Knowledge-Based Systems 274 (2023) 110658

Contents lists available at ScienceDirect

Knowledge-Based Systems

journal homepage: www.elsevier.com/locate/knosys

Federated learning for secure IoMT-applications in smart healthcare systems: A comprehensive review

Sita Rani [a], Aman Kataria [b], Sachin Kumar [c], Prayag Tiwari [d,*]

[a] Department of Computer Science & Engineering, Guru Nanak Dev Engineering College, Ludhiana 141006, Punjab, India
[b] CSIR-CSIO, Chandigarh 160030, India
[c] Big Data and Machine Learning Lab, South Ural State University (National Research University), 454080, Chelyabinsk, Russian Federation
[d] School of Information Technology, Halmstad University, Sweden

ARTICLE INFO

Article history:
Received 22 November 2022
Received in revised form 9 March 2023
Accepted 17 May 2023
Available online 22 May 2023

Keywords:
Data security
Encryption
Federated learning
IoT
IoMT
Machine learning
Privacy
Smart healthcare
Security mechanisms

ABSTRACT

Recent developments in the Internet of Things (IoT) and various communication technologies have reshaped numerous application areas. Nowadays, IoT is assimilated into various medical devices and equipment, leading to the progression of the Internet of Medical Things (IoMT). Therefore, various IoMT-based healthcare applications are deployed and used in the day-to-day scenario. Traditionally, machine learning (ML) models use centralized data compilation and learning that is impractical in pragmatic healthcare frameworks due to rising privacy and data security issues. Federated Learning (FL) has been observed as a developing distributed collective paradigm, the most appropriate for modern healthcare framework, that manages various stakeholders (e.g., patients, hospitals, laboratories, etc.) to carry out training of the models without the actual exchange of sensitive medical data. Consequently, in this work, the authors present an exhaustive survey on the security of FL-based IoMT applications in smart healthcare frameworks. First, the authors introduced IoMT devices, their types, applications, datasets, and the IoMT security framework in detail. Subsequently, the concept of FL, its application domains, and various tools used to develop FL applications are discussed. The significant contribution of FL in deploying secure IoMT systems is presented by focusing on FL-based IoMT applications, patents, real-world FL-based healthcare projects, and datasets. A comparison of FL-based security techniques with other schemes in the smart healthcare ecosystem is also presented. Finally, the authors discussed the challenges faced and potential future research recommendations to deploy secure FL-based IoMT applications in smart healthcare frameworks.

1. Introduction

In the past few years, exponential growth has been observed in medical data generation through smart healthcare systems [1]. Most of the data are gathered using the Internet of Things (IoT). The IoT assimilated into various medical devices and equipment, led to the evolution of the Internet of Medical Things (IoMT). IoMT has captured almost all the medical domains [2]. Nowadays, in smart healthcare systems, medical sensors are integrated into wearable devices, home-based and hospital-based equipment. These smart medical devices have the potential to observe patients' health continuously in real-time. Even medical robots can do surgeries and other medical tasks like remote monitoring, patient care, etc. [3,4].

The huge volume of data gathered using IoMT provides new space for the development and amalgamation of advanced computational techniques to analyze, process, store, and utilize to improve the quality of treatment and care [5,6]. Voluminous healthcare data is commonly mutilated and scattered due to the convoluted constitution of IoMT in healthcare systems. Different stakeholders, like hospitals, laboratories, doctors, etc., may have access to vital medical data of their patients. These medical records are extremely delicate due to the sensitive health information of human beings that require secure access and less communication delay [7]. Strict guidelines like Health Insurance Portability and Accountability Act (HIPAA) [8] are framed to administer the process of interpreting and using such data. It causes many challenges for various advanced data processing techniques, such as ML, DL, etc., requiring a huge volume of training data [9].

Federated Learning (FL) is an archetype gaining massive acceptance due to its ability to learn with mutilated delicate data. It works on the concept of distributed learning by using a

* Corresponding author.
E-mail addresses: cse_sita@gndec.ac.in (S. Rani), ammankataria@gmail.com (A. Kataria), kumars@susu.ru (S. Kumar), prayag.tiwari@hh.se (P. Tiwari).

https://doi.org/10.1016/j.knosys.2023.110658

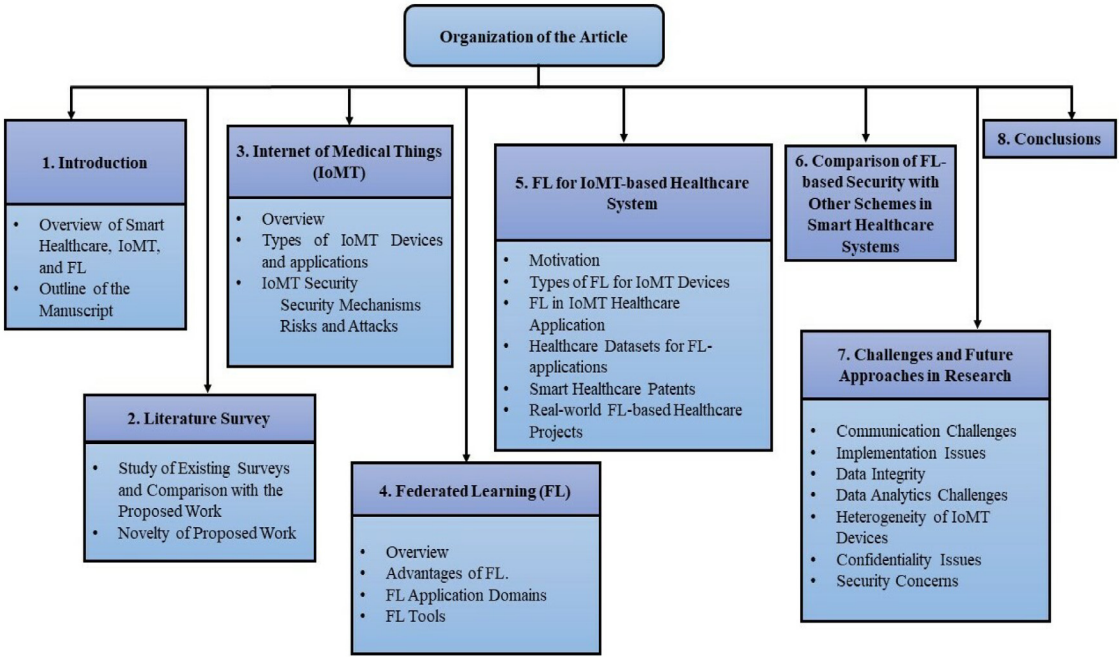

Fig. 1. Organization of the manuscript.

global shared model from which data is kept in the local places/institutions of origination. The global model is placed on a centralized server. FL retains an extensive potential to analyze distributed healthcare data. While using the FL model, medical data/records remain with the individuals/patients and hospitals depending upon the type of application [10,11] which ensures their privacy.

The fundamental objectives of the proposed work are to survey the framework of IoMT and associated security risks and project FL's role in securing IoMT applications. In this paper, after a brief introduction, the authors present an insightful discussion on IoMT devices/equipment, FL applications, and FL's role in developing secure IoMT applications. Authors have explored the potential of FL techniques in various IoMT applications by discussing recent developments, like FL-based IoMT applications, various patents filed/published in the domain, real-world projects, and FL-based public healthcare datasets. FL-based IoMT security is also compared with the security aspects of other technologies in the healthcare sector. In the end, the authors discussed the various challenges and open research directions to deploy IoMT applications in the smart healthcare ecosystem. The detailed organization of the article is depicted in Fig. 1.

2. Literature survey

In the past few years, a lot of work has been carried out by researchers by focusing on the domains of smart healthcare systems, FL, and IoMT. Many researchers emphasized FL's role in IoT, IoMT, Industry 4.0, and smart healthcare.

In [12], the authors expressed concern about two major industrial issues: distributed sources and data security. FL is presented as the most appropriate solution to address both of these issues. In this work, the authors proposed a comprehensive framework comprising horizontal, vertical, and transfer FL. The authors discussed the FL architecture in detail and comprehensively reviewed its various application areas. A detailed comparison of FL with privacy-preserving ML, distributed machine learning, edge computing, and federated databases are also discussed in this paper. The authors concluded their work by presenting the potential research directions.

In [1], the rapid development of medical data generated due to ICT's integration into healthcare is emphasized. The data are generated from numerous sources, like hospitals, patients, laboratories, the pharmaceutical industry, insurance companies, etc. But due to the sensitive nature of medical records, their exchange among the various stakeholders is challenging from security aspects. The authors of this paper presented the FL model as one of the key role players in assuring the security of health records and reviewed the various FL technologies in this particular domain. Applications of FL in other domains, like finance, smart retail, etc., are also briefed.

In [13], the authors presented high communication costs, heterogeneity of the systems and statistical methods, and privacy as the major challenges in optimizing distributed problems. These issues are the key drivers of the shift from conventional learning to FL in various domains. FL framework optimizes the learning process and preserves data privacy. The authors concluded their work by discussing the future research directions to design FL models for real-life situations.

In [14], authors introduced FL as a decentralized framework, fundamentally to address data security and privacy issues. Basic characteristics, open-source framework, and types of FL are discussed in detail. In this paper, the authors emphasized that FL models are deployed to address the major issues associated with communication cost, heterogeneity, privacy, and data security. ML applications in healthcare, mobile devices, industrial processes, etc., are also discussed. The work is concluded by presenting possible research directions to deploy FL models/applications.

In [15], the authors described the significant role played by AI, ML, and DL in various medical domains like radiology, medicine, disease detection, pathology, drug design, genomics, etc. Advanced ML and DL models use massive datasets during training to obtain clinical-level efficiency whilst being secure. In this work, FL is introduced as a developing paradigm to handle the issues of data administration and security. FL-based healthcare models do not require patients' data to be transmitted beyond the boundaries of the institution where they are stored. This work describes the benefits of deploying healthcare models to

various stakeholders like clinicians, hospitals, medical practitioners, providers, manufacturers, and researchers. Various challenges faced in designing FL-based healthcare models, like data heterogeneity, security, and traceability, are also briefed.

In [16], the authors discussed the revolutionary change in Industry 4.0 by integrating the Industrial Internet of Things (IIoT). It was highlighted that to assure data privacy in the smart industry is the biggest challenge faced by various stakeholders. The authors presented the vital role played by FL in addressing this challenge in Industry 4.0. The FL deployment model ensures data security in the end devices, at the time of transfer, and on the cloud servers. The vital contribution of FL to data security is justified by giving suitable examples in the automobile industry and healthcare domains. The authors highlighted security, less communication cost, better performance of the communication networks, and scalability as the fundamental factors behind the assimilation of FL in IIoT.

In [17], the authors introduced FL as a new paradigm to enhance security and privacy in smart environments. The sensitivity of data gathered in the domains of healthcare, smart cities, smart industry, banking, etc., is also highlighted. The authors emphasized the integration of FL in the healthcare sector as a revolution to address the various issues related to healthcare data, disease detection, medical image retrieval, and economic information availability. This paper presents a systematic study on blockchain-facilitated FL techniques to secure medical records. Blockchain-based horizontal, vertical, and transfer federated learning techniques are also presented. The authors concluded their work with open research directions.

In [18], the authors emphasized the role of IoT and mobile devices in gathering voluminous data in smart city environments. These vital data are used to train various AI and ML models that can help society prosper. Regardless of their persuasiveness, these centralized models involve many security and privacy concerns, leading to limited support for the smart city environment. The authors introduced FL as a novel framework to address security issues in various smart city applications, including smart healthcare, transportation, education, industry, finance, etc. The competence of FL to address these challenges in a smart environment is characterized and presented comprehensively. Open research opportunities in deploying FL models in various smart city domains are also presented.

In [19], the authors discussed remote healthcare monitoring as a need of the hour. Real-time management of data gathered through distributed healthcare devices is a challenge. All-time availability of data helps healthcare providers in taking important decisions timely. Still, many issues are associated with it, like data security, computational complexity, mobility of the patients, etc. FL, in association with other advanced technologies like cloud computing and fog computing, helps to address these challenges. The authors emphasized the important role played by the FL-facilitated IoMT system in encountering COVID-19. The processing tasks which can be executed on the fog layer in an FL model are also discussed. Various open research issues and possible research directions in employing FL for dealing with pandemics are also explained.

In [20], the authors introduced FL as a distributed form of ML where the model is trained through local data on different nodes. It does not require training data to be shifted to the central node, which improves security. In many applications, FL is facilitated by edge computing by using the computational resources of the edge servers. In this paper, the authors discussed the applications of edge federated learning in the domains of healthcare, vehicular networks, and recommendation systems. Major concerns that need to be considered during the design of edge FL models are the selection of APIs, characteristics of the edge devices, network topologies and configuration, and data flow models. Although edge FL systems are trained on the same line as FL systems, their design and development are relatively complex. The authors also highlighted that even an internal node from the edge network might be malignant and may attack and harm other nodes' training process. Security and privacy issues of edge FL systems are discussed in detail.

In [21], the authors highlighted the relevance of the volume of training data in deep learning systems by focusing on the domain of healthcare. It has been discussed that highly data-driven models greatly enhance the quality of services provided by clinical institutions. The sensitivity of healthcare data is one of the major concerns in the domain of healthcare, so it demands a high level of security during storage and transit. Transferring medical data to a centralized server for learning a deep learning model experiences privacy and ownership issues. The authors discussed the role of FL systems in addressing these challenges, where a global training model supported by a central aggregator server trains the model. But, the performance of FL models is limited by the factors of data partitioning, distribution, protection policies, and standard datasets. The authors discussed data streaming, hybrid data partitioning, and incentive criteria for contributors of medical data as open research directions to deploy FL models in the healthcare sector.

In [22], the authors emphasized the need for economical and better-quality healthcare services. Security and privacy are considered important measures of quality services. Security threats faced in the domain of healthcare are discussed in this work. The authors presented a DL-based secure system for smart healthcare applications. FL mechanism ensures the user's ownership of integral data in a distributed framework. A novel approach is used further to ensure privacy during the aggregation of partial models after training. The accuracy of this model is observed to be 81.9%, while all privacy-preserving approaches were implemented.

In [23], the authors introduced FL as an emerging paradigm for implementing ML applications. This system highly deviates from the centralized models and on-location analysis of data. The detailed architecture of FL systems is presented in this work. Due to the centralized approach in model training, DL systems are secure and away from communication overheads. In this paper, the authors presented an in-depth comparison of the DL and FL systems. Various challenges faced in the deployment of FL models are presented. Deploying distributed models, quality data, a well-defined distributed framework, configuration of hosting devices, data transfer, and aggregation structure are the major pre-requisites and challenges. The authors also discussed the various DL approaches used to address ML techniques' privacy and security issues. Maximum resource utilization is also observed as one of the fundamental objectives in DL models.

In [24], the authors emphasized ICT and medical technologies' significant role in gathering medical data. The collection, storage, processing, and analysis of voluminous healthcare data play a vital role in the development of clinical research. The authors emphasized the privacy and confidentiality of medical data and suggested FL as one of the most appropriate frameworks. In this work, the authors correlated the federated optimization scheme with the secure transmission-based Princess algorithm. The federated optimization scheme is observed to perform better than the Princess algorithm in terms of communication delays.

In [25], the role played by IoT devices in gathering a huge volume of data is highlighted. Transmitting voluminous data to the common central server for traditional centralized learning is a challenging task. It is affected by communication delays, data transmission costs, security issues, etc. FL is a collaborative model where training is done without the actual transfer of data to the centralized server. It ensures the privacy and security of users'

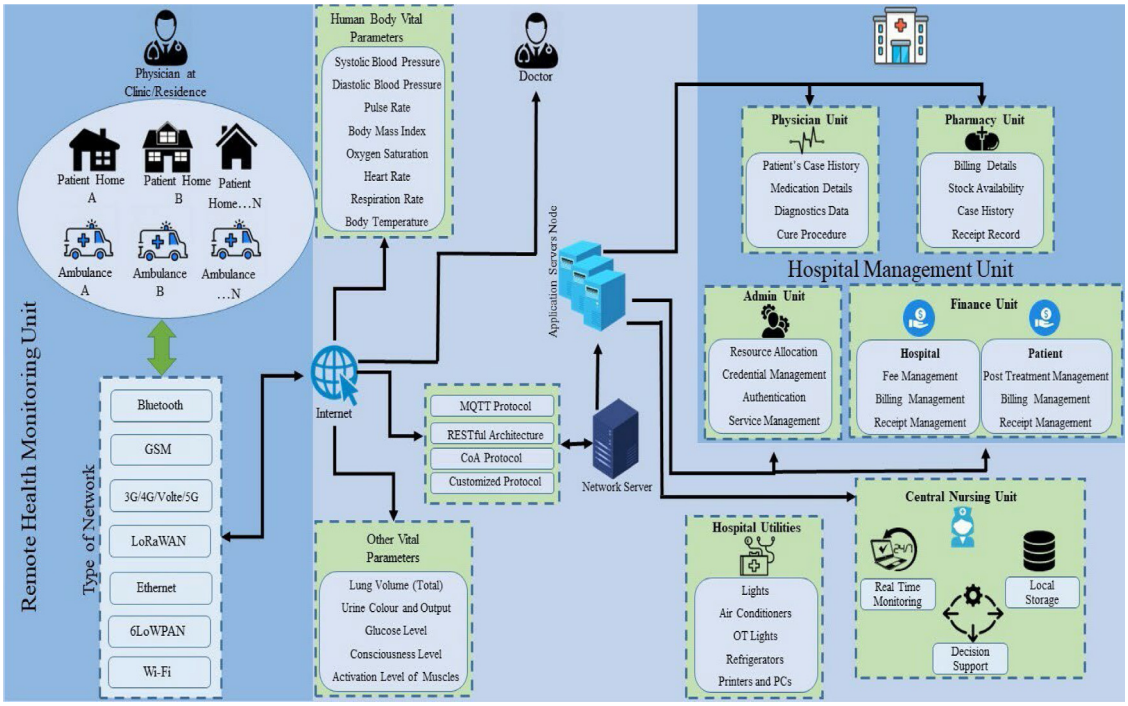

Fig. 2. Smart healthcare framework.

data. In this paper, the authors reviewed the role of FL in the IoT-based applications. Data security, better performance, flexibility, and scalability are the key reasons behind the deployment of FL models for IoT frameworks. The authors explained the application of FL in the domains of industry 4.0, smart homes and smart cities, healthcare, automated vehicles, and virtual reality. The authors concluded the paper by mentioning major challenges in deploying FL models in the IoT framework, i.e., limited bandwidth and on-device computational power, heterogeneity, lack of trustworthiness, and availability of the devices.

In [26], the authors emphasized the rapid development of FL usage in smart healthcare systems. ML applications in different areas of smart healthcare are discussed in this work. A systematic review is conducted to study the vital role of FL in the different sub-domains of healthcare systems. It was observed that major work is done in the area of data security, aggregation mechanisms, data analysis, and FL-based healthcare frameworks. The authors concluded their work by presenting a detailed FL architecture for training an electronic health record model in a smart healthcare ecosystem.

In [10], the authors highlighted the significant role performed by ICT, IoT, and AI in the healthcare sector. In the traditional scenario, centralized techniques were used for the collection, analysis, and processing of data which are observed as inefficient in highly scalable and data-sensitive modern healthcare systems. The authors presented FL as a distributed AI paradigm where multiple nodes participate in training healthcare models without transmitting highly sensitive healthcare data to centralized servers. In this work, the authors presented an exhaustive survey on the application of FL in the healthcare sector. The use of horizontal FL, Vertical FL, and FTL frameworks in the domain of smart healthcare is also explained in this work. The authors presented the motivation and need for using FL in healthcare. Five advanced forms of FL are presented in this work, i.e., Resource-aware FL, Inventive-aware FL, secure FL, privacy-improved FL, and personalized FL. This work presents various FL applications in the smart healthcare domain. The authors concluded their work by presenting various challenges faced in deploying FL models in the healthcare sector.

In the proposed work, the authors emphasized the major security issues and concerns experienced in the practical use of IoMT devices deployed in smart healthcare systems and the role of FL in addressing these challenges. Table 1 summarizes the comparison of existing work done in the domain and proposed work based on various parameters. It has been observed that the various aspects covered in this work, i.e., IoMT security, FL and its role in IoMT and smart healthcare security, real-life FL-based healthcare projects, and patents are not presented in any single existing survey, which is the major novelty of the proposed work.

3. IoMT

Recent developments in various computational areas, like Artificial Intelligence (AI), ML, IoT, Bigdata, etc., have contributed significantly to various domains [28–32]. These technologies have benefitted the domain of smart healthcare tremendously. Smart healthcare systems provide several services, i.e., remote monitoring and patient care, nursing care, admin services, pharmacy, physician services, laboratory, and utility services, for the convenience of all the stakeholders. In a smart healthcare framework, all the service-providing units are administered through different types of networks and connected through the internet (Shown in Fig. 2).

Due to revolutionized growth in IoT devices, the healthcare domain is entering a completely digital era [33]. Various advanced technologies and platforms are evolving to develop a unique functional structure for the healthcare sector [34,35]. This transformation is occurring under the control of advanced synchronization of science and technology, and their support to the continuously evolving healthcare system.

The IoMT is one of the most contemporary developments which has revolutionized the healthcare world. It has captured the entire smart healthcare framework. The amalgamation of circular economy models with IoMT has given the smart healthcare

Table 1
Comparison of characteristics of the proposed work with existing surveys.

Ref. No.	Year	Taxonomy	Types of FL	Applica-tions	Datasets	Security issues	Security mechanisms	Challenges	Future research directions	Projects	Patents
[12]	2019	FL	✔	✔	✘	✘	✘	✘	✔	✘	✘
[1]	2021	FL, Health informatics	✘	✔	✘	✔	✘	✘	✘	✘	✘
[13]	2020	FL	✘	✘	✘	✔	✘	✔	✔	✘	✘
[14]	2020	FL	✔	✔	✔	✔	✘	✔	✔	✘	✘
[15]	2020	Fl and Digital health	✘	✘	✘	✘	✘	✔	✔	✘	✘
[16]	2021	FL and Industrial Internet of Things	✘	✔	✔	✔	✔	✔	✔	✘	✘
[17]	2021	FL, Blockchain, Smart environment	✔	✘	✘	✘	✘	✔	✔	✘	✘
[18]	2020	FL, Smart city	✘	✔	✘	✘	✘	✔	✔	✘	✘
[19]	2021	FL, Data pre-processing	✘	✔	✔	✘	✘	✔	✔	✘	✘
[20]	2021	Federated learning, Edge computing	✘	✔	✘	✔	✘	✔	✔	✘	✘
[27]	2021	FL, Healthcare	✔	✔	✘	✘	✘	✔	✔	✘	✘
[22]	2022	FL, Healthcare	✘	✔	✘	✘	✘	✔	✔	✘	✘
[23]	2021	FL	✘	✔	✘	✔	✔	✔	✔	✘	✘
[24]	2022	FL, Big data, Healthcare	✘	✘	✘	✔	✔	✘	✘	✘	✘
[25]	2022	FL, Internet of Things	✘	✔	✔	✘	✘	✘	✘	✘	✘
[26]	2022	FL, Healthcare	✘	✘	✘	✔	✔	✘	✘	✘	✘
[10]	2022	FL, Smart healthcare	✔	✔	✘	✘	✘	✔	✔	✔	✘
Current review		FL, IoMT security	✔	✔	✔	✔	✔	✔	✔	✔	✔

sector a new direction by facilitating convenient data accessibility, economical patient care and treatment services, rapid system deployment, and enhanced efficiency [36,37].

A typical IoMT-system comprises 4 four layers, i.e., sensor layer, gateway layer, cloud layer, and visualization layer, which are used to gather, transmit, store, and present medical data respectively (shown in Fig. 3). These layers are connected in cyberspace.

3.1. Types of IoMT devices

IoMT devices are utilized in many healthcare applications, like physical therapy [38], pandemic administration [39,40], health monitoring [41], COVID-19 diagnosis [42,43], diabetes detection [44], cancer diagnosis, etc. Among a few prominent applications, in [45], the authors introduced the integration of IoMT and ML to recognize user emotional states. In [4], the authors gathered users' emotional states using IoMT. In [46], the authors proposed an ML model to decode patients' emotional states. In [47], a remote health monitoring system to classify routine life activities is presented. Additionally, it has been observed that the accuracy of the results obtained using various AI and ML algorithms for IoMT data is outstanding [48–50].

Different types of IoMT devices (Shown in Fig. 4) are used at the various layers of a smart healthcare system to cater to all these services. The interconnection of these IoMT devices is managed by various protocols [2], summarized in Table 2.
Some of the prominent categories of IoMT devices are discussed below [2]:

- **Wearables:** Smart healthcare devices are used to gather patients' data, observe them, and improve their well-being in real-time and economically. Smart watches, blood-pressure and glucose-level monitors, heart-rate devices, fitness bands, etc., fall under this category [51–57].
- **Home-sited IoMT Devices:** Various types of test and first-aid kits, treatment devices, infant care equipment, feeding devices, infusion pumps, voiding equipment, ventilators, etc., fall under this category of IoMT that are used outside but can connect with the hospital-sited devices and care providers using internet [58,59].
- **Hospital-sited IoMT Devices and Equipment:** Hospitals need to be well equipped in terms of staff and medical equipment for all types of situations and emergency conditions. A high degree of readiness can help in providing patients with the required treatment. So, medical donations are very crucial in such circumstances. Among these, surgical tables, anaesthesia machines, electro-surgical systems, defibrillators, etc., are some of the main hospital-sited smart equipment [60].

Many dedicated IoMT applications/systems are designed to cater to the needs of various stakeholders, shown in Table 3.

3.2. IoMT security

While on one side, the use of IoMT has entirely transformed the healthcare sector, on the other side, many issues are evolving, inclusive of costly infrastructure, overburdened communication networks, inadequate policies and standards, and security [61,62]. The security of data is one of the major concerns nowadays [63]. It is one of the main risks to the advancement of the socio-technical healthcare systems. Nowadays, it is axiomatic that the requirement of security to align with all other aspects is mandatory for the success and development of technology-equipped healthcare systems. But, the usage of IoMT has expanded the space for cyber-attacks [64]. In 2016, one of the world-renowned pharmaceutical and medical device companies, i.e., Johnson and Johnson, disclosed the susceptibility of its one product to cyber-attacks. A security expert raised this issue after personally using the insulin pump as a patient, although the hazard probability was low. Similarly, the new and evolving technological trends in healthcare, like defibrillators, pacemakers, etc., also cause a rise in security threats [65]. Consequently, the pertinent study of risk in IoMT is imperative to realize a fair idea of the security landscape in the domain of healthcare.

Table 2
IoMT interconnection protocols.

Name of the protocol	Type	Layer	Range
Bluetooth	Wireless	Physical layer	Short
6LoWPan 4G/LTE		Adaption layer Medium Access Control (MAC) layer	Medium
Wi-Fi, 802.1x		Physical layer Data Link layer	
Zigbee		Physical layer MAC layer	
Z-wave		Physical layer Mac layer Transport layer Network layer Application layer	
M2M Internet Protocol (IP)		Application layer Network layer	Long

Table 3
Various IoMT applications/systems.

S. No.	IoMT Applications/Systems	Type of application	Location of execution	Key features	Cloud compatibility	Portability
1	Zanthion	Medical alert system	Indoor and outdoor	Can be worn by the patient as jewelry or clothing.	✓	✓
2	QardioCore	ECG monitor	Indoor and outdoor	Can monitor blood pressure, diabetes, heart rate irregularities, and cholesterol.	✘	✓
3	Sensor metrix	Temperature monitoring of hospital freezers	Indoor	Monitors the temperature of blood samples, medicines, and other medical materials.	✘	✘
4	Up by Jawbone	Fitness tracker	Indoor and outdoor	Counts calories, monitors human weight, sleep patterns, and other aspects of human health.	✓	✓
5	Propeller's Breezhaler device	Asthma monitor	Indoor and outdoor	Can monitor several symptoms of asthma of the patient.	✓	✓
6	UroSense	Catheter with sensor	Indoor	Can monitor patients' urine output using a catheter which can help in detecting urine infection in the early stage.	✓	✓
7	Aware point	Patient location tracker	Indoor and outdoor	Can track the location of the patient, especially suffering from Alzheimer	✓	✓

Like any other IoT-based system, there are three fundamental categories of cyber security doctrines in IoMT: integrity, confidentiality, and availability.

- **Integrity** is a trait that assures that medical information cannot be altered or damaged using unauthorized processes or techniques.
- **Confidentiality** is the trait that guarantees access to medical data only to authentic users through valid processes and devices.
- The trait of **availability** expresses the state of being usable.

Every fundamental principle is associated with significant protection mechanism [66], depicted in Fig. 5.

Along with this, there are a few additional security concerns, discussed below [67–69]:

- **Non-cancellation of request:** It assures the grant of every request initiated by a genuine user for electronic healthcare records. A digital signature is one of the techniques that can be used to safeguard IoMT devices and smart healthcare systems.
- **Authentication:** It strengths to endorse the integrity of a user trying to connect to the healthcare system. Bilateral authentication is the best method for both the client and server to authenticate mutually.
- **Authorization:** The competence to permit the authenticated user to access and perform the tasks on medical data to which they are authorized. Authorization can be practiced using various access control mechanisms.
- **Anonymity:** The ability of the system to maintain privacy related to the identities of the patients and healthcare providers from unauthorized users.
- **Secrecy:** Two types of secrecies are applied in the exchange of keys. Forward secrecy is to ensure the safety of the keys to be exchanged in the future even if previously transmitted keys are compromised, and vice-versa for backward secrecy. These keys can further be time-synchronized for the sender and receiver nodes.
- **Secure key swap:** It focuses on the potential to safeguard the exchange of keys among the communicating nodes, i.e., sender and receiver.
- **Resilience:** It restricts the system analyst from masquerading as any unauthorized user to access sensitive information. A combination of cryptographic hash function and asymmetric key can be used to make an IoMT system resilient to unauthorized access.
- **Session key-appliance:** The communicating nodes are required to synchronize using session keys once the authentication process is done. A combination of the keys and cryptographic hash function can also be utilized to implement this practice.

In the last few years, researchers have carried out many surveys in the domain of smart healthcare and IoMT Security [64, 70–74]. The authors presented an IoMT security taxonomy and risk assessment in [61]. There are several guidelines issued by the manufacturers and vendors for secure deployment and usage of

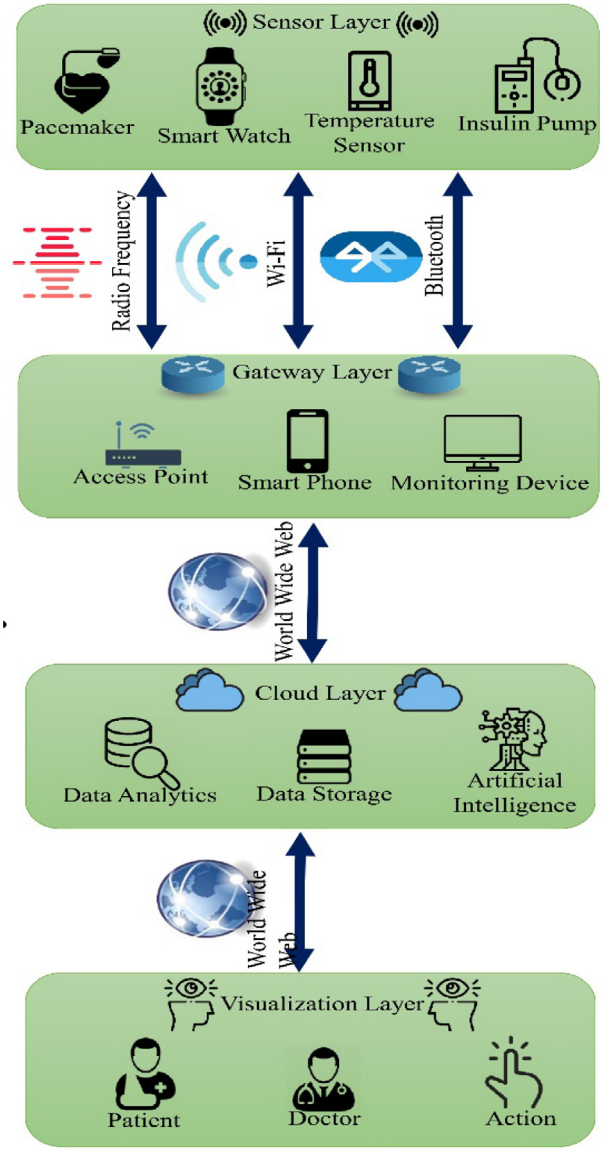

Fig. 3. IoMT-system architecture.

IoMT, which fall under three major security domains discussed below [67]:

- **Device Level Security:** The patient's medical records are collected using sensors planted in various IoMT devices. These sensing devices may experience both hardware and software attacks, like disturbing device hardware, data tampering, etc., which may be life-threatening to the patients. So, security mechanisms are required to protect these devices against cyber and physical attacks.
- **Network Security:** Medical data transmitted over communication networks are also prone to various types of attacks. Data in transit may be altered or even blocked from being transmitted. Suitable security techniques are also highly required to ensure safe data transmission in the IoMT framework.
- **Data Security:** Once collected, the patient's medical data are transmitted to the cloud server. Cloud servers are prone to illegitimate access and manipulation, Denial-of-Service (DoS) attacks, etc. Consequently, suitable security systems need to be practiced to secure data on the cloud servers.

3.2.1. IoMT security mechanisms

A variety of techniques exist for the security of the IoMT framework. These techniques can be categorized as symmetric-key, asymmetric-key, and keyless techniques, as depicted in Fig. 6.

Symmetric and asymmetric methods are based on cryptographic techniques. But keyless methods are non-cryptographic. The cryptographic methods can further be classified as one-factor and two-factor authentication. In two-factor authentication, an additional second-level authentication technique is used along with the one factor-authentication.

- **Symmetric-key Cryptography**

In this technique, a secret key is created and shared among communicating nodes, shown in Fig. 7. The key is shared before the actual transfer of data. The same key is used for both the encryption and decryption of data. The techniques/algorithms which allow the integration of symmetric key techniques to secure IoMT systems are hierarchical access [69], wireless signal features [94], a cryptographic hash function (CHF) using XOR [91,95–98], Gait dependent method [93], facial recognition [92], and pattern-based technique [99]. These techniques are used to secure sensitive medical data in various IoMT applications.

- **Asymmetric-key Cryptography**

In this technique, a pair of keys named public and private keys are generated. As clear from the name, the public key is known to all the nodes, whereas the private key is only known to the owner. Encryption is done using the public key, and decryption using the private key owned by the receiver, as shown in Fig. 8.

A few very well-known algorithms that fall into this category are the elliptic-curve cryptography (ECC) algorithm [100] and Rivest–Shamir–Adleman (RSA) [101]. ECC is generally used for IoMT security compared to RSA due to its small key size and faster processing [102]. Asymmetric-key algorithms can be integrated with CHF [68,103–105] for the secure exchange of medical data among various entities of an IoMT system. It can also be amalgamated with homomorphic encryption [102,106–108], digital signatures [109,110], and smart cards [75] to secure IoMT from unauthorized access and other types of cyber-attacks [76–79,83–87].

- **Keyless Techniques**

This set of techniques deals with the methods that instrument IoMT security without using pre-generated and exchanged keys. The commonly used techniques which fall under this category are biometrics [111,112], proxy-based techniques [113,114], token-based techniques [67,115,116], and light-based methods [117]. Blockchain technology and artificial intelligence, as keyless techniques [88,89,118–120], are playing very crucial roles in securing medical records in IoMT systems.

3.2.2. IoMT system risks and attacks

The Major focus of this section is the attack landscape of IoMT. Broadly, IoMT attacks can be categorized as physical and network attacks. It has been observed that most of the attacks are administered using keyless techniques due to ease of attempt and management.

- **Physical Attacks**

The physical units of an IoMT system are targeted under various attacks. Sensors are the most commonly attacked components to steal patients' sensitive data and security keys. Physical attacks comprise token stealing [75], impersonation (replicating biometric features to impersonate a valid user) [68,98,111], tampering (any un-authorized change to IoMT data at the time of collection, transfer, or data store) [92,103,111], side-channel attacks (occur at the time of data exchange among IoMT devices and can be

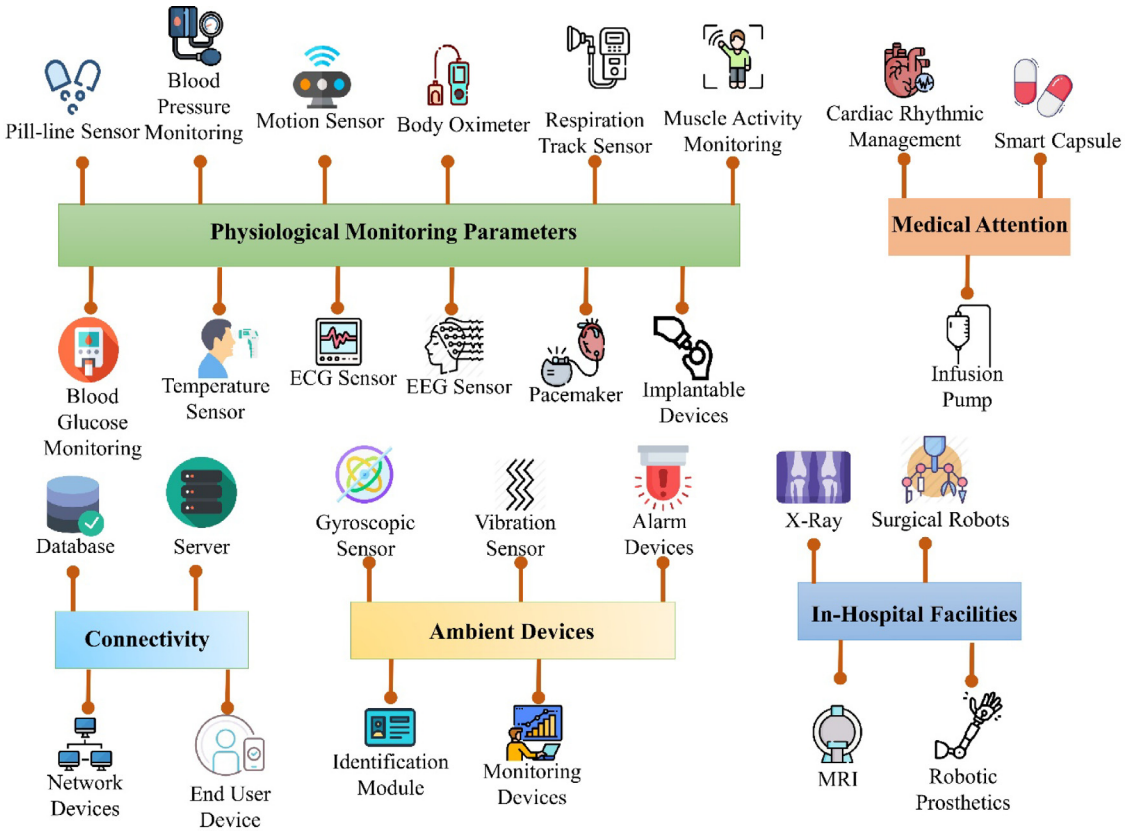

Fig. 4. Categories of IoMT devices.

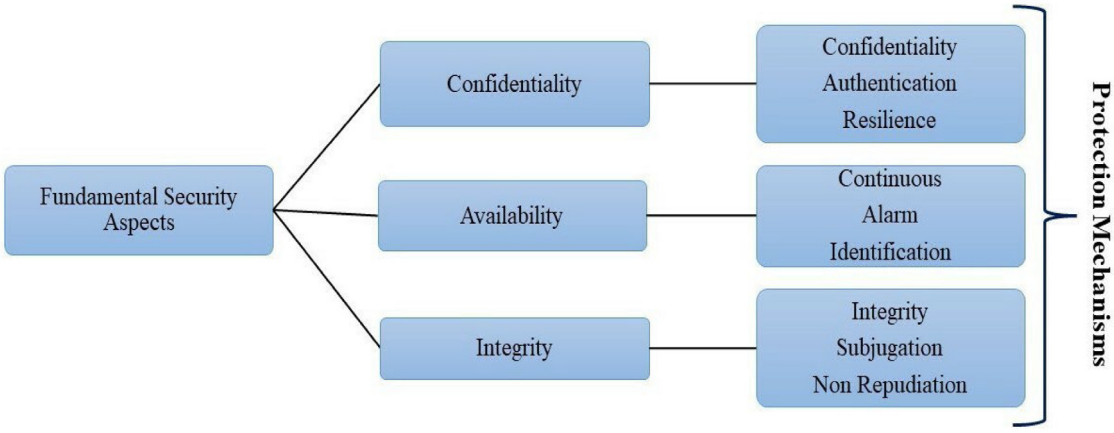

Fig. 5. IoMT: Security aspects and protection mechanisms.

detected using blockchain and AI) [89], and desynchronization. Desynchronization results in faster battery discharge as most of the IoMT have limited battery life [88].

- **Network Attacks**

These attacks intend to steal sensitive medical data which is in transit. They also hamper the communication link between the different layers of an IoMT system. Denial-of-Service (DoS) [121], sniffing, Man-in-the Middle [68,69,90], Relay, Replay [122], clock synchronization [123], parallel session [124], brute force [125], and stepping stone attacks [126] are the commonly attempted attacks under this category.

The rapid developments in the field of IoMT have improved the quality of services and care for patients. At the same time, it has caused a sharp rise in cyber-attacks that have visualized the internet as a scary place for the healthcare sector. Over time, cybersecurity experts have detected various types of cyber-attacks that could certainly endanger data. In [127], the authors introduced DoS, eavesdropping, and malware attacks as the most hazardous cyber-attacks that can harm the security of IoMT [128], discussed below:

- **DoS Attack**

During a DoS attack, various computing resources available in a healthcare system are clogged by a malicious user by sending multiple requests or data packets [129,130]. DoS attack disturbs the accessibility of an IoMT device/wearable to stop a patient from obtaining treatment and healthcare providers to access medical data [2].

Table 4
Summarization of attacks and preventive techniques.

Sr. No.	Ref.	Name of attacks	Consequence	Corrective measure
1	[75]	Physical security token loss	• Authorization • Authentication • Forward secrecy • Anonymity	• Asymmetric (two-factor)
2	[76–79]	Impersonation		• Asymmetric • Keyless
3	[80–84]	Tampering	• Data confidentiality • Data integrity	• Symmetric (two-factor) • Keyless
4	[85–87]	Side channel		• Keyless
5	[88]	RF jamming	• Availability	
6	[88]	DoS/DDoS		
7	[89,90]	Sniffing	• Data confidentiality	• Keyless • Symmetric/asymmetric (two-factor)
8	[25,68,69]	MITM	• Data confidentiality • Authorization	
9	[69,88]	Relay	• Authorization	
10	[75,89,91,92]	Replay		
11	[75]	Clock synchronization	• Secure key exchange	• Asymmetric (two-factor)
12	[75]	Parallel session	• Authentication • Authorization	
13	[93]	Brute force		• Keyless
14	[93]	Stepping stone		

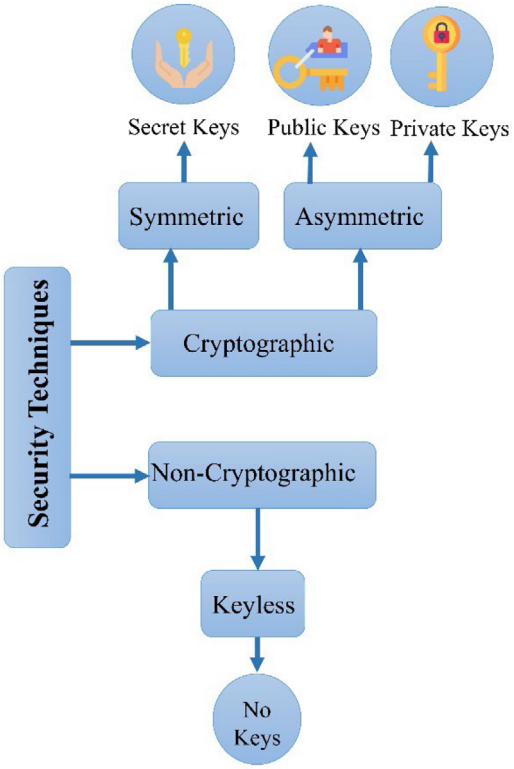

Fig. 6. IoMT framework: Security techniques.

• **Eavesdropping Attack**
It is one of the most frequently used attacks to steal data from biomedical sensors [131]. It is executed by the malicious attacker either by listening to the data communicated over the network (passive eavesdropping) or by generating multiple numbers of friendly requests (active eavesdropping) [132–134]. The sensitive health parameters of the patients are intercepted using eavesdropping attacks [135].

• **Malware Attack**
The various IoMT devices are sensitive to a variety of malware attacks. The most common types of these attacks are viruses, Trojans, botnets, worms, spyware, and many more [136]. In [137,138], the authors emphasized the automatically spreading trait of malware. They not only intimidate the integrity and privacy of IoMT but also have the potential to forcefully close down any network server [139]. They can also cause unauthorized access to healthcare data and IoMT devices. Consequently, managing malware attacks needs to be given serious thought as it can cause severe harm to IoMT devices and systems.

Various types of attacks and respective security mechanisms are summarized in Table 4.

4. Federated Learning (FL)

ML plays a very significant role in numerous application domains [140–144] as the traditional ML algorithms work on a centralized approach for model training. The major challenges faced in this framework are data privacy and communication cost [16]. Consequently, the normal ML framework is unsuitable for processing the huge amount of medical data gathered using mobile and distributed IoMT. It originates the need for an advanced learning model which may complete the training process on distributed nodes. The most appropriate solution for this problem is FL [1,13,145–147]. FL works on the concept of on-site device learning. FL algorithms even have the potential to process data gathered using IoT in real-time [148]. These nodes are equipped with a complete operating system and a high degree of processing units which prepare them to execute complex ML algorithms independently. Data generated from the end user or any of the devices deployed at the hospital or home need not be communicated to the other sites or centralized servers. It ensures data privacy [149]. Using this technique, each IoT can train the model itself for locally gathered data but does not require communication with the centralized cloud server. Then each IoMT uploads the partially trained local model to the centralized cloud server. Due to this advantage of FL, along with healthcare [150], it is being adopted in a variety of other domains likewise smart homes, smart cities [18], industry, cyber security, etc.

The term 'Federated Learning' (FL) was popularized by the world-renowned technology company 'Google' in 2016 [151]. FL is an advanced ML archetype that yields an unbiased representative and preserves data privacy [152,153]. The model is trained at the client site utilizing local data in every iteration. These clients may be IoT devices, wearables, different organizational

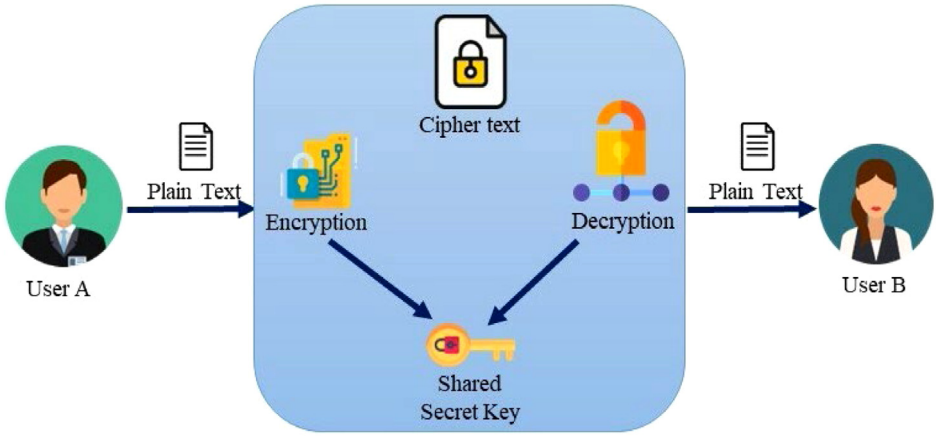

Fig. 7. Symmetric key security.

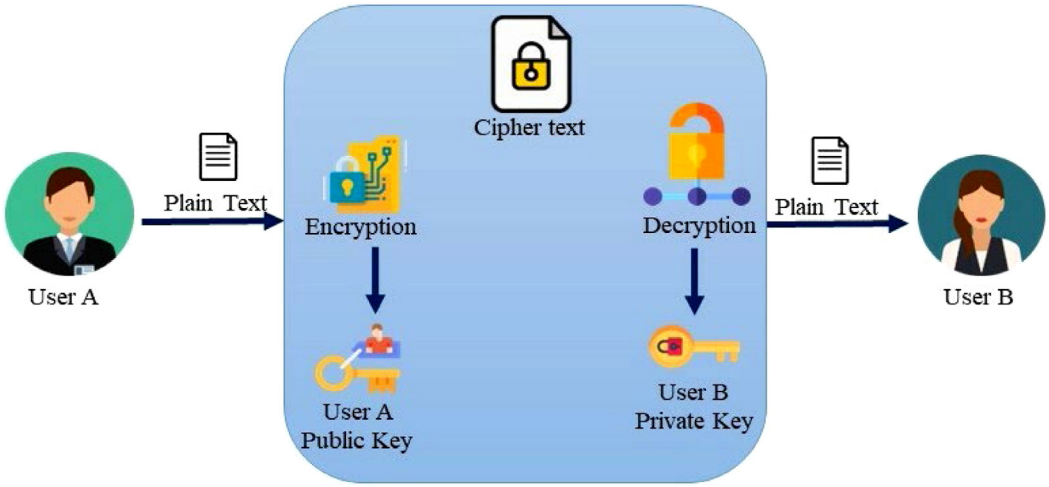

Fig. 8. Asymmetric key security.

data warehouses, smartphones, or datacenters. After training, model updates from these sites are transferred to the centralized server and aggregated without using any unprocessed data from the local sites (shown in Fig. 9).

As the clients taking part in the FL do not correspond to the transfer of data samples, it confirms security and privacy [10,154,155]. The global training model lodged at the server develops an aggregated model by aligning the different client model parameters. Consequently, clients are trained collaboratively in distinction to the shared model by the server [156–158]. The main benefits of FL in comparison to classical ML models are the security of data, compressed latency, and low power usage [159–161]. Along with the privacy of delicate user information, it also caters to the users of different client nodes with customized ML models for improved user involvement [162].

For Mathematical representation, let us assume there is X number of active clients carrying data. Let D_X represent the distribution of data linked to every client X, and N_X is the count of specimens available with that client. $N = \sum_{x=1}^{X} \binom{N}{x} N_x$ is the complete specimen size [1]. FL problems help in finding the solution to experimental risk minimization problems of the type represented in [163–165]:

$$\min_{l \in R^d} F(l) : = \sum_{x=1}^{X} \frac{N_x}{N} F_x(l) \quad \text{where } F_x(l) := \frac{1}{Nx} \sum_{a_i \in D_X}^{n} F_i(l) \qquad (1)$$

Here the model parameter is represented by l. The loss function is represented by f_i, which is dependent on an input–output data pair, i.e., (a_i, b_i). Here $a_i \in R^d$ and $b_i \in R$ or b_i are in the range of -1 to 1. The mathematical models of FL face statistical, communicational efficiency, and security challenges when implemented in various application domains [166,167].

The key features of FL, i.e., safeguarding user's privacy, enhancing the model's performance, scalability, and decreasing data transfer cost, add several advantages to its various applications [10,168].

4.1. FL application domains

Due to the fundamental features, FL has a diversified field of applications in the domains equipped with smart devices. Here, we focus on some of the prominent areas as shown in Fig. 10:

- **Smart Homes:** Smart homes equipped with smart devices are in huge demand due to their comfort. They also contribute to the populace's quality of life (QoL) [169]. Different wireless smart gadgets and devices like smart cameras, smart bulbs, smart fans, smart doorbells, and other smart appliances are competent to communicate with each other and are managed remotely with the help of smartphone

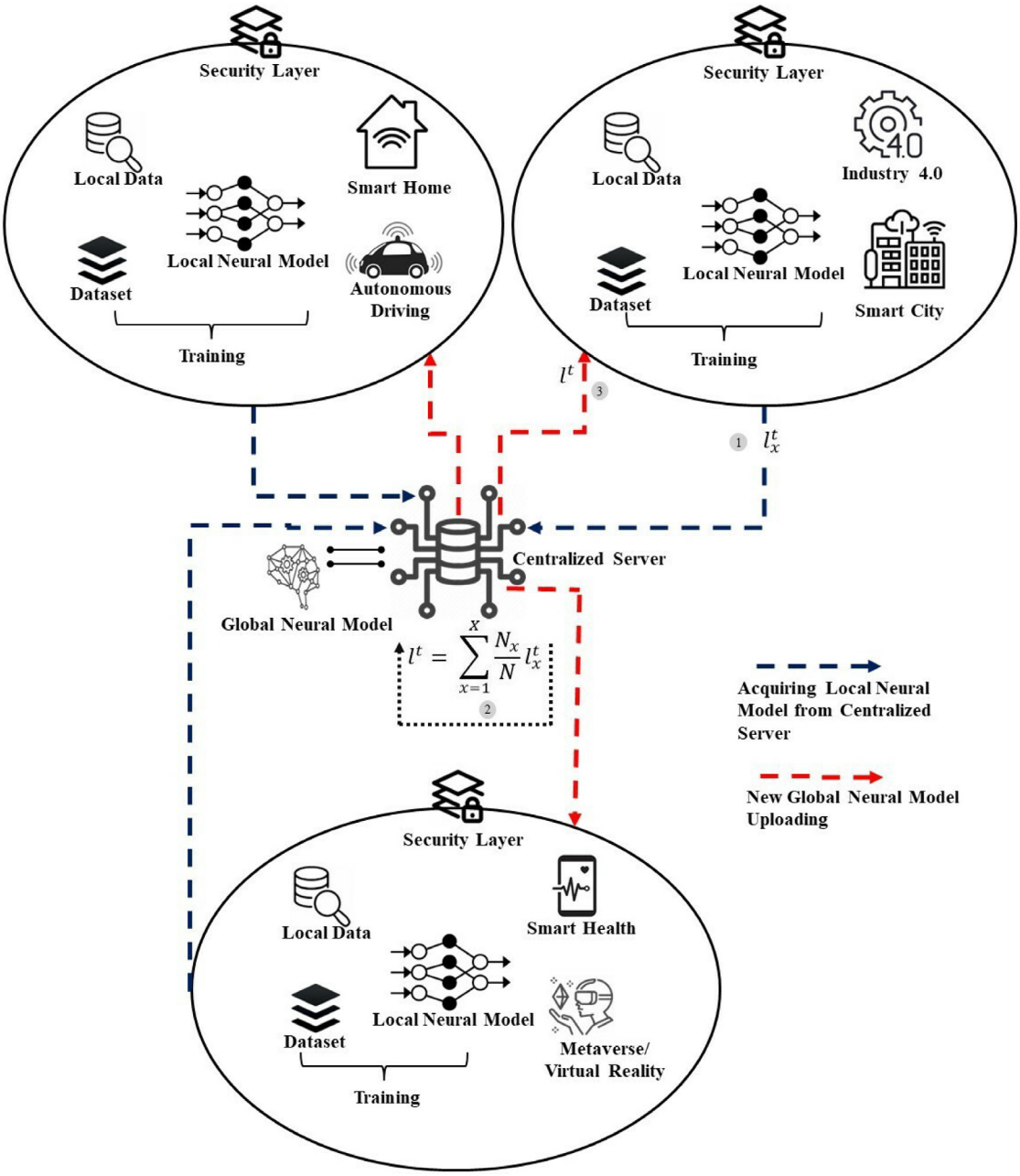

Fig. 9. Distributed training and aggregation of local updates: Federated learning framework.

apps and microcontrollers. On one side, these remotely controlled IoT devices make human life convenient, but in parallel, the probability of data leakage also increases. In [170], the authors proposed an FL model equipped with divergent privacy to minimize the possibility of voice data outflow. In [171], authors proposed another framework to secure communication among smart gadgets and appliances in a smart home environment managed by wi-fi routers.

- **Smart Cities:** A significant development is occurring in smart cities with the evolution of more efficient city operations, improving the residents' QoL [172–174]. Many IoT-enabled smart devices make the real-time administration of physical objects convenient and cater to the residents with much-needed information about climate, traffic, healthcare services, transportation, public safety, etc. In [175], the authors proposed an FL model to manage the dynamic departure of city buses considering important parameters, i.e., weather conditions and actual traffic on the roads. In [176], the authors introduced Distream, the first-ever dynamic distributed model for live video analysis captured by smart cameras while preserving privacy in reality.

- **Healthcare:** With the amalgamation of IoT devices in the daily lives of the residents, the privacy of personal medical data has turned into a compelling agenda. Many smart gadgets are used to collect various health parameters like blood pressure, glucose level, heartbeat, etc. In comparison to any other kind of data, medical records are more sensitive, and there are strict government regulations to restrict hearing [177]. To ensure the security of medical records, in [178], the authors proposed an FL training model which permits every hospital to engage in the process of training using its records. In [179], the authors proposed another FL model

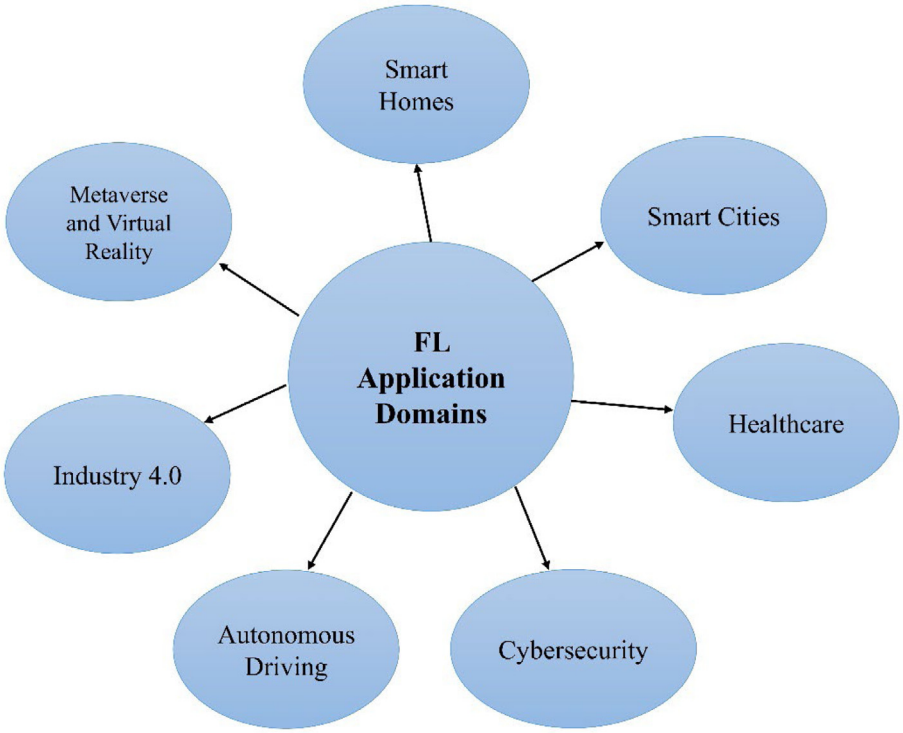

Fig. 10. FL application domains [25].

for the IoMT. In [180], another FL framework has been proposed in which different hospitals can collaborate to train a model for the analysis of CT scans of patients who are COVID-19-infected.

- **Cybersecurity:** Due to the fast expansion of smart networks, the volume of cyber-attacks is also increasing exponentially, as proved during the Mirai attack taking advantage of the falsified routers and webcams [181]. These types of attacks have alerted us to assess the risks associated with smart healthcare devices. Using FL, models can be designed and deployed near the edge to protect smart devices from cyber-attacks. In [182], the authors proposed an FL-based intrusion detection technique in gateways for smart devices, i.e., DIoT. In [183], the authors introduced IoTDefender, another FL-based model to detect vengeful traffic/data. Recently, the FeDML environment [184–188] proposed an FL framework developed especially for smart devices. This framework is designed to detect unrepresentative traffic. The proposed model was experimented with Raspberry Pi to ensure the deployment of the model on smart devices.
- **Autonomous Driving:** With the evolution of the Internet of Vehicular Things (IoVT), autonomous driving is continuously approaching normal living. Practicing a dependable autonomous-driving system requires continual real-time transfer of data with the environment, which may likely cause data and privacy leakage. There is also the possibility of communication delay, which may result in the inappropriate response of the driving system to the movement of the vehicles. These challenges can be addressed using FL-dependent edge computing in automated driving systems. FL can also contribute to developing more sensitive models to local real-time vehicular changes. The authors in [189] introduced a blockchain-based FL model for dependable vehicular networks. The integration of blockchain in vehicular networks assures the secure exchange of autonomous vehicles' locally trained models by providing more dependable networks. The unification of blockchain and FL could be integrated at various levels in the architectural setup. In this model, the authors utilized the practical Byzantine Fault Tolerance (pBFT) protocol for the assimilation of blockchain into vehicular networks. This protocol ensures a more secure network by allocating the various services to different devices [190]. Using this framework, each vehicle in the network will utilize the distributed model. With this model, both the issues faced by autonomous vehicles were managed to a great extent in VNet systems.
- **Industry 4.0.** The swift evolution in the domain of IIoT has caused major developments in the usage of ICT in the area of manufacturing. The concept of Industry 4.0 was introduced due to the amalgamation of connectivity and availability of real-time data from IIoT [191]. Two major challenges are faced in the industry 4.0 ecosystem, i.e., insufficiency of the data originating from a single factory and commercial value of the data generated from various IIoT. In [192], authors introduced a blockchain-facilitated FL model for data exchange among the IIOT. The proposed model is deployed using permissioned blockchain and federated learning. Various IIoT are connected through permissioned blockchain-secured network that makes the exchange of local models safely trained at the base stations or other smart industrial equipment. These industrial entities are called super nodes as integrated with computing power and storage. In permissioned blockchain transactions are categorized as retrieval and data sharing transactions. Due to privacy issues and limited storage, permissioned blockchain only retrieves related data using FL but keeps a record of all data sharing. The outcome obtained with the prospective model validated the benefits of using FL in IIoT.
- **Metaverse and Virtual Reality.** The most recent contemplated term in the digital world is "metaverse". It is believed as the next genesis of the internet. It is assumed to facilitate perfectly connected, immense, and captivating networked 3D virtual reality using traditional personal computing. It will also facilitate the functioning of augmented and virtual

Table 5
Various tools to deploy federated learning models.

Ref. No.	Tool/ Framework	Organization/Developer	Description	Web Link
[197]	FATE	Webank	It is a secure framework to facilitate the deployment of industry-grade FL solutions.	https://fate.fedai.org/
[198]	OpenFL	Intel	It is a framework for the development of multiplatform Apps.	https://www.openfl.org/
[199]	NVIDIA Clara	Nvidia	It is an AI-facilitated high-performance framework for constructing, managing and deploying medical imaging systems.	https://www.nvidia.com/en-in/clara/
[200]	Substra	Owkin	It facilitates privacy — meticulous FL models where various stakeholders cooperate for learning in a distributed environment.	https://www.labelia.org/en/ppfl
[197]	IBM Federated Learning	IBM	It helps collect, clean, and train data (even in different formats) on an enterprise scale without actual migration and aids the process of model training, complying with privacy, and security of data.	https://www.ibm.com/docs/en/cloud-paks/cp-data/4.0?topic=models-federated-learning-tech-preview
[201]	TensorFlow Federated	Google	It is an open-source framework to facilitate distributed computation and collaborative learning of the model.	https://www.tensorflow.org/federated
[202]	PySyft	OpenMined	It is an open-source library for developing privacy-preserving FL models and secure distributed computations.	https://pysyft.readthedocs.io/
[203]	PyGrid	OpenMined	It is a peer-to-peer framework for designing and developing FL models and secure data analytics.	https://pypi.org/project/PyGrid/

reality devices [193]. In this ecosystem, clients have their resources and can cooperate with other users using virtual entities. Metaverse provides a unique platform for a variety of application domains, i.e., manufacturing, business, education, entertainment, etc. Various emerging technologies, like AI, ML, DL, IoT, Blockchain, Cloud Computing, Edge and Fog Computing, 5G, and beyond, will contribute immensely to the metaverse development. The digital twin of the resources, entities, and environment is created to develop an amalgamation of the virtual and real world. Along with the physical presentation, the digital twin can also present real-time information by processing the various types of data gathered using IoT devices.

In various applications, FL enables the different smart devices to participate in the model training process in a distributed environment. But the volume of data available on different participating nodes is not the same which raises the bias of the training model and also increases the disparity between the local and global models. In [194], the authors proposed a self-balancing FL model to manage imbalanced data and give improved accuracy in mobile systems. In another technique, i.e., FlexCFL, in which the participating nodes with low training disparity are grouped which causes a communication efficient system with higher accuracy [195]. In FL models, various edge devices participate in model training without transferring the data to a central server and these devices have limited and varying resources. Edge devices with heterogeneous setups cause a fall in accuracy which is another challenge in the FL framework. To overcome this problem, a novel framework named FedSAE is proposed that studies the task competition history of the participating edge node to anticipate the nominal workload for it [196].

In each of the application domains, several applications of FL are deployed using various tools summarized in Table 5.

5. FL for IoMT-based healthcare applications

In this section, the fundamental interests and technological needs of using FL in smart healthcare systems are described in detail.

5.1. Motivations

To emphasize the fundamental interests, existing limitations of the modern healthcare systems need to be described, and afterward, the major rewards that FL can endeavor are discussed in detail:

5.1.1. Limitations of smart healthcare systems

The major limitations of using smart healthcare systems are discussed below:

- **Security and Privacy Issues**

As previously articulated, the use of conventional ML-based techniques for implementing smart healthcare systems needs sharing/communication of data to the centralized servers or cloud, which causes security attacks. It may result in unauthorized access to sensitive medical records during transmission, or third parties can take advantage of accessing data from cloud servers directly without taking the permission of data owners [204]. These limitations cause severe security, data theft, and confidentiality issues. However, the centralized servers or cloud infrastructure, equipped with high computational power, can handle voluminous data efficiently for the training of the models and prediction at the cost of privacy [205].

- **Shortage of Available Medical Datasets Online**

In real life, smart healthcare systems need voluminous data for the implementation of ML-based models. But there is a shortage of online medical datasets, especially on a single site. Insufficient data may result in inefficient models, which may further cause the need for manual data investigation and mining [206]. One way-out to address this issue is to transfer the data between various healthcare sites to facilitate efficient mining. But due to institutional guidelines and increasing privacy issues, it is very challenging to access the data of others for the training of the ML- application models [207]. Consequently, resolving this issue of limited datasets is of preeminent emphasis in the domain of smart healthcare systems.

- **Confined Performance of ML-based Healthcare Models**

Due to restricted access to healthcare data, the trained models cannot provide the required level of accuracy. An alternative

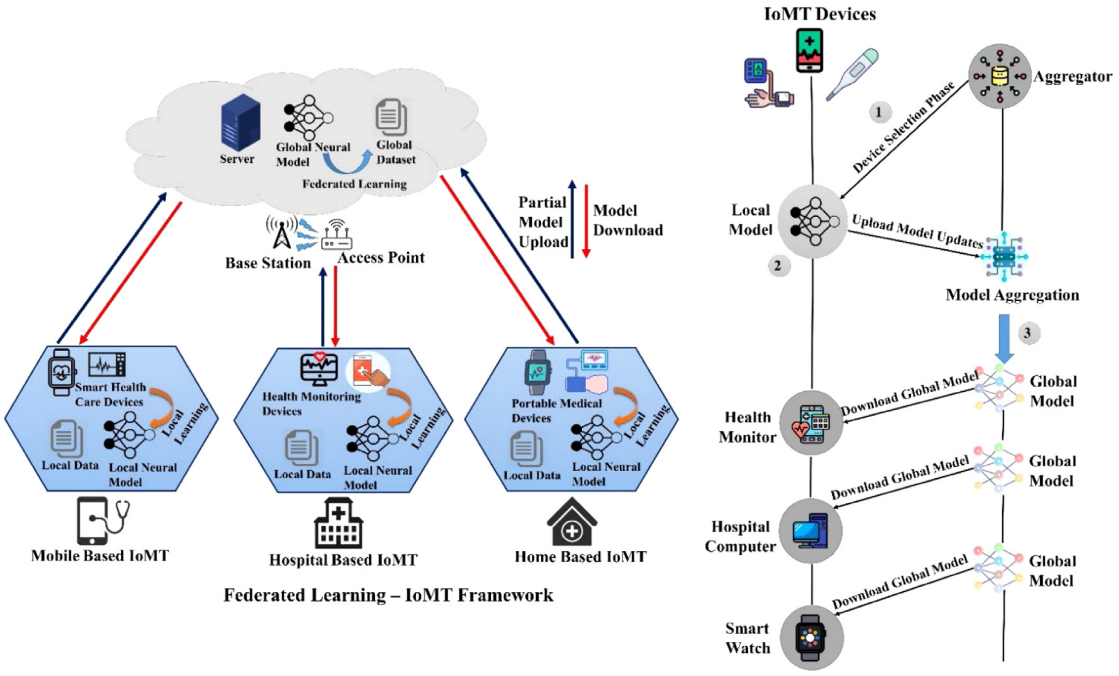

Fig. 11. FL-based IoMT healthcare framework.

method to address this issue is data augmentation which is applied using generative adversarial networks (GANs) [208]. But this technique is again limited by a lack of diversity in the datasets, which again impacts the accuracy of the model. So, limited data availability is one of the main challenges in deploying ML-based healthcare models.

- **High Cost Involved in Healthcare Model Training**

Conventional ML-based healthcare systems are affected by communication delays while transferring voluminous medical data to the cloud/centralized servers [209]. It requires more bandwidth and may create a network bottleneck. As the number of medical devices increases, limited battery life becomes a major issue in off-loading onsite data to the cloud.

5.1.2. Advantages of using FL in smart healthcare applications

After a thorough study of IoMT-facilitated smart healthcare systems, it has been observed that FL has the potential to benefit smart healthcare systems, as discussed below:

- **Improved Data Privacy**

In FL-facilitated healthcare systems, medical records remain on local healthcare sites and medical devices. Data need not be transmitted to the centralized servers/cloud. Partial training of the model is done onsite in a distributed manner, requiring only local updates. The concept of distributed model training reduces the security and privacy issues associated with medical data and ensures a higher level of health data security [210]. It further contributes to the development of safe, smart, and sustainable healthcare systems.

- **Considerable Trade-off between Services and Accuracy**

In comparison to traditional centralized learning models, FL models provide a considerable trade-off between services and accuracy along with data security and privacy administration [211]. FL models are scalable and generalizable with minor compromises in accuracy.

- **Economical Healthcare Data Mining**

As in FL-based learning, there is no need to offload voluminous medical data from IoMT to the server, resulting in reduced communication costs. FL-Based learning requires less bandwidth as the only model gradient is communicated over the network, which limits the probability of bottlenecks in extensive healthcare networks [212].

5.2. FL and its types for IoMT-based healthcare applications

This section discusses the fundamental idea of FL and the essential forms of FL that are utilized in smart healthcare.

5.2.1. Fundamental principle

The general FL-smart healthcare process involves the crucial elements listed below, as depicted in Fig. 11.

- **The Process of System Start-up and Selection of the Client:** The aggregation server chooses the healthcare analytics goal, such as autonomous human motion detection and medical imaging, as well as specifications of the model, such as task categorization prognosis and learning specifications, such as the number of neural nodes and their rate of learning. In addition, the server decides whether clients are eligible to participate in the FL process and notifies them accordingly.
- **Knowledge Sharing and Localized Training:** After identifying a subset of the clients participating in the learning mechanism, the server will deliver an initial model to launch the distributed training. This model will include an initial global gradient. During each transmission phase, every client builds its local model with its dataset and determines the model renewal, such as the gradient for neural networks. Up till the model training is complete, this process is repeated. Each client then modifies its model and transmits it for aggregation, done by the server.
- **Aggregation and Downloading the Model:** Once the server has accepted all the updates from the clients that have been chosen, then those updates are aggregated. By illustration, the model averaging strategy found in Google's Federated Averaging (FedAvg) algorithm can be employed [213]. With weights corresponding to the size of the dataset at each client site, this method takes an element-wise average of the gradient parameters of regional models. The global model will then be updated and distributed to all the participating clients. Each client will use the received model as a base for the later level of learning. In this way, the FL mechanism is repeated until the global loss function mingles or the required degree of precision is attained.

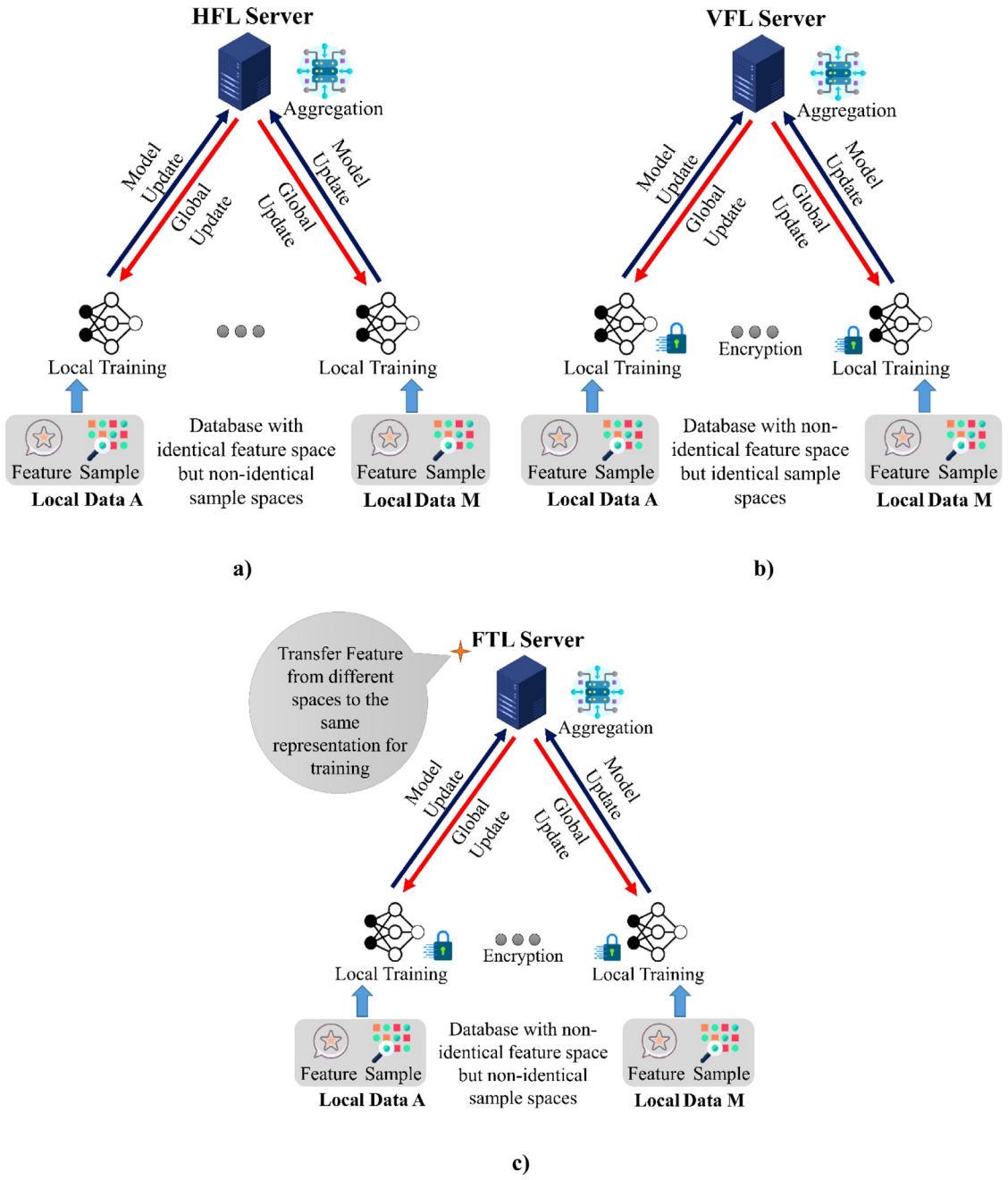

Fig. 12. Types of FL for IoMT applications in smart healthcare systems (a) HFL (b) VFL (c) FTL.

5.2.2. Types of FL adopted in smart healthcare systems

In light of the recent developments that have been made in the FL algorithms and employed in smart healthcare, FL can be characterized into three different classes, which are shown in Fig. 12.

- **Horizontal Federated Learning (HFL):** Fig. 12(a) depicts how HFL's healthcare client nodes can train a distributed shared common model by utilizing their local datasets. These local partial datasets share the common feature space but have distinct segment spaces (presented in Fig. 12(a)). Consequently, the local FL nodes can utilize a common artificial intelligence algorithm to train their datasets. After that, the server constructs a global model by combining the local changes communicated by local clients to construct a global update without directly accessing local data [213]. Diagnosis of speech disorders is a common example of HFL in smart healthcare. This would involve different users speaking the same sentence (in the feature space) on their smartphones in a variety of voices (in the segment space) and then using server's average of local speaking updates to provide a global speech recognition model.
- **Vertical Federated Learning (VFL):** Fig. 12(b) depicts how the VFL process is used for the training of health datasets with common segment space but separate feature spaces. In particular, the problem of segment overlap in dispersed clients can be addressed by employing techniques dependent on entity alignment, which is further integrated with encryption approaches in the local training of the datasets [214]. An example of VFL in the context of IoT-based applications is a collaborative learning model between hospitals and insurance firms in a smart healthcare environment. For

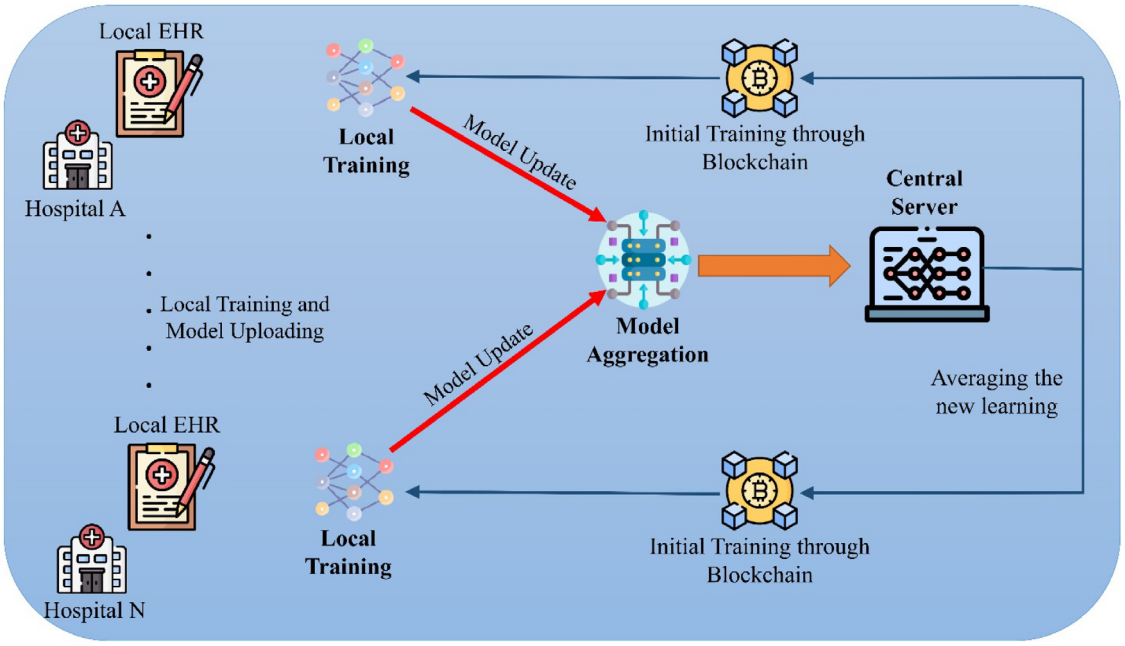

Fig. 13. Federated learning with blockchain to secure EHRs.

example, a healthcare provider and an insurance provider with a common patient population and distinct data features can work together to train a single AI model in a VFL process. Hospitals' previous medical records and insurance companies' healthcare costs are a few examples of data that can be used to make better healthcare decisions.

- **Federated Transfer Learning (FTL):** Fig. 12(c) illustrates how FTL manages the datasets with disparate segment spaces and feature spaces in comparison to VFL systems. Feature values can be computed from various feature spaces to a single copy using a method called transfer learning. This representation can then be used to train local datasets [215]. Encryption techniques are used to preserve privacy at the time of gradient exchange between the distributed client nodes and the server [216]. In the realm of smart healthcare, FTL can assist in disease identification through international collaboration with many hospitals that treat a variety of patients (segment space) using a variety of treatment protocols (feature space). So, FTL can augment the output of the communal AI model, resulting in improved diagnostic accuracy.

5.3. FL in IoMT healthcare applications

This section is aimed to discuss the significant role of FL in IoMT healthcare applications. FL is benefitting many areas, including management of electronic healthcare records (EHRs), remote patient monitoring, medical imaging, and disease detection and diagnosis, presented below:

- **Electronic Healthcare Records (EHRs) Management**

Most of the healthcare data and medical parameters are collected using IoMT deployed at various sites. The gathered medical information is managed using EHRs. EHRs are used for computation, disease diagnosis, and also to promote various research activities in the healthcare sector. One of the dominant issues experienced using conventional AI techniques is security and privacy threat during data transmission and analysis. As EHRs are highly sensitive, just the elimination of metadata is not enough to protect the confidentiality of the patients in highly complex healthcare systems where many stakeholders can access the database to cater to their common day-to-day needs [217]. FL has the potential to present more dependable models for the analytics of highly sensitive medical data. It preserves data privacy through the cooperation of distributed entities for data analysis and processing. In [178,218–228], the authors presented various FL-based models/ protocols for secure model training, disease diagnosis in a distributed environment, patient integrity disclosure, patients' classification based on symptoms and diseases, secure healthcare network management, etc. The authors used different intelligent classification and optimization techniques in their work. Blockchain is observed as one of the most promising technologies to secure distributed data and decentralized systems [229]. In the blockchain, data is stored as a sequence of blocks that are associated using the cryptographic hash of the proceeding block and make an abiding chain [230]. As, every block encloses a header, a sequence of transactions, and a pointer to the previous block. In case, anyone tries tinkering with a block need to modify all the headers indicating the previous block. Every new transaction occurring in the chain is stored in the ledger and shared with all associates over the network [231]. Depending upon the type of application, various consensus algorithms are available to make all the associates convinced of a common dataset and add a new block to the chain. Due to the decentralized approach of blockchain technology, it is highly used for the secure exchange of local models in FL systems. The security level of FL-based healthcare models to manage EHRs can be enhanced by implementing blockchain solutions for data communication among distributed entities [232,233], shown in Fig. 13. Another major challenge is the heterogeneity of various EHR systems in the FL framework. In [234], the authors proposed a novel technique to consolidate heterogeneous EHR suitable for a specific FL scheme.

- **Remote Health Monitoring**

The need for intelligent solutions to manage remote health monitoring is developing day by day. The remote health care and monitoring domain encompass individuals, home patients, and

hospitals. FL-based models can be deployed to provide home-centric health monitoring by using a globally distributed framework managed by a server, e.g., a cloud server, and preserves privacy by keeping sensitive patient data locally [235]. IoMT devices scattered at different homes train a customized model using ML techniques and the patient's dataset. The model gradient is updated for the cloud server and other homes. Along with data security, it gives more accurate results for personalized predictions. In [236–241], the authors proposed various FL-based models using wearable, home-stationed, and hospital-stationed IoMT devices for assisted living, obesity control, activity recognition, analysis, and prediction of psychological disorders, mood prediction, ischemic heart attack, etc.

• **Medical Imaging**

Intelligent centralized medical data imaging is challenging as it requires the collaboration of many medical institutions and laboratories [242]. FL has evolved as an encouraging framework to aid the tasks of huge-scale medical imaging without the requirement of sharing sensitive medical data in any public domain, thus, addressing security issues. Visual data require more bandwidth, so on-site training of FL models also helps to manage network congestion. In [150,243–250], various FL-based models for studying patient variation, brain tumor segmentation, MRI scan analysis, diagnosis of acute neurological symptoms, MRI reconstruction, MRI study, breast cancer classification, etc., are proposed by different researchers with varying degrees of accuracy.

• **COVID-19 Analysis and Detection**

The whole world in affected by the spread of COVID-19. It has turned into large-scale health distress for most countries. Many intelligent techniques presented compelling results in early apprehension of this disease. But, during the pandemic, gathering plentiful data for training the models for COVID-19 detection was a challenge due to patient privacy concerns. At this time, FL evolved as the most viable paradigm for training the models in a distributed environment to preserve user data privacy. Consequently, various institutions can participate in model training to secure their COVID-19 data sources. In FL-based models, only gradients are communicated but not the complete datasets. In [151,251–258], many FL-based models are proposed for the analysis of medical images like X-ray, CT scans, etc., to detect various types of abnormalities that help in the analysis and diagnosis of COVID-19.

The various FL-based IoMT applications discussed above are summarized in Table 6.

The various datasets used to implement different FL-based healthcare applications are presented in Table 7.

To provide solutions to various challenges experienced in the different application domains of smart healthcare systems and to develop more efficient systems, several patents have been filed from time to time. Some of the prominent patents filed in the area in the last few years are summarized in Table 8.

In Table 9, the authors present various examples of real-world FL-based projects in the domain of smart healthcare.

6. Comparison of FL-based security with other security schemes in smart healthcare systems

Along with FL, some other technologies/schemes are used to deploy secure intelligent healthcare systems, as discussed in Table 10.

It has been observed that federated learning is beneficial to process decentralized data in distributed healthcare frameworks to ensure data security and ownership. During performance comparison of FL-based intelligent healthcare systems with other schemes, it has been observed that along with data security FL-based systems facilitate local training of the models that reduces communication delays/cost. Blockchain-based FL models are also developed to further enhance data privacy and manage various types of malicious threats in healthcare systems to improve service quality [233,300–302]. In [299], the authors presented an encryption-based FL model for smart healthcare systems to ensure data privacy. In this work, local models are trained on distributed healthcare nodes that are further protected using homomorphic encryption. Consequently, FL models are giving a remarkable performance to enhance the security of smart healthcare systems individually and even in collaboration with other schemes/technologies.

7. Challenges faced and future approaches to research

In this section, the authors discuss the primary difficulties and potential future avenues of study in the field of FL-based IoMT Security:

• **Communication Challenges in FL-facilitated IoMT Applications**

Most of the patient's health parameters and other medical data are gathered using IoMT devices. Communication performs a very important role in FL-enabled IoMT applications as a data transmission channel amidst medical device/equipment users and aggregation servers. Since every IoMT device needs to communicate the model updates to the aggregation server, the security of data transmission between IoMT devices and the aggregation server is crucial. Numerous studies have revealed that effective scheduling and security techniques need to be practiced in such situations to pick a working group of IoMT gadgets [303–307]. The rapid and unpredictable changes in wireless channels present another significant obstacle to the secure exchange of learning updates [22]. Consideration of more dependable design aims may help mitigate the impact of user attrition [216,308]. The ubiquity and standardization of communication protocols, device technology, deployment conditions, and aggregation methodologies are just some of the many challenges that must be overcome. When it comes to healthcare services that are allowed by FL, it is also obvious that there is no standardized or all-encompassing instrument to evaluate the efficacy of the various techniques that might be taken to solve the same problem. However, since these strategies are offered for a variety of healthcare settings and that different network configurations or datasets are utilized to evaluate their efficacy, it is challenging to compare and contrast these strategies. A guideline on the architectural and design aspects of FL is offered in IEEE Std 3652.1–2020, which was issued not too long ago [309]. By following this guideline, this problem can be overcome. Furthermore, this guideline presents important problems concerning FL, including privacy, security, performance efficiency, and economic feasibility, in addition to evaluation schemes and performance measures of FL systems. In addition, there are significant issues associated with the availability of universal communication protocols and the standardization of device hardware, deployment situations, and aggregation methodologies which will significantly contribute to addressing the challenges associated with IoMT applications in smart healthcare systems.

• **Specifications for the Implementation of Federated IoMT Applications**

Despite several examples of successful FL-enabled IoMT applications, currently, no approved technique exists to compare and contrast the efficacy of different methods. Several blockchain solutions have been proposed for FL systems to eliminate the necessity for a centralized server and to ensure the reliability of local updates from various IoMT devices. Comparing these methods is challenging since they are presented for various (healthcare) contexts, and their performance is evaluated using different

Table 6
Classification and description of FL-based IoMT applications in smart healthcare systems.

Application domain	Ref. No.	Type of FL	Beneficiary	Accumulator	Description	Disadvantages
EHR organization and management	[217]	Horizontal federated learning	Hospital	Cloud server	A collective learning model using FL for EHRs organization and management.	The confluence of the FL model is not verifiable.
	[222]		Radiology patient center		An FL model for managing EHRs using split learning	The degree of complexity in training the model is not verified.
	[218]		Smartphone	Data server	An FL technique to anticipate hospitalization of the patients.	The exact accuracy of the model is not predicted.
	[220]		Hospital		An FL model for training of EHRs using differential privacy.	The workability of differential privacy in real-time FL models needs to be emphasized
	[259]		Hospital		An FL method for preterm-birth data study.	The complexity of on-site training needs to be studied.
Remote health monitoring	[235]	Vertical federated learning	Smartphone	Cloud server	An FL technique for observing remote patient activities.	The protected aggregation needs to be examined.
	[238]		Mobile devices		An FL-facilitated remote event monitoring technique to aid healthcare operations.	The proposed method is not compared with other FL-based methods.
	[236]	Federated transfer learning	Wearable gadgets		A personalized FTL technique for remote patient activity detection.	The cost of data communication and the degree of complexity of training the model are not discussed.
	[237]	Horizontal federated learning	Hospital	Data center	A two-level FNLP method for obesity analysis	The concept of privacy preservation needs to be incorporated during FL training.
	[239]		Medicinal locations		An FL technique for country-wide medical insurance data analysis in the US.	Challenges related to legal issues among medicinal bodies need to be addressed.
	[240]		Mobile devices		An FL model for mood prediction.	The usage of resources for training and the security/privacy of mobile devices needs to be emphasized.
Medical imaging	[246]	Horizontal federated learning	Hospital	Data center	An FL technique to diagnose the acute neurological syndrome	The technique is very simple, and additional simulation is needed.
	[243]		Medicinal Locations		An FL-based framework for the analysis of brain MRI	The practical angle for taring of FL-model for MRI scan needs to be emphasized.
	[260]		Hospital		An FL-based model for medical images with differential confidentiality for collective protected training.	The proposed FL model needs to be compared with DL techniques.
	[245]		MRI machine	Cloud server	A more secure FL-model for brain imaging	FL confluence is not analyzed.
	[242]	Vertical federated learning	Hospital	Federated server	An improved FL model for the reconstruction of medical images	The accuracy of the model is not discussed.

(*continued on next page*)

network configurations and data sets. The ubiquitous availability and standardization of IoMT hardware, communication protocols and standards, deployment conditions, and aggregation methodologies also pose significant difficulties.

• The Integrity of Data Used for Healthcare Training in an IoMT-Federated Environment

Due to variations in computing resources and data quality among healthcare facilities, training quality might suffer significantly.

Table 6 (*continued*).

Application domain	Ref. No.	Type of FL	Beneficiary	Accumulator	Description	Disadvantages
COVID-19 analysis and detection	[252]	Horizontal federated learning	Healthcare institutions	Data center	An FL-model to diagnose COVID-19 using chest X-ray images	Information loss during FL communication is not studied.
	[258]		Hospital		Different compilations to diagnose COVID-19 using FL.	FL confluence is not studied.
	[151]		Data clients		A live amalgam FL technique to diagnose COVID-19 from CT scan images.	The learning efficiency of the model is not verified.
	[254]		Hospital		An FL-based method for collective detection of COVID-19.	Model details are nor emphasized.
	[261]	Vertical federated learning	Healthcare institutions	Cloud server	An FL-based model to identify COVID regions using chest CT scan images on data from three nations.	A detailed study of FL communication needs to be provided.
	[257]		Hospital	Aggregator	An FDL-model to detect lung anomaly in CT scan of COVID-19 patients.	Communication delays during model training are not considered.

Table 7
Various healthcare datasets used in the latest FL-applications.

Dataset Category	Name	Ref. No.
Medical image characterization	Facial Emotion Recognition (FER) 2013 [262]	[21]
	Autism Brain Imaging Data Exchange (ABIDE) I [263]	[248]
	Public COVID-19 Image Data Collection [264]	[252,265,266]
Electronic health record	The eICU collaborative research database [267].	[223,268,269]
	WESAD (Wearable Stress and Affect Detection) [270]	[271]
	MobiAct [272]	[235]
	Flamby	[273]
	Human Activity Recognition (HAR) [274]	[236,275]
	Medical Information Mart for Intensive Care (MIMIC) III [276]	[224]
Medical image segmentation	Brain Tumor Image Segmentation Benchmark (BraTS) 2017 and 2018 [277]	[150]
	SPIE-AAPM PROSTATEx dataset [278]	[242,279]

Incentives designed to encourage hospitals and other health institutions to use high-quality patient data and health parameters for training and to send dependable updates to the aggregate server is a potential approach. One of the most significant aspects of building incentive systems is to use game theory and the blockchain [212,310–313]. The model training needs (such as data typecasting, mapping learning rates, and mapping training purpose-characterization) should be structured adaptively so that FL entities such as healthcare providers, physicians, and patients may simply and correctly modify their actions. Because these alterations can have an impact on both the IoMT-FL application design and the underlying framework of the learning models, it is important to create flexible FL strategies that can accommodate these modifications. The capacity to use historical data to improve FL model adaptation to future occurrences makes AI a viable tool. By way of illustration, DRL is used to create an incentive mechanism in case traditional methods underperform when feature dimensionality is sufficiently high [314].

- **Challenges to Comprehensive Health Data Analytics in the Real-world**

Patients in a real-world IoMT-equipped healthcare setting may have varying types of data (text, photos, audio, time series) and health parameters (blood group, HB level, heart rate, facial images, and other body parameters) at their disposal. Tentatively, all the FL methods presented in the literature are usually tested on small datasets with few characteristics. Although both proposals [220,260] are intended for confidential FL-based healthcare services, the former is assessed using the diabetic retinopathy dataset, and the latter uses the electronic health record dataset. Moreover, new heterogeneous FL mechanisms need to be created, wherein various stakeholders can use different models during collaboration, but a centralized server may manage this diversity using private ensemble learning [315]. An imperative approach is provided in this paper to facilitate the use of the collection of different models without the need to formally combine the information at a central place.

- **FL models for Heterogeneous IoMT Devices**

Usually, various IoMT devices in the FL scheme have diversified hardware and software characteristics. These IoMT devices also come from different vendors and are trained on different platforms with different operating systems. Even different learning frameworks are used for the training of local models that results in varying model compositions for aggregation [25]. All these heterogeneities cause major challenges in designing the system. These diversities also result in significant data communication problems. In the IoMT framework, the data gathered using various healthcare devices and wearables are commonly divergent in characteristics and dimensions that result in the discreteness of the local data storing formats of the participating nodes in the FL scheme. So, any FL framework designed for IoMT must be able to adapt these diversities for efficient training and improved performance [316].

- **Next-Generation Networks for Federated Learning in IoMT-healthcare**

Although 5G networks are less in use and commercially deployed, much work has been done on upcoming 6G wireless systems. Applications like smart cities, intelligent healthcare, Industry 5.0, smart grids, smart transportation, holographic telepresence, and

Table 8
Summary of the patents published/granted in various application domains of smart healthcare.

Ref.	Patent no.	Title	Year (Published/ Granted)	Inventors	Key features
[280]	US 11, 410, 776 B1	Systems and Methods for Formal Threat Analysis of a Smart Healthcare System	2022	Mohammad Ashiqur Rahman, Nur Imtiazul Haque	Formal investigation of various types of threats in a smart healthcare system which are executed by altering sensor values.
[281]	US 11, 430, 566 B2	Scanner Devices for Identifying and Storing Information Emitted by Implanted Medical Devices	2022	Leandro Estevan Ochoa, Joel Ochoa	Studying scanner devices and equipment to reveal and store information delegated by embedded healthcare devices
[281]	US 11, 045, 106 B2	System and Method for Detecting and Diagnosing Diseases and Use of the Same	2021	Julius Chin - Hong Shu, Robert C. Allison	Diagnosis of the disease with a device to discover angiogenesis using a microwave scanner
[282]	US 10, 897, 924 B2	Systems and Methods for Monitoring of Fractional Gluconeogenesis and Targeting of Fractional Gluconeogenesis via Nutritional Support	2021	George A. Brooks, Michael A. Horning	Analyzing the metabolic state of the patients during physical or brain traumatic injury, stress, and any other health issue which may impact the immunity of a patient.
[283]	US 11, 115, 475 B2	Software - Defined Implantable Ultrasonic Device for Use in the Internet of Medical Things	2021	Tommaso Melodia, Giuseppe Enrico Santagati	Design and implementation of IoMT-based methods and wearable devices for the transmission of ultrasonic signals through skin tissues.
[284]	US 10, 660, 522 B2	Electronic Delivery of Information in Personalized Medicine	2020	Janos Redei	A network system to transfer vital information related to personalized medicine using data streams is designed and implemented.
[285]	US 2020/0251225 A1	Health Information Transformation System	2020	John Christopher Murrish, Kanakasabha Kailasam, Douglas S. McNair, Michael Alan Ash, Thomas Anthony Fangman	Methods, systems, and readable media are designed and implemented to transform raw healthcare data into relevant information by indexing and mapping.
[286]	US 10, 332, 639 B2	Cognitive Collaboration with Neurosynaptic Imaging Networks, Augmented Medical Intelligence and Cybernetic Workflow Streams	2019	James Paul Smurro	The amalgamation of developing applications, methods, techniques, and tools for using ML in healthcare to facilitate brisk adaptive learning in healthcare devices and equipment
[287]	US 2019/0355472 A1	Computer-Implemented System and Methods for Predicting the Health and Therapeutic Behavior of Individuals using Artificial Intelligence, Smart Contracts, and Blockchain	2019	John D. Kutzko	Implementation of an intelligent Blockchain-based secure system for studying the health of a patient and response to the treatment.
[288]	US 10, 139, 393 B2	Systems and Methods for Monitoring of Blood Lactate and Targeting of Blood Lactate Via Nutritional Support	2018	George A. Brooks, Michael A. Horning	Design and implementation of a method to manage authorized access to medical records in a healthcare network.
[289]	US 9, 305, 140 B2	System and Method of Applying State of Being to Healthcare Delivery	2016	Howard Federoff, Orphir Frieder, Eric Burger	Designing a system to help to choose the right treatment by remote monitoring of the health status of the patient.

individualized body area networks are made possible with the advent of 6G. In the meantime, a plethora of brand-new technologies, including quantum computing, compressive sensing, blockchain, THz and visible light communications, 3D networking, and huge intelligence surfaces, are being developed to fulfill the far more stringent standards of 6G [317]. New healthcare services made possible by 6G, as well as issues about integrating FL functionalities on prospective 5G/6G IoMT devices and their usage (such as body implants and wearable gadgets) for mass FL-facilitated healthcare applications. In the era of IoMT devices and equipment, forthcoming e-health services will benefit from FL features, improving patients' quality of life and decreasing their hospital visits [318].

- **Assured Confidentiality and Distributed Learning**

Despite FL's promising future in safeguarding users' personal information, several privacy concerns must be addressed head-on, especially in the IoMT framework, where medical parameters and health records are extremely sensitive. Membership supposition attacks, accidental data leakage, and generative adversarial networks are the three main types of FL privacy concerns [319]. An adversary may try to verify the integrity of the FL health data collection, for instance, by misusing the global FL model. When the patient's device updates the global models to the

Table 9
Real-world FL-based healthcare projects.

Ref. No.	Domain	Country	Companies/ Institutions involved	Platform	Technology used	Description
[10]	Healthcare associations	UK	Nvidia, Owkin, and King's College, London	• Owkin Connect • NVIDIA Clara	• AI • Blockchain	It facilities various medical domains like neuro degenerative problems, cancer diagnosis and treatment, heart diseases diagnosis
[10]	Medical imaging	US	Intel	• Intel Xeon Scalable processors • Intel Software Guard Extensions (Intel SGX)	• DL	It contributes towards the development of advanced FL-based healthcare models while preserving the privacy of patients' data.
[261]	COVID-19	Japan, China, and Italy	Hubei University, China, Self-Defense Forces Central Hospital, Tokyo, and San Paolo Hospital, Milan	Not Specified.	• ML • Image processing	Under this project, the chest CT image of the patient is segmented to diagnose COVID-19 without leaking the patient's information.

Table 10
FL and other security techniques used in intelligent smart healthcare systems.

Technology/Scheme used for IoMT security	Ref. No.	Security taxonomy	Methods used	Advantages
ML	[290,291]	Authentication Intrusion detection Malware detection Access control	Naïve Bayes k-Nearest Neighbor (KNN) Decision Tree (DT) Artificial Neural Networks (ANN) Support-vector Machine (SVM)	Data security
Blockchain	[292–295]	Data ownership and integrity	Immutable ledgers	Data security Decentralized data storage
Cryptography	[296–298]	Data integrity	Public-key cryptography Private-key cryptography	Data security
FL	[22,299]	Enhances privacy Data ownership	HFL VFL FTL	Data security Decentralized data storage Decreases communication delays and cost

centralized server located at the hospitals or other health organizations, the information about the patient may be deduced. Utilizing differential privacy, artificial intelligence, and state-of-the-art cryptographic approaches offers promise for designing privacy-preserving techniques for FL-based IoMT applications. Many researchers have proposed various solutions to improve users' privacy in FL systems [220,260,320,321]. Researching topics like the impact of artificial noise on model updates in FL-based IoMT applications has huge importance in the domain of healthcare.

- **Smart Healthcare with FL: Security Concerns**

Many clients in an FL-based smart healthcare system might potentially serve as attackers, trying to poison model updates or provide false data to lower the quality of the aggregation models. An attacker might contaminate vital information during local data training or alter local updates during model transfer between the central server and the local clients to deteriorate security. Some serious privacy risks, such as information leaks, arise when an external attacker launches assaults on the server to obtain information about the aggregated global model. When it comes to FL-based smart healthcare systems, figuring out how to fix these security flaws is a major obstacle. Data breach is a serious problem, but there are a few ways to prevent them from happening in training datasets, one of which is differential privacy [322]. To further safeguard clients from data alterations and assaults, establishing secure aggregation techniques is an attractive option. These techniques would offer a double-masking framework to encrypt the local updates and execute the process of key sharing across the central server and the clients [323].

8. Conclusions

Machine learning is playing a very vital role in numerous healthcare applications and smart healthcare systems. A major portion of healthcare data is gathered using IoMT. FL has been observed as a developing collaborative ML paradigm that has stimulated an acute interest in comprehending secure, scalable, and privacy-preserving healthcare systems and IoMT-applications. Due to the lack of an extensive review of the security of FL-based IoMT applications, the authors have presented a comprehensive review of the security of IoMT-applications developed using the FL framework. In this work, authors introduced IoMT devices, their types, security domains and aspects, and various protection mechanisms. Then, the concept of FL has been discussed in detail, covering its advantages, application domains, and various tools used to deploy FL-based models. Then, the authors introduced the key reasons for deploying FL in IoMT-based healthcare applications by presenting the advantages. Various types of FL models deployed to secure IoMT applications are also explored in this work. Then, the major IoMT application domains of FL in the area of smart healthcare are presented in detail, covering security and management of electronic health records, remote monitoring, medical imaging, and pandemic analysis and diagnosis. The authors also presented the different FL healthcare datasets used in various applications. Various prominent patents and real-world FL projects in smart healthcare applications are among the key contributions of this article. Finally, the authors presented the key challenges and possible future research recommendations in IoMT-applications. The role of FL in IoMT-applications is expected to expand in the security of IoMT-based healthcare applications. FL is expected to contribute significantly to the design

and development of large-scale secure IoMT-applications and cause a paradigm shift from centralized to distributed operations ensuring user privacy in smart healthcare operations.

CRediT authorship contribution statement

Sita Rani: Data curation, Conceptualization, Visualization, Writing – original draft, Writing – review & editing. **Aman Kataria:** Data curation, Visualization, Writing – original draft. **Sachin Kumar:** Data curation, Conceptualization, Supervision, Writing – original draft. **Prayag Tiwari:** Data curation, Investigation, Validation, Visualization, Writing – original draft.

Declaration of competing interest

The authors declare no conflict of interests.

Data availability

No data was used for the research described in the article.

Acknowledgments

Sachin Kumar is thankful for the support of Russian Science Foundation Regional Grant Number: 23-21-10009.

Funding statement

There was no external funding received for the preparation of this article.

References

[1] J. Xu, B.S. Glicksberg, C. Su, P. Walker, J. Bian, F. Wang, Federated learning for healthcare informatics, J. Healthc. Inform. Res. 5 (2021) 1–19.
[2] J.-P.A. Yaacoub, et al., Securing internet of medical things systems: Limitations, issues and recommendations, Future Gener. Comput. Syst. 105 (2020) 581–606.
[3] R.A. Beasley, Medical robots: current systems and research directions, J. Robot. 2012 (2012).
[4] J. Rosen, B. Hannaford, Doc at a distance, IEEE Spectr. 43 (2006) 34–39.
[5] R. Miotto, F. Wang, S. Wang, X. Jiang, J.T. Dudley, Deep learning for healthcare: review, opportunities and challenges, Brief. Bioinform. 19 (2018) 1236–1246.
[6] F. Wang, A. Preininger, AI in health: state of the art, challenges, and future directions, Yearb. Med. Inform. 28 (2019) 016–026.
[7] Y. Xu, G. Xu, C. Ma, Z. An, An advancing temporal convolutional network for 5G latency services via automatic modulation recognition, IEEE Trans. Circuits Syst. II (2022).
[8] L.O. Gostin, National health information privacy: regulations under the health insurance portability and accountability act, JAMA 285 (2001) 3015–3021.
[9] Y. LeCun, Y. Bengio, G. Hinton, Deep learning, Nature 521 (2015) 436–444.
[10] D.C. Nguyen, et al., Federated learning for smart healthcare: A survey, ACM Comput. Surv. 55 (2022) 1–37.
[11] Y. Kumar, R. Singla, Federated learning systems for healthcare: perspective and recent progress, in: Federated Learning Systems, 2021, pp. 141–156.
[12] Q. Yang, Y. Liu, T. Chen, Y. Tong, Federated machine learning: Concept and applications, ACM Trans. Intell. Syst. Technol. 10 (2019) 1–19.
[13] T. Li, A.K. Sahu, A. Talwalkar, V. Smith, Federated learning: Challenges, methods, and future directions, IEEE Signal Process. Mag. 37 (2020) 50–60.
[14] L. Li, Y. Fan, M. Tse, K.-Y. Lin, A review of applications in federated learning, Comput. Ind. Eng. 149 (2020) 106854.
[15] N. Rieke, et al., The future of digital health with federated learning, NPJ Digit. Med. 3 (2020) 1–7.
[16] P. Boopalan, et al., Fusion of federated learning and industrial internet of things: A survey, Comput. Netw. (2022) 109048.
[17] D. Li, Z. Luo, B. Cao, Blockchain-based federated learning methodologies in smart environments, Cluster Comput. 25 (2022) 2585–2599.
[18] J.C. Jiang, B. Kantarci, S. Oktug, T. Soyata, Federated learning in smart city sensing: Challenges and opportunities, Sensors 20 (2020) 6230.
[19] L.C. Fourati, A. Samiha, Federated learning toward data preprocessing: COVID-19 context, in: 2021 IEEE International Conference on Communications Workshops (ICC Workshops), IEEE, 2021, pp. 1–6.
[20] Q. Xia, W. Ye, Z. Tao, J. Wu, Q. Li, A survey of federated learning for edge computing: Research problems and solutions, High-Confid. Comput. 1 (2021) 100008.
[21] P. Chhikara, P. Singh, R. Tekchandani, N. Kumar, M. Guizani, Federated learning meets human emotions: A decentralized framework for human–computer interaction for iot applications, IEEE Internet Things J. 8 (2020) 6949–6962.
[22] J. Li, et al., A federated learning based privacy-preserving smart healthcare system, IEEE Trans. Ind. Inform. 18 (2021).
[23] S. AbdulRahman, H. Tout, H. Ould-Slimane, A. Mourad, C. Talhi, M. Guizani, A survey on federated learning: The journey from centralized to distributed on-site learning and beyond, IEEE Internet Things J. 8 (2020) 5476–5497.
[24] G. Dhiman, et al., Federated learning approach to protect healthcare data over big data scenario, Sustainability 14 (2022) 2500.
[25] T. Zhang, L. Gao, C. He, M. Zhang, B. Krishnamachari, A.S. Avestimehr, Federated learning for the internet of things: applications, challenges, and opportunities, IEEE Internet Things Mag. 5 (2022) 24–29.
[26] R.S. Antunes, C. André da Costa, A. Küderle, I.A. Yari, B. Eskofier, Federated learning for healthcare: Systematic review and architecture proposal, ACM Trans. Intell. Syst. Technol. 13 (2022) 1–23.
[27] C.-R. Shyu, et al., A systematic review of federated learning in the healthcare area: From the perspective of data properties and applications, Appl. Sci. 11 (2021) 11191.
[28] M.A. Rahman, M.S. Hossain, An internet-of-medical-things-enabled edge computing framework for tackling COVID-19, IEEE Internet Things J. 8 (2021) 15847–15854.
[29] S. Rani, et al., Threats and corrective measures for IoT security with observance of cybercrime: A survey, Wirel. Commun. Mob. Comput. 2021 (2021).
[30] S. Rani, et al., Amalgamation of advanced technologies for sustainable development of smart city environment: A review, IEEE Access 9 (2021) 150060–150087.
[31] R. Kumar, S. Rani, M.A. Awadh, Exploring the application sphere of the internet of things in industry 4.0: A review, bibliometric and content analysis, Sensors 22 (2022) 4276.
[32] D. Kothandaraman, et al., Decentralized link failure prevention routing (DLFPR) algorithm for efficient internet of things, Intell. Autom. Soft Comput. 34 (2022) 655–666.
[33] S. Vishnu, S.J. Ramson, R. Jegan, Internet of medical things (IoMT)-An overview, in: 2020 5th International Conference on Devices, Circuits and Systems, ICDCS, IEEE, 2020, pp. 101–104.
[34] S. Vishnu, S.J. Ramson, K.L. Raju, T. Anagnostopoulos, Simple-link sensor network-based remote monitoring of multiple patients, in: Intelligent Data Analysis for Biomedical Applications, Elsevier, 2019, pp. 237–252.
[35] L.P. Malasinghe, N. Ramzan, K. Dahal, Remote patient monitoring: a comprehensive study, J. Ambient Intell. Humaniz. Comput. 10 (2019) 57–76.
[36] T. Szydło, M. Konieczny, Mobile devices in the open and universal system for remote patient monitoring, IFAC-PapersOnLine 48 (2015) 296–301.
[37] M.V. Ramesh, S. Anand, P. Rekha, A mobile software for health professionals to monitor remote patients, in: 2012 Ninth International Conference on Wireless and Optical Communications Networks, WOCN, IEEE, 2012, pp. 1–4.
[38] Y. Yang, X. Wang, Z. Ning, J.J. Rodrigues, X. Jiang, Y. Guo, Edge learning for Internet of Medical Things and its COVID-19 applications: A distributed 3C framework, IEEE Internet Things Mag. 4 (2021) 18–23.
[39] Y. Abdulsalam, M.S. Hossain, COVID-19 networking demand: An auction-based mechanism for automated selection of edge computing services, IEEE Trans. Netw. Sci. Eng. (2020).
[40] I. Ahmed, M. Ahmad, J.J. Rodrigues, G. Jeon, S. Din, A deep learning-based social distance monitoring framework for COVID-19, Sustainable Cities Soc. 65 (2021) 102571.
[41] G. Muhammad, M.S. Hossain, N. Kumar, EEG-based pathology detection for home health monitoring, IEEE J. Sel. Areas Commun. 39 (2020) 603–610.
[42] K. El Asnaoui, Y. Chawki, Using X-ray images and deep learning for automated detection of coronavirus disease, J. Biomol. Struct. Dyn. 39 (2021) 3615–3626.
[43] M. Shorfuzzaman, M.S. Hossain, MetaCOVID: A siamese neural network framework with contrastive loss for n-shot diagnosis of COVID-19 patients, Pattern Recognit. 113 (2021) 107700.
[44] N. Asiri, M. Hussain, F. Al Adel, N. Alzaidi, Deep learning based computer-aided diagnosis systems for diabetic retinopathy: A survey, Artif. Intell. Med. 99 (2019) 101701.

[45] R.P. Singh, M. Javaid, A. Haleem, R. Suman, Internet of things (IoT) applications to fight against COVID-19 pandemic, Diabetes Metab. Syndr.: Clin. Res. Rev. 14 (2020) 521–524.
[46] H. Jelodar, Y. Wang, R. Orji, S. Huang, Deep sentiment classification and topic discovery on novel coronavirus or COVID-19 online discussions: NLP using LSTM recurrent neural network approach, IEEE J. Biomed. Health Inf. 24 (2020) 2733–2742.
[47] M.S. Hossain, G. Muhammad, Emotion recognition using secure edge and cloud computing, Inform. Sci. 504 (2019) 589–601.
[48] H. Lin, S. Garg, J. Hu, X. Wang, M.J. Piran, M.S. Hossain, Privacy-enhanced data fusion for COVID-19 applications in intelligent Internet of medical Things, IEEE Internet Things J. 8 (2020) 15683–15693.
[49] M.Z. Alom, et al., A state-of-the-art survey on deep learning theory and architectures, Electronics 8 (2019) 292.
[50] M.S. Hossain, G. Muhammad, Emotion-aware connected healthcare big data towards 5G, IEEE Internet Things J. 5 (2017) 2399–2406.
[51] S.G.J. Yuen, J. Park, A. Ghoreyshi, A. Wu, User Identification via Motion and Heartbeat Waveform Data, ed: Google Patents, 2017.
[52] A. Naditz, Telemedicine named one of space race's top tech breakthroughs, Telemed. e-Health 15 (2009) 735–736.
[53] M.B. Pinto, A. Yagnik, Fit for life: A content analysis of fitness tracker brands use of Facebook in social media marketing, J. Brand Manag. 24 (2017) 49–67.
[54] S.V. Kasl, S. Cobb, Health behavior, illness behavior and sick role behavior: I. Health and illness behavior, Arch. Environ. Health: Int. J. 12 (1966) 246–266.
[55] M. Swan, Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0, J. Sens. Actuator Netw. 1 (2012) 217–253.
[56] R. Wang, et al., Accuracy of wrist-worn heart rate monitors, Jama Cardiol. 2 (2017) 104–106.
[57] P. Marrow, et al., Agents in decentralised information ecosystems: the diet approach, 2001.
[58] K. Hung, Y.-T. Zhang, 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, IEEE, 2004, pp. 5384–5387.
[59] N.R. Council, The Role of Human Factors in Home Health Care: Workshop Summary, 2010.
[60] L. Perry, R. Malkin, Effectiveness of Medical Equipment Donations to Improve Health Systems: How Much Medical Equipment is Broken in the Developing World?, Vol. 49, ed: Springer, 2011, pp. 719–722.
[61] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, C. Tsatsoulis, Review of security and privacy for the Internet of Medical Things (IoMT), in: 2019 15th International Conference on Distributed Computing in Sensor Systems, DCOSS, IEEE, 2019, pp. 457–464.
[62] H. Abbas Khalaf, Patient privacy: A secure medical care by collection, preservation, and secure utilization of medicinal e-records based on IoMT, in: Next Generation of Internet of Things, Springer, 2023, pp. 253–267.
[63] G. Xu, M. Hu, C. Ma, Secure and smart autonomous multi-robot systems for opinion spammer detection, Inform. Sci. 576 (2021) 681–693.
[64] M. Papaioannou, et al., A survey on security threats and countermeasures in internet of medical things (IoMT), Trans. Emerg. Telecommun. Technol. 33 (2022) e4049.
[65] M. Kumar, S. Verma, A. Kumar, M.F. Ijaz, D.B. Rawat, ANAF-IoMT: a novel architectural framework for IoMT enabled smart healthcare system by enhancing security based on RECC-VC, IEEE Trans. Ind. Inform. (2022).
[66] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications, IEEE Internet Things J. 4 (2017) 1125–1142.
[67] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, R. Jain, Recent advances in the internet-of-medical-things (IoMT) systems security, IEEE Internet Things J. 8 (2020) 8707–8718.
[68] P. Kasyoka, M. Kimwele, S. Mbandu Angolo, Certificateless pairing-free authentication scheme for wireless body area network in healthcare management system, J. Med. Eng. Technol. 44 (2020) 12–19.
[69] T. Belkhouja, S. Sorour, M.S. Hefeida, Role-based hierarchical medical data encryption for implantable medical devices, in: 2019 IEEE Global Communications Conference, GLOBECOM, IEEE, 2019, pp. 1–6.
[70] F. Alsubaei, A. Abuhussein, V. Shandilya, S. Shiva, IoMT-SAF: Internet of medical things security assessment framework, Internet Things 8 (2019) 100123.
[71] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, C. Douligeris, Security in IoMT communications: A survey, Sensors 20 (2020) 4828.
[72] A.H.M. Aman, W.H. Hassan, S. Sameen, Z.S. Attarbashi, M. Alizadeh, L.A. Latiff, IoMT amid COVID-19 pandemic: Application, architecture, technology, and security, J. Netw. Comput. Appl. 174 (2021) 102886.
[73] T. Vaiyapuri, A. Binbusayyis, V. Varadarajan, Security, privacy and trust in IoMT enabled smart healthcare system: a systematic review of current and future trends, Int. J. Adv. Comput. Sci. Appl. 12 (2021).
[74] S. Razdan, S. Sharma, Internet of Medical Things (IoMT): overview, emerging technologies, and case studies, IETE Tech. Rev. (2021) 1–14.
[75] A. Kumari, S. Jangirala, M.Y. Abbasi, V. Kumar, M. Alam, ESEAP: ECC based secure and efficient mutual authentication protocol using smart card, J. Inf. Secur. Appl. 51 (2020) 102443.
[76] S. Tu, et al., Security in fog computing: A novel technique to tackle an impersonation attack, IEEE Access 6 (2018) 74993–75001.
[77] S. Tu, et al., Reinforcement learning assisted impersonation attack detection in device-to-device communications, IEEE Trans. Veh. Technol. 70 (2021) 1474–1479.
[78] D. Gafurov, E. Snekkenes, T.E. Buvarp, Robustness of biometric gait authentication against impersonation attack, in: OTM Confederated International Conferences on the Move to Meaningful Internet Systems, Springer, 2006, pp. 479–488.
[79] B. Lakshmi, B.S. Lakshmi, R. Karthikeyan, Detection and prevention of impersonation attack in wireless networks, Int. J. Adv. Res. Comput. Sci. Technol. 2 (2014) 267–270.
[80] R. Skowyra, et al., Effective topology tampering attacks and defenses in software-defined networks, in: 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN, IEEE, 2018, pp. 374–385.
[81] K. Lemke, Embedded security: Physical protection against tampering attacks, in: Embedded Security in Cars, Springer, 2006, pp. 207–217.
[82] M. Bellare, D. Cash, R. Miller, Cryptography secure against related-key attacks and tampering, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2011, pp. 486–503.
[83] D.-W. Huang, W. Liu, J. Bi, Data tampering attacks diagnosis in dynamic wireless sensor networks, Comput. Commun. 172 (2021) 84–92.
[84] M.N. Aman, K. Javed, B. Sikdar, K.C. Chua, Detecting data tampering attacks in synchrophasor networks using time hopping, in: 2016 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), IEEE, 2016, pp. 1–6.
[85] F.-X. Standaert, Introduction to side-channel attacks, in: Secure Integrated Circuits and Systems, Springer, 2010, pp. 27–42.
[86] R. Spreitzer, V. Moonsamy, T. Korak, S. Mangard, Systematic classification of side-channel attacks: A case study for mobile devices, IEEE Commun. Surv. Tutor. 20 (2017) 465–488.
[87] E. Prouff, M. Rivain, Masking against side-channel attacks: A formal security proof, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2013, pp. 142–159.
[88] X. Chen, H. Zhu, D. Geng, W. Liu, R. Yang, S. Li, Merging RFID and blockchain technologies to accelerate big data medical research based on physiological signals, J. Healthc. Eng. 2020 (2020).
[89] S. Saif, S. Biswas, S. Chattopadhyay, Intelligent, secure big health data management using deep learning and blockchain technology: an overview, in: Deep Learning Techniques for Biomedical and Health Informatics, 2020, pp. 187–209.
[90] S.C. Sethuraman, V. Vijayakumar, S. Walczak, Cyber attacks on healthcare devices using unmanned aerial vehicles, J. Med. Syst. 44 (2020) 1–10.
[91] Z. Xu, C. Xu, W. Liang, J. Xu, H. Chen, A lightweight mutual authentication and key agreement scheme for medical Internet of Things, IEEE Access 7 (2019) 53922–53931.
[92] V.H. Tutari, B. Das, D.R. Chowdhury, A continuous role-based authentication scheme and data transmission protocol for implantable medical devices, in: 2019 Second International Conference on Advanced Computational and Communication Paradigms, ICACCP, IEEE, 2019, pp. 1–6.
[93] Y. Sun, B. Lo, An artificial neural network framework for gait-based biometrics, IEEE J. Biomed. Health Inf. 23 (2018) 987–998.
[94] M.F. Awan, K. Kansanen, S. Perez-Simbor, C. Garcia-Pardo, S. Castelló-Palacios, N. Cardona, RSS-based secret key generation in wireless in-body networks, in: 2019 13th International Symposium on Medical Information and Communication Technology, ISMICT, IEEE, 2019, pp. 1–6.
[95] A. Ashok, P. Poornachandran, K. Achuthan, Secure authentication in multimodal biometric systems using cryptographic hash functions, in: International Conference on Security in Computer Networks and Distributed Systems, Springer, 2012, pp. 168–177.
[96] P.P. Pittalia, A comparative study of hash algorithms in cryptography, Int. J. Comput. Sci. Mob. Comput. 8 (2019) 147–152.
[97] E. Testa, M. Soeken, L. Amarù, G. De Micheli, Reducing the multiplicative complexity in logic networks for cryptography and security applications, in: 2019 56th ACM/IEEE Design Automation Conference, DAC, IEEE, 2019, pp. 1–6.

[98] B.A. Alzahrani, A. Irshad, A. Albeshri, K. Alsubhi, A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks, Wirel. Pers. Commun. 117 (2021) 47–69.
[99] S. Maji, et al., A low-power dual-factor authentication unit for secure implantable devices, in: 2020 IEEE Custom Integrated Circuits Conference, CICC, IEEE, 2020, pp. 1–4.
[100] N. Koblitz, A. Menezes, S. Vanstone, The state of elliptic curve cryptography, Des. Codes Cryptogr. 19 (2000) 173–193.
[101] B.P.U. Ivy, P. Mandiwa, M. Kumar, A modified RSA cryptosystem based on 'n'prime numbers, Int. J. Eng. Comput. Sci. 1 (2012) 63–66.
[102] V.J. Jariwala, D.C. Jinwala, AdaptableSDA: secure data aggregation framework in wireless body area networks, in: Wearable and Implantable Medical Devices, Elsevier, 2020, pp. 79–114.
[103] T. Bhatia, A.K. Verma, G. Sharma, Towards a secure incremental proxy re-encryption for e-healthcare data sharing in mobile cloud computing, Concurr. Comput.: Pract. Exper. 32 (2020) e5520.
[104] Z.-W. Xu, Cloud-sea computing systems: Towards thousand-fold improvement in performance per watt for the coming zettabyte era, J. Comput. Sci. Tech. 29 (2014) 177–181.
[105] M. Moh, R. Raju, Machine learning techniques for security of Internet of Things (IoT) and fog computing systems, in: 2018 International Conference on High Performance Computing & Simulation, HPCS, IEEE, 2018, pp. 709–715.
[106] A. Acar, H. Aksu, A.S. Uluagac, M. Conti, A survey on homomorphic encryption schemes: Theory and implementation, ACM Comput. Surv. 51 (2018) 1–35.
[107] G. Kalyani, S. Chaudhari, An efficient approach for enhancing security in Internet of Things using the optimum authentication key, Int. J. Comput. Appl. 42 (2020) 306–314.
[108] X. Yi, R. Paulet, E. Bertino, Homomorphic encryption, in: Homomorphic Encryption and Applications, Springer, 2014, pp. 27–46.
[109] B. Poettering, S. Rastikian, Sequential digital signatures for cryptographic software-update authentication, in: European Symposium on Research in Computer Security, Springer, 2022, pp. 255–274.
[110] C. Easttom, N. Mei, Mitigating implanted medical device cybersecurity risks, in: 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference, UEMCON, IEEE, 2019, pp. 0145–0148.
[111] G. Zheng, et al., Finger-to-heart (F2H): Authentication for wireless implantable medical devices, IEEE J. Biomed. Health Inf. 23 (2018) 1546–1557.
[112] G. Zheng, W. Yang, M. Johnstone, R. Shankaran, C. Valli, Securing the elderly in cyberspace with fingerprints, in: Assistive Technology for the Elderly, Elsevier, 2020, pp. 59–79.
[113] S. Kulaç, A new externally worn proxy-based protector for non-secure wireless implantable medical devices: Security jacket, IEEE Access 7 (2019) 55358–55366.
[114] S. Kulaç, Security belt for wireless implantable medical devices, J. Med. Syst. 41 (2017) 1–9.
[115] Z. Yang, Q. Zhou, L. Lei, K. Zheng, W. Xiang, An IoT-cloud based wearable ECG monitoring system for smart healthcare, J. Med. Syst. 40 (2016) 1–11.
[116] W. Youssef, A.O. Zaid, M.S. Mourali, M.H. Kammoun, RFID-based system for secure logistic management of implantable medical devices in tunisian health centres, in: 2019 IEEE International Smart Cities Conference (ISC2), IEEE, 2019, pp. 83–86.
[117] A. Mosaif, S. Rakrak, A Li-Fi based wireless system for surveillance in hospitals, Biomed. Spectrosc. Imaging 8 (2019) 81–92.
[118] V. Manjula, R. Thalapathi Rajasekaran, Security vulnerabilities in traditional wireless sensor networks by an intern in IoT, blockchain technology for data sharing in IoT, in: Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm, Springer, 2020, pp. 579–597.
[119] A.A. Hady, A. Ghubaish, T. Salman, D. Unal, R. Jain, Intrusion detection system for healthcare systems using medical and network data: A comparison study, IEEE Access 8 (2020) 106576–106584.
[120] L. Gupta, T. Salman, M. Zolanvari, A. Erbad, R. Jain, Fault and performance management in multi-cloud virtual network services using AI: A tutorial and a case study, Comput. Netw. 165 (2019) 106950.
[121] C. Deng, D. Zhang, G. Feng, Resilient practical cooperative output regulation for MASs with unknown switching exosystem dynamics under DoS attacks, Automatica 139 (2022) 110172.
[122] R. Font, J.M. Espín, M.J. Cano, Experimental analysis of features for replay attack detection-results on the ASVspoof 2017 Challenge, in: Interspeech, 2017, pp. 7–11.
[123] Y.-C. Wu, Q. Chaudhari, E. Serpedin, Clock synchronization of wireless sensor networks, IEEE Signal Process. Mag. 28 (2010) 124–138.
[124] B. Hidasi, M. Quadrana, A. Karatzoglou, D. Tikk, Parallel recurrent neural network architectures for feature-rich session-based recommendations, in: Proceedings of the 10th ACM Conference on Recommender Systems, 2016, pp. 241–248.
[125] S. Salamatian, W. Huleihel, A. Beirami, A. Cohen, M. Médard, Centralized vs decentralized targeted brute-force attacks: Guessing with side-information, IEEE Trans. Inf. Forensics Secur. 15 (2020) 3749–3759.
[126] L. Wang, J. Yang, X. Xu, P.-J. Wan, Mining network traffic with the-means clustering algorithm for stepping-stone intrusion detection, Wirel. Commun. Mob. Comput. 2021 (2021).
[127] M.K. Hasan, et al., A review on security threats, vulnerabilities, and counter measures of 5G enabled internet-of-medical-things, Iet Commun. 16 (2022) 421–432.
[128] I. Butun, P. Österberg, H. Song, Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures, IEEE Commun. Surv. Tutor. 22 (2019) 616–644.
[129] J. Ibarra, H. Jahankhani, J. Beavers, Biohacking capabilities and threat/attack vectors, in: Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity, 2020, pp. 117–131.
[130] S. Singh, H. Rezaii, J.-F. Bousquet, J. Craig, Channel access model to predict impact of authentication attack on AIS, in: OCEANS 2018 MTS/IEEE Charleston, IEEE, 2018, pp. 1–5.
[131] J. Beavers, S. Pournouri, Recent cyber attacks and vulnerabilities in medical devices and healthcare institutions, in: Blockchain and Clinical Trial: Securing Patient Data, 2019, pp. 249–267.
[132] M. Kim, E. Hwang, J.-N. Kim, Analysis of eavesdropping attack in mmwave-based WPANs with directional antennas, Wirel. Netw. 23 (2017) 355–369.
[133] V. Anh, P. Cuong, P. Vinh, Context-aware mobility based on π-calculus in internet of thing: A survey, in: Context-Aware Systems and Applications, and Nature of Computation and Communication, ed: Springer, Berlin, 2019.
[134] E. Hamadaqa, W. Adi, Clone-resistant authentication for medical operating environment, in: 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), IEEE, 2020, pp. 757–762.
[135] A.-T. Fadi, B.D. Deebak, Seamless authentication: for IoT-big data technologies in smart industrial application systems, IEEE Trans. Ind. Inform. 17 (2020) 2919–2927.
[136] W. Meng, W. Li, L. Zhu, Enhancing medical smartphone networks via blockchain-based trust management against insider attacks, IEEE Trans. Eng. Manage. 67 (2019) 1377–1386.
[137] S. Zeadally, E. Adi, Z. Baig, I.A. Khan, Harnessing artificial intelligence capabilities to improve cybersecurity, IEEE Access 8 (2020) 23817–23837.
[138] L.E.S. Jaramillo, Malware detection and mitigation techniques: Lessons learned from mirai DDOS attack, J. Inf. Syst. Eng. Manag. 3 (2018) 19.
[139] H.-M. Sun, C.-E. Shen, C.-Y. Weng, A flexible framework for malicious open XML document detection based on APT attacks, in: IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), IEEE, 2019, pp. 2005–2006.
[140] P. Arunachalam, et al., Synovial sarcoma classification technique using support vector machine and structure features, Intell. Autom. Soft Comput. 32 (2021) 1241–1259.
[141] K. Banerjee, et al., A machine-learning approach for prediction of water contamination using latitude, longitude, and elevation, Water (Switzerland) 14 (2022) 728.
[142] S. Rani, P. Bhambri, M. Chauhan, A machine learning model for kids' behavior analysis from facial emotions using principal component analysis, in: 2021 5th Asian Conference on Artificial Intelligence Technology, ACAIT, IEEE, 2021, pp. 522–525.
[143] A. Kataria, D. Agrawal, S. Rani, V. Karar, M. Chauhan, Prediction of blood screening parameters for preliminary analysis using neural networks, in: Predictive Modeling in Biomedical Data Mining and Analysis, Elsevier, 2022, pp. 157–169.
[144] V. Ranga, S. Gupta, P. Agrawal, J. Meena, Pathological analysis of blood cells using deep learning techniques, Recent Adv. Comput. Sci. Commun. (Former.: Recent Pat. Comput. Sci.) 15 (2022) 397–403.
[145] P. Kairouz, et al., Advances and open problems in federated learning, Found. Trends Mach. Learn. 14 (2021) 1–210.
[146] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, Y. Gao, A survey on federated learning, Knowl.-Based Syst. 216 (2021) 106775.
[147] A.Z. Tan, H. Yu, L. Cui, Q. Yang, Towards personalized federated learning, IEEE Trans. Neural Netw. Learn. Syst. (2022).
[148] N. Bibi, M. Sikandar, I. Ud Din, A. Almogren, S. Ali, IoMT-based automated detection and classification of leukemia using deep learning, J. Healthc. Eng. 2020 (2020).
[149] J. Konečný, H.B. McMahan, F.X. Yu, P. Richtárik, A.T. Suresh, D. Bacon, Federated learning: Strategies for improving communication efficiency, 2016, arXiv preprint arXiv:1610.05492.
[150] M.J. Sheller, et al., Federated learning in medicine: facilitating multi-institutional collaborations without sharing patient data, Sci. Rep. 10 (2020) 1–12.
[151] W. Zhang, et al., Dynamic-fusion-based federated learning for COVID-19 detection, IEEE Internet Things J. 8 (2021) 15884–15891.

[152] H.B. McMahan, E. Moore, D. Ramage, B.A. y Arcas, Federated learning of deep networks using model averaging, 2016, arXiv preprint arXiv:1602.05629, vol. 2.
[153] S. Kit Lo, Q. Lu, C. Wang, H.-Y. Paik, L. Zhu, A systematic literature review on federated machine learning: From a software engineering perspective, 2020, arXiv e-prints, p. arXiv:2007.11354.
[154] Y. Liu, X. Yuan, Z. Xiong, J. Kang, X. Wang, D. Niyato, Federated learning for 6G communications: Challenges, methods, and future directions, China Commun. 17 (2020) 105–118.
[155] M. Alazab, S.P. RM, M. Parimala, P.K.R. Maddikunta, T.R. Gadekallu, Q.-V. Pham, Federated learning for cybersecurity: Concepts, challenges, and future directions, IEEE Trans. Ind. Inform. 18 (2021) 3501–3509.
[156] P. Singh, M.K. Singh, R. Singh, N. Singh, Federated learning: Challenges, methods, and future directions, in: Federated Learning for IoT Applications, Springer, 2022, pp. 199–214.
[157] S. Agrawal, et al., Federated learning for intrusion detection system: Concepts, challenges and future directions, Comput. Commun. (2022).
[158] X. Yin, Y. Zhu, J. Hu, A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions, ACM Comput. Surv. 54 (2021) 1–36.
[159] C. Shen, J. Xu, S. Zheng, X. Chen, Resource rationing for wireless federated learning: Concept, benefits, and challenges, IEEE Commun. Mag. 59 (2021) 82–87.
[160] M. Aledhari, R. Razzak, R.M. Parizi, F. Saeed, Federated learning: A survey on enabling technologies, protocols, and applications, IEEE Access 8 (2020) 140699–140725.
[161] G. Xu, H. Li, S. Liu, K. Yang, X. Lin, Verifynet: Secure and verifiable federated learning, IEEE Trans. Inf. Forensics Secur. 15 (2019) 911–926.
[162] J. Kang, Z. Xiong, D. Niyato, Y. Zou, Y. Zhang, M. Guizani, Reliable federated learning for mobile networks, IEEE Wirel. Commun. 27 (2020) 72–80.
[163] J. Konečný, B. McMahan, D. Ramage, Federated optimization: Distributed optimization beyond the datacenter, 2015, arXiv preprint arXiv:1511.03575.
[164] J. Konečný, H.B. McMahan, D. Ramage, P. Richtárik, Federated optimization: Distributed machine learning for on-device intelligence, 2016, arXiv preprint arXiv:1610.02527.
[165] V. Kulkarni, M. Kulkarni, A. Pant, Survey of personalization techniques for federated learning, in: 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), IEEE, 2020, pp. 794–797.
[166] S. Caldas, et al., Leaf: A benchmark for federated settings, 2018, arXiv preprint arXiv:1812.01097.
[167] V. Smith, C.-K. Chiang, M. Sanjabi, A.S. Talwalkar, Federated multi-task learning, in: Advances in Neural Information Processing Systems, Vol. 30, 2017.
[168] Q.-V. Pham, K. Dev, P.K.R. Maddikunta, T.R. Gadekallu, T. Huynh-The, Fusion of federated learning and industrial Internet of Things: A survey, 2021, arXiv preprint arXiv:2101.00798.
[169] Y. Jie, J.Y. Pei, L. Jun, G. Yun, X. Wei, Smart home system based on iot technologies, in: 2013 International Conference on Computational and Information Sciences, IEEE, 2013, pp. 1789–1791.
[170] F. Granqvist, M. Seigel, R. van Dalen, Á. Cahill, S. Shum, M. Paulik, Improving on-device speaker verification using federated learning with privacy, 2020, arXiv preprint arXiv:2008.02651.
[171] X. Lei, G.-H. Tu, C.-Y. Li, T. Xie, M. Zhang, SecWIR: Securing smart home IoT communications via wi-fi routers with embedded intelligence, in: Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services, 2020, pp. 260–272.
[172] H. Arasteh, et al., Iot-based smart cities: A survey, in: 2016 IEEE 16th International Conference on Environment and Electrical Engineering, EEEIC, IEEE, 2016, pp. 1–6.
[173] A.S. Syed, D. Sierra-Sosa, A. Kumar, A. Elmaghraby, IoT in smart cities: a survey of technologies, practices and challenges, Smart Cities 4 (2021) 429–475.
[174] H. Rajab, T. Cinkelr, IoT based smart cities, in: 2018 International Symposium on Networks, Computers and Communications, ISNCC, IEEE, 2018, pp. 1–4.
[175] A. Moradipari, N. Tucker, T. Zhang, G. Cezar, M. Alizadeh, Mobility-aware smart charging of electric bus fleets, in: 2020 IEEE Power & Energy Society General Meeting, PESGM, IEEE, 2020, pp. 1–5.
[176] X. Zeng, B. Fang, H. Shen, M. Zhang, Distream: scaling live video analytics with workload-adaptive distributed edge intelligence, in: Proceedings of the 18th Conference on Embedded Networked Sensor Systems, 2020, pp. 409–421.
[177] B.C. Drolet, J.S. Marwaha, B. Hyatt, P.E. Blazar, S.D. Lifchez, Electronic communication of protected health information: privacy, security, and HIPAA compliance, J. Hand Surg. 42 (2017) 411–416.
[178] D. Liu, T. Miller, R. Sayeed, K.D. Mandl, Fadl: Federated-autonomous deep learning for distributed electronic health record, 2018, arXiv preprint arXiv:1811.11400.
[179] B. Yuan, S. Ge, W. Xing, A federated learning framework for healthcare iot devices, 2020, arXiv preprint arXiv:2005.05083.
[180] B. Yan, et al., Experiments of federated learning for COVID-19 chest X-ray images, in: International Conference on Artificial Intelligence and Security, Springer, 2021, pp. 41–53.
[181] E. Bertino, N. Islam, Botnets and internet of things security, Computer 50 (2017) 76–79.
[182] T.D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, A.-R. Sadeghi, DÏoT: A federated self-learning anomaly detection system for IoT, in: 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), 2019, pp. 756–767.
[183] Y. Fan, Y. Li, M. Zhan, H. Cui, Y. Zhang, Iotdefender: A federated transfer learning intrusion detection framework for 5 g iot, in: 2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE), IEEE, 2020, pp. 88–95.
[184] T. Zhang, C. He, T. Ma, L. Gao, M. Ma, S. Avestimehr, Federated learning for internet of things, in: Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems, 2021, pp. 413–419.
[185] C. He, et al., Fedcv: a federated learning framework for diverse computer vision tasks, 2021, arXiv preprint arXiv:2111.11066.
[186] C. He, et al., Fedgraphnn: A federated learning system and benchmark for graph neural networks, 2021, arXiv preprint arXiv:2104.07145.
[187] B.Y. Lin, et al., Fednlp: A research platform for federated learning in natural language processing, 2021, arXiv preprint arXiv:2104.08815.
[188] C. He, et al., Fedml: A research library and benchmark for federated machine learning, 2020, arXiv preprint arXiv:2007.13518.
[189] S. Otoum, I. Al Ridhawi, H.T. Mouftah, Blockchain-supported federated learning for trustworthy vehicular networks, in: GLOBECOM 2020-2020 IEEE Global Communications Conference, IEEE, 2020, pp. 1–6.
[190] O. Alfandi, S. Otoum, Y. Jararweh, Blockchain solution for iot-based critical infrastructures: Byzantine fault tolerance, in: NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium, IEEE, 2020, pp. 1–4.
[191] L.D. Xu, E.L. Xu, L. Li, Industry 4.0: state of the art and future trends, Int. J. Prod. Res. 56 (2018) 2941–2962.
[192] Y. Lu, X. Huang, Y. Dai, S. Maharjan, Y. Zhang, Blockchain and federated learning for privacy-preserved data sharing in industrial IoT, IEEE Trans. Ind. Inform. 16 (2019) 4177–4186.
[193] L.-H. Lee, et al., All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda, 2021, arXiv preprint arXiv:2110.05352.
[194] M. Duan, D. Liu, X. Chen, R. Liu, Y. Tan, L. Liang, Self-balancing federated learning with global imbalanced data in mobile systems, IEEE Trans. Parallel Distrib. Syst. 32 (2020) 59–71.
[195] M. Duan, et al., Flexible clustered federated learning for client-level data distribution shift, IEEE Trans. Parallel Distrib. Syst. 33 (2021) 2661–2674.
[196] L. Li, et al., Federated learning with workload-aware client scheduling in heterogeneous systems, Neural Netw. 154 (2022) 560–573.
[197] I. Kholod, et al., Open-source federated learning frameworks for IoT: A comparative review and analysis, Sensors 21 (2020) 167.
[198] G.A. Reina, et al., OpenFL: An open-source framework for federated learning, 2021, arXiv preprint arXiv:2105.06413.
[199] S.A. Harmon, et al., Artificial intelligence for the detection of COVID-19 pneumonia on chest CT using multinational datasets, Nature Commun. 11 (2020) 1–7.
[200] H. Cai, D. Rueckert, J. Passerat-Palmbach, 2Cp: Decentralized protocols to transparently evaluate contributivity in blockchain federated learning environments, 2020, arXiv preprint arXiv:2011.07516.
[201] Q. Li, et al., A survey on federated learning systems: vision, hype and reality for data privacy and protection, IEEE Trans. Knowl. Data Eng. (2021).
[202] A. Ziller, et al., Pysyft: A library for easy federated learning, in: Federated Learning Systems, Springer, 2021, pp. 111–139.
[203] V. Turina, Z. Zhang, F. Esposito, I. Matta, Combining split and federated architectures for efficiency and privacy in deep learning, in: Proceedings of the 16th International Conference on Emerging Networking EXperiments and Technologies, 2020, pp. 562–563.
[204] J.-J. Yang, J.-Q. Li, Y. Niu, A hybrid solution for privacy preserving medical data sharing in the cloud environment, Future Gener. Comput. Syst. 43 (2015) 74–86.
[205] C. Xu, N. Wang, L. Zhu, K. Sharif, C. Zhang, Achieving searchable and privacy-preserving data sharing for cloud-assisted E-healthcare system, IEEE Internet Things J. 6 (2019) 8345–8356.
[206] M. Frid-Adar, I. Diamant, E. Klang, M. Amitai, J. Goldberger, H. Greenspan, GAN-based synthetic medical image augmentation for increased CNN performance in liver lesion classification, Neurocomputing 321 (2018) 321–331.

[207] M. Staffa, et al., An OpenNCP-based solution for secure eHealth data exchange, J. Netw. Comput. Appl. 116 (2018) 65–85.
[208] Z. Che, Y. Cheng, S. Zhai, Z. Sun, Y. Liu, Boosting deep learning risk prediction with generative adversarial networks for electronic health records, in: 2017 IEEE International Conference on Data Mining, ICDM, IEEE, 2017, pp. 787–792.
[209] D.C. Nguyen, P.N. Pathirana, M. Ding, A. Seneviratne, BEdgeHealth: A decentralized architecture for edge-based IoMT networks using blockchain, IEEE Internet Things J. 8 (2021) 11743–11757.
[210] Y. Zhao, et al., Privacy-preserving blockchain-based federated learning for IoT devices, IEEE Internet Things J. 8 (2020) 1817–1829.
[211] C. Ma, et al., On safeguarding privacy and security in the framework of federated learning, IEEE Netw. 34 (2020) 242–248.
[212] L.U. Khan, et al., Federated learning for edge networks: Resource optimization and incentive mechanism, IEEE Commun. Mag. 58 (2020) 88–93.
[213] Y. Cheng, Y. Liu, T. Chen, Q. Yang, Federated learning for privacy-preserving AI, Commun. ACM 63 (2020) 33–36.
[214] S. Yang, B. Ren, X. Zhou, L. Liu, Parallel distributed logistic regression for vertical federated learning without third-party coordinator, 2019, arXiv preprint arXiv:1911.09824.
[215] S. Sharma, C. Xing, Y. Liu, Y. Kang, Secure and efficient federated transfer learning, in: 2019 IEEE International Conference on Big Data (Big Data), IEEE, 2019, pp. 2569–2576.
[216] J. So, B. Güler, A.S. Avestimehr, Turbo-aggregate: Breaking the quadratic aggregation barrier in secure federated learning, IEEE J. Sel. Areas Inf. Theory 2 (2021) 479–489.
[217] Y. Zhao, M. Li, L. Lai, N. Suda, D. Civin, V. Chandra, Federated learning with non-iid data, 2018, arXiv preprint arXiv:1806.00582.
[218] M. Hao, H. Li, G. Xu, Z. Liu, Z. Chen, Privacy-aware and resource-saving collaborative learning for healthcare in cloud computing, in: ICC 2020-2020 IEEE International Conference on Communications, ICC, IEEE, 2020, pp. 1–6.
[219] T.S. Brisimi, R. Chen, T. Mela, A. Olshevsky, I.C. Paschalidis, W. Shi, Federated learning of predictive models from federated electronic health records, Int. J. Med. Inform. 112 (2018) 59–67.
[220] O. Choudhury, et al., Differential privacy-enabled federated learning for sensitive health data, 2019, arXiv preprint arXiv:1910.02578.
[221] K. Wei, et al., Federated learning with differential privacy: Algorithms and performance analysis, IEEE Trans. Inf. Forensics Secur. 15 (2020) 3454–3469.
[222] P. Vepakomma, O. Gupta, T. Swedish, R. Raskar, Split learning for health: Distributed deep learning without sharing raw patient data, 2018, arXiv preprint arXiv:1812.00564.
[223] L. Huang, A.L. Shea, H. Qian, A. Masurkar, H. Deng, D. Liu, Patient clustering improves efficiency of federated machine learning to predict mortality and hospital stay time using distributed electronic medical records, J. Biomed. Inform. 99 (2019) 103291.
[224] L. Huang, Y. Yin, Z. Fu, S. Zhang, H. Deng, D. Liu, LoAdaBoost: Loss-based AdaBoost federated machine learning with reduced computational complexity on IID and non-IID intensive care data, Plos One 15 (2020) e0230706.
[225] B. Sabri, J. Fethi, V. Neethu, M. Shabir, E. Haithum, M. Michel, Federated uncertainty-aware learning for distributed hospital ehr data, 2019, ed.
[226] P. Papadopoulos, W. Abramson, A.J. Hall, N. Pitropakis, W.J. Buchanan, Privacy and trust redefined in federated machine learning, Mach. Learn. Knowl. Extr. 3 (2021) 333–356.
[227] S.R. Pfohl, A.M. Dai, K. Heller, Federated and differentially private learning for electronic health records, 2019, arXiv preprint arXiv:1911.05861.
[228] D.C. Nguyen, P.N. Pathirana, M. Ding, A. Seneviratne, Blockchain and edge computing for decentralized EMRs sharing in federated healthcare, in: GLOBECOM 2020-2020 IEEE Global Communications Conference, IEEE, 2020, pp. 1–6.
[229] Z. Tian, M. Li, M. Qiu, Y. Sun, S. Su, Block-DEF: A secure digital evidence framework using blockchain, Inform. Sci. 491 (2019) 151–165.
[230] Z. Lv, L. Qiao, M.S. Hossain, B.J. Choi, Analysis of using blockchain to protect the privacy of drone big data, IEEE Netw. 35 (2021) 44–49.
[231] K. Cai, H. Chen, W. Ai, X. Miao, Q. Lin, Q. Feng, Feedback convolutional network for intelligent data fusion based on near-infrared collaborative IoT technology, IEEE Trans. Ind. Inform. 18 (2021) 1200–1209.
[232] S. Aich, et al., Protecting personal healthcare record using blockchain & federated learning technologies, in: 2022 24th International Conference on Advanced Communication Technology, ICACT, IEEE, 2022, pp. 109–112.
[233] S. Singh, S. Rathore, O. Alfarraj, A. Tolba, B. Yoon, A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology, Future Gener. Comput. Syst. 129 (2022) 380–388.
[234] J. Kim, K. Hur, S. Yang, E. Choi, Universal EHR federated learning framework, 2022, arXiv preprint arXiv:2211.07300.
[235] Q. Wu, X. Chen, Z. Zhou, J. Zhang, Fedhome: Cloud-edge based personalized federated learning for in-home health monitoring, IEEE Trans. Mob. Comput. (2020).
[236] Y. Chen, X. Qin, J. Wang, C. Yu, W. Gao, Fedhealth: A federated transfer learning framework for wearable healthcare, IEEE Intell. Syst. 35 (2020) 83–93.
[237] D. Liu, D. Dligach, T. Miller, Two-stage federated phenotyping and patient representation learning, in: Proceedings of the Conference. Association for Computational Linguistics. Meeting, Vol. 2019, NIH Public Access, 2019, p. 283.
[238] G.K. Gudur, S.K. Perepu, Federated learning with heterogeneous labels and models for mobile activity monitoring, 2020, arXiv preprint arXiv:2012.02539.
[239] D. Liu, K. Fox, G. Weber, T. Miller, Confederated machine learning on horizontally and vertically separated medical data for large-scale health system intelligence, 2019, arXiv preprint arXiv:1910.02109.
[240] X. Xu, et al., Federated depression detection from multi-source mobile health data, 2021, arXiv preprint arXiv:2102.09342.
[241] X. Tan, C.-C.H. Chang, L. Tang, A tree-based federated learning approach for personalized treatment effect estimation from heterogeneous data sources, 2021, arXiv preprint arXiv:2103.06261.
[242] Z. Yan, J. Wicaksana, Z. Wang, X. Yang, K.-T. Cheng, Variation-aware federated learning with multi-source decentralized medical image data, IEEE J. Biomed. Health Inf. 25 (2020) 2615–2628.
[243] S. Silva, B.A. Gutman, E. Romero, P.M. Thompson, A. Altmann, M. Lorenzi, Federated learning in distributed medical databases: Meta-analysis of large-scale subcortical brain data, in: 2019 IEEE 16th International Symposium on Biomedical Imaging (ISBI 2019), IEEE, 2019, pp. 270–274.
[244] F. Ucar, D. Korkmaz, COVIDiagnosis-Net: Deep Bayes-SqueezeNet based diagnosis of the coronavirus disease 2019 (COVID-19) from X-ray images, Med. Hypotheses 140 (2020) 109761.
[245] W. Li, et al., Privacy-preserving federated brain tumour segmentation, in: International Workshop on Machine Learning in Medical Imaging, Springer, 2019, pp. 133–141.
[246] U.C. Srivastava, D. Upadhyay, V. Sharma, Intracranial hemorrhage detection using neural network based methods with federated learning, 2020, arXiv preprint arXiv:2005.08644.
[247] P. Guo, P. Wang, J. Zhou, S. Jiang, V.M. Patel, Multi-institutional collaborations for improving deep learning-based magnetic resonance image reconstruction using federated learning, in: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2021, pp. 2423–2432.
[248] X. Li, Y. Gu, N. Dvornek, L.H. Staib, P. Ventola, J.S. Duncan, Multi-site fMRI analysis using privacy-preserving federated learning and domain adaptation: ABIDE results, Med. Image Anal. 65 (2020) 101765.
[249] M.Y. Lu, et al., Federated learning for computational pathology on gigapixel whole slide images, Med. Image Anal. 76 (2022) 102298.
[250] H.R. Roth, et al., Federated learning for breast density classification: A real-world implementation, in: Domain Adaptation and Representation Transfer, and Distributed and Collaborative Learning, Springer, 2020, pp. 181–191.
[251] M. Loey, F. Smarandache, N.E.M. Khalifa, Within the lack of chest COVID-19 X-ray dataset: a novel detection model based on GAN and deep transfer learning, Symmetry 12 (2020) 651.
[252] I. Feki, S. Ammar, Y. Kessentini, K. Muhammad, Federated learning for COVID-19 screening from Chest X-ray images, Appl. Soft Comput. 106 (2021) 107330.
[253] D.C. Nguyen, M. Ding, P.N. Pathirana, A. Seneviratne, Blockchain and AI-based solutions to combat coronavirus (COVID-19)-like epidemics: A survey, IEEE Access 9 (2021) 95730–95753.
[254] R. Kumar, et al., Blockchain-federated-learning and deep learning models for covid-19 detection using ct imaging, IEEE Sens. J. 21 (2021) 16301–16314.
[255] Q.-V. Pham, D.C. Nguyen, T. Huynh-The, W.-J. Hwang, P.N. Pathirana, Artificial intelligence (AI) and big data for coronavirus (COVID-19) pandemic: a survey on the state-of-the-arts, IEEE Access 8 (2020) 130820.
[256] F. Qian, A. Zhang, The value of federated learning during and post-COVID-19, Int. J. Qual. Health Care 33 (2021) mzab010.
[257] Q. Dou, et al., Federated deep learning for detecting COVID-19 lung abnormalities in CT: a privacy-preserving multinational validation study, NPJ Digit. Med. 4 (2021) 1–11.
[258] B. Liu, B. Yan, Y. Zhou, Y. Yang, Y. Zhang, Experiments of federated learning for covid-19 chest x-ray images, 2020, arXiv preprint arXiv:2007.05592.
[259] S. Boughorbel, F. Jarray, N. Venugopal, S. Moosa, H. Elhadi, M. Makhlouf, Federated uncertainty-aware learning for distributed hospital ehr data, 2019, arXiv preprint arXiv:1910.12191.

[260] M. Malekzadeh, B. Hasircioglu, N. Mital, K. Katarya, M.E. Ozfatura, D. Gündüz, Dopamine: Differentially private federated learning on medical data, 2021, arXiv preprint arXiv:2101.11693.
[261] D. Yang, et al., Federated semi-supervised learning for COVID region segmentation in chest CT using multi-national data from China, Italy, Japan, Med. Image Anal. 70 (2021) 101992.
[262] I.J. Goodfellow, et al., Challenges in representation learning: A report on three machine learning contests, in: International Conference on Neural Information Processing, Springer, 2013, pp. 117–124.
[263] A. Di Martino, et al., The autism brain imaging data exchange: towards a large-scale evaluation of the intrinsic brain architecture in autism, Mol. Psychiatry 19 (2014) 659–667.
[264] J.P. Cohen, P. Morrison, L. Dao, COVID-19 image data collection, 2020, arXiv preprint arXiv:2003.11597.
[265] L. Zhang, B. Shen, A. Barnawi, S. Xi, N. Kumar, Y. Wu, FedDPGAN: federated differentially private generative adversarial networks framework for the detection of COVID-19 pneumonia, Inf. Syst. Front. 23 (2021) 1403–1415.
[266] M. Abdul Salam, S. Taha, M. Ramadan, COVID-19 detection using federated machine learning, Plos One 16 (2021) e0252573.
[267] T.J. Pollard, A.E. Johnson, J.D. Raffa, L.A. Celi, R.G. Mark, O. Badawi, The eICU Collaborative Research Database, a freely available multi-center database for critical care research, Sci. Data 5 (2018) 1–13.
[268] J. Cui, H. Zhu, H. Deng, Z. Chen, D. Liu, FeARH: Federated machine learning with anonymous random hybridization on electronic medical records, J. Biomed. Inform. 117 (2021) 103735.
[269] D. Cha, M. Sung, Y.-R. Park, Implementing vertical federated learning using autoencoders: Practical application, generalizability, and utility study, JMIR Med. Inform. 9 (2021) e26598.
[270] P. Schmidt, A. Reiss, R. Duerichen, C. Marberger, K. Van Laerhoven, Introducing wesad, a multimodal dataset for wearable stress and affect detection, in: Proceedings of the 20th ACM International Conference on Multimodal Interaction, 2018, pp. 400–408.
[271] J.C. Liu, J. Goetz, S. Sen, A. Tewari, Learning from others without sacrificing privacy: Simulation comparing centralized and federated machine learning on mobile health data, JMIR mHealth uHealth 9 (2021) e23728.
[272] G. Vavoulas, C. Chatzaki, T. Malliotakis, M. Pediaditis, M. Tsiknakis, The mobiact dataset: Recognition of activities of daily living using smartphones, in: International Conference on Information and Communication Technologies for Ageing Well and e-Health, Vol. 2, SciTePress, 2016, pp. 143–151.
[273] J. Ogier du Terrail, et al., FLamby: Datasets and benchmarks for cross-silo federated learning in realistic healthcare settings, 2022, arXiv e-prints, p. arXiv:2210.04620.
[274] D. Anguita, A. Ghio, L. Oneto, X. Parra Perez, J.L. Reyes Ortiz, A public domain dataset for human activity recognition using smartphones, in: Proceedings of the 21th International European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning, 2013, pp. 437–442.
[275] Y. Chen, X. Sun, Y. Jin, Communication-efficient federated deep learning with layerwise asynchronous model update and temporally weighted aggregation, IEEE Trans. Neural Netw. Learn. Syst. 31 (2019) 4229–4238.
[276] A.E. Johnson, et al., MIMIC-III, a freely accessible critical care database, Sci. Data 3 (2016) 1–9.
[277] B.H. Menze, et al., The multimodal brain tumor image segmentation benchmark (BRATS), IEEE Trans. Med. Imaging 34 (2014) 1993–2024.
[278] G. Litjens, O. Debats, J. Barentsz, N. Karssemeijer, H. Huisman, Prostatex challenge data, Cancer Imaging Arch. 10 (2017) K9TCIA.
[279] K.V. Sarma, et al., Federated learning improves site performance in multicenter deep learning without data sharing, J. Am. Med. Inform. Assoc. 28 (2021) 1259–1264.
[280] M.A. Rahman, N.I. Haque, Systems and Methods for Formal Threat Analysis of a Smart Healthcare System, ed: Google Patents, 2022.
[281] L.E. Ochoa, J. Ochoa, Scanner Devices for Identifying and Storing Information Emitted by Implanted Medical Devices, ed: Google Patents, 2022.
[282] M.A. Horning, G.A. Brooks, Systems and Methods for Monitoring of Fractional Gluconeogenesis and Targeting of Fractional Gluconeogenesis Via Nutritional Support, ed: Google Patents, 2018.
[283] T. Melodia, G.E. Santagati, Software-Defined Implantable Ultrasonic Device for Use in the Internet of Medical Things, ed: Google Patents, 2021.
[284] J. Redei, Electronic Delivery of Information in Personalized Medicine, ed: Google Patents, 2020.
[285] J.C. Murrish, K. Kailasam, D.S. McNair, M.A. Ash, T.A. Fangman, Health Information Transformation System, ed: Google Patents, 2020.
[286] J.P. Smurro, Cognitive Collaboration with Neurosynaptic Imaging Networks, Augmented Medical Intelligence and Cybernetic Workflow Streams, ed: Google Patents, 2019.
[287] J.D. Kutzko, Computer-Implemented System and Methods for Predicting the Health and Therapeutic Behavior of Individuals using Artificial Intelligence, Smart Contracts and Blockchain, ed: Google Patents, 2019.
[288] M.A. Horning, G.A. Brooks, Systems and Methods for Monitoring of Blood Lactate and Targeting of Blood Lactate Via Nutritional Support, ed: Google Patents, 2018.
[289] H. Federoff, O. Frieder, E. Burger, System and Method of Applying State of Being to Health Care Delivery, ed: Google Patents, 2016.
[290] A. Binbusayyis, H. Alaskar, T. Vaiyapuri, M. Dinesh, An investigation and comparison of machine learning approaches for intrusion detection in IoMT network, J. Supercomput. (2022) 1–20.
[291] D. Unal, S. Bennbaia, F.O. Catak, Machine learning for the security of healthcare systems based on Internet of Things and edge computing, in: Cybersecurity and Cognitive Science, Elsevier, 2022, pp. 299–320.
[292] A.A. Süzen, B. Duman, Protecting the privacy of IoT-based health records using blockchain technology, in: Internet of Medical Things: Remote Healthcare Systems and Applications, 2021, p. 35.
[293] V. Puri, A. Kataria, V. Sharma, Artificial intelligence-powered decentralized framework for Internet of Things in Healthcare 4.0, Trans. Emerg. Telecommun. Technol. (2021) e4245.
[294] P. Pandey, R. Litoriya, Securing and authenticating healthcare records through blockchain technology, Cryptologia 44 (2020) 341–356.
[295] R.K. Marangappanavar, M. Kiran, Inter-planetary file system enabled blockchain solution for securing healthcare records, in: 2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP), IEEE, 2020, pp. 171–178.
[296] H. Elmogazy, O. Bamasag, Securing healthcare records in the cloud using attribute-based encryption, Comput. Inf. Sci. 9 (2016) 60–67.
[297] R. Kumar, R. Tripathi, Secure healthcare framework using blockchain and public key cryptography, in: Blockchain Cybersecurity, Trust and Privacy, Springer, 2020, pp. 185–202.
[298] B. Mahapatra, R. Krishnamurthi, A. Nayyar, Healthcare models and algorithms for privacy and security in healthcare records, in: Security and Privacy of Electronic Healthcare Records: Concepts, Paradigms and Solutions, 2019, p. 183.
[299] L. Zhang, J. Xu, P. Vijayakumar, P.K. Sharma, U. Ghosh, Homomorphic encryption-based privacy-preserving federated learning in iot-enabled healthcare system, IEEE Trans. Netw. Sci. Eng. (2022).
[300] Y. Chang, C. Fang, W. Sun, A blockchain-based federated learning method for smart healthcare, Comput. Intell. Neurosci. 2021 (2021).
[301] V. Drungilas, E. Vaičiukynas, M. Jurgelaitis, R. Butkienė, L. Čeponienė, Towards blockchain-based federated machine learning: Smart contract for model inference, Appl. Sci. 11 (2021) 1010.
[302] A. Rehman, S. Abbas, M. Khan, T.M. Ghazal, K.M. Adnan, A. Mosavi, A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique, Comput. Biol. Med. 150 (2022) 106019.
[303] B. Xu, W. Xia, J. Zhang, T.Q. Quek, H. Zhu, Online client scheduling for fast federated learning, IEEE Wirel. Commun. Lett. 10 (2021) 1434–1438.
[304] W. Xia, T.Q. Quek, K. Guo, W. Wen, H.H. Yang, H. Zhu, Multi-armed bandit-based client scheduling for federated learning, IEEE Trans. Wireless Commun. 19 (2020) 7108–7123.
[305] S. Luo, X. Chen, Q. Wu, Z. Zhou, S. Yu, HFEL: Joint edge association and resource allocation for cost-efficient hierarchical federated edge learning, IEEE Trans. Wireless Commun. 19 (2020) 6535–6548.
[306] H.H. Yang, Z. Liu, T.Q. Quek, H.V. Poor, Scheduling policies for federated learning in wireless networks, IEEE Trans. Commun. 68 (2019) 317–333.
[307] A. Rahman, et al., Federated learning-based AI approaches in smart healthcare: concepts, taxonomies, challenges and open issues, Cluster Comput. (2022) 1–41.
[308] K. Bonawitz, et al., Practical secure aggregation for federated learning on user-held data, 2016, arXiv preprint arXiv:1611.04482.
[309] F. Qiang, T. Lixin, L. Richard, White Paper-IEEE Federated Machine Learning, 2021.
[310] J. Xu, H. Wang, L. Chen, Bandwidth allocation for multiple federated learning services in wireless edge networks, IEEE Trans. Wireless Commun. 21 (2021) 2534–2546.
[311] J. Li, et al., Blockchain assisted decentralized federated learning (BLADE-FL): Performance analysis and resource allocation, IEEE Trans. Parallel Distrib. Syst. 33 (2021) 2401–2415.
[312] J. Kang, Z. Xiong, D. Niyato, S. Xie, J. Zhang, Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory, IEEE Internet Things J. 6 (2019) 10700–10714.
[313] Y. Sarikaya, O. Ercetin, Motivating workers in federated learning: A stackelberg game perspective, IEEE Netw. Lett. 2 (2019) 23–27.
[314] J. Zhao, X. Zhu, J. Wang, J. Xiao, Efficient client contribution evaluation for horizontal federated learning, in: ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP, IEEE, 2021, pp. 3060–3064.

[315] C.A. Choquette-Choo, et al., Capc learning: Confidential and private collaborative learning, 2021, arXiv preprint arXiv:2102.05188.
[316] E. Diao, J. Ding, V. Tarokh, HeteroFL: Computation and communication efficient federated learning for heterogeneous clients, 2020, arXiv preprint arXiv:2010.01264.
[317] C. De Alwis, et al., Survey on 6G frontiers: Trends, applications, requirements, technologies and future research, IEEE Open J. Commun. Soc. 2 (2021) 836–886.
[318] L. Mucchi, et al., How 6G technology can change the future wireless healthcare, in: 2020 2nd 6G Wireless Summit (6G SUMMIT), IEEE, 2020, pp. 1–6.
[319] V. Mothukuri, R.M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, G. Srivastava, A survey on security and privacy of federated learning, Future Gener. Comput. Syst. 115 (2021) 619–640.
[320] M. Wu, D. Ye, J. Ding, Y. Guo, R. Yu, M. Pan, Incentivizing differentially private federated learning: A multidimensional contract approach, IEEE Internet Things J. 8 (2021) 10639–10651.
[321] R. Kerkouche, G. Acs, C. Castelluccia, P. Genevès, Privacy-preserving and bandwidth-efficient federated learning: An application to in-hospital mortality prediction, in: Proceedings of the Conference on Health, Inference, and Learning, 2021, pp. 25–35.
[322] R. Hu, Y. Guo, H. Li, Q. Pei, Y. Gong, Personalized federated learning with differential privacy, IEEE Internet Things J. 7 (2020) 9530–9539.
[323] H. Fereidooni, et al., SAFELearn: secure aggregation for private federated learning, in: 2021 IEEE Security and Privacy Workshops, SPW, IEEE, 2021, pp. 56–62.