Hindawi
Journal of Sensors
Volume 2022, Article ID 1863838, 30 pages
https://doi.org/10.1155/2022/1863838

Review Article

A Taxonomy on Smart Healthcare Technologies: Security Framework, Case Study, and Future Directions

Sachi Chaudhary,[1] **Riya Kakkar**,[1] **Nilesh Kumar Jadav**,[1] **Anuja Nair**,[1] **Rajesh Gupta**,[1] **Sudeep Tanwar**,[1] **Smita Agrawal**,[1] **Mohammad Dahman Alshehri**,[2] **Ravi Sharma**,[3] **Gulshan Sharma**,[4] **and Innocent E. Davidson**[5]

[1]*Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat 382481, India*
[2]*Department of Computer Science, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia*
[3]*Centre for Inter-Disciplinary Research and Innovation, University of Petroleum and Energy Studies, P.O. Bidholi Via-Prem Nagar, Dehradun 248001, India*
[4]*Department of Electrical Engineering Technology, University of Johannesburg, Johannesburg 2006, South Africa*
[5]*Department of Electrical Power Engineering, Durban University of Technology, Steve Biko Campus, Durban 4001, South Africa*

Correspondence should be addressed to Anuja Nair; anuja.nair@nirmauni.ac.in, Sudeep Tanwar; sudeep.tanwar@nirmauni.ac.in, Smita Agrawal; smita.agrawal@nirmauni.ac.in, and Innocent E. Davidson; innocentd@dut.ac.za

Received 17 December 2021; Accepted 22 June 2022; Published 5 July 2022

Academic Editor: Paulo Jorge Sequeira Gonçalves

There is a massive transformation in the traditional healthcare system from the specialist-centric approach to the patient-centric approach by adopting modern and intelligent healthcare solutions to build a smart healthcare system. It permits patients to directly share their medical data with the specialist for remote diagnosis without any human intervention. Furthermore, the remote monitoring of patients utilizing wearable sensors, Internet of Things (IoT) technologies, and artificial intelligence (AI) has made the treatment readily accessible and affordable. However, the advancement also brings several security and privacy concerns that poorly maneuvered the effective performance of the smart healthcare system. An attacker can exploit the IoT infrastructure, perform an adversarial attack on AI models, and proliferate resource starvation attacks in smart healthcare system. To overcome the aforementioned issues, in this survey, we extensively reviewed and created a comprehensive taxonomy of various smart healthcare technologies such as wearable devices, digital healthcare, and body area networks (BANs), along with their security aspects and solutions for the smart healthcare system. Moreover, we propose an AI-based architecture with the 6G network interface to secure the data exchange between patients and medical practitioners. We have examined our proposed architecture with the case study based on the COVID-19 pandemic by adopting unmanned aerial vehicles (UAVs) for data exchange. The performance of the proposed architecture is evaluated using various machine learning (ML) classification algorithms such as random forest (RF), naive Bayes (NB), logistic regression (LR), linear discriminant analysis (LDA), and perceptron. The RF classification algorithm outperforms the conventional algorithms in terms of accuracy, i.e., 98%. Finally, we present open issues and research challenges associated with smart healthcare technologies.

1. Introduction

Over the past decade, the healthcare industry has witnessed a drastic improvement in treatment procedures and methodologies. It majorly comprises healthcare professionals, medical equipment, laboratories, etc., to provide appropriate medical facilities for the patients [1, 2]. In the traditional healthcare system, patients have to be present physically to interact with doctors for their treatment [3]. But, as estimated in [4], it is getting challenging for the traditional healthcare system to monitor a huge number of patients with chronic diseases. Especially, approximated in the

research study [4], with the increase in population, senior citizens are going to be most affected by a serious illness in the next 20 years. Due to this, they have to regularly get their checkup done or meet doctors, which involve the endurance of high costs for the medical treatments. As predicted from the year 2017 to 2027, costs involved in healthcare in the USA are going to witness a huge increase from 17.9% to 19.4% of the GDP [5]. Therefore, healthcare systems have to monitor patients to handle a huge number of patients with chronic diseases and make the treatment affordable and easily accessible to them. Otherwise, due to delay in treatment or cost issues, patient may not get the required medical treatment for their illness [1–6].

Therefore, the traditional healthcare system is gradually digitizing into the smart healthcare system with the advancement in the Internet of Things (IoT), smart devices, and emerging information technology (IT) [7]. A smart healthcare system helps doctors to monitor patients remotely. As mentioned earlier, patients have to meet or get an appointment to communicate with the doctors depending on their illness regularly. It can be difficult for a person with a physical disability to depend on someone to get their checkup done by the doctors. So, smart healthcare systems help to keep track of patients' health with early identification of illness, reduced traveling, lowered hospital costs, less burden on hospital staff, etc., with the help of emerging technologies [8]. According to [9], smart healthcare can be defined as communication between patients and doctors to monitor patient's health regularly. The smart healthcare system can observe patients' health at a distance based on the two principles using various technologies and smart devices. One such principle is using wearable and implantable devices (WID) combined with sensors, IoT, and artificial intelligence (AI) which can be used to communicate a patient's body symptoms or traits wirelessly [9]. Nowadays, doctors are utilizing wireless sensor networks such as wireless body area networks (WBAN) to monitor patients' health and provide them reliable and efficient treatment [8, 10].

Another principle can be the utilization of advanced IT techniques such as IoT, cloud, and big data to process and extract the filtered data about the patient's health and illness symptoms from the WID with the help of WBAN [11]. This data can be further transmitted to the healthcare professionals or staff to monitor the patient's health accordingly. For example, if a patient is suffering from an incurable disease, they can be immediately admitted to the hospital by informing their staff about the situation. But, if the patient can be treated remotely by providing them with some prescription, then it can reduce the burden on medical staff and also reduce the costs for patients traveling, leading to a decrease in their overall costs [12].

Therefore, smart healthcare and its advanced technologies completely digitize the traditional healthcare industry so that healthcare professionals can keep track of patients' body symptoms to cure the disease accordingly. Many researchers have surveyed various smart healthcare technologies using different wearable sensors and devices. For example, Balakrishnan [13] presents a brief survey on IoT-based frameworks to monitor patients' health using edge or fog computing technologies for intelligent healthcare. Sadawi et al. [14] conducted a survey on IoT and blockchain-based architecture to ensure the security and efficiency in the system using dew and cloudlet computing. It mainly focuses on providing privacy and efficiency for the healthcare or supply chain management sector [15, 16].

Later, Dong and Yao [17] also presented an extensive IoT-based survey to control and prevent COVID-19 combined with fog-cloud platform. They have reviewed the various technologies such as AI, big data, and fog computing to prevent the effect of COVID-19. The authors in [18] present a comprehensive survey on machine learning-based big data analytics for IoT smart healthcare systems to overcome the challenges of the traditional healthcare system. Sobhan et al. [19] also surveyed machine learning techniques integrated with various sensors and their technologies to monitor patients remotely if they are suffering from heart or breathing-related diseases.

Now, most researchers have presented architecture to overcome the security and privacy issues of the smart healthcare system for remote patient monitoring. But, they have not discussed the latency and various security attacks in their surveys such as modification attack, integrity attack, tampering with data, DDoS attack, and single point of failure that can occur in transmitting the data of patient's health and their private information to the healthcare professionals. Therefore, an AI-based architecture integrated with a 6G communication network is proposed for smart healthcare technologies to mitigate the aforementioned issues. We have conducted a comprehensive survey on smart healthcare technologies such as wearable devices, body area networks, and digital healthcare systems that can remotely monitor patients. We have introduced an AI-based architecture to enable the secure, efficient, and reliable processing of patients' health data using the RF classification method. The incorporated 6G communication network with its features of low latency (<1 ms) and high availability ($<99.99999\%$) ensures efficient and reliable communication between patients and doctors. This helps get the healthcare staff the required information about the patient's health to give them prescriptions accordingly.

Figure 1 presents the technological revolutions in smart healthcare technologies, which initiates from 2001 in which first telesurgery was performed. After that, several technologies were introduced in smart healthcare, with the emergence of telemedicine and AI in 2020 and 2021. In the future, advancements in smart healthcare technologies can introduce virtual medical centers with the assisting robots for remote monitoring of patients.

1.1. Scope of the Survey. Smart wearable technology requires observing the activities of the human body continuously. The BANs consisting of human movement detection systems, body sensors, devices, and sensor networks for monitoring human activities along with its challenges are presented in [20]. A remote IoT-driven health monitoring system for ill patients is required in times of emergency. In this aspect, Shaikh et al. [21] presented several healthcare strategies and challenges using IoT. Medical data is complex and analyzing big data for predicting required results is even

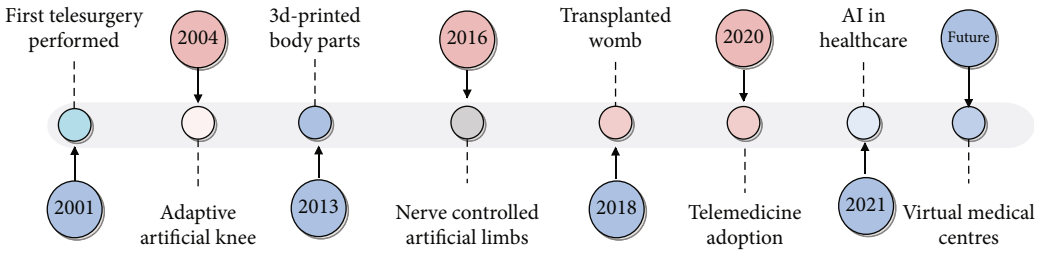

Figure 1: Timeline of smart healthcare technologies.

more difficult. Saranya and Asha [22] discussed various machine learning algorithms used in big data analytics, the importance of big data analytics in healthcare, and characteristics features of big data.

Cloud of Things (CoT) is aimed at providing extensive computing comprising IoT capabilities in an on-demand fashion. Mahmoud et al. [23] surveys CoT architectures and their application in healthcare and emphasizes energy-efficient solutions, in which quality of service and performance is considered. E-healthcare, U-healthcare, wireless health checking, etc., are different healthcare techniques used in IoT. Diwaker et al. [24] focuses on the same along with security and privacy methods for healthcare applications. Multimodal data-driven methods have been a driving force for smart healthcare systems with various applications from disease prediction to diagnosis and treatment. Cai et al. [25] proposes types of decision-making processes, multimodal association mining, and multimodal data fusion that have been employed in healthcare systems.

Mobile-healthcare devices play a significant role in exchanging data between doctor and patient. So, blockchain technology proposed in [26] protects data using consensus algorithms and smart contracts to provide design for an attack-free secure model. Cyber-Physical Systems (CPS) have diverse applications in healthcare, Amin et al. [27] presented a survey of state-of-the-art applications for monitoring and medication intake along with challenges like security, system usability, heterogeneous data management, and energy consumption. The context-awareness feature deals with users' contextual information based on current situations. Due to its importance, Vahdat-Nejad et al. [28] classified several context-aware healthcare systems along with their advanced techniques and shortcomings. Fog computing is aimed at providing services with less latency and high data security. Shakir and Karimpour [29] presented various fog computing platforms to perform balancing of the load in smart healthcare applications.

Recognizing patients' emotions using deep learning algorithms helps build efficient healthcare surveillance systems. Dhuheir et al. [30] presented a neural network-based healthcare monitoring system using speech, facial, and audio-visual emotion recognition. Yang et al. [31] reviewed IoT-enabled mobile healthcare technologies along with studying detailed smart health monitoring systems and types of sensor devices used along with IoT. Kadu and Singh [32] surveyed e-Healthcare telemedicine systems based on the Internet of Medical Things (IoMT) and AI, which facilitates in managing information creating significant improvements in the global health sector, especially telemedicine. Balakrishnan [13] presented a survey on IoT-based intelligent framework for healthcare. They studied the hybrid model of cloud and IoT design and AI used for wearable sensor networks and real-time applications, providing early medical care designs to the most recent fog computing smart healthcare frameworks [33]. Zhang et al. [34] deliver a comprehensive analysis of security and privacy risks, requirements, and solutions using blockchain applications in healthcare.

Table 1 shows the comparative analysis of various state-of-the-art smart healthcare surveys with the proposed survey. All these surveys conducted by the researchers have not included the security and privacy issues of patients' health data in smart healthcare systems. To fill this gap, we have presented an exhaustive survey on smart healthcare technologies, including wearable devices, BANs, and the digital healthcare system. An AI-based architecture is proposed to secure the patients' privacy data while transmitting it to medical staff for prescription or treatment.

1.2. Motivation

(i) As per the literature, most researchers have surveyed the smart healthcare technologies for remote monitoring of patients, but they have not considered all the smart technologies, including wearable devices, body area networks, and digital healthcare

(ii) The existing literature mainly emphasizes monitoring patients using smart healthcare technologies such as IoT and cloud for smart healthcare, which is vulnerable to latency, reliability, and various security attacks. Also, there is no discussion on a case study for smart healthcare technologies to ensure patient data privacy

(iii) Motivated from this, we have presented a comprehensive survey on smart healthcare technologies such as wearable devices, body area networks, and digital healthcare to monitor patients' health with security, efficiency, and reliability. We have also studied a case study based on the UAV-assisted secure healthcare for the COVID-19 outbreak

1.3. Research Contributions. The major research contributions are listed as follows.

(i) We presented an exhaustive survey on smart healthcare technologies, including wearable devices, BANs, and the digital healthcare system

Table 1: Comparative analysis of various state-of-the-art smart healthcare surveys with the proposed survey.

Author	Year	Purpose	Pros	Cons
[21]	2018	Survey of smart healthcare systems using IoT	Improved safety for patients, better decisions related to patient's health, easy access to information, and resources	Data integrity, reliability, trust management issues, security issues with sensor data, and no focus on efficient communication
[22]	2019	Survey on big data analytics in healthcare	Better EHR maintenance, efficient, and emergency prediction for patients health	No consideration of security attacks such as modification attack, integrity attack, and DDoS attacks against patients health data
[23]	2019	CoT for healthcare, a survey on energy efficiency perspective	Investigated solutions to deal with energy efficiency issues	Scalability issues, quality of service, and performance issues
[24]	2019	Survey on IoT healthcare techniques	A feasible solution to monitor patients remotely	Security and privacy issues in IoT-based devices
[25]	2019	Survey of multimodal data driven-smart healthcare systems, its approaches and applications	Intelligent decision making and interactive decision support using healthcare devices	Challenges in big data utilization and no discussion of various security and malicious attacks
[26]	2020	Survey on consensus algorithms for mobile-healthcare in blockchain network	Security against 51% attack and double-spending attack	Attacks on the network in healthcare devices, no process discussed to update the data during failure time in blockchain
[27]	2020	CPS and smart homes in healthcare, its current state and challenges	Medication reminder systems in smart homes, detection of pill ingestion, an improved system for people with cognitive impairment, and medical status monitoring in smart homes	Security and privacy issues, no method for heterogeneous data management, no focus to reduce energy consumption, and collaboration between different systems are the significant issues with the safe integration of CPS
[28]	2021	Survey on context-aware healthcare systems	Improved assisted living for patients, a better quality of contextual information, better management in emergency situations	Focuses only on a few diseases and particular contextual information, no effort to categorize new types of illness
[29]	2021	Survey on load balancing in fog computing in smart healthcare systems	Reduced access time, low energy consumption, improved accuracy, and high productivity	No consideration of transmission cost of data, degradation in performance in data transmission
[30]	2021	Survey on emotion recognition for healthcare surveillance systems using neural networks	Help detect depression and stress early in order to start medication and monitor patients	Facial and speech recognition can be misleading in monitoring a patients' health
[34]	2021	Survey on security and privacy for healthcare blockchain	Provides security and privacy risks, requirements, technologies, applications, and solutions for the same	Only focus on security leads to less advancements in smart healthcare technologies and functions
[35]	2021	Survey on integration of blockchain and AI in EHR sharing	Increased efficiency, service, personalization by integrating technologies, and solutions for improving healthcare ecosystem	Highly prone to security breaches and various malicious attacks
[31]	2022	Survey on IoT-enabled mobile healthcare technologies and challenges	Combine different techniques to support professional and commercial health monitoring IoT networks	Security and privacy issues on patient data
The proposed survey	2022	Survey on smart healthcare technologies using AI-based secure architecture	Secure against various attacks	—

(ii) We proposed an AI-based healthcare architecture incorporated with 6G networks to enable secure and transparent real-time data transmission between doctors and patients

(iii) We presented a case study on UAV-assisted secure healthcare for the COVID-19 outbreak

(iv) Finally, we highlighted various open issues and future research directions in smart healthcare technologies

1.4. Methods and Materials. This paper is aimed at providing a deep understanding of smart and secure healthcare by adopting AI and a 6G network. The authors started with a

literature review to form a concrete taxonomy on various smart healthcare technologies and different attacks possible on those technologies. The authors have explored different research articles from reputed research databases such as IEEEXplore, Springer Nature, Science Direct, Elsevier, MDPI, ACM digital, IET, Wiley, and technical research blogs from the Internet. The keywords used in traversing this topic were smart healthcare, smart and secure healthcare, wearable technologies, wireless body area network, IoT sensors in smart healthcare, AI/ML techniques in smart healthcare, and open issues and challenges in smart healthcare.

1.5. Organization. The organization of the rest of the paper is as follows. Section 2 presents a taxonomy of smart healthcare technologies. Section 3 provides the security aspects of smart healthcare. Section 4 discusses the proposed approach for smart healthcare. Section 5 elaborates the case study of our proposed architecture for the COVID-19 outbreak based on UAVs. Section 6 provides the various open issues and research challenges in smart healthcare. Finally, Section 7 concludes the paper.

2. Taxonomy on Smart Healthcare Technologies

Smart healthcare technologies have gradually developed. These technologies use the IoT, big data analytics, ML, blockchain, and AI to make healthcare more approachable, efficient, and personalized. We present some key technologies and applications of smart healthcare like wearable devices, body area networks, and digital healthcare as shown in Figure 2. These can be presented as follows.

2.1. Wearable Devices. Wearable devices in healthcare facilitate a patient to maintain their health actively. To be diagnosed early for timely treatment, patients can keep track of their body symptoms, such as heart rate monitoring and any chronic disease symptoms. This helps doctors to use this data to provide personalized healthcare plans. Table 2 shows the analysis of various state-of-the-art smart healthcare schemes for wearable devices. We can classify these wearable devices into five categories, which are mentioned as follows.

2.1.1. Head-Mounted. It consists of devices worn over the head/neck area. They are mainly used to assist surgeons, provide valuable solutions to patients, and improve the population's overall health. We identified five subcategories within head-mounted, which are mentioned as follows.

(1) Smart Eyewear. Smart glasses have gained popularity due to virtual reality and augmented reality advancements. The features of smart glasses are Bluetooth, focus camera, photo, video viewer, microphone, Global Positioning System (GPS), information storage, gyroscopic sensors, accelerometer, communication-notification, gaming, etc. Smart eyewear has real-time applications in many sectors, as mentioned in [47]. In an atmospheric study, in the chemical industry to sense harmful gases, in the food sector to scan food packets and quality check, virtual gaming, in healthcare, smart glasses are used to provide voice-enabled instruction to blind patients and varied applications. Kim et al. [48] proposed unique smart glasses for human visual augmentation based on human intention and scene and converting the view into speech. Later, the authors in [49] presented a smart eyewear for free walking using spatial mapping, mixed reality, and motion tracking. Even after having many features, smart eyewear's industrial usage is less due to safety issues, privacy issues, and less awareness of usage.

(2) Headphones. Bluetooth headsets were among the first wearable devices designed to make hands-free calls, play music, take voice commands, make customized settings on the mobile, provide sensors for activity detection, real-time language translation, and real-time noninvasive feedback. Due to these features, it can offer great competition to the wrist bands if issues like lower battery life and other lower processing capacities are solved [50]. Rosa and Yang in [36] discussed that headphones could also be used for cardiovascular and stress management with the ECG, impedance, and acceleration monitors. Then, Baumgartner et al. [51] proposed a self-fitting headphone for mild-to-moderate hearing loss with features to adjust the volume of acoustic signals as well as the dynamics.

(3) Hearing Aids. People having hearing loss have increased in the past decade, leading to the eventual increase in the usage by the suffering ones. Hearing aids provide hearing solutions and perform personalized functions. Previously, hearing aids had different problems like the poor sound quality and background noises. The advancement in digital signal processing has improved the performance of hearing aids and Bluetooth low energy protocol, enabling it to answer phone calls, provide voice assistance, listen to music, launch apps on smartphones, etc. A hearing aid can be intelligently used for audio noise cancellation, creating personal sound zones, specific audio broadcast, public audio alerts, and customized sound streaming for objects using Bluetooth low-energy-enabled hearing devices as presented in [52]. The traditional hearing aids amplify multisource sound, which leads the wearer to be unable to abstract the exact information conveyed when the source objects are television or mobile phone. Rajan et al. [53] proposed an IoT-based secured and efficient hearing aid based on chip property of microcontrollers that helps in the separation of acoustic sounds. Then, Han et al. [54] presented a system based on deep neural networks to reduce environmental noises and provide real-time speech enhancement.

(4) Immersive Helmets. These are virtual reality helmets having a small optic display in the front. They have many features like 3D video gaming. In medicine, during operations, they facilitate a surgeon with X-ray data and MRI imagining along with the real view of the patient. It helps in aviation by including protective visors and night vision devices. In the military, it helps by displaying information like maps and thermal imagining data, and in engineering to view 3D views of computer-aided designs, in the entertainment industry by providing virtual cinema and much higher

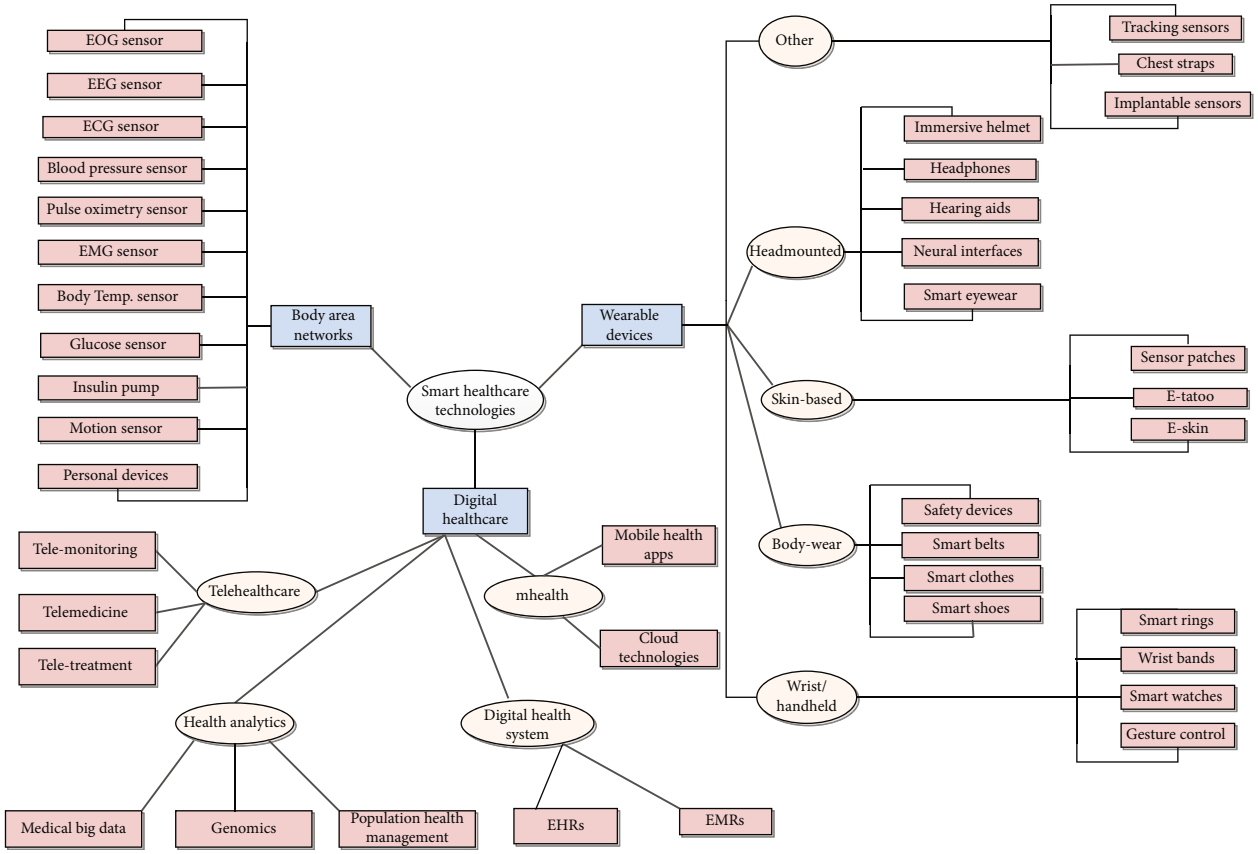

Figure 2: Taxonomy on smart healthcare technologies.

resolution. These helmets are also used in training like driving, shooting, welding, and medical training, where the real-life training is either too costly or life-threatening [55, 56].

(5) Neural Interfaces. These devices interact with the nervous system to stimulate or record activities. These devices are either placed internally in the brain, externally connected, or inserted in the nervous system to guide an activity or record movements. They are currently used to treat brain tremors and Parkinson's disease as movement simulators and cochlear implants to covey speech to people with hearing loss. It can be used to boost memory or concentration by transcranial stimulation and by the gamer to control digital objects and play without any physical contact as discussed in [57]. In the future, the neural interface devices have a high scope of development in fields like direct brain-to-brain communication, monitoring activities to support good health, and enhancing human concentration power and memory. But, due to critical issues such as privacy, human rights, and autonomy, neural interface devices are not used popularly.

2.1.2. Wrist/Handheld. Wrist-held smart devices' main application is fitness tracking, contactless communication, and notification. It comprises of wearable devices worn on the wrist or hand. We identify four categories within wrist held smart devices, which can be defined as follows.

(1) Smart Watches. They are one of the most popular wearable devices. Usually, smartwatches can function in two ways, as presented in [58]. Firstly, communication and notification by connecting to other devices using Bluetooth and complementing features like receiving notification calls, performing microinteractions like taking voice commands, limited web browsing, setting reminders, and app launching on mobile. Krainyk et al. [59] proposed another function, i.e., monitoring human physiological signals and biomechanics, thus providing fitness tracking. Users can record their day-to-day activities like workout time, calories burnt, sleep time, and step count. Enamamu et al. in [37] state that they can also be used to determine heart rate and body temperature using galvanic cell response and also remind users of personal activity as mentioned in [60], thus benefiting an individual's health.

(2) Wrist Bands. These devices have similarities with smartwatches but do not have a display screen to perform functions like communication and detailed monitoring of human signals. Wrist bands are specially designed to track health and fitness activities and have a limited form factor compared to smartwatches. Cai et al. in [61] presented their features like heart rate trackers, pulse oximeter, EEG tracker, ECG tracker, calories burnt, and step count. Rao et al. [62] show that step count and daily activities are tracked differently in various fitness bands and provides how daily activities can be assessed for helpful health predictions along with

Table 2: Comparative analysis of various state-of-the-art smart healthcare schemes for wearable devices.

Author	Year	Wearable devices	Objectives	Pros	Cons
Rosa and Yang [36]	2017	Headphones	Proposed a smart wireless headphone for cardiovascular and stress monitoring	Reduces power expenditure, saves computational resources, increases life expectancy	Reliability issues, relevance of physiological retrieved data is not completely trustable
Enamamu et al. [37]	2017	Smart watch	Presented a smart watch-based body temperate authentication using galvanic skin response sensors	Increased functionality, capacity, easy communication, and secured authentication technique	Does not function if varied body temperature found due to health issues, time-consuming
Ko et al. [38]	2017	Tracking sensors	A single camera-based 3D tracking for outdoor fall detection towards smart healthcare	Accurate human tracking, improved performance, compact structure, and an advantage for elders	Camera distance limitation and complex
Gacem et al. [39]	2019	Smart eyewear	Presented smart assistive glasses equipped with augmented reality for Alzheimer's patient's	Increases independence, cost-efficient, and location tracking	Security and privacy issues for patients, removal of glasses proves to be risky for patients
Zhang et al. [40]	2019	E-tattoo	Proposed an out of hospital care, body movement data collection using e-skin sensor	Improves quality of chronic pain management, early diagnosis, and prevents unnecessary admission to hospitals	Security issues, data collected cannot be trusted in all situations
Baek et al. [41]	2020	Smart shoes	Presented a deep learning-based heart rate estimation using smart shoes sensor	Easy to record, robust, accurate estimation	Inconvenient to use when direct contact to users required
Rabbani et al. [42]	2021	Implantable	Proposed an implantable fluorescence image sensor for monitoring of immune response in cancer therapy	Real-time monitoring, exact disease progression, therapy assessment, and provide personalized care	Imposes higher latency, small amount of disruption caused
Gourob et al. [43]	2021	Gesture control device	A robotic hand that is controlled with vision-based hand gesture recognition system	Easy human-robot interactions for patients to function using hand gestures and used in adverse places	Multiple interpretations, complex nonrigid properties of hand, and recognition issues
Basaklar et al. [44]	2021	Smart clothes	Presented a wearable device and low-power design for smart health applications, challenges, and opportunities	Low-power consumption, accessible, provides personalized care, provides early diagnosis, and no manual charging required	Comparable size and weight constraints, not comfortable always
Kumar and Mufti [45]	2021	Wrist handheld devices	Presented impact of coronavirus on global cloud-based wearable tracking devices	Remote health monitoring, screening, tracking all without transmission of virus, decreases burden of healthcare industry	Security and privacy issues of patient data
Behera [46]	2022	Sensor patches	Discussed chipless RFID sensors for wearable applications	Wireless data capturing, on-body sensing, and real-time monitoring of vital signs	Security and privacy issues and costly for mass implementation

the methods for accurate fitness activity measurement. Kumar and Mufti [45] show the impact of coronavirus on global cloud-based wearable tracking devices, which facilitated monitoring and tracking of patients without transmission of virus hence lowering the burden of doctors at the time of shortage of workforce.

(3) Gesture Control Devices. These devices can recognize and stimulate movements in the human body, allowing one to interact with and control objects without direct physical contact. It enables a user to perform hand gestures to connect with smartphones and perform various functionalities with hand gestures as input signals. These devices consist of a portable accelerometer and surface electromyographical (EMG) sensor as discussed in [63]. It is beneficial for impaired or disabled patients for interaction and communication purposes. Gourob et al. in [43] discussed these devices that can be utilized as vision-based gesture recognition system.

(4) Smart Rings. As they are small, they tend to have specific and limited features compared to smartwatches and wrist bands. They are generally designed to alert users about notifications on mobile phones, make secured payments, and track human activities, and also can be used as a safety device in case of emergency [64] and provide ambient sensing. Smart rings establish synergy between the tech and

fashion industry, and in the next few years, we might see expensive smart rings made out of gold. The authors in [65] discussed the application of smart rings; i.e., they can be connected to smartphones using Bluetooth and provide wireless charging without impacting the users.

2.1.3. Skin-Based Smart Devices. These devices can be adhered to or tattooed on the skin. They can be classified into three major categories, i.e., sensor patches that are microdevices embedded with sensor, E-tattoo, and E-skin which are miniature real-looking tattoo or skin patches integrated with sensors and circuits. Their primary function is to monitor essential vital signs in the human body, disease diagnosis, and monitoring. These devices are classified as follows.

(1) Sensor Patches. These devices are designed for sensory/haptic applications to monitor human body physiological signals and postural activities as investigated in [58]. They are generally used to determine essential vital signs monitoring, body temperature, postures, heart rate, pulse rate, track medication taking, etc. The haptic application includes lowering depression levels, posture training, drug delivery to specific body parts, and disease diagnosis. Sensor patches are connected to the display-enabled smart devices using Bluetooth or radio frequency signals. Zhang et al. in [66] explored a similar design to flexible strain sensors with a wide working range and reliability that can be used in human motion monitoring. Behera [46] presented a unique chipless RFID sensors which are traditionally costly for mass usage in wearable devices. The framework provides wireless data capturing, on-body sensing, and real-time monitoring of vital signs.

(2) E-Tattoo. They are seen as temporary tattoos that use flexible circuits for wireless data transmission and sensory purposes. Due to their persistence on the body for a long time, they should be ultra-thin and ultra-soft and exhibit high performance. Lu [67] designed an electronic tattoo that possesses the abovementioned features and can even be applied as human-mimetic robots. Their functions include observing human biological signals, communication, notification, and making secured chip-based payments. Yin et al. [68] explored these E-tattoos that are comfortable and versatile as they comprise of microphone for voice assistance and body sensors to detect human essential body rates like ECG, temperature, and hydration and also provide customized functions.

(3) E-Skin. They are used in the form of electronic skin, which is stretchable and comfortable, having similar features with E-tattoo smart devices. They are used for cardless secured payments, adverse environment detection, data transmission, health data collection, movement detection, treatment of diseases virtually, preventing unnecessary admissions to hospitals, improving quality of chronic pain management in patients' bodies, etc., thus improving the overall medical and healthcare facilities as proposed in [40].

2.1.4. Body Wear Devices. It comprises of mainly clothing items that serve as smart wearables such as smart clothes, smart shoes, and smart belts. They are majorly used for monitoring human physiological signals, biomechanics, health and activity monitoring for early diagnosis and prognosis, ambient sensing for hazardous environments, and sensory-haptic applications such as therapeutic messages.

(1) Smart Clothes. They provide affordable and accessible smart healthcare options with the help of edge computing, wireless sensing, electronic surveillance, and low-powered architectures. These devices help in providing more personalized health solutions. Yang and Cheng [69] presented the wide variety of stretchable sensors, which facilitates the collection of real-time data without disturbing users' daily activities and reports of children, old, and chronic patients. Sensors like accelerometers, gyroscopes, and magnetometers are embedded into small packages. Similarly, flexible sensors in the clothes measure hip and knee angles and biosensors track activities like ECG and EMG rates. Finally, AI algorithms process the real-time data and connect it to smart health applications installed in smart mobile phones as discussed in [44].

(2) Smart Shoes. They comprise an integrated monitoring circuit and sensors that provide fitness and biomedical information, including movement tracker, step counter, calories burnt, foot oxygen concentration, and heart rate determination. Bluetooth is used for wireless communication between the display platform and the module system. Hwang et al. [70] proposed a system in which pressure sensors shut down the devices to prevent unnecessary battery usage when no pressure feedback is received on shoes. Various smart shoes systems have been proposed like real-time monitoring of patients using smart shoe insole system [71], healthcare shoe system to monitor gait in elderly patients, and foot odor detection as studied in [72].

(3) Smart Belts. Smart belts as smart wearable devices have various applications in healthcare. They can be used to correct posture, help in reducing abdominal obesity as studied in [73], fetus health monitoring in pregnant women using flex sensor belts [74], and analyzing body data. The main focus is to provide proper guidance regarding overall health by tracking daily activities like sitting time, step count, and waist size.

2.1.5. Other Devices. They consist of other wearable devices, such as implantable sensors inserted in the body parts, straps, various tracking sensors, and safety devices for monitoring and analyzing a person's health. These devices can be described as follows:

(1) Implantable. Implantable electronic devices can detect medical changes and immediately take action like therapeutic measures, diagnosis, and treatment through a single message. They comprise of sensors, actuators, and signal processing protocols. These devices are surgically implanted into the human body. These devices are highly energy-efficient, integrated circuits, and work on their own power for a long time. They are used to electronically stimulate the

nervous system to treat pain, depression, diabetes, and high blood pressure. They are used for targeted therapies without any side effects with the patient's specific situation. Various devices have been developed in this field, such as Molley et al. [75] presented a next-generation self-supporting cardiovascular implantable device that monitors and analysis patient's health constantly and Vaddiraju et al. [76] explored a needle-implantable wireless device for continuous glucose monitoring.

(2) Chest Straps. The chest straps are designed to be flexible, stretchable, and comfortable. The sensors embedded have various functions like lessening chronic pains and measuring breathing rate. Then, Hung et al. [77] explored the monitored respiratory system with an accelerometer strap on the chest. Similarly, Rachim and Chung [78] discussed a wearable smart strap for mobile ECG monitoring using Bluetooth connection and providing real-time heart rate monitoring to prevent emergency conditions and improve the life quality of ill patients.

(3) Tracking Sensors. These devices are based on the Global System for Mobile Communications (GSM)/GPS technologies to track and monitor patients' real-time health to provide efficient medical care when required. This can bridge the gap between patients and doctors in case of emergency. Aziz et al. [79] presented a model in which sensors can capture the data and compare the data with configured threshold via microcontroller that is defined by doctors instruction for patients health. If there is any case of emergency, a short message can be sent to the doctor's mobile number along with the measured body rates through the GSM module. The GPS provides the current location of the patient. This helps in end-to-end connection to healthcare. Akbulut and Akan [80] discussed various features of these devices such as respiration rate tracker, nerves signs tracker, ECG sensor, glucose sensor, body temperature sensor, blood pressure sensor, blood oxygen sensor, and accelerometer in the smart wearable patient tracking system.

2.2. Body Area Networks. Body area networks (BANs) refer to a wireless network for smart computing devices. They consist of several sensors and smart devices that act as data gateway and provide an interface to view and manage BANs devices. It provides low-power sensors connected to human body parts or externally used and communicates using telecommunication networks. BANs include benefits like continuous monitoring of patient vitals using ECG sensor, EOG sensor, EEG sensor, blood pressure sensor, temperature sensor, and glucose sensor. It also improves quality in medical health care, providing personal devices like motion sensors, postural devices, and artificial body parts. BANs are majorly used for medical applications; it provides remote healthcare monitoring and telemedicine with the help of IT and communication. BANs are specially used for patients with chronic diseases or older people. It is also used to track the performance of athletes. Jani et al. [81] investigated an ECG and EMG sensor for determining biometric and medical information. Chu [82] presented an EEG sensor for brain injuries, treatment, and keeping track of daily emotional-social interactions. Similarly, Narasimhan et al. [83] discussed about a blood pressure monitor for real-time monitoring and Anuar and Leow [84] proposed a body temperature sensor for continuous monitoring and avoid heat strokes. Table 3 provides the comparative analysis of these state-of-the-art smart healthcare schemes for BANs.

These devices consist of actuators and sensors around the human body, which can be in-body or on-body, to monitor human body parts and deliver either impulses or medicine. They function with a wireless communication link to an access point or hub connected to the sensors on the body. BANs provide low power consumption devices [89] with self-healing facility, high security as Tian et al. [90] also presented a high-efficient and robust WBAN. Gupta et al. [3] presented a smart healthcare monitoring system using WBANs, attaining varied psychological parameters such as body temperature, heart rate, oxygen level, and vital signs and providing on-time treatment. Similarly, Zou et al. [87] proposed a multiparameter sensor system for healthcare applications. Hodgkiss and Djahel [88] using BANs presented a fuzzy vault-enabled smart healthcare system for high security of patient data and real-time sensing.

2.3. Digital Healthcare. Digital healthcare is a broad concept that includes interaction between technology and healthcare. It aims to provide cost-effectiveness, satisfy individual patient needs, standard medical procedures, and treatment based on real-time data, and improve healthcare services. With the help of advancements in technology such as wearable devices, telehealthcare, and mobile health apps, patients can stay healthy without much effort. Table 4 presents the analysis of the various state-of-the-art smart healthcare schemes for digital healthcare, which can be further divided as follows:

2.3.1. Telehealthcare. It deals with the remote exchange of clinical data between patients and doctors and provides medical services from remote places using information and communication technologies (ICT). It uses advanced technologies such as artificial intelligence, IoT, big data, and cloud technologies to make an efficient and effective distant healthcare [98].

(1) Telemonitoring. It refers to continuous or noncontinuous monitoring of a patient's body by healthcare professionals remotely for medical follow-ups and taking required decisions. It has gained popularity at the time of COVID-19. Quintanar-Gomez et al. [99] have explored its various functions such as blood pressure, heart rate monitoring using multilayer perceptrons, and pulse rate variability and also keeping track of patient's body parameters like temperature and pulse rate. It also provides periodic updates with reports without exposing them to costly diagnosis procedures as presented in [100].

(2) Teletreatment. It refers to remote treatment procedures using medical robots combined with physician expertise to provide health facilities at any remote place, at low cost,

Table 3: Comparative analysis of various state-of-the-art smart healthcare schemes for BANs.

Author	Year	Body area networks	Objectives	Pros	Cons
Jani et al. [81]	2017	ECG and EMG sensors	Proposed a design of a low-power, low-cost ECG and EMG sensor for wearable biometric and medical applications	Consumes low-power, is cost-effective, and is highly portable	Reliability issues, less durable due to compact size
Narasimhan et al. [83]	2018	Blood pressure sensor	Presented a finger wearable blood pressure monitor	Convenient, painless procedure, early intervention of hypertension, and accurate	Irregular heart rate affects the accuracy and can be erroneous
Chu [82]	2018	EEG sensor	Presented a wearable sensor for brain EEG signal-oriented applications	Used in treatment of various brain injuries, enhance everyday social and emotional interactions, wireless wearable	Poor spatial resolution, not used for pinpointing exact source of defect or activity
Anuar and Leow [84]	2019	Body temperature sensor	Proposed a noninvasive core body temperature sensor for continuous monitoring	Remote monitoring, avoid heat strokes, wireless system, and highly reliable	Invasive method is not comfortable for continuous use
Matsushita and Kaneshima[85]	2019	Motion sensors	Presented a motion sensing eyewear for daily healthcare monitoring	Monitor daily activity of users, real-time healthcare monitoring	Reliability issues, security, and durability issues
Hsu et al. [86]	2020	WBAN	Three-factor UCSSO scheme with fast authentication and privacy protection for telecare medicine information systems	Secure against malicious attacks and low overhead	No focus on tamper resistance and nonrepudiation attack
Gupta et al. [3]	2021	Smart sensors	Investigated a smart healthcare monitoring system using WBAN	Reliable information, stable living for patients, reduced medical cost	Security issues against DDoS attack, man-in-the-middle attack, and single point of failure
Gupta et al. [3]	2021	WBAN	Presented smart healthcare monitoring system using WBANs	Monitoring psychological parameters such as temperature, heart rate, and vital signs and provide real-time diagnosis	Security, privacy, and big data analysis issues
Zou et al. [87]	2021	Multiparameter sensor	Proposed a multiphysiological parameters integrated medical system for healthcare application	Collects body temperature, ECG, heart rate, oxygen saturation (SpO_2), blood glucose, and blood pressure	Patient data insecurity at the cloud platform
Hodgkiss and Djahel [88]	2022	BANs	Proposed fuzzy vault-enabled authentication in BANs-based smart healthcare	Real-time sensing of human biometrics, improved communication overhead, and highly secure	Limited power and computational capabilities

providing fast recovery, and saving various resources. Teletreatment can treat various diseases, operate remotely using a telesurgery system, and provide feedback. Gupta et al. [101] explored various telesurgery systems; some of them are widely used in [102].

(3) Telemedicine. It refers to e-medicine, diagnosis, and consultations using telecommunication interfaces. It has various benefits like increased convenience to patients, reduced cancellations of appointments, and increased access, and thus encouraging a healthy lifestyle. Jeyanthi et al. [103] proposed a secured cloud-based telemedicine system that reduces delay cost, increases availability, and reduces administrative burdens. Su [104] designed a diagnosis assistant system for breast diseases patients. Saini et al. in [97] surveyed various e-healthcare telemedicine frameworks built on IoMT and AI, in which the flow of emergency is prioritized for diagnosis and treatment. The proposed system outperforms traditional systems in security and trust aspects.

2.3.2. mHealth. It is also known as mobile health. It refers to the wireless technology for medicine and healthcare practices supported by mobile devices. In a nutshell, it means healthcare installed on your mobile phone. It provides personal digital assistance, monitoring health, tracking fitness, and daily activities to keep people fit and healthy.

(1) Cloud Technologies. Cloud technologies in healthcare refer to the practice of instructing remote servers connected through the Internet to store, manage, and analyze healthcare-related big data. It helps to increase efficiency with a decrease in cost. It has functions like medical record managing and performing back-end operations and also helps in the creation of mHealth apps. Several cloud-based

Table 4: Comparative analysis of various state-of-the-art smart healthcare schemes for digital healthcare systems.

Author	Year	Digital healthcare	Objectives	Pros	Cons
Vardhini et al. [91]	2016	Genomics	Proposed a genomics revolution treatment for diseases and opening new frontiers for precision medicine	Personalized care, disease treatment solutions, and reliable and intelligent model	Inaccurate for some treatment cases; use of big data is time-consuming
Kobayashi and Homma [92]	2019	Telemonitoring	Presented an analysis of telemonitoring multivital data for alert detection on telehealthcare system	Increases life expectancy, reduces medical cost, helps in acute disease detection, and prevents progression of fatal conditions	Sometimes inaccurate for analyzing big data and reliability issues while using only vital data
Yang and Chen [93]	2019	Medical big data	Analysis and visualization implementation of medical big data resource sharing mechanism based on deep learning	Improvised visualization, display of medical data, processing, and resource sharing	High security and privacy threat, misuse of medical data, and proper analysis of big data is a hard process
Koren and Prasad [94]	2020	Electronic health records	Proposed personal wireless data in formal electronic health records and future potential of medical things data	Provides quality solution, monitors vital signs and conditions, provides personalized healthcare, and leads to better decision related to health management	Cyber security threats, privacy issues, and proper utilization of big data is not yet achieved
Lehmann et al. [95]	2021	mHealth	Proposed an approach for multidisciplinary evaluation of mHealth applications	Quality assurance, low distortion, solves problem of undifferentiated mHealth applications	Reliability issues, not useful for treatment, and diagnosis of fatal diseases
Chiu et al. [96]	2021	Mobile health apps	Presented an interactive mobile app for self-supervised health management	Interactive health management system, provides feedback, records user health information, impacts positively on people's health	Daily activity tracking can cause security and privacy issues; positive feedback can sometimes be misleading
Saini et al. [97]	2021	Telemedicine	Analyzed e-healthcare telemedicine system based on IoMT and AI	Prioritizes the flow of emergency healthcare transactions, outperforms real-time healthcare systems, secures, and is trustworthy	Less prior transaction may get ignored sometimes
Kadu and Singh [32]	2022	Digital health systems	Proposed smart contract-based transaction prioritization scheme for smart healthcare	Provides unique alternatives, information analysis cooperation, intelligent aid diagnosis, and continuous monitoring	Need to develop its capacities and adaptability and security issues

healthcare systems have been proposed. Tawalbeh and Habeeb [105] studied mobile cloud computing-based smart healthcare systems. Another researcher presented an IoT and cloud-based healthcare diagnosis that uses sensors to collect real-time data and predict the severity of diseases based on database [106]. Later, Esposito et al. [107] explored a blockchain and cloud technology-based secure and private healthcare system to provide convenience and availability to the patients.

(2) Wearable Devices. These devices are used to provide communication and notification in daily use and provide various health-related benefits such as monitoring and diagnosing health conditions and vitals of the human body, tracking medications, following the recovery of post-operation patients, and fitness tracking. Hung et al. [108] studied wearable medical devices for telehome using multisensor data fusion and wireless technology. Then, Sharma et al. [109] presented a smart wearable device based on Intel curie platform that aims to make it portable, easy to use, low power usage, accurate, and consistency in its functions related to fitness tracking and wireless data transmission and communication.

(3) Mobile Health Apps. They allow doctors to effectively communicate with patients and providers and provide 24/7 healthcare facilities to patients and the ability of personalized healthcare per user. But, the poor people living in rural areas have limited healthcare resources. Pasha et al. [110] designed a neural network-based mobile app that has pretrained disease predictions for users. Chiu et al. [96] proposed an interactive mobile app for self-supervised health management along with a feedback system that increases the likelihood of people becoming healthier.

2.3.3. Digital Health Systems. It refers to combining technology with healthcare systems. These systems are aimed at providing improved and cost-effective medical services. It uses innovative technology, computing platforms, real-time data, connectivity, software, and sensors to configure systems efficiently. Patients can now stay fit in an easy and secure way.

(1) Electronic Health Records. Electronic health records (EHRs) contain all the information from health centers involved in patient care. They make real-time information related to patients instantly available to authorized persons. It contains treatment and medical details of the patient and includes the broader scope of a patient's healthcare. They deliver various functions like providing a patient's medical history, treatment plans, medications list, diagnoses to be done, allergies, laboratory and test results, and X-rays. They also guide authorized persons regarding evidence-based tools based on the records. The main feature of EHRs is sharing digital records with other devices across different healthcare organizations. With the rapid growth of smart technology, healthcare solutions have also increased with personalized health data. Koren and Prasad [94] presented an EHR system that merges this medical data with central systems and helps in better decision making and providing improved healthcare solutions. EHRs are published using traditional systems, which are time-consuming. An innovative system was proposed in [111], which involves features like voice assistance, editing ability, medical image processing, and interactive schedules to provide a convenient tool to physicians.

(2) Electronic Medical Records. Electronic medical records (EMRs) are a digital form of paper records in health centers and hospitals. They contain important information collected by the medical staff in the hospital, which doctors mainly use for treatment and diagnosis. EMRs enable doctors to track data with time, identify patient visits, observe patients, and improve overall healthcare quality. Some patients need continuous or emergency care after discharge, for which Intawong et al. [112] designed a seamless EMR for healthcare management that exchanges data to community hospitals and is reliable and effective for patients requiring urgent care. Vardhini et al. [91] proposed a blockchain and smart contract-based framework to resolve the problem of EMRs, i.e., misuse of data and security, which has been solved by providing data privacy, interportability, and accessibility. Kadu and Singh [32] proposed an SCs-based transaction prioritization architecture for digital healthcare. It provides creative alternative solutions with intelligent aid diagnosis and continuous monitoring facility.

2.3.4. Health Analytics. It refers to using large amounts of collected data to provide healthcare systems with actionable intuition. These perceptions are developed through analytical disciplines such as big data analysis to deliver fact-based intelligent decision-making systems. These decisions improve the planning process, management activities, future predictions, and intelligent learning in succession.

(1) Medical Big Data. Big data in the medical field can be used by commercial, academic, government, and public sectors as it includes overall health data. It can be analyzed to improve decisions and make predictions of diseases and emergency medical conditions. Li et al. [113] resolve the redundancy problems of medical big data through a data midplatform; i.e., it is not well connected and has critical failures such as missing information, data disparity, and isolated information. Yang and Chen [93] explored deep learning-based medical big data resource sharing that fastens the data analyzing and visualization of data collection and system requirements.

(2) Genomics. Genomics refers to the genome and DNA data of an organism. It requires a large amount of storage and good software that supports it. It studies the biological aspects of human organs such as heart disease, asthma, diabetes, and cancer. These diseases are caused due to environmental as well as genetics. The data that drives genomics and its fundamental biology basis is called genomics data. Using this data is complex; hence, Kuznetsov et al. [114] presented a cross-platform immersive virtual reality system to enable graph genome interaction and analysis. Campbell [115] investigated a model that provides a novel treatment for diseases using genomics and new technology for precision medicine that opens a new research scope in this field.

(3) Population Health Management. It focuses on the well-being of the population as a whole. It follows financial and care models for the patients and manages their data records. It functions through primary health care, data analytics, long-distance management, and doctor consultancy. The main aim is to reduce per capita cost, enhance patient experience with the data-driven technology, and improve populations' overall health. Panicacci et al. [116] presented a population health management system to identify high-risk patients using machine learning algorithms. Similarly, Wu and Gao [117] designed a TCM five-pattern system to prevent health-related issues in older people of the community and provide the necessary treatment.

3. Security Aspects of Smart Healthcare

3.1. Key Security Attacks on Smart Healthcare. The smart healthcare technologies, such as wearable devices, BANs, and digital healthcare, are vulnerable to various security attacks, such as spoofing, data manipulation, injection, and social engineering attacks, as shown in Figure 3 that deteriorate the performance of the smart healthcare system.

3.1.1. Attacks against Healthcare Data (EHR/EMR). EHR and EMR data from digital healthcare systems are most susceptible to security attacks. A patient's confidentiality and privacy are deeply disturbed because of such attacks. These data present in digital form can be used for remote health monitoring purposes and are trusted between patient, doctor, and hospital. Various attacks are mentioned below.

(1) Key Logger Attack. While entering a patient's data, keystrokes can be detected by running a key logger program [118]. The attacker acquires the credentials for illegally accessing the patient's health data based on keystrokes.

(2) Phishing Attack. In this attack [119], a patient falls into the trap of an adversary by filling their health information using an illegitimate email link sent by an adversary. The

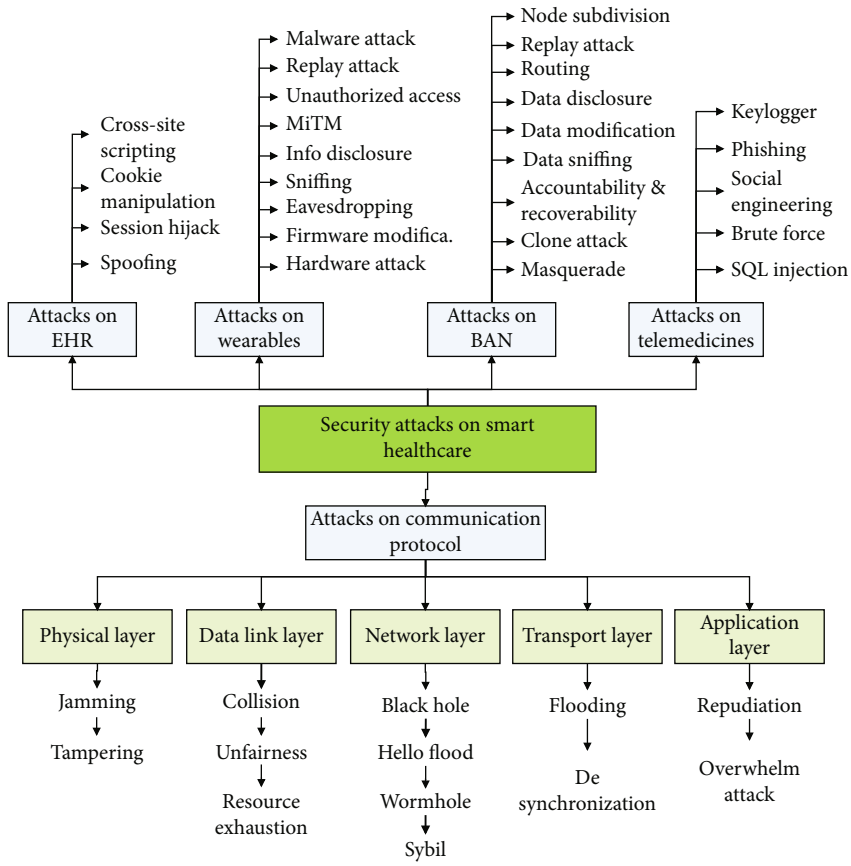

Figure 3: Taxonomy of different security attacks on smart healthcare.

input received from the email link is used for blackmailing and money laundering.

(3) Social Engineering Attack. Due to the increased presence of a user on social media due to Internet services, an attacker can trick the system by impersonating a legitimate user to gain access to the patient record [120].

(4) Brute Force Attack. It uses a trial and error method for guessing the password of a system to access the complete information of the patient healthcare data from the hospital.

(5) SQL Injection. When a patient or doctor is entering data, malicious SQL queries are injected into the forms filled by the user. This leads to access to the database contents to exploit the information stored in the database.

3.1.2. Attacks on Telemedicine. Telemedicine refers to continuous or noncontinuous monitoring of a patient's body by healthcare professionals remotely for medical follow-ups and taking required decisions. The information exchange between healthcare professionals and patients is susceptible to various attacks, as mentioned below.

(1) IP Address Spoofing Attack. In this attack, to launch the DoS attack at the service provider side, the attacker creates forged IP packets from one system that appears to be created on different systems.

(2) Cross-Site Scripting Attack. The attacker injects malicious code into the web application to execute malicious scripts in this attack to obtain the patient's cookies. The attacker gains access to the patient's file system, webcam, microphone, and geographical location by impersonating them. XSS is the most vulnerable way of cross-site scripting.

(3) Cookie Manipulation Attack. In this attack, the attacker manipulates and forges the cookies to steal the patient's identity. Generally, our username and password are stored in the form of stored cookies. Once filled in a web application form, the data also gets stored inside cookies. Hence, the attacker can access all these data if the stored cookie can be manipulated. A patient/doctor's financial, medical, or any other personal sensitive data can be accessed by this attack.

(4) Session Hijacking Attack. In this attack, the attacker hijacks a current and legitimate session of the patient/doctor to access the information being exchanged by hijacking session parameters. The attacker can take part in an ongoing conversation after the same [121].

(5) DNS Spoofing Attack. DNS spoofing attacks service providers. In this attack, by spoofing the domain name system (DNS), the attacker redirects the entire traffic to his machine. The attacker manipulates the DNS entries, which returns the attacker's IP address to the users instead of a legitimate IP address. Hence, patients/doctors start

interacting with the attacker and unknowingly leak their sensitive healthcare data.

3.1.3. Attacks against Healthcare Physical Devices (Wearable/Implantable/Medical Equipment). Wearables, implantable, and medical equipment read real-time healthcare data of a patient and transmit the same to paired smartphones or any storage device for later analysis. This data is confidential and private about a user. Various security vulnerabilities and attacks are possible on the aforementioned devices due to their resource-constrained nature and insecure proprietary protocols while manufacturing. Such attacks are mentioned below.

(1) Hardware Attack. Hardware attacks are implemented by introducing Trojan into the implantable devices. They create malfunctions in the embedded integrated chips (IC) and are complex to detect.

(2) Firmware Modification Attack. In the case of wearables and implantables, a device's hardware is controlled by a program stored in nonvolatile memory. Firmware modification attack tries to modify that program to get control of the hardware. To improve user experience, continuous firmware updates are essential. And thus, attacks make use of these firmware updates to inject malicious firmware into the device [122]. This attack is performed by reverse engineering communication protocol and application code.

(3) Eavesdropping Attack. In this attack, an unauthorized entity intercepts users' personal information. In wearable and implantable devices, Bluetooth and radio frequency are susceptible to eavesdropping. Marin et al. [123] showed these devices undergo traffic analysis through tools such as Ubertooth, Wireshark, and Adafruit and succumb to eavesdropping.

(4) Sniffing Attack. In this attack, traffic is sniffed and analyzed using hardware and software sniffers. Static MAC addresses are analyzed from the advertisement packets for performing sniffing. Using scanning devices, sensitive healthcare data can be extracted to plaintext through traffic analysis [124].

(5) Information Disclosure Attack. In this attack, an unauthorized entity exposes the information due to a weak communication channel or device. Rahman et al. [125] showed an information disclosure attack on fitness trackers by reverse-engineering the communication protocol. Lack of encryption mechanism and authentication leads to extracting sensitive healthcare data [126].

(6) Man in the Middle (MITM) Attack. In this attack, an attacker intercepts the communication between two authorized and legitimate entities and learns about the prevailed data. Rieck [122] shows MITM attack in fitness trackers by reverse engineering the firmware version.

(7) Unauthorized Access and Spoofing Attack. In wearables, implantables, and medical equipment, an attacker accesses sensitive healthcare data unfairly due to security vulnerabilities and can spoof the healthcare service providers. It can be done by brute-forcing the secure pin used for traffic analysis and pairing [127].

(8) Replay Attack. In this attack, an adversary corrupts or impersonates valid packets transmitted by the medical devices. It can be done by manipulating the defects of encryption, hard-coded MAC addresses used for pairing or authentication.

(9) Ransomware DOS Attack. This is a traditional DOS attack where medical equipment is hacked by attackers and is inaccessible unless the desired ransom is paid to the attacker. It is performed because of outdated operating systems [128] and insecure protocols. The unavailability of medical equipment can be fatal for human life in emergencies.

3.1.4. Attacks against WBAN. WBAN, despite having several benefits, attracts attackers for luring various security attacks due to their design, open-access environment, and portability. Healthcare applications impose strict requirements such as data integrity, availability, data confidentiality, authentication, and data freshness on the reliability of data delivery in end-to-end systems. WBAN suffers from various security attacks, as mentioned below.

(1) Masquerade Attack. In this attack, an attacker masquerades the identity information of a legitimate WBAN node by using a fake identity to avoid detection. The attacker accesses a system by using stolen login IDs and passwords, dodging the authentication mechanism, or manipulating security vulnerabilities. A masquerade node can create a severe threat by launching DoS attacks on medical applications. Using biometric or key management authentication schemes can prevent an adversary from impersonating a WBAN node.

(2) Clone Attack. In this attack, an attacker replicates legitimate nodes by obtaining credentials of a WBAN node. It secretly copies the ID and introduces itself, i.e., the cloned ID, as an authorized node to the network. It affects the authentication requirement of WBAN and helps attackers gain illegitimate access, alter health data and conduct false data injection.

(3) Accountability and Revocability Attack. This attack concentrates on key abuse. A WBAN node shares the access key with unauthorized users and abuses their access privileges, thus gaining access to the secret key to decrypt the healthcare data. WBAN nodes are bound to be accountable for policies that preserve patient data and revoke the same when found maliciously violating it.

(4) Battery Depletion Attack. In this attack, the attacker exhausts constrained resources such as battery power or processor cycles by sending false data to a target BANs node. This attack makes the target BANs node perform intensive processing to reply to erroneous packets or retransmit them to other nodes. The quick depletion of sensor battery power hence reduces its lifetime for collecting sensitive healthcare data.

(5) Data Sniffing/Snooping Attack. In this attack, an attacker sitting on an insecure network path between a WBAN node and a medical server gains access to the traffic flow of data passively containing sensitive healthcare data, node IDs, routing updates, etc., for later analysis. It affects the confidentiality requirement in WBAN and can be prevented by employing a key distribution scheme.

(6) Data Modification Attack. Data modification attacks affect authentication, availability, integrity, and nonrepudiation requirement in WBAN. An attacker modifies/replaces/alters data either partly or entirely traveling between WBAN nodes. Falsification of data may lead to severe consequences on a patient's life. A digital signature or keyed hash function can avoid data modification attacks.

(7) Data Disclosure Attack. This attack affects the confidentiality and privacy requirement in WBAN, where sensitive data is revealed to unauthorized users using unsolicited means. This leaked data can be spread all over the network. Access control and encipherment techniques on the network layer can prevent data disclosure attacks.

(8) Routing Attack. In this active malicious attack, the routing table is poisoned to transmit data packets to faulty destinations by editing the entries in the routing table, causing severe damage to the network. This attack affects the authentication, availability, integrity, and confidentiality requirement in WBAN.

(9) Replay Attack. Replay attack affects hardware and software resources in WBAN where an attacker intercepts the messages traded between authorized users. The attacker deliberately delays or replays the same to the legitimate receiver to enforce aggregate result change.

(10) Node Subversion Attack. This attack is on privacy by capturing and performing cryptanalysis on WBAN nodes deployed in the network to access sensitive data such as node ID, security policies, routing information, and security keys.

3.1.5. Attacks on Communication Protocol Stack. For data exchange to occur, a secure communication channel is required, which is governed by a set of communication protocols. An attacker aims to exploit the communication channel to take control over the entire communication protocol stack. Various attacks are mentioned below for the same.

(1) Physical Layer. The physical layer is responsible for radio frequency generation and selection, modulation of bits, signal detection, and bit-wise encryption. Following attacks are possible for the physical layer where a radio-based medium is used.

(a) Jamming

Jamming is a type of attack in which the attacker sends radio frequencies that interfere with the frequencies used by the sensor node. Here, an attacker generates a radio signal randomly with a frequency matching the one sent by sensor nodes. The radio signal sent by the attacker interferes with the other signal transmitted by a sensor node and receives within the attacker's range cannot receive any message. Thus, the nodes in the range of attacker signals become inaccessible as long as these jamming signals continue and no messages can be either given or received among the affected nodes and other sender nodes.

(b) Tampering

Tampering refers to stealing sensitive information such as cryptographic keys provided with physical access to the node. Tamper-proofing a node is a defense mechanism to this attack where a node vaporizes its memory when tried to get accessed maliciously.

(2) Data Link Layer. The data link layer provides shared access channels such as carrier sense multiple access (CSMA) to all neighboring nodes. This layer faces issues related to the collision of data packets, resource-constrained environment due to repeated retransmission, etc., which are encountered on this layer. Such various attacks are listed below.

(a) Collision

A collision occurs when more than one node attempts to transmit data packets on the same frequency simultaneously. This results in updation of data portion resulting in checksum mismatch at the destination, leaving the packet discarded. An attacker can deliberately cause collisions of data packets if gained access to the data link layer.

(b) Exhaustion of resources

When corrupted packets are transmitted continuously and repeatedly, it leads to resource-constrained scenarios such as battery depletion and energy depletion, thus leading to resource exhaustion.

(c) Unfairness

Unfairness occurs because of repeated collision-based MAC layer attacks and harsh use of MAC layer priority mechanisms. Unfairness is a partial DoS attack leading to performance degradation.

(3) Network Layer. The network layer is responsible for reliable end-to-end delivery. The data packets travel through a set of nodes acting as routers having information about the network route a packet will take. Hence, security attacks are possible on this layer on the routing protocols. Mentioned below are attacks on energy, power, and memory-efficient routing protocols.

(a) Black hole attack

A black hole is formed by vehicles refusing to participate in communication or drop their packets. Hence, entire traffic gets directed to a node having no public existence.

(b) HELLO flood attack

The adversary node uses a powerful transmitter in this attack and floods the network with a high-quality route. This high-quality route attracts all data packets from other nodes, hoping to have a better path from sender to destination, but such a path does not exist. Thus, the attacker receives all the data packets.

(c) Warmhole attack

A wormhole creates a shortcut route between two distant nodes in this attack. An attacking node disrupts routing by short-circuiting the network, thus not allowing the usual packets to flow through a legitimate path. The attacker can monitor the traffic or damage the data flow.

(d) Sybil attack

This is one of the hazardous attacks in which multiple identities exist of a malicious node. Hence, it is challenging to decide the legitimacy of a node from where information is received.

(4) Transport Layer. The transport layer is responsible for end-to-end communication services between applications running on multiple hosts. Attacks on the transport layer disrupt the application processes and hinder the delivery process. Two such attacks at the transport layer are mentioned below.

(a) Flooding

In this attack, the attacker broadcasts the victim node with many connection establishment requests to drain its resources, thus generating a flooding attack. This attack can be preserved by limiting the number of connections a node can accept.

(b) Desynchronization

In this attack, an adversary uses a fake sequence number and copies a message multiple times to one or both the end nodes of an active connection. This results in desynchronization, forcing nodes to retransmit the messages resulting in draining of the resources of a victim node.

(5) Application Layer. The application layer is responsible for providing support, interface, and services to end-user, such as email services and database services. Any attack on this layer will restrict access to such services.

(a) Overwhelm attack

An attacker drains a node's energy and absorbs network bandwidth by overwhelming the network by forwarding a mass amount of traffic to the base station, thus causing the network to jam and not allowing essential services to the end-user.

(b) Repudiation attack

These attacks lead to denial of participation from all parts of the communication channel called repudiation. This results in nonservice to the end-user because of participation denial from the malicious node.

3.2. Classification of Security Solutions for Smart Healthcare. As discussed in the previous section, smart healthcare systems succumb to multiple attacks based on access to healthcare data, communication channels, physical devices, data storage, etc. Many researchers have developed security frameworks, architectures, algorithms, protocols, software services, policies, and tools to secure healthcare systems. Classification of security solutions for smart healthcare is presented in this section.

3.2.1. Password-Based Solutions. A basic authentication scheme is a password-based scheme, quite popular in our day-to-day applications. It requires a user to remember their password to login onto a system and access the services provided by the system. A password-based scheme is susceptible to brute force attacks where an attacker tries to guess the password by using multiple permutations and combinations. Wei et al. [129] have achieved authentication in WBAN employing low entropy password-based scheme and achieved anonymity. But, the authentication scheme suffers from high communication costs because of the length of the messages affecting the bandwidth. Liu et al. [130] proposed an authentication scheme using a custom password authentication algorithm that generates dynamic passwords achieving anonymity, privacy, and security. It outperforms other password-based techniques in terms of computational and communication costs. However, forward secrecy is not considered by the scheme. Kim et al. [131] proposed a three-party password authentication scheme with a key exchange that preserves user anonymity and prevents impersonation attacks.

3.2.2. Biometric-Based Solutions. A biometric-based authentication scheme verifies the user's physiological and biological traits and matches them with those already stored in the system. It is challenging to forge, copy, or break a biometric-based authentication. Although, sometimes, due to errors in the design, or the nonstability of biometric traits, the authentication fails. Fingerprint, heart rate, iris, voice, hand geometry, retina, ECG, PPG, etc. are considered biometric characteristics. Arya et al. [132] used a fingerprint biometric authentication scheme for WBAN applications. It used a mutual authentication and key establishment procedure. But it does not justify security in WBAN applications. Koya and Deepthi [133] used ECG biometric authentication scheme for WBAN applications. It provides better security than other ECG biometric schemes and performs better. Tan and Chung [134] used ECG biometric authentication along with cryptographic techniques such as elliptic curve and Diffie-Hellman. The scheme protects user identity but provides only conditional privacy. Mohammedi et al. [135] proposed a lightweight biometric authentication scheme for remote patient monitoring using elliptic curve

encryption. The scheme justified lower communication and computation costs with lower storage. Shakil et al. [136] proposed BAMHealthCloud for securing e-medical data using a MapReduce framework. The said system performed better than other biometric schemes.

3.2.3. Cryptographic Solutions. Cryptographic-based solutions can be divided into symmetric-key cryptography, asymmetric key cryptography, and hash key cryptography. Many researchers have given solutions using multiple cryptographic algorithms such as AES, DES, SHA, Triple DES, RSA, ECC, DSA, and MAC. Sharma and Bhatt [137] used quantum mechanics to secure IoT-based healthcare systems to overcome security challenges such as scalability, data confidentiality, and mobility. Gaikwad et al. [138] proposed using elliptic curve cryptography (ECC) for securing e-health data. Time and computation cost was considered in this scheme. Chen et al. [139] proposed an anonymous mutual authentication scheme on WBAN for wearable sensors. This scheme prevents impersonation, spoofing, and offline identity guessing attacks. Jegadeesan et al. [140] presented a privacy-preserving anonymous authentication scheme to provide security and privacy to users' data along with achieving low communication and computation costs. Shen et al. [141] used the ECC algorithm to create a certificateless authentication protocol with low computation cost and high security.

3.2.4. Access Control-Based Solutions. Unauthorized access can be restricted by employing access control mechanisms for protecting e-health data. Dankar and Badji [142] presented a risk-aware secure framework to store e-health data. Firstly, the risk is identified on the data and the access control mechanism determines the level of data protection on the risk. Later, the data is stored. Hence, it offers data protection against unauthorized access. Rajput et al. [143], Shahnaz et al. [144], and Xu et al. [145] used access control mechanisms by employing blockchain for securing e-health data. The first focuses on securing data during emergencies, the second focuses on off-chain scaling, and the last focuses on sharing symmetric keys between patient and staff. Wu et al. [146] demonstrated access control schemes on implantable medical devices. Lounis et al. [147] proposed ciphertext policy attribute-based encryption (CP-ABE) to achieve performance and flexibility in medical wireless sensor networks. Yang et al. [148] proposed a fine-grained access control mechanism for updating access policy without any data leakage.

3.2.5. Digital Signature-Based Solutions. Digital signatures are used to acquire authentication and nonrepudiation of digital messages and documents. By employing the hash function over the data, the sender node generates the message digest and is further signed using its private key, then forwarded to the receiver node. The destination node confirms the signature by utilizing the sender's public key. The data is extracted by using the hash function if the result is valid. Alzubi [149] proposed a blockchain-based Lamport Merkle Digital Signature, which authenticates by creating a tree where the leaf nodes contain sensitive patient information obtained by the hash function. Abkari et al. [150] use a radio frequency identification system for monitoring hospital data and tracking medicines using a digital signature. Kumar et al. [151] proposed ElGamal digital signature with rabbit and serpent algorithm for securing healthcare data streaming. Margheri et al. [152] demonstrated digital signature for provenance tracking of any medical document containing healthcare data. Wu et al. [153] used hash with SHA-256 along with blockchain for cross-enterprise document sharing.

3.2.6. Key Management-Based Solutions. Key management solutions help provide data security. It involves cryptographic key generation required to encrypt/decrypt data, key renewal, agreement of keys between communicating entities, secret key distribution, and revocation of keys. Donmez and Nigussie [154] presented a key management scheme, LoRaWAN, for monitoring healthcare systems. This scheme stores lifetime root keys in end devices susceptible to physical attacks and lacks mechanisms to update the root keys. If the root keys are exposed, the session security will be compromised. Jiang et al. [155] proposed an end-to-end session key management scheme for a wearable healthcare monitoring system. This scheme overcomes desynchronization attacks. He and Zeadally [156] presented a symmetric key generation-based authentication protocol scheme for ambient assisted living systems (AAL).

3.2.7. Machine Learning-Based Solutions. Machine learning (ML) models play a significant role in healthcare systems. Applications of ML range from disease diagnosis from EHR data, medical image analysis, real-time health monitoring, vulnerability detection, and providing security towards threats on healthcare data. Few such works are discussed here. Salem et al. [157] presented an anomaly detection scheme using support vector machine (SVM) and linear regression models on wireless medical sensor networks. Rajendran et al. [158] used machine learning approaches for enhancing security and privacy in edge intelligence in healthcare applications. Pirbhulal et al. [159] propounded an ML-based biometric security framework on ECG signals. Begli et al. [160] created an intrusion detection system using SVM against DoS attack and user to root (U2R) attack for remote healthcare monitoring system. Sengan et al. [161] created a dynamic, secure aware routing by ML to secure healthcare data. ISTHMUS is proposed by Arora et al. [162] where the ML approach is used to secure cloud-based healthcare architecture. This scheme is secure, robust, and scalable and provides real-time monitoring. SVM and fuzzy C-means clustering is used by Marwan et al. [163] for data protection against untrusted clouds storing healthcare data.

3.2.8. Blockchain-Based Solutions. Blockchain technology has emerged as a significant area for providing security in many applications, majorly in the healthcare domain. We studied many applications where blockchain is used for securing e-health records, medical networks, medical devices, etc. Li et al. [164] designed a blockchain-based

reliable data storage system for preserving the privacy of healthcare data. The authors used AES as a cryptographic algorithm for protecting the anonymity of the user and its data. Fan et al. [165] proposed blockchain-based MedBlock, to account for the scarcity of data management and data sharing policies in the EMR system. In this solution, hospitals can upload their data on MedBlock and ones with the right decryption key can retrieve the same. Nguyen et al. [166] proposed a framework integrating blockchain and InterPlanetary File System (IPFS) for sharing e-health data in a mobile cloud environment. They used smart contracts for secure e-health data [167]. But, data confidentiality is still not on point. Wang et al. [168] propounded a blockchain-based privacy-preserving scheme for e-health data where the cloud stores encrypted text of e-health data and blockchain stores keyword encrypted text to search and share the data. Abou-Nassar et al. [169] implemented DITrust chain using Ethereum and Ripple for securing trust in IoT healthcare systems. Islam and Young Shin [170] propounded a blockchain-based healthcare scheme for assisting unmanned aerial vehicles (UAV) in providing security to health data collected from users using UAV and stored on the nearest server in the UAV path. Miyachi and Mackey [171] presented hOCBS, a privacy-preserving blockchain-based framework for leveraging healthcare using on-chain and off-chain system design.

3.2.9. Telehealthcare-Based Solutions. In the era of COVID-19, telehealthcare has emerged as one of the safest approaches for communication between patient and doctor. It refers to continuous or noncontinuous monitoring of a patient's body by healthcare professionals remotely for medical follow-ups and taking required decisions. Telehealthcare includes telemonitoring, teletreatment, telemedicine, and telesurgery. All these approaches are susceptible to numerous attacks, and research work is done in this area to secure the same. Thanki and Kothari [172] presented a multilevel secure watermarking scheme to secure medical images in telemedicine applications without compromising the quality of medical images. Mansour and Parah [173] used Lagrange's interpolation polynomial and bit substitution for creating reversible data hiding for securing e-health data in telemedicine applications. Gupta et al. [101] proposed AaYusH, an Ethereum-based smart contract and IPFS protocol for securing telesurgery systems in healthcare 4.0. The authors outperformed the performance on latency and data storage cost. Kordestani et al. [174] proposed HapiChain, a blockchain-based scheme for telemedicine applications. It ensures healthcare data security, scalability, and reliability using DApps as a platform. Gupta et al. [175] proposed BITS, a blockchain-based 6G-enabled tactile Internet telesurgical system addressing security, high data storage cost, privacy, and latency issues. Gupta et al. [176] propounded BATS, a blockchain and AI-based drone-assisted telesurgery system underlying 6G network. The use of IPFS led to low storage cost, low packet loss ratio, and low bandwidth consumption as compared to the previous approach [101].

(1) Hardware-Based Solutions. Hardware-based solutions include employing physical unclonable functions (PUF) that use one-way hash functions. Xie et al. [177] proposed a lightweight authentication scheme for BAN sensors using PUF. The body sensors establish a shared secret to secure the data exchange between the implants with low overhead. Tan et al. [178] propounded a cloud-assisted and PUF-based authentication scheme for WBAN using multiple hops. It resulted in reduced storage overhead and reduced data transmission loss. Wang et al. [179] use PUF for securing BAN sensor pairs without any encryption schemes and preventing impersonation attacks.

4. The Proposed Approach

The integration of smart healthcare in users' daily activities has improved their quality of life. It has many entities such as wearable devices, IoT sensors, mobile devices, dynamic databases to access information, and the Internet. They continuously connected to share real-time healthcare data from wearable devices to different predictive services to improve users' health. However, this approach is vulnerable to various security issues such as distributed denial of service (DDoS), session hijacking, privilege escalation, and injection attacks, where an attacker can easily manipulate the healthcare data to misguide the healthcare specialist. Therefore, there is a need for a secure architecture that can analyze such malicious behavior of the attacker. This section introduces the working of the proposed architecture that is divided into three layers as shown in Figure 4, i.e., data acquisition, data analysis, and application layer. A comprehensive description of each layer is as follows.

4.1. Data Acquisition Layer. This layer constitutes multiple IoT sensors placed on the human body in the proposed architecture, such as smart bands, hearing aids, neural interfaces, and immersive helmets. These sensors collect the real-time health status of the body; for example, EEG records any abnormalities in the brain, smart shoes provide a person's posture, calories, and step count, and smartwatches monitor blood pressure, heart, and respiration rates. These wearable devices come with an implicit application interface in the smartphone. As a result, the data is collected in the smartphone using a 6G network interface [180]. The data is stored inside some centralized system, such as a healthcare information system (HIS), which is generally acquired by nation-states. This healthcare information is crucial for any medical practitioner, doctor, drug specialist, and medical institution to predict an unknown disease and develop a drug for a pandemic, population management, and decision-making process. The recent coronavirus outbreak is a perfect example elucidating the importance of healthcare data to medical institutions such as the World Health Organization (WHO). The clinical and health data of all the COVID-19 patients makes it possible to develop an extensive range of COVID-19 vaccines. Conversely, due to the high necessity of this data, it is always susceptible to attackers. The healthcare data carry valuable information of the users such as social security numbers, radiological images, insurance claims, and diagnosis records. An attacker can perform data tampering and network attacks that seize

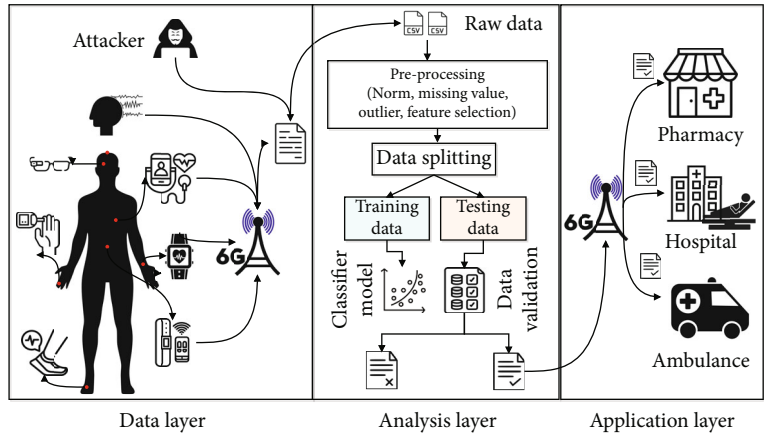

Figure 4: AI-based smart and secure healthcare architecture.

the data for nefarious purposes. Therefore, an AI-based architecture has been proposed to analyze the network attacks and classify the correct and attacked data.

4.2. Data Analytic Layer. This layer consolidates ML classifiers to analyze the healthcare data for malicious conduct. To achieve this, a log file that is maintained by every wearable device has to be acquired for analysis purposes. A raw dataset can be formed by analyzing the network activities and critical warnings in the log file. The collected raw dataset is converted into an ML-based compatible format, i.e., a comma-separated value (CSV) file. It has healthcare data of all the users utilizing wearable devices connected to their bodies and the attack data. The attack data can misguide the doctors, which can risk human life, and hence need to eradicate from the normal data, whereas the normal data guide the doctors to diagnose the patient further. From the perspective of ML, it is a binary classification problem; that is, normal data is classified as 0 and attack data is classified as 1. To accomplish the classification task, the raw dataset needs to be preprocessed before passing it to the learning models, as it has outliers that can mislead the classifiers. If the data is not normalized, it means few values are small in the data columns and few are large. Missing values in the columns can make the learning model biased. Consequently, preprocess steps equipped with outlier detection, normalization, filling missing values, and feature selection are applied to the dataset. While doing so, it also needs to verify the imbalanced dataset problem, in which if the majority class is higher than the minority class, the ML model gets biased towards the majority class. Resampling techniques such as oversampling and undersampling can vividly balance the dataset. Next, the balanced dataset is divided into train and test data to validate the final prediction. The output is based on various performance metrics such as accuracy, precision, recall, and Matthews correlation coefficient (MCC) value. It is challenging to decide which metrics are reliable for proper classification, as each has its pros and cons. The MCC value has been taken as the final metric to fix this obscurity because it is popularly used in binary classification problems.

4.3. Application Layer. The data analytics layer classifies the valid data from the attack data and forwards it to the application layer via a 6G network interface. This layer comprises different use cases such as hospitals, pharmacies, ambulances, and medical institutions where validated healthcare data is utilized for rapid drug development, early diagnosis, easy tracking and reporting of disorder, and faster clinical trials. This layer also deals with quick information sharing between the wearable device and medical specialists in a medical emergency. For example, a patient at a remote location and stuck with a heart attack, his wearable device tries to send this information via a cellular network to the nearby hospitals. The conventional cellular networks such as 4G and 5G are not competent enough to send this information readily to the medical staff. This is because it has low data rates (20/10 Gbps), high latency (100 ns), and low reliability (10^{5}). Therefore, the benefits of a 6G network such as ultra-low latency (<1 ms), ubiquitous high-speed data connectivity (1 Tbps), scalable connectivity (10^{9} devices/sqm), and ultra-high reliability (99.99999%) are accompanied in the proposed architecture. A 6G-enabled proposed framework augments the application layer by quickly sharing the healthcare data with the medical staff, improving human life expectancy.

Figure 5 shows the sequence flow of the proposed approach, initiating with taxonomy on smart healthcare technologies. The taxonomy is classified into wearable devices, body area networks, and digital healthcare. Then, security aspects of smart healthcare have been discussed, after which various security solutions for smart healthcare have been presented. To mitigate these security issues in smart healthcare technologies, an AI-based architecture has been proposed with a 6G network consisting of data acquisition, data analytic, and application layers.

5. UAV-Assisted Secure Healthcare for COVID-19 Outbreak: A Case Study

The COVID-19 pandemic is one of the difficult outbreaks the world has faced in recent years. COVID-19 is an infectious disease that spreads quickly from an infected person's

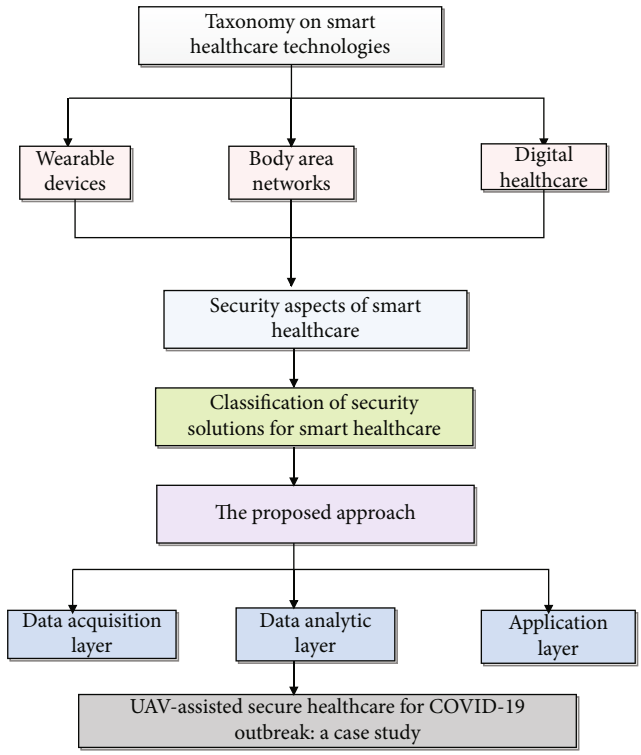

Figure 5: Sequence flow of the proposed survey.

mouth or nose when they sneeze or cough. Therefore, it is difficult for doctors to provide adequate medical treatment to COVID-19 patients without carrying proper precautionary measures. Despite personal protective equipment (PPE) kits, disposable gloves, disinfectants, antibiotics, and other possible preventive measures, COVID-19 is still a crisis that has impacted mental health and the nation's economy. Therefore, there is a requirement for a technology that collects COVID-19 patient data, limits physical contact, and reduces the spread of infection. Integrating UAVs in such situations can help in fighting the growing number of COVID-19 patients. UAVs are especially used in remote locations for healthcare delivery, where they fastly deliver critical medicines, vaccines, and blood packages. However, due to the surface transmission in COVID-19, such as a person who has the virus coughed or sneezed gets touched by the other person and the person gets contaminated with coronavirus. This hugely affects the medical doctors and coworkers who continuously contact the COVID-19 patient for their regular checkups and follow-ups. Therefore, a UAV-assisted smart and secure healthcare has been proposed as shown in Figure 6 to mitigate the aforementioned issue. UAVs are used to acquire the healthcare data of ground users using their wearable devices. Based on the assumption that every user has a fitness tracker (smart band) which has measurements such as oxygen saturation (SpO_2), heart rate, temperature, and blood pressure, which is crucial for COVID-19 cases. In the COVID-19 layer, UAVs collect the abovementioned measurements and share them with the application layer via a 6G network interface. Additionally, UAVs are equipped with imaging and IoT sensors; for example, thermal sensors can identify a user with a temperature greater than the COVID-19 temperature threshold, that is, 37.8°C or greater. Furthermore, the COVID-19 patients are disjointed from the typical hospitals and shifted to different COVID-19 medical centers due to the contagious virus. However, these centers are infrastructure-less; hence, it has to contact the hospital every time they need an update on the patient.

Thus, UAVs can be beneficial for faster content delivery between hospitals and COVID-19 centers. It can collect the data from the wearable device of the COVID-19 patient and share it with the hospital. The UAV can share the information with the relay UAV using UAV-to-UAV communication if the hospital is far away.

5.1. Dataset Description. Nevertheless, the security of the aforementioned approach is in question because an attacker can proliferate their attack and manage to tamper with the healthcare data. For example, an attacker can target wearable devices to exploit them and acquire users' medical data or broadcast a DDoS on resource-constrained devices, i.e., wearable sensors. The medical data is critical for doctors; based on this data, the doctors start their diagnosis. Hence, it is essential to prevent the medical data from the attacker who tries to manipulate it for their malicious intent. We have used a wearable healthcare dataset with normal and attack data to analyze this. The original dataset has 188697 $\times$ 52 numbers of columns and rows. The dataset has been generated using different IoT sensors placed with a patient bed, to which an MQ Telemetry Transport- (MQTT-) based attack has been performed by the attackers. A Wireshark tool has been deployed between the communication link to sniff and capture the network traffic as raw data. Later this data is converted into an appropriate CSV format as an input to the ML model. The raw dataset has outliers, missing and vague values, and unnormalized data, which needs to be processed before sending it to the ML model. Therefore, the dataset is verified against the abovementioned issues using various python functions. The dataset has a large feature space of 52 features, which needs to be reduced using principal component analysis (PCA). It works on the principle of eigenvalues and eigenvectors, which indicates the necessary features to be included in the dataset. Figure 7 illustrates the cumulative variance graph signifies that the initial 23 features contain 94% of the variance. Therefore, we have reduced the features space from 52 to 25 in our dataset.

Next, the processed data is divided into a training and testing dataset, where the training data is validated against the test data. It is then further delivered to multiple ML classifiers such as RF, linear discriminant analysis (LDA), ridge, logistic regression, naive Bayes, and perceptron to classify the normal and malicious data. From Figure 8, it can be seen that RF got 98% of accuracy and outperformed compared to other classifiers. The high accuracy is due to its versatility in solving classification problems, efficient decision-making, robustness to outliers, and less impact by noise. The RF uses high correlation in decision trees by splitting a random set of features. As a result, the RF algorithm considers a small set of features instead of all the features for training the model.

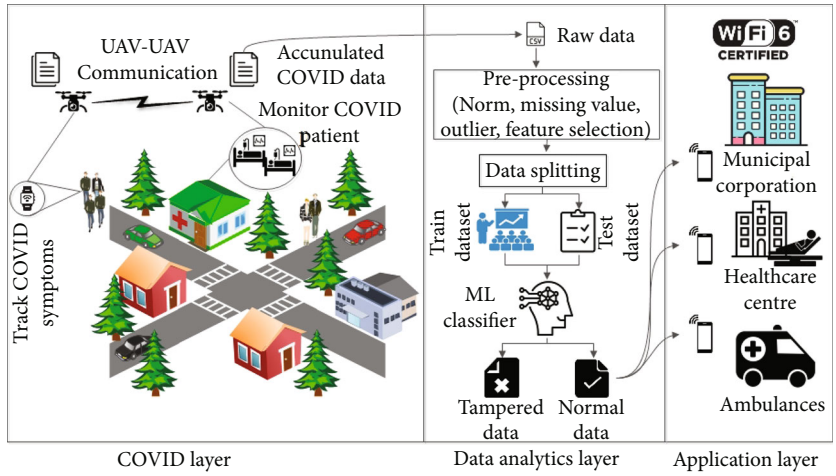

Figure 6: AI-assisted smart and secure healthcare for COVID-19.

In addition, it has the versatility in handling binary, numeric, and categorical features in training. One of the significant issues of the binary classification problem is its unbalanced dataset, where accuracy fluctuates as per the dominant class. This is adequately handled by the sampling and the RF algorithm, which minimizes the overall error rate of the class, influencing the proposed architecture to achieve higher accuracy. Contrary, the LDA algorithm is slightly underrated due to its overfitting problem with large datasets; however, the performance of LDA still matches with the RF. Ridge algorithm is an extension to the logistic regression, where a hyperparameter is utilized to improve the accuracy; however, the problem lies in its high bias and low interpretability model that reduces the algorithm's accuracy. Additionally, a perceptron is a fundamental neural network that needs more number of hidden layers to provide better accuracy. However, doing so increases the computational complexity of the model. Therefore, we have applied only one hidden layer to reduce the complexity, but it significantly reduces the model's accuracy.

Moreover, in Figure 9, a log-loss score graph has been composed to assess the performance of the classifiers. It displays how close is the prediction values to the actual values. The higher the divergence of the prediction values from the actual values, the higher the log-loss score. It is apparent from the graph that the perceptron has a considerable log-loss score value, and therefore, there is an exponential rise in the graph curve, whereas the RF has a minuscule log-loss score value, and hence, it is near to 0. Some of the merits of the proposed solution are as follows.

(i) Use of wearable technology and adopting UAV communication can help in providing instant medical treatment despite an outbreak

(ii) System's latency is reduced to <1 ms

(iii) Increases the system's reliability and scalability to 99.99999% and 1099 devices/sqm, respectively

(iv) Enhances the security and privacy of the smart healthcare system using AI models

6. Open Issues and Research Challenges/Future Challenges and Research Opportunities

In this section, we consolidated open security issues and research challenges in smart healthcare technology.

6.1. Security. The data generated by the various wearable devices and BANs can encounter various security and privacy issues in the smart healthcare system as patients data may contain their personal information that is being shared among different medical staff before sending it to the doctors. Also, data needs to be secure from multiple sensors and wireless technologies through which hackers can attack to get their personal information. Thus, there is a need to adapt counter security measures to provide the security and confidentiality in the smart healthcare system.

6.2. Data Sharing. In smart healthcare system, data from the IoT devices gets shared to the healthcare professionals, but there is no certainty that how their data is getting processed and how many people are involved in it before sending it to the doctors. For example, if some attacker tampers with the data, then patients can get the wrong medicine or even get no prescription by the doctors. It can lead to the delay in their treatment or may be more threatening for their health. Therefore, there is a need to control the data sharing or introduce a mechanism to secure the data transmission in the smart healthcare system.

6.3. Voluminous Data. A considerable amount of data is collected from various wearable devices attached to human bodies. Furthermore, this data is continuously changing as per the patient's health status. To manage such a dynamic and massive amount of information is a cumbersome task. Moreover, different kinds of data need to be stored in a different kind of format. For example, an IoT sensor captures the EEG of the brain, which is in an image format, to run an ML model on it; it needs to be converted into a CSV format. Hence, there is a need to have an efficient

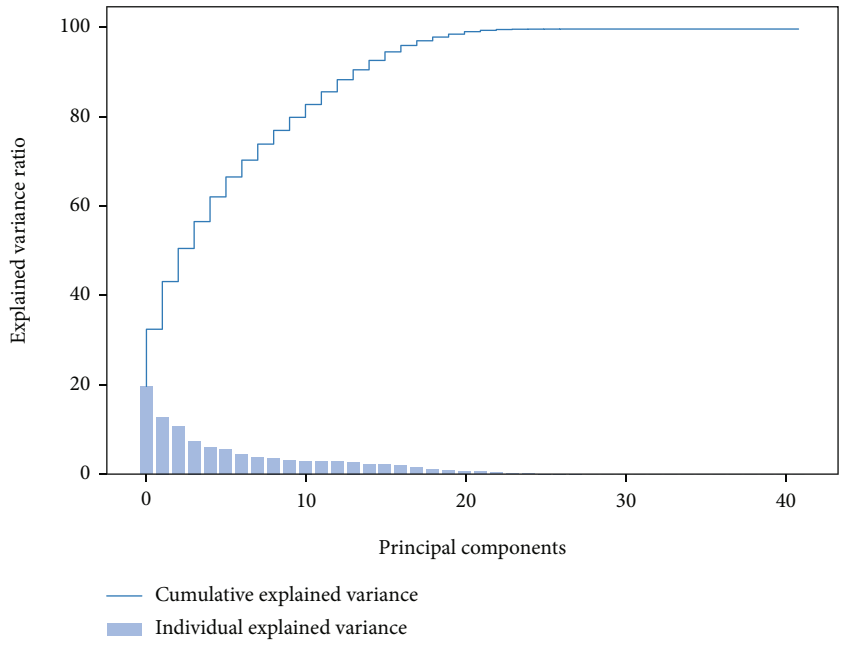

Figure 7: Cumulative variance by feature space.

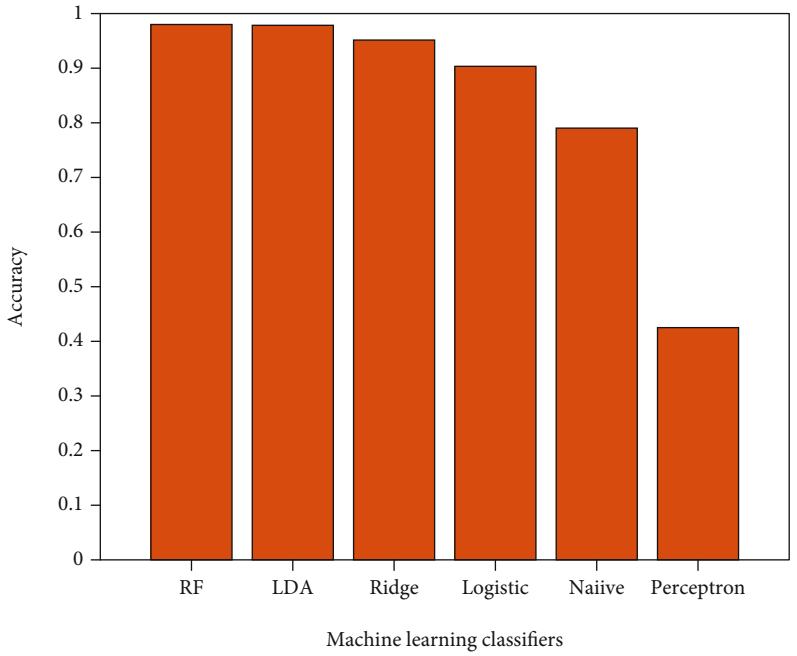

Figure 8: Accuracy comparison.

storage mechanism that converts the file according to the need of an application.

6.4. High Power Consumption. Wearable devices are battery-constrained devices that continuously monitor and track the patient's health status; in doing so, it consumes a large amount of power from the battery. Consequently, the user needs to charge it multiple times. To resolve this issue, the user needs to put their devices in sleep mode at regular intervals when not monitoring the health status.

6.5. Lack of Standardization. Multiple devices are used in the smart healthcare systems to relay healthcare data. Each device has a different set of protocols and configurations to share this information with medical staff. However, there is no centralized consensus or standardization available for communication, implementation, and deployment of IoT sensors in the healthcare sector. Hence, there is a need to do research on this aspect where the IoT devices with different standards and protocols can communicate without any hinderance.

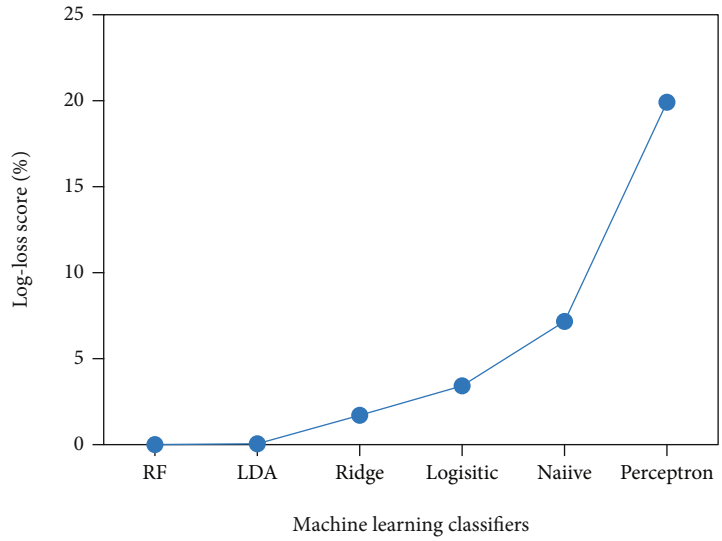

Figure 9: Log-loss score of ML classifiers.

6.6. Computationally Expensive. Consolidating ML to assimilate smart and secure healthcare is computationally expensive. The reason behind this is the voluminous healthcare data, which an ML model has to execute. As the size of the dataset increases, the execution time of ML increases. As a consequence, the prediction service responds delinquently to the medical staff in case of an emergency. Hence, a deep learning-based model has to be utilized in the smart healthcare system to overcome this issue.

7. Conclusion

In this paper, we presented a comprehensive survey on smart healthcare technologies such as wearable devices, BANs, and digital healthcare to encounter security and privacy issues in the smart healthcare system. In addition, a comparative analysis of various state-of-the-art healthcare schemes has been discussed. Based on it, we presented a taxonomical classification of different smart healthcare technologies with their security issues. Then, we propose an AI-based secure and reliable architecture incorporating a 6G network interface for smart healthcare technologies. The employed AI model ensures the secure transmission of healthcare data to healthcare professionals. Furthermore, to evaluate the proposed architecture, we have studied a case study on the COVID-19 pandemic to devise a UAV-assisted secure healthcare framework to prevent it from security attacks. Finally, we have discussed open issues and research challenges for smart healthcare technologies. In the future, we will explore a novel solution by amalgamating blockchain technology and AI models to enhance the security and reliability of smart healthcare technologies.

Data Availability

No data were associated with this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by Taif University Researchers Supporting Project number (TURSP-2020/126), Taif University, Taif, Saudi Arabia.

References

[1] S. Hermes, T. Riasanow, E. K. Clemons, M. Bohm, and H. Krcmar, "The digital transformation of the healthcare industry: exploring the rise of emerging platform ecosystems and their influence on the role of patients," *Business Research*, vol. 13, no. 3, pp. 1033–1069, 2020.

[2] J. Vora, S. Tanwar, S. Tyagi, N. Kumar, and J. J. P. C. Rodrigues, "Home-based exercise system for patients using IoT enabled smart speaker," in *2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 1–6, Dalian, China, 2017.

[3] M. Gupta, S. Tanwar, A. Rana, and H. Walia, "Smart healthcare monitoring system using wireless body area network," in *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*, pp. 1–5, Noida, India, 2021.

[4] O. Taiwo and A. E. Ezugwu, "Smart healthcare support for remote patient monitoring during COVID-19 quarantine," *Informatics in Medicine Unlocked*, vol. 20, article 100428, 2020.

[5] S. Zeadally, F. Siddiqui, Z. Baig, and A. Ibrahim, *Smart Healthcare: Challenges and Potential Solutions Using Internet of Things (IoT) and Big Data Analytics*, PSU Research Review, 2020.

[6] M. W. Condry, X. I. Quan, and M. Fang, "Digital health: innovation, opportunity and challenges," in *IECON 2020 the 46th Annual Conference of the IEEE Industrial Electronics Society*, pp. 3408–3412, Singapore, 2020.

[7] T. O. K. Zaw, S. Muthaiyah, and A. Jasbi, "Contextualization of smart healthcare: a systematic review," in *2021 7th International Conference on Research and Innovation in Information Systems (ICRIIS)*, pp. 1–6, Johor Bahru, Malaysia, 2021.

[8] L. P. Malasinghe, N. Ramzan, and K. Dahal, "Remote patient monitoring: a comprehensive study," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 1, pp. 57–76, 2019.

[9] G. Devedžić, S. Koceski, and S. P. Savić, "A brief overview of enabling technologies for digital medicine and smart healthcare," in *2021 10th Mediterranean Conference on Embedded Computing (MECO)*, pp. 1–5, Budva, Montenegro, 2021.

[10] S. Tanwar, S. Tyagi, N. Kumar, and M. S. Obaidat, "LA-MHR: learning automata based multilevel heterogeneous routing for opportunistic shared spectrum access to enhance lifetime of WSN," *IEEE Systems Journal*, vol. 13, no. 1, pp. 313–323, 2019.

[11] S. Tian, W. Yang, J. M. Le Grange, P. Wang, W. Huang, and Z. Ye, "Smart healthcare: making medical care more intelligent," *Global Health Journal*, vol. 3, no. 3, pp. 62–65, 2019.

[12] P. Sundaravadivel, E. Kougianos, S. P. Mohanty, and M. K. Ganapathiraju, "Everything you wanted to know about smart health care: evaluating the different technologies and components of the Internet of Things for better health," *IEEE Consumer Electronics Magazine*, vol. 7, no. 1, pp. 18–28, 2018.

[13] L. Balakrishnan, "An Internet of Things (IoT) based intelligent framework for healthcare–a survey," in *2021 3rd International Conference on Signal Processing and Communication (ICPSC)*, pp. 243–251, Coimbatore, India, 2021.

[14] A. Al Sadawi, M. S. Hassan, and M. Ndiaye, "A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges," *IEEE Access*, vol. 9, pp. 54478–54497, 2021.

[15] P. Thakkar, K. Varma, V. Ukani, S. Mankad, and S. Tanwar, "Combining user-based and itembased collaborative filtering using machine learning," in *Information and Communication Technology for Intelligent Systems*, S. C. Satapathy and A. Joshi, Eds., pp. 173–180, Springer Singapore, Singapore, 2019.

[16] P. Kumar and M. Sharma, "Data, machine learning, and human domain experts: none is better than their collaboration," *International Journal of Human–Computer Interaction*, pp. 1–14, 2021.

[17] Y. Dong and Y.-D. Yao, "IoT platform for COVID-19 prevention and control: a survey," *IEEE Access*, vol. 9, pp. 49929–49941, 2021.

[18] W. Li, Y. Chai, F. Khan et al., "Editorial: cognitive computing for Internet of Multimedia Things," *Mobile Networks and Applications*, vol. 26, no. 1, pp. 234–252, 2021.

[19] S. Sobhan, S. Islam, M. Valero, H. Shahriar, and S. I. Ahamed, "Data analysis methods for health monitoring sensors: a survey," in *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*, pp. 669–676, Madrid, Spain, 2021.

[20] S. Sharma, M. Tripathi, and V. Mishra, "Survey paper on sensors for body area network in health care," in *2017 International Conference on Emerging Trends in Computing and Communication Technologies (ICETCCT)*, pp. 1–6, Dehradun, India, 2017.

[21] Y. Shaikh, V. Parvati, and S. Biradar, "Survey of smart healthcare systems using Internet of Things (IoT)," in *2018 International Conference on Communication, Computing and Internet of Things (IC3IoT)*, pp. 508–513, Chennai, India, 2018.

[22] P. Saranya and P. Asha, "Survey on big data analytics in health care," in *2019 International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pp. 46–51, Tirunelveli, India, 2019.

[23] M. M. Mahmoud, J. J. Rodrigues, and K. Saleem, "Cloud of Things for healthcare: a survey from energy efficiency perspective," in *2019 International Conference on Computer and Information Sciences (ICCIS)*, pp. 1–7, Sakaka, Saudi Arabia, 2019.

[24] C. Diwaker, A. Jangra, and A. Rani, "Survey on IoT health care techniques," in *2019 5th International Conference on Signal Processing, Computing and Control (ISPCC)*, pp. 383–385, Solan, India, 2019.

[25] Q. Cai, H. Wang, Z. Li, and X. Liu, "A survey on multimodal data-driven smart healthcare systems: approaches and applications," *IEEE Access*, vol. 7, pp. 133583–133599, 2019.

[26] M. Rwibasira and R. Suchithra, "A survey paper on consensus algorithm of mobile-healthcare in blockchain network," in *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*, pp. 1–5, Vellore, India, 2020.

[27] S. Amin, T. Salahuddin, and A. Bouras, "Cyber physical systems and smart homes in healthcare: current state and challenges," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, pp. 302–309, Doha, Qatar, 2020.

[28] H. Vahdat-Nejad, Z. Abbasi-Moud, S. A. Eslami, and W. Mansoor, "Survey on context-aware healthcare systems," in *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 1190–1196, NV, USA, 2021.

[29] H. M. Shakir and J. Karimpour, "Survey on load balancing in fog computing in smart healthcare system," in *2021 International Conference on Advanced Computer Applications (ACA)*, pp. 128–131, Maysan, Iraq, 2021.

[30] M. Dhuheir, A. Albaseer, E. Baccour, A. Erbad, M. Abdallah, and M. Hamdi, "Emotion recognition for healthcare surveillance systems using neural networks: a survey," in *2021 International Wireless Communications and Mobile Computing (IWCMC)*, pp. 681–687, Harbin City, China, 2021.

[31] Y. Yang, H. Wang, R. Jiang, X. Guo, J. Cheng, and Y. Chen, "A review of IoT-enabled mobile healthcare: technologies, challenges, and future trends," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9478–9502, 2022.

[32] A. Kadu and M. Singh, "Comparative analysis of e-health care telemedicine system based on Internet of Medical Things and artificial intelligence," in *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*, pp. 1768–1775, Trichy, India, 2021.

[33] V. Prasad, M. Bhavsar, and S. Tanwar, "Influence of monitoring: fog and edge computing," *SCPE*, vol. 20, no. 2, pp. 365–376, 2019.

[34] R. Zhang, R. Xue, and L. Liu, "Security and privacy for healthcare blockchains," *IEEE Transactions on Services Computing*, pp. 1–1, 2021.

[35] L. Omrčen, H. Leventić, K. Romić, and I. Galić, "Integration of blockchain and AI in EHR sharing: a survey," in *2021 International Symposium ELMAR*, pp. 155–160, Zadar, Croatia, 2021.

[36] B. M. G. Rosa and G. Z. Yang, "Smart wireless headphone for cardiovascular and stress monitoring," in *2017 IEEE 14th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, pp. 75–78, Eindhoven, Netherlands, 2017.

[37] T. S. Enamamu, N. Clarke, P. Haskell-Dowland, and F. Li, "Smart watch based body-temperature authentication," in *2017 International Conference on Computing Networking and Informatics (ICCNI)*, pp. 1–7, Lagos, Nigeria, 2017.

[38] M. Ko, S. Kim, K. Lee, M. Kim, and K. Kim, "Single camera based 3D tracking for outdoor fall detection toward smart healthcare," in *2017 2nd International Conference on Bioengineering for Smart Technologies (BioSMART)*, pp. 1–4, Paris, France, 2017.

[39] M. A. Gacem, S. Alghlayini, W. Shehieb, M. Saeed, A. Ghazal, and M. Mir, "Smart assistive glasses for Alzheimer's patients," in *2019 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, pp. 1–5, Ajman, United Arab Emirates, 2019.

[40] Y. Zhang, P. Delir Haghighi, F. Burstein, L. Wei Yap, W. Cheng, and F. Cicuttini, "Out-of-hospital body movement data collection using E-skin sensors," in *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 346–348, Kyoto, Japan, 2019.

[41] S. Baek, H. Eom, Y. S. Hariyani et al., "Deep learning based heart rate estimation using smart shoes sensor," in *2020 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)*, pp. 1–4, Seoul, Korea (South), 2020.

[42] R. Rabbani, H. Najafiaghdam, M. M. Ghanbari et al., "Towards an implantable fluorescence image sensor for real-time monitoring of immune response in cancer therapy," in *2021 43rd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC)*, pp. 7399–7403, Mexico, 2021.

[43] J. Hossain Gourob, S. Raxit, and A. Hasan, "A robotic hand: controlled with vision based hand gesture recognition system," in *2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI)*, pp. 1–4, Rajshahi, Bangladesh, 2021.

[44] T. Basaklar, Y. Tuncel, S. An, and U. Ogras, "Wearable devices and low-power design for smart health applications: challenges and opportunities," in *2021 IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED)*, pp. 1–1, Boston, MA, USA, 2021.

[45] D. Kumar and T. Mufti, "Impact of coronavirus on global cloud based wearable tracking devices," in *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, pp. 1–5, Noida, India, 2021.

[46] S. K. Behera, "Chipless RFID sensors for wearable applications: a review," *IEEE Sensors Journal*, vol. 22, no. 2, pp. 1105–1120, 2022.

[47] N. M. Kumar, N. Kumar Singh, and V. K. Peddiny, "Wearable smart glass: features, applications, current progress and challenges," in *2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT)*, pp. 577–582, Bangalore, India, 2018.

[48] H.-W. Kim, M. Y. Kim, S.-H. Yang, K.-Y. Kim, H.-M. Son, and Y.-J. Lee, "Smart wearable robot glasses for human visual augmentation based on human intention and scene understanding," in *2010 International Symposium on Optomechatronic Technologies*, pp. 1–5, Toronto, ON, Canada, 2010.

[49] Q. Zhou, D. Yu, M. N. Reinoso, J. Newn, J. Goncalves, and E. Velloso, "Eyes-free target acquisition during walking in immersive mixed reality," *IEEE Transactions on Visualization and Computer Graphics*, vol. 26, no. 12, pp. 3423–3433, 2020.

[50] B. V. Varun, S. M. Kusuma, and G. Reddy, "AI-edge based voice responsive smart headphone for user context-awarenes," in *2020 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, pp. 1–5, Bangalore, India, 2020.

[51] H. Baumgartner, A. Schulz, A. Hein, I. Holube, and T. Herzke, "A fitting method for headphones to compensate individual hearing impairments," in *2009 3rd International Conference on Pervasive Computing Technologies for Healthcare*, pp. 1–8, London, UK, 2009.

[52] E. Garcia-Espinosa, O. Longoria-Gandara, A. Veloz-Guerrero, and G. G. Riva, "Hearing aid devices for smart cities: a survey," in *2015 IEEE First International Smart Cities Conference (ISC2)*, pp. 1–5, Guadalajara, Mexico, 2015.

[53] B. Rajan, B. Bhavana, K. R. Anusha, G. Kusumanjali, and G. S. Pavithra, "IoT based smart and efficient hearing aid using arm cortex microcontroller," in *2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)*, pp. 229–233, Bengaluru, India, 2020.

[54] J. Y. Han, W. Z. Zheng, R. J. Huang, Y. Tsao, and Y. H. Lai, "Hearing aids app design based on deep learning technology," in *2018 11th International Symposium on Chinese Spoken Language Processing (ISCSLP)*, pp. 495-496, Taipei, Taiwan, 2018.

[55] *Introduction to Information Sciences and Technology*December 2021, https://sites.psu.edu/ist110pursel/2018/03/20/immersive-helmet/.

[56] *Virtual Reality Immersive Helmets*December 2021, https://www.google.co.in/amp/s/www.livescience.com/amp/62042-helmets-one-strange-rock.html.

[57] *iHuman Perspective: Neural Interfaces*December 2021, https://royalsociety.org/topics-policy/projects/ihuman-perspective/.

[58] S. Seneviratne, Y. Hu, T. Nguyen et al., "A survey of wearable devices and challenges," *IEEE Communications Surveys Tutorials*, vol. 19, no. 4, pp. 2573–2620, 2017.

[59] Y. Krainyk, Y. Darnapuk, and I. Simakova, "Software system for physical activity monitoring: smart watch case," in *2020 IEEE 5th International Symposium on Smart and Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS)*, pp. 1–4, Dortmund, Germany, 2020.

[60] K. C. Lee, K. E. Seong, and S. J. Kang, "Self-organizing watch platform for assisting and reminding personal activity," in *2013 IEEE 7th International Conference on Self-Adaptation and Self-Organizing Systems Workshops*, pp. 15-16, Philadelphia, PA, USA, 2013.

[61] Q. Cai, J. Sun, L. Xia, and X. Zhao, "Implementation of a wireless pulse oximeter based on wrist band sensor," in *2010 3rd International Conference on Biomedical Engineering and Informatics*, vol. 5, pp. 1897–1900, Yantai, China, 2010.

[62] R. R. Rao, A. Singh, and V. Kamath, "Assessment of step accuracy and usability of activity trackers," in *2018 3rd*

International Conference on Contemporary Computing and Informatics (IC3I), pp. 38–42, Gurgaon, India, 2018.

[63] S. M. Mankar and S. A. Chhabria, "Review on hand gesture based mobile control application," in *2015 International Conference on Pervasive Computing (ICPC)*, pp. 1-2, Pune, India, 2015.

[64] N. R. Sogi, P. Chatterjee, U. Nethra, and V. Suma, "SMARISA: a raspberry pi based smart ring for women safety using IoT," in *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)*, pp. 451–454, Coimbatore, India, 2018.

[65] S. Nguyen, C. Duong, and R. Amirtharajah, "A smart health tracking ring powered by wireless power transfer," in *2021 IEEE Wireless Power Transfer Conference (WPTC)*, pp. 1–4, San Diego, CA, USA, 2021.

[66] S. Zhang, A. Chhetry, S. Sharma, C. Park, and J. Y. Park, "An Mxene-Edot nanocomposite based strain sensor patch for wireless human motion monitoring," in *2021 21st International Conference on Solid-State Sensors, Actuators and Microsystems (Transducers)*, pp. 341–344, Orlando, FL, USA, 2021.

[67] N. Lu, "Soft electronics for human-centered robotics," in *2021 IEEE International Conference on Flexible and Printable Sensors and Systems (FLEPS)*, pp. 1–1, Manchester, United Kingdom, 2021.

[68] L. Yin, P. Deng, J. Ma et al., "Large-area, fully conformable, μm-thick e-tattoo for high-fidelity in situ personal health monitoring," in *2019 IEEE 19th International Conference on Nanotechnology (IEEENANO)*, pp. 211–214, Macao, China, 2019.

[69] M. Yang and J. Cheng, "Research and development of smart health monitoring clothing system," in *2018 37th Chinese Control Conference (CCC)*, pp. 8231–8234, Wuhan, China, 2018.

[70] P.-Y. Hwang, C.-C. Chou, W.-C. Fang, and C.-M. Hwang, "Smart shoes design with embedded monitoring electronics system for healthcare and fitness applications," in *2016 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)*, pp. 1-2, Nantou, Taiwan, 2016.

[71] S. Saidani, R. Haddad, and R. Bouallegue, "A prototype design of a smart shoe insole system for real-time monitoring of patients," in *2020 6th IEEE Congress on Information Science and Technology (CiSt)*, pp. 116–121, Agadir - Essaouira, Morocco, 2020.

[72] T. Thepudom, T. Seesaard, W. Donkrajang, and T. Kerdcharoen, "Healthcare shoe system for gait monitoring and foot odor detections," in *2013 IEEE 2nd Global Conference on Consumer Electronics (GCCE)*, pp. 81-82, Tokyo, Japan, 2013.

[73] H. Nam, J.-H. Kim, and J.-I. Kim, "Smart belt: a wearable device for managing abdominal obesity," in *2016 International Conference on Big Data and Smart Computing (BigComp)*, pp. 430–434, Hong Kong, 2016.

[74] L. M. Borges, N. Barroca, F. J. Velez, and A. S. Lebres, "Smart-clothing wireless flex sensor belt network for foetal health monitoring," in *2009 3rd International Conference on Pervasive Computing Technologies for Healthcare*, pp. 1–4, London, UK, 2009.

[75] A. Molley, K. Beaumont, T. Kirimi et al., "Challenges to the development of the next generation of self-reporting cardiovascular implantable medical devices," *IEEE Reviews in Biomedical Engineering*, vol. 15, pp. 260–272, 2022.

[76] S. Vaddiraju, M. Kastellorizios, A. Legassey, D. Burgess, F. Jain, and F. Papadimitrakopoulos, "Needle-implantable, wireless biosensor for continuous glucose monitoring," in *2015 IEEE 12th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, pp. 1–5, Cambridge, MA, USA, 2015.

[77] P. Hung, S. Bonnet, R. Guillemaud, E. Castelli, and P. T. N. Yen, "Estimation of respiratory waveform using an accelerometer," in *2008 5th IEEE International Symposium on Biomedical Imaging: From Nano to Macro*, pp. 1493–1496, Paris, France, 2008.

[78] V. P. Rachim and W.-Y. Chung, "Wearable noncontact armband for mobile ECG monitoring system," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 10, no. 6, pp. 1112–1118, 2016.

[79] K. Aziz, S. Tarapiah, S. H. Ismail, and S. Atalla, "Smart real-time healthcare monitoring and tracking system using GSM/GPS technologies," in *2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC)*, pp. 1–7, Muscat, Oman, 2016.

[80] F. P. Akbulut and A. Akan, "Smart wearable patient tracking systems," in *2015 Medical Technologies National Conference (TIPTEKNO)*, pp. 1–4, Bodrum, Turkey, 2015.

[81] A. B. Jani, R. Bagree, and A. K. Roy, "Design of a low-power, low-cost ECG & EMG sensor for wearable biometric and medical application," in *2017 IEEE SENSORS*, pp. 1–3, Glasgow, UK, 2017.

[82] N. N. Chu, "Wearable sensors for brain EEG signal oriented applications," in *2018 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1–1, Las Vegas, NV, USA, 2018.

[83] R. Narasimhan, T. Parlikar, G. Verghese, and M. V. McConnell, "Finger-wearable blood pressure monitor," in *2018 40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pp. 3792–3795, Honolulu, HI, USA, 2018.

[84] H. Anuar and P. L. Leow, "Non-invasive core body temperature sensor for continuous monitoring," in *2019 IEEE International Conference on Sensors and Nanotechnology*, pp. 1–4, Penang, Malaysia, 2019.

[85] S. Matsushita and R. Kaneshima, "Motion sensing eyewear for daily healthcare monitoring," in *2019 IEEE 8th Global Conference on Consumer Electronics (GCCE)*, pp. 925–928, Osaka, Japan, 2019.

[86] C.-L. Hsu, T.-V. Le, M.-C. Hsieh, K.-Y. Tsai, C.-F. Lu, and T.-W. Lin, "Three-factor UCSSO scheme with fast authentication and privacy protection for telecare medicine information systems," *IEEE Access*, vol. 8, pp. 196553–196566, 2020.

[87] F. Zou, Z. Wang, S. Ma, L. Li, and Y. Cheng, "Multi-physiological parameters integrated medical system for home healthcare application," in *2021 IEEE 14th International Conference on ASIC (ASICON)*, pp. 1–4, Kunming, China, 2021.

[88] J. Hodgkiss and S. Djahel, "Securing fuzzy vault enabled authentication in body area networks-based smart healthcare," *IEEE Consumer Electronics Magazine*, vol. 11, no. 1, pp. 6–16, 2022.

[89] H.-J. Yoo and J. Bae, "Low energy wireless body area network systems," in *2013 IEEE International Wireless Symposium (IWS)*, pp. 1-2, Beijing, China, 2013.

[90] X. Tian, M. Zhang, and J. S. Ho, "Robust and high-efficiency wireless body area networks with spoof surface plasmons on

clothing," in *2019 IEEE MTT-S International Microwave Symposium (IMS)*, pp. 1507–1510, Boston, MA, USA, 2019.

[91] B. Vardhini, S. N. Dass, R. Sahana, and R. Chinnaiyan, "A blockchain based electronic medical health records framework using smart contracts," in *2021 International Conference on Computer Communication and Informatics (ICCCI)*, pp. 1–4, Coimbatore, India, 2021.

[92] N. Kobayashi and S. Homma, "Analysis of telemonitoring multi vital data for alert detection on telecare system," in *2019 IEEE 1st Global Conference on Life Sciences and Technologies (LifeTech)*, pp. 123-124, Osaka, Japan, 2019.

[93] Y. Yang and T. Chen, "Analysis and visualization implementation of medical big data resource sharing mechanism based on deep learning," *IEEE Access*, vol. 7, pp. 156077–156088, 2019.

[94] A. Koren and R. Prasad, "Personal wireless data in formal electronic health records: future potential of Internet of Medical Things data," in *2020 23rd International Symposium on Wireless Personal Multimedia Communications (WPMC)*, pp. 1–4, Okayama, Japan, 2020.

[95] N. J. Lehmann, F. Spielmann, B. George et al., "mHealthAtlas-an approach for the multidisciplinary evaluation of mHealth applications," in *2020 IEEE International Conference on E-health Networking, Application & Services (HEALTHCOM)*, pp. 1–5, Shenzhen, China, 2021.

[96] S.-M. Chiu, Y.-C. Chen, J.-W. Lin, C.-H. Tsai, and C. Lee, "Interactive mobile app for self-supervised health management," in *2021 IEEE 3rd Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability (ECBIOS)*, pp. 199–201, Tainan, Taiwan, 2021.

[97] A. Saini, D. Wijaya, N. Kaur, Y. Xiang, and L. Gao, "LSP: lightweight smart contract-based transaction prioritization scheme for smart healthcare," *IEEE Internet of Things Journal*, 2022.

[98] J. H. Han and J. Y. Lee, "Digital healthcare industry and technology trends," in *2021 IEEE International Conference on Big Data and Smart Computing (BigComp)*, pp. 375–377, Jeju Island, Korea (South), 2021.

[99] J. Quintanar-Gomez, D. Robles-Camarillo, F. R. Trejo-Macotela, and I. Campero-Jurado, "Telemonitoring device of blood pressure and heart rate through multilayer perceptrons and pulse rate variability," *IEEE Latin America Transactions*, vol. 19, no. 7, pp. 1233–1241, 2021.

[100] T. Ninikrishna, M. Kumar, N. Kumar, P. Karn, and S. V. Rachana, "An efficient IoT based body parameters telemonitoring system," in *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, pp. 1167–1171, Coimbatore, India, 2020.

[101] R. Gupta, A. Shukla, and S. Tanwar, "Aayush: a smart contract-based telesurgery system for healthcare 4.0," in *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, Dublin, Ireland, 2020.

[102] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and B. Sadoun, "Habits: blockchain-based telesurgery framework for healthcare 4.0," in *2019 International Conference on Computer, Information and Telecommunication Systems (CITS)*, pp. 1–5, Beijing, China, 2019.

[103] N. Jeyanthi, R. Thandeeswaran, and H. Mcheick, "SCT: secured cloud based telemedicine," in *The 2014 International Symposium on Networks, Computers and Communications*, pp. 1–4, Hammamet, Tunisia, 2014.

[104] L. Su, "Application of telemedicine diagnosis assistant system for breast diseases patients," in *2020 13th International Conference on Intelligent Computation Technology and Automation (ICICTA)*, pp. 453–456, Xi'an, China, 2020.

[105] L. A. Tawalbeh and S. Habeeb, "An integrated cloud based healthcare system," in *2018 Fifth International Conference on Internet of Things: Systems, Management and Security*, pp. 268–273, Valencia, Spain, 2018.

[106] M. Suguna, M. Ramalakshmi, J. Cynthia, and D. Prakash, "A survey on cloud and Internet of Things based healthcare diagnosis," in *2018 4th International Conference on Computing Communication and Automation (ICCCA)*, pp. 1–4, Greater Noida, India, 2018.

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

[108] K. Hung, Y. Zhang, and B. Tai, "Wearable medical devices for tele-home healthcare," in *The 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, vol. 2, pp. 5384–5387, San Francisco, CA, USA, 2004.

[109] N. Sharma, Z. Shareef, and S. Reddy, "Fit-wit: design and development of wearable healthcare device based on Intel Curie platform," in *2017 International Conference on Computing, Communication and Automation (ICCCA)*, pp. 1271–1276, Greater Noida, India, 2017.

[110] M. F. Pasha, H. S. Lee, A. Widhiasi, R. Purba, A. Mansour, and R. Budiarto, "Neural nework-based mobile app framework to aid resource-poor setting community health," in *2020 International Conference on Computing and Information Technology (ICCIT-1441)*, pp. 1–5, Tabuk, Saudi Arabia, 2020.

[111] N. Butt and J. Shan, "Cybercare: a novel electronic health record management system," in *2016 IEEE First International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, pp. 326-327, Washington, DC, USA, 2016.

[112] K. Intawong, P. Ong-artborirak, and W. Boonchieng, "Seamless electronic medical record for health management system in emergency patients," in *2021 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunication Engineering*, pp. 189–192, Cha-am, Thailand, 2021.

[113] D. Li, Z. Ye, L. Li, X. Wei, B. Qin, and Y. Li, "Practical data mid-platform design and implementation for medical big data," in *2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, vol. 1, pp. 1042–1045, Chengdu, China, 2019.

[114] M. Kuznetsov, A. Elor, S. Kurniawan et al., "The immersive graph genome explorer: navigating genomics in immersive virtual reality," in *2021 IEEE 9th International Conference on Serious Games and Applications for Health (SeGAH)*, pp. 1–8, Dubai, United Arab Emirates, 2021.

[115] S. Campbell, "The precise - and wild - genomics revolution: genomics provides novel treatments for disease and is opening new frontiers for precision medicine," *IEEE Pulse*, vol. 7, no. 5, pp. 20–25, 2016.

[116] S. Panicacci, M. Donati, L. Fanucci, I. Bellin, F. Profili, and P. Francesconi, "Population health management exploiting machine learning algorithms to identify high-risk patients," in *2018 IEEE 31st International Symposium on Computer-*

Based Medical Systems (CBMS), pp. 298–303, Karlstad, Sweden, 2018.

[117] H. B. Wu and H. Gao, "The application of TCM five-pattern personality and constitution identification system in population health management of elderly people in community," in *2018 9th International Conference on Information Technology in Medicine and Education (ITME)*, pp. 300–303, Hangzhou, China, 2018.

[118] R. Sharma, N. Sharma, and M. Mangla, "An analysis and investigation of infostealers attacks during COVID'19: a case study," in *2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC)*, pp. 443–449, Jalandhar, India, 2021.

[119] M. Abdelhamid, "The role of health concerns in phishing susceptibility: survey design study," *Journal of Medical Internet Research*, vol. 22, no. 5, article e18394, 2020.

[120] S. Venkatesha, K. R. Reddy, and B. Chandavarkar, "Social engineering attacks during the COVID-19 pandemic," *SN Computer Science*, vol. 2, no. 2, pp. 1–9, 2021.

[121] R. Gupta, S. Tanwar, N. Kumar, and S. Tyagi, "Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: a systematic review," *Computers & Electrical Engineering*, vol. 86, pp. 1–12, 2020.

[122] J. Rieck, "Attacks on fitness trackers revisited: a case-study of unfit firmware security," 2016, https://arxiv.org/abs/1604.03313.

[123] E. Marin, D. Singelee, F. D. Garcia, T. Chothia, R. Willems, and B. Preneel, "On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them," in *Proceedings of the 32nd Annual Conference on Computer Security Applications, ACSAC '16*, pp. 226–236, New York, NY, USA, 2016.

[124] D. Kim, S. Park, K. Choi, and Y. Kim, "Burnfit: analyzing and exploiting wearable devices," in *Information Security Applications*, H. W. Kim and D. Choi, Eds., pp. 227–239, Springer International Publishing, Cham, 2016.

[125] M. Rahman, B. Carbunar, and U. Topkara, "Secure management of low power fitness trackers," *IEEE Transactions on Mobile Computing*, vol. 15, no. 2, pp. 447–459, 2016.

[126] S. Banerjee, V. Odelu, A. K. Das et al., "Design of an anonymity-preserving group formation based authentication protocol in global mobility networks," *IEEE Access*, vol. 6, pp. 20673–20693, 2018.

[127] M. Zhang, A. Raghunathan, and N. K. Jha, "Towards trustworthy medical devices and body area networks," in *Proceedings of the 50th Annual Design Automation Conference, DAC '13*, New York, NY, USA, 2013.

[128] S. R. Zahra and M. Ahsan Chishti, "Ransomware and Internet of Things: a new security nightmare," in *2019 9th International Conference on Cloud Computing, Data Science Engineering (Confluence)*, pp. 551–555, Noida, India, 2019.

[129] F. Wei, P. Vijayakumar, J. Shen, R. Zhang, and L. Li, "A provably secure password-based anonymous authentication scheme for wireless body area networks," *Computers & Electrical Engineering*, vol. 65, pp. 322–331, 2018.

[130] X. Liu, R. Zhang, and M. Zhao, "A robust authentication scheme with dynamic password for wireless body area networks," *Computer Networks*, vol. 161, pp. 220–234, 2019.

[131] M. Kim, J. Moon, D. Won, and N. Park, "Revisit of password-authenticated key exchange protocol for healthcare support wireless communication," *Electronics*, vol. 9, no. 5, p. 733, 2020.

[132] A. Arya, C. Reddy, and T. Limbasiya, "An improved remote user verification scheme in wireless body area networks," *Procedia Computer Science*, vol. 113, pp. 113–120, 2017.

[133] A. M. Koya and P. P. Deepthi, "Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network," *Computer Networks*, vol. 140, pp. 138–151, 2018.

[134] H. Tan and I. Chung, "Secure authentication and group key distribution scheme for WBANs based on smartphone ECG sensor," *IEEE Access*, vol. 7, pp. 151459–151474, 2019.

[135] M. Mohammedi, M. Omar, W. Aitabdelmalek, A. Mansouri, and A. Bouabdallah, "Secure and lightweight biometric-based remote patient authentication scheme for home healthcare systems," in *2018 International Symposium on Programming and Systems (ISPS)*, pp. 1–6, Algiers, Algeria, 2018.

[136] K. A. Shakil, F. J. Zareen, M. Alam, and S. Jabin, "BAM-HealthCloud: a biometric authentication and data management system for healthcare data in cloud," *Journal of King Saud University-Computer and Information Sciences*, vol. 32, no. 1, pp. 57–64, 2020.

[137] A. Sharma and A. P. Bhatt, "Quantum cryptography for securing IoT-based healthcare systems," in *Limitations and Future Applications of Quantum Cryptography*, pp. 124–147, IGI Global, 2021.

[138] V. Gaikwad, R. Somkuwar, M. Barde, J. Burde, and T. Vaidya, "Authentication using elliptical curve cryptography for e-healthcare system," *Journal of Network Security and Data Mining*, vol. 3, no. 1, 2020.

[139] C.-M. Chen, B. Xiang, T.-Y. Wu, and K.-H. Wang, "An anonymous mutual authenticated key agreement scheme for wearable sensors in wireless body area networks," *Applied Sciences*, vol. 8, no. 7, p. 1074, 2018.

[140] S. Jegadeesan, M. Azees, N. R. Babu, U. Subramaniam, and J. D. Almakhles, "EPAW: efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (WBANs)," *IEEE Access*, vol. 8, pp. 48576–48586, 2020.

[141] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," *Future Generation Computer Systems*, vol. 78, pp. 956–963, 2018.

[142] F. K. Dankar and R. Badji, "A risk-based framework for biomedical data sharing," *Journal of Biomedical Informatics*, vol. 66, pp. 231–240, 2017.

[143] A. R. Rajput, Q. Li, M. Taleby Ahvanooey, and I. Masood, "EACMS: emergency access control management system for personal health record based on blockchain," *IEEE Access*, vol. 7, pp. 84304–84317, 2019.

[144] A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," *IEEE Access*, vol. 7, pp. 147782–147795, 2019.

[145] J. Xu, K. Xue, S. Li et al., "Healthchain: a blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8770–8781, 2019.

[146] L. Wu, X. Du, M. Guizani, and A. Mohamed, "Access control schemes for implantable medical devices: a survey," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1272–1283, 2017.

[147] A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal, "Healing on the cloud: secure cloud architecture for medical

wireless sensor networks," *Future Generation Computer Systems*, vol. 55, pp. 266–277, 2016.

[148] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving fusion of IoT and big data for e-health," *Future Generation Computer Systems*, vol. 86, pp. 1437–1455, 2018.

[149] J. A. Alzubi, "Blockchain-based Lamport Merkle digital signature: authentication tool in IoT healthcare," *Computer Communications*, vol. 170, pp. 200–208, 2021.

[150] S. El Abkari, S. Kaissari, J. El Mhamdi, A. Jilbab, and E. H. El Abkari, "RFID system for hospital monitoring and medication tracking using digital signature," in *Digital Technologies and Applications*, S. Motahhir and B. Bossoufi, Eds., pp. 1051–1060, Springer International Publishing, Cham, 2021.

[151] U. Kumar, R. K. Pathak, and A. Kumar, "Handling secure healthcare data streaming using R2E algorithm," in *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, pp. 732–737, Coimbatore, India, 2020.

[152] A. Margheri, M. Masi, A. Miladi, V. Sassone, and J. Rosenzweig, "Decentralised provenance for healthcare data," *International Journal of Medical Informatics*, vol. 141, article 104197, 2020.

[153] H. Wu, Y. Shang, L. Wang, L. Shi, K. Jiang, and J. Dong, "A patient-centric interoperable framework for health information exchange via blockchain," in *ICBTA 2019*, pp. 76–80, Association for Computing Machinery, New York, NY, USA, 2019.

[154] T. C. M. Donmez and E. Nigussie, "Key management through delegation for LoRaWAN based healthcare monitoring systems," in *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)*, pp. 1–6, Oslo, Norway, 2019.

[155] Q. Jiang, J. Ma, C. Yang, X. Ma, J. Shen, and S. A. Chaudhry, "Efficient end-to-end authentication protocol for wearable health monitoring systems," *Computers & Electrical Engineering*, vol. 63, pp. 182–195, 2017.

[156] D. He and S. Zeadally, "Authentication protocol for an ambient assisted living system," *IEEE Communications Magazine*, vol. 53, no. 1, pp. 71–77, 2015.

[157] O. Salem, A. Guerassimov, A. Mehaoua, A. Marcus, and B. Furht, "Anomaly detection in medical wireless sensor networks using SVM and linear regression models," *IJEHMC*, vol. 5, no. 1, pp. 20–45, 2014.

[158] S. Rajendran, S. K. Mathivanan, P. Jayagopal et al., "Emphasizing privacy and security of edge intelligence with machine learning for healthcare," *International Journal of Intelligent Computing and Cybernetics*, vol. 15, no. 1, pp. 92–109, 2022.

[159] S. Pirbhulal, N. Pombo, V. Felizardo, N. Garcia, A. H. Sodhro, and S. C. Mukhopadhyay, "Towards machine learning enabled security framework for IoT-based healthcare," in *2019 13th International Conference on Sensing Technology (ICST)*, pp. 1–6, Sydney, NSW, Australia, 2019.

[160] M. Begli, F. Derakhshan, and H. Karimipour, "A layered intrusion detection system for critical infrastructure using machine learning," in *2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE)*, pp. 120–124, Oshawa, ON, Canada, 2019.

[161] S. Sengan, O. I. Khalaf, P. Vidya Sagar, D. K. Sharma, L. Arokia Jesu Prabhu, and A. A. Hamad, "Secured and privacy-based IDS for healthcare systems on E-medical data using machine learning approach," *International Journal of Reliable and Quality E-Healthcare*, vol. 11, no. 3, pp. 1–11, 2022.

[162] A. Arora, A. Nethi, P. Kharat et al., "Isthmus: secure, scalable, real-time and robust machine learning platform for healthcare," 2019, https://arxiv.org/abs/1909.13343.

[163] M. Marwan, A. Kartit, and H. Ouahmane, "Security enhancement in healthcare cloud using machine learning," *Procedia Computer Science*, vol. 127, pp. 388–397, 2018.

[164] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, "Blockchain-based data preservation system for medical data," *Journal of Medical Systems*, vol. 42, no. 8, pp. 1–13, 2018.

[165] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "Medblock: efficient and secure medical data sharing via blockchain," *Journal of Medical Systems*, vol. 42, no. 8, pp. 1–11, 2018.

[166] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure EHRs sharing of mobile cloud based e-health systems," *IEEE Access*, vol. 7, pp. 66792–66806, 2019.

[167] R. Kakkar, R. Gupta, S. Tanwar, and J. J. P. C. Rodrigues, "Coalition game and blockchain-based optimal data pricing scheme for ride sharing beyond 5G," *IEEE Systems Journal*, pp. 1–10, 2021.

[168] Y. Wang, A. Zhang, P. Zhang, and H. Wang, "Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain," *IEEE Access*, vol. 7, pp. 136704–136719, 2019.

[169] E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O.-Y. Song, A. K. Bashir, and A. A. Abd El-Latif, "DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems," *IEEE Access*, vol. 8, pp. 111223–111238, 2020.

[170] A. Islam and S. Young Shin, "A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things," *Computers & Electrical Engineering*, vol. 84, article 106627, 2020.

[171] K. Miyachi and T. K. Mackey, "hOCBS: a privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design," *Information Processing & Management*, vol. 58, no. 3, article 102535, 2021.

[172] R. Thanki and A. Kothari, "Multi-level security of medical images based on encryption and watermarking for telemedicine applications," *Multimedia Tools and Applications*, vol. 80, no. 3, pp. 4307–4325, 2021.

[173] R. F. Mansour and S. A. Parah, "Reversible data hiding for electronic patient information security for telemedicine applications," *Arabian Journal for Science and Engineering*, vol. 46, pp. 9129–9144, 2021.

[174] H. Kordestani, K. Barkaoui, and W. Zahran, "Hapichain: a blockchain-based framework for patient-centric telemedicine," in *2020 IEEE 8th International Conference on Serious Games and Applications for Health (SeGAH)*, pp. 1–6, Vancouver, BC, Canada, 2020.

[175] R. Gupta, U. Thakker, S. Tanwar, M. S. Obaidat, and K.-F. Hsiao, "Bits: a blockchain-driven intelligent scheme for telesurgery system," in *2020 International Conference on Computer, Information and Telecommunication Systems (CITS)*, pp. 1–5, Hangzhou, China, 2020.

[176] R. Gupta, A. Shukla, and S. Tanwar, "BATS: a blockchain and AI-empowered drone-assisted telesurgery system towards 6G," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 4, pp. 2958–2967, 2021.

[177] L. Xie, W. Wang, X. Shi, and T. Qin, "Lightweight mutual authentication among sensors in body area networks through physical unclonable functions," in *2017 IEEE International Conference on Communications (ICC)*, pp. 1–6, Paris, France, 2017.

[178] X. Tan, J. Zhang, Y. Zhang, Z. Qin, Y. Ding, and X. Wang, "A PUF-based and cloud-assisted lightweight authentication for multi-hop body area network," *Tsinghua Science and Technology*, vol. 26, no. 1, pp. 36–47, 2021.

[179] W. Wang, X. Shi, and T. Qin, "Encryption-free authentication and integrity protection in body area networks through physical unclonable functions," *Smart Health*, vol. 12, pp. 66–81, 2019.

[180] K. Sheth, K. Patel, H. Shah, S. Tanwar, R. Gupta, and N. Kumar, "A taxonomy of AI techniques for 6G communication networks," *Computer Communications*, vol. 161, pp. 279–303, 2020.