. 102886, 2021.

36. Atat R., Liu L., Wu J., Li G., Ye C. and Yang Y., "Big data meet cyber-physical systems: A panoramic survey," *IEEE Access*, Vol. 6, pp. 73603–73636, 2018.

37. S. Sharma, and M. Nekovee. "Demo abstract: A demonstration of automatic configuration of openflow in wireless ad hoc networks," in *IEEE INFOCOM 2019 – IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Paris, France, 2019, pp. 953–954.

38. Fatokun T., Nag A. and Sharma S., "Towards a blockchain assisted patient owned system for electronic health records," *Electronics*, Vol. 10, no. 5, pp. 580, 2021.

AUTHORS

Sahshanu Razdan is currently a student at National College of Ireland, pursuing his masters degree in cloud computing. Prior to this, he worked at CloudAge and Innovation Diagnostic Labs Pvt. Ltd, Pune on big data and cloud projects for 3 years. His current research interests include the design and evaluation of authentication frameworks in cloud-fog computing, internet of things and internet of medical things.

Email: x19177453@student.ncirl.ie

Sachin Sharma is working as a lecturer in Communications Engineering at Technological University Dublin. Prior to this, he worked as a lecturer in computing and a programme director at the National College of Ireland. He performed his post-doctoral research as an experienced researcher at NEC Laboratories Europe. He holds the Doctor of Philosophy (PhD) degree in computer science engineering from Ghent University, Belgium and the Master of Technology (MTech) degree in computer applications from Indian Institute of Technology, Delhi, India. His current research interests include the design and evaluation of software defined networks, network function virtualization, ad hoc networks, machine learning and internet of things.

Corresponding author. Email: Sachin.Sharma@TUDublin.ie