


**Please cite the Published Version**

Alzu'Bi, Ahmad, Alomar, Ala'a, Alkhaza'Leh, Shahed, Abuarqoub, Abelrahman and Hammoudeh, Mohammad  (2024) A review of privacy and security of edge computing in smart healthcare systems: issues, challenges, and research directions. Tsinghua Science and Technology, 29 (4). pp. 1152-1180. ISSN 1007-0214

**DOI:** <https://doi.org/10.26599/TST.2023.9010080>

**Publisher:** Tsinghua University Press

**Version:** Published Version

**Downloaded from:** <https://e-space.mmu.ac.uk/635041/>

**Usage rights:**  [Creative Commons: Attribution 4.0](https://creativecommons.org/licenses/by/4.0/)

**Additional Information:** This is an open access article which first appeared in Tsinghua Science and Technology

**Enquiries:**

If you have questions about this document, contact [openresearch@mmu.ac.uk](mailto:openresearch@mmu.ac.uk). Please include the URL of the record in e-space. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from <https://www.mmu.ac.uk/library/using-the-library/policies-and-guidelines>)

# A Review of Privacy and Security of Edge Computing in Smart Healthcare Systems: Issues, Challenges, and Research Directions

Ahmad Alzu'bi\*, Ala'a Alomar, Shahed Alkhaza'leh, Abdelrahman Abuarqoub, and  
Mohammad Hammoudeh

**Abstract:** The healthcare industry is rapidly adapting to new computing environments and technologies. With academics increasingly committed to developing and enhancing healthcare solutions that combine the Internet of Things (IoT) and edge computing, there is a greater need than ever to adequately monitor the data being acquired, shared, processed, and stored. The growth of cloud, IoT, and edge computing models presents severe data privacy concerns, especially in the healthcare sector. However, rigorous research to develop appropriate data privacy solutions in the healthcare sector is still lacking. This paper discusses the current state of privacy-preservation solutions in IoT and edge healthcare applications. It identifies the common strategies often used to include privacy by the intelligent edges and technologies in healthcare systems. Furthermore, the study addresses the technical complexity, efficacy, and sustainability limits of these methods. The study also highlights the privacy issues and current research directions that have driven the IoT and edge healthcare solutions, with which more insightful future applications are encouraged.

**Key words:** data privacy; edge computing; fog computing; healthcare systems; intelligent edges

## 1 Introduction

Edge computing paradigms and the Internet of Things (IoTs) have led to a global technological revolution, which has enabled the creation of a wide range of intelligent healthcare services organized over the Internet to improve the quality of care, the proposed

- Ahmad Alzu'bi, Ala'a Alomar, and Shahed Alkhaza'leh are with Department of Computer Science, Jordan University of Science and Technology, Irbid 22110, Jordan. E-mail: agalzubi@just.edu.jo; amalomar20@cit.just.edu.jo; ssalkhazaleh20@cit.just.edu.jo.
- Abdelrahman Abuarqoub is with Cardiff School of Technologies, Cardiff Metropolitan University, Cardiff CF5 2YB, UK. E-mail: aabuarqoub@cardiffmet.ac.uk.
- Mohammad Hammoudeh is with Department of Information and Computer Science, King Fahd University of Petroleum and Minerals, Dhahran 31261, Kingdom of Saudi Arabia. E-mail: m.hammoudeh@kfupm.edu.sa.

\* To whom correspondence should be addressed.

Manuscript received: 2023-05-30 ; revised: 2023-06-30;

accepted: 2023-07-27

treatment, and the cost of healthcare service<sup>[1, 2]</sup>. IoT devices generate a massive quantity of patient data which are stored on servers and exchanged among healthcare specialists for treatment purposes. The processing of this big data poses a major issue in the creation of real-time responses and secured applications. Therefore, there is a demand for designing and implementing effective solutions to improve network bandwidth, service, security, and more. These technologies include cloud computing, mobile cloud computing<sup>[3]</sup>, fog computing<sup>[4]</sup>, microdata center, cloudlet<sup>[5]</sup>, and edge computing.

Smart healthcare harnesses cutting-edge information technologies, such as artificial intelligence and big data, constituting a new wave in the field. It aims at integrating patients and doctors onto a shared platform, intelligent health monitoring is achieved through the analysis of daily human activities. The most common method for storing and processing data in the smart healthcare system is cloud computing. The major healthcare data and services are hosted on cloud servers

available on the Web. Wireless Body Sensor Networks (WBAN)<sup>[6]</sup> are being applied in the healthcare industry using cloud computing technologies. WBAN is used to perform remote health monitoring with smart real-time devices or sensors linked to people. As a result, the sensor nodes generate an enormous amount of data. For example, patient monitoring systems use specific parameters, such as heart rate to decide whether there are some risks related to critical patients with heart and lung disease, breathing problems, paralysis, and brain hemorrhage. Additionally, they can be watched by sending images or videos while exercising with body sensors.

Massive amounts of data must be processed; however, cloud computing is unable to handle this volume of data because it arrives from numerous sources over various networks. When several users seek access at the same time, the network bandwidth and transmission speed suffer. Simultaneously, remotely stored data are vulnerable to security and privacy risks. In cloud computing, access control and data leakage are key concerns. Before being transferred to the cloud, data are frequently encrypted to protect them from an intruder. However, searching for such encrypted data is a challenging task, which can lead to significant bandwidth, cost, and storage shortages when each time the complete encryption/decryption procedure is required. Because of this, traditional cloud computing systems are unable to handle real-time applications, like remote patient care in emergency scenarios. This problem motivates us to investigate existing technologies in the realm of edge computing and IoT based solutions capable of handling data privacy and access control with minimal latency and processing time.

Edge computing has recently emerged as a solution to the aforementioned challenges, gaining significant attention and interest from both academic and business communities. It is considered a good solution for protecting the privacy and security of patient data<sup>[7, 8]</sup>. The edge computing layer provides data processing close to the data source (healthcare network), reduces transmission costs, efficiently manages big data, increases data processing speed, and resolves security and privacy problems. Although there are several benefits to such technology, it poses some challenges that need to be tackled, particularly when it comes to data security and privacy. Since connected devices often have limited resources (e.g., low computing

power), they are particularly vulnerable to cyber and physical threats.

There has been a lot of research done to solve the difficulties mentioned above. Some of the studies address IoT security in general without considering privacy in healthcare using edge computing<sup>[9-11]</sup>. However, there is a lack of studies aiming at addressing the issues related to the use of intelligent edges in the domain of healthcare systems. Motivated by security and privacy concerns, research gaps, and a scarcity of existing literature on edge computing in the healthcare industry, this study discusses these gaps and addresses these flaws. Furthermore, an extensive investigation of the existing body of literature regarding the privacy and security concerns associated with edge computing is presented, focusing particularly on healthcare systems. The main objectives of this work could be summarized as follows:

- (1) Providing a comprehensive overview of edge computing, its applications, and architectural aspects. We also describe privacy and security in the context of edge-based healthcare systems.

- (2) Describing the security and privacy needs for users' or patients' data using six key criteria: privacy, confidentiality, availability, integrity, authentication, and access control.

- (3) Providing an in-depth exploration of the most recent security and privacy solutions in healthcare that are based on edge computing.

- (4) Discussing some open challenges in-depth and giving insights into several potential future research directions in the context of healthcare systems using edge computing environment.

The remaining part of this paper is structured as follows. Section 2 describes the scope of this research; Section 3 introduces the methodology adopted to conduct this review study; Section 4 discusses the edge computing architecture and the functional requirements of secure healthcare systems; Section 5 presents the primary concerns pertaining to privacy and security in healthcare systems that utilize edge computing; Section 6 reviews the current solutions dedicated to data security and privacy and countermeasures for mitigating attacks on edge computing; Section 7 highlights the most pressing issues and future research prospects; and Section 8 concludes this paper.

## 2 Related Study

Several studies have been conducted to address privacy

and security issues in healthcare systems. The majority of these studies have provided insight into privacy concerns and their remedies in various sections of the healthcare sector. They have analyzed several privacy and security options for intelligent healthcare systems that leverage edge computing paradigms to distribute data across multiple specialists. However, this paper is a comprehensive overview that aims at highlighting the main privacy and security issues in the context of edge-based healthcare systems, providing a comprehensive review of the recent data security and privacy solutions, and discussing the open security and privacy challenges of edge computing and architectures in smart healthcare systems.

A recent study was introduced by Algarni<sup>[12]</sup> to discuss security issues in healthcare but without the use of edge computing. It covers intelligent healthcare security and privacy, analysis, assessments, and classifications. Hathaliya and Tanwar<sup>[13]</sup> concentrated on utilizing blockchain technologies to deliver insights for future applications, and they presented a comparative review of the security and privacy in Healthcare 4.0, including the technology and parameters to address security and privacy concerns.

Sun et al.<sup>[14]</sup> discussed the existing security and confidentiality methods on the Internet of Medical Things (IoMT), focusing on data encryption, access management, trustworthy third-party audits, data anonymization, and data search. However, the study includes many assessments of the general security and privacy issues, but excludes the healthcare domain. Xiao et al.<sup>[15]</sup> reviewed the most important and fundamental edge computing threats, which account for 82% of the most current threats reported by Statista<sup>[16]</sup>. Yahuza et al.<sup>[17]</sup> and Zhang et al.<sup>[18]</sup> provided an overview of the classification of edge computing's privacy and security requirements, as well as the cutting-edge techniques employed to address these issues. To satisfy privacy requirements, Pussewalage and Oleshchuk<sup>[19]</sup> carried out a methodical examination of privacy-preserving strategies utilized in e-health solutions.

Some articles deal with security without addressing privacy, or vice versa. Roman et al.<sup>[20]</sup> assessed the security threats, problems, and processes prevalent in all edge models based on similarities and collaboration venues. They demonstrated that advancements in specific-domain paradigms should be considered by all cutting-edge healthcare paradigms. Huang et al.<sup>[21]</sup>

examined some of the difficulties associated with privacy protection, attack mitigation, access control, key management, and anomaly detection based on edge computing. Rao and Bertino<sup>[22]</sup> addressed the fundamental privacy-building elements, such as differential privacy and homomorphic encryption. They showed the privacy solutions for three common forms of data usage crucial for edge-based problems, which are data aggregation approaches, crowdsourcing, and traffic information services and point of interest services.

More recent studies<sup>[23–25]</sup> have discussed more issues related to the computing edge technologies used for healthcare systems. Hartman et al.<sup>[23]</sup> reviewed the main issues and challenges of using edge and fog computing compared to cloud and legacy technologies. However, unlike this study, our research specifically focuses on addressing the privacy and security concerns associated with edge computing as a central theme. Table 1 summarizes the main characteristics of the recent related studies. Our study is distinguished by providing a comprehensive review of privacy and security issues in the domain of healthcare that uses edge computing technologies.

### 3 Methodology of the Study

The approach taken in this survey promotes the repeatability of the results obtained through a series of clearly defined steps. These steps are: (1) define the research questions; (2) formulate the keywords to search literature repositories; (3) select and filter the articles; and (4) discuss the results with suitable classification. The first stage is to decide which research questions the literature review will answer. This includes a Major Question (MQ) and three Specific Questions (SQ), which are:

- MQ: What are the current solutions available to secure and maintain the privacy of edge computing in modern healthcare systems?
- SQ1: What are the most important research questions and solutions addressed in the literature?
- SQ2: How should the existing privacy/security solutions in smart healthcare systems be classified?
- SQ3: What are the principal challenges and future research directions?

Based on these study questions, we set the keywords to search and extract the raw corpus from the literature databases. The keywords include the most significant terms in our core research topic, as well as their

**Table 1** Summary of the existing related studies.

Reference	Year	Covered issue	Privacy	Security	Edge computing	Healthcare
[12]	2019	Healthcare security and privacy	√	√	×	√
[13]	2020	Blockchain-based security/privacy	√	√	×	√
[14]	2018	Security/privacy solutions in IoMT	√	√	×	√
[15]	2019	Fundamental threats and attacks	×	√	√	×
[17]	2020	Classification of security requirements	√	√	√	×
[18]	2018	Data protection and privacy	√	√	√	×
[19]	2016	Privacy-preserving for e-health solutions	√	√	×	√
[20]	2018	Security threats and challenges	×	√	√	×
[21]	2020	Edge computing security	×	√	√	×
[22]	2019	Privacy solutions in edge computing	√	×	√	×
[23]	2022	Edge computing issues in healthcare	√	√	√	√
[24]	2022	Intelligent monitoring using edge computing	√	×	√	√
[25]	2022	Security issues in cloud, fog, and edges	×	√	√	×
This study	2023	Edge-based healthcare security/privacy	√	√	√	√

popular synonyms. We extract the search results from the ACM explorer, ScienceDirect, and IEEE Xplore using the following keywords: “edge computing”, “security”, “privacy”, “healthcare”, “privacy edge computing healthcare”, and “security edge computing healthcare”. Also, we evaluate the publishers’ interest in this research topic. The mechanism of joining these keywords adopted as follows:

- (“security”  $\wedge$  “edge computing”)  $\vee$  (“privacy”  $\wedge$  “edge computing”);
- (“security”  $\wedge$  “edge computing”  $\wedge$  “healthcare”)  $\vee$  (“privacy”  $\wedge$  “edge computing”  $\wedge$  “healthcare”);
- “privacy edge computing healthcare”  $\wedge$  “security edge computing healthcare”.

We obtain the articles from the leading journals and conferences as follows: 771 articles from ACM, 865 articles from ScienceDirect, and 32 articles from IEEE repositories. Next, the raw corpus retrieved and collected is evaluated and filtered to generate the final list of relevant studies. The filtering process is controlled by the following criteria:

**(1) Period:** Include the articles written in English and published between 2015 to 2022.

**(2) Scope:** Apply a preliminary screening to weed out articles that are not particularly pertinent to the scope of this study, i.e., the articles do not mainly handle privacy, security, edge computing, or smart healthcare.

**(3) Duplication:** Exclude analogous publications focusing on minor concepts and discard any duplicates.

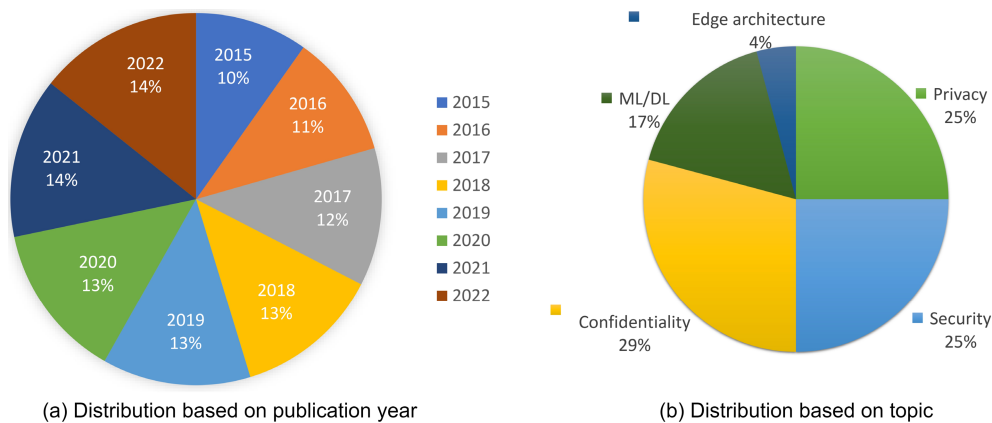
Consequently, we generate a collection of 1609 articles, from which we chose the most relevant

comprehensive studies for review and discussion in this study. The first observation drawn from the search and filtering procedure is that the utilization of edge computing technologies and algorithms in healthcare is expanding rapidly. Figure 1a demonstrates how articles are distributed by year of publication. The final collection includes 14% of articles published in 2021 and 14% of articles published in the first quarter of 2021. The analysis and discussion of the literary corpus is the final step in this systematic review. Figure 1b shows the distribution of research articles in the resulting literature corpus grouped by topics. We provide here a brief analysis of each of these categories with recent representative works in literature.

The literature corpus is classified into five general topics, as discussed in the following subsections, which are: (1) privacy of edge computing in healthcare; (2) security of edge computing in healthcare; (3) confidentiality guarantees for training data; (4) Machine Learning (ML)/Deep Learning (DL) models; and (5) edge computing architecture.

### 3.1 Privacy of edge computing in healthcare

This group encompasses the studies which propose secure and intelligent medical monitoring services based on edge computing solutions. Rahman et al.<sup>[26]</sup> described a safe therapeutic framework using blockchain-based Mobile Edge Computing (MEC) that allows patients to own and manage their personal data without the involvement of a third party. Kumar and Tripathi<sup>[27]</sup> employed the blockchain and InterPlanetary File System (IPFS) cluster to improve the scalability of



**Fig. 1** Distribution of articles in literature corpus.

IoMT healthcare systems, providing secure access to patient data simultaneously. Tripathi et al.<sup>[28]</sup> investigated a smart city ecosystem with technology-enabled healthcare and proposed a privacy-preserving Smart Medical System (SMS) architecture.

Given blockchain's popularity as a distributed architecture for authenticating data, many studies have been conducted to investigate its applicability to edge computing. Saha et al.<sup>[29]</sup> proposed an e-healthcare framework that addresses privacy concerns with Electronic Medical Records (EMRs). In a multi-server edge computing environment, Wang et al.<sup>[30]</sup> presented a blockchain-assisted handover method for Intelligent Telehealth Systems (ITS), that permits effective authentication, stringent privacy, and computational load transfer. ElRahman and Alluhaidan<sup>[31]</sup> utilized blockchain technology with IoT architectures to assess the absolute patient data privacy, unaltered data transfer, and safe transmission of patient examination findings.

### 3.2 Security of edge computing in healthcare

The second set of literature studies focus on the use of individual security techniques to guarantee the confidentiality of medical data. Hewa et al.<sup>[32]</sup> developed an MEC and blockchain-based secure service architecture to access and control patients' data using smart contracts. Abou-Nassar et al.<sup>[33]</sup> introduced a blockchain-based Decentralized Interoperable Trust (DIT) framework for IoT regions, with an intelligent contract ensuring budget authentication and the Indirect Trust Inference System (ITIS) reducing semantic gaps and improving Trustworthy Factor (TF) estimates via network nodes and edges. Li et al.<sup>[34]</sup> also created an architecture for Software-Defined Network (SDN) based edge computing in an IoT-enabled

healthcare system. The framework employs an authentication mechanism to authenticate IoT devices. After that, the device gathers patient data and sends them to edge servers. The SDN controller, which controls load balancing, network optimization, and resource use for the healthcare system, is connected to the edge servers.

However, scenarios requiring data exchange between possibly dishonest parties call for the implementation of various security measures, such as MedRec, which Azaria et al.<sup>[35]</sup> presented as a decentralized record management system that manages EMRs using blockchain technology. MedRec provides identification, secrecy, accountability, and data sharing. Christo et al.<sup>[36]</sup> also focused on deploying the Elliptic Curve Cryptography (ECC) technology, a lightweight authentication solution for data sharing success, discussing two key aspects of data security: data authentication and secrecy. Li et al.<sup>[37]</sup> also introduced safe edge computing technology (namely EdgeCare) for mobile healthcare systems, where data management is decentralized and collaborative. In general, the studies discussed above have investigated several distributed edge computing designs.

### 3.3 Data confidentiality

Medical data are inherently sensitive. The confidentiality of specific data items used to train models makes it one of the most demanding requirements for edge computing in healthcare applications. To guarantee the validity of Electronic Healthcare Records (EHRs) embedded in blockchains, Guo et al.<sup>[38]</sup> collaborated with several authorities using an attribute-based signature technique. Multiple authorities are incorporated into the Attribute-Based Signature (ABS) and suggest a Multiple Access-

ABS (MA-ABS) scheme that fits the requirements of the blockchain structure while ensuring information anonymity and immutability to protect patient privacy in a blockchain-based EHR system. Also, Egala et al.<sup>[39]</sup> demonstrated the Smart Healthcare system for Patients in ICU (SHPI), which uses blockchain technology and cryptography techniques to ensure protected patient data and reliable medical records.

Various existing approaches are combined with encryption to increase data confidentiality. Such a strategy on edge computing enables data processing while data are still encrypted. Al Omar et al.<sup>[40]</sup> proposed a healthcare solution to ensure patient privacy and transparency regarding insurance policies. These policies are kept on the blockchain in order to make the user's insurance policy more transparent. Additionally, users can safely store personal data and healthcare information on the blockchain, including test results, prescriptions, and diagnostic reports. Cryptographic technologies, such as the ECC encryption algorithm, are used to keep the patient's data private. Jan et al.<sup>[41]</sup> also provided a simple mutual authentication method for Industrial Cyber-Physical Systems (I-CPS) to safeguard wearable devices' and their data's privacy. The approach is based on client-server interaction architecture and provides symmetric encryption for secure interactions between entities. An AI-enabled Hidden Markov Model (HMM) is utilized to forecast the privacy risk associated with patient data after mutual authentication.

Islam and Shin<sup>[42]</sup> presented a blockchain-based health monitoring method that collects health data from users' wearable devices using UAVs. A user encrypts health data before sending them using the UAV's public key. After gathering health data, the UAV decrypts them and transfers them via UAV to the nearest MEC server. If MEC servers detect any problems with health data, they will notify the user as well as any nearby hospitals in the event of an emergency. Guo et al.<sup>[43]</sup> suggested a hybrid blockchain and edge node paradigm that allows the multi-authority ABE scheme to encrypt EHR data stored on the edge node and the Attribute-Based Multi-Signature (ABMS) method to validate user signatures while maintaining the privacy of sensitive information. Based on the Lamport-Merkle Digital Signature (LMDS), Alzubi<sup>[44]</sup> proposed a secure blockchain-assisted approach for medical IoT devices. The LMDS Generation (LMDSG) model creates a tree with leaves

that reflect the hash function of private patient medical data to initially authenticate IoT devices. A Centralized Healthcare Controller (CHC) uses the LMDS Verification (LMDSV) to identify the origin of the LMDSG.

### 3.4 ML/DL models

Since machine learning is dependent on vast amounts of medical data, it is essential to keep the data from leaking. Ma et al.<sup>[45]</sup> developed a privacy-preserving eXtreme Gradient Boost (XGBoost) over encrypted model parameters known as Lightweight Privacy-preserving Medical Edge (LPME), which modifies the XGBoost model using the edge model. In another experience related to the Corona pandemic, Vadrevu et al.<sup>[46]</sup> broadcast patient data to the public using several applications to maintain patient privacy without using any techniques to protect individual privacy. After completing the COVID-19 test, the government is informed of the subject's infection or lack thereof. If a person is infected with a virus, such details are shielded using K-anonymity, l-diversity, or differential quality.

Due to the difficulty of using Artificial Neural Networks (ANN) in mobile medical networks, Guo et al.<sup>[47]</sup> proposed a Federated Edge Learning (FEL) system for mobile devices that can safely and effectively analyze distributed private data in parallel to train medical ML models. Tasks for monitoring and training are partially transferred from the mobile device to the hospital's private server. The data are then stored on the devices of the users, while scattered hospitals merge their models to form a global model to increase diagnostic quality.

There has been a notable increase in research attention directed toward fundamental machine learning algorithms, with an emphasis on enhancing their scalability and decentralization. For example, a significant portion of the work proposed by Alabdulatif et al.<sup>[48]</sup> applies well-known distributed designs in the context of edge computing. The authors developed a secure Edge-of-Things (EoT) platform, which can gather, track, and analyze biosignal data in real time. Early disease identification and treatment are made possible by the EoT framework, potentially lowering disease-related harm and lengthening many lives. When data are stored in EoT databases on the cloud, Fully Homomorphic Encryption (FHE) is utilized to assure end-to-end data privacy, with

K-Means Clustering (KMC) and Fuzzy C-Means (FCM) approaches.

### 3.5 Edge computing architecture

The last group of literature studies focus on the development of complete architectures for edge computing applications in healthcare. They are more concerned with the combination of existing techniques, as well as the overall distributed architecture required for edge computing. For instance, Bosri et al.<sup>[49]</sup> proposed a user-centric edge-based architecture, known as HIDEchain, that assures safe edge computation for healthcare by keeping user information transaction logs on the blockchain. In Section 4.1, we elaborate more on the edge computing architectures in smart healthcare systems.

## 4 Architectural and Functional Requirements of Edge Computing for Healthcare Systems

In this section, the key concepts, functional architecture, and confidentiality requirements of edge computing are presented for smart healthcare systems. For healthcare systems, functional requirements establish the intended functionality of a system, while architectural requirements specify the manner in which the system should be designed and structured.

### 4.1 Characteristics of computing environments

The main notion behind the use of cloud computing is to store and access data and programs over the Internet rather than on local computing equipment. Cloud computing enables organizations to rapidly expand their accessible storage without needing to maintain additional servers on-site. Data may also be gathered from numerous sites and devices, and accessed at any time and from any locations<sup>[50, 51]</sup>. Subsequently, Cisco introduces the fog computing concept, which extends cloud computing to the edge of an enterprise's network<sup>[52]</sup>. With data processing taking place in a fog node or IoT gateway, fog computing brings intelligence down to the Local Area Network (LAN) level of network architecture. It simply involves moving your computers closer to the sensors which are communicating with. Trains are one example of fog computing. As part of the introduction of the industrial IoT<sup>[53–55]</sup>, smart trains and tracks are being supplied with a new generation of technologies and sensors, with trains acting as the primary hub for all data

gathered from these sensors. The difficulty is that, because trains travel so quickly, maintaining a connection with the cloud is challenging. This problem can be avoided by placing a set of fog computing nodes in the locomotive.

The design of fog computing, on the other hand, relies on many links in a communication chain to transmit data from the physical world of our assets into the digital realm of information technology. Each of these connections has the tendency to fail. Consequently, the emergence of edge computing enables local data processing, resulting in decreased traffic to the central repository. It lowers potential failure points and streamlines the fog communication chain. Edge computing is the processing of sensor data toward individual data sources, close to the logical edge of the network and away from centralized nodes. In essence, it moves computing tasks closer to the edge of the network. In other words, this process takes place a great deal closer to the data's original source, rather than transferring all the data back to the cloud for analysis and execution. Edge devices can be anything with sophisticated processing, storage, and functionality, such as routers, switches, and sensors that collect data.

Edge computing enables computing technologies at the network's edge, reducing latency closer to the requests, upstreaming data for IoT services, and downstreaming data for cloud services. A smartphone, for example, as an edge is the interface between people and the cloud, a gateway in a smart home is the interface between house things and the cloud, and a Micro Data Center (MDC) or a Cloudlet<sup>[56]</sup> is the interface between a mobile device and the cloud. The crucial aspect of edge computing is that computation should occur close to data sources<sup>[57]</sup>. The edge computing paradigm has several advantages over the traditional cloud computing model, including real-time data processing and analysis, high levels of security and privacy protection, scalability, robustness, low traffic, and location awareness<sup>[58, 59]</sup>. Therefore, Edge computing is particularly supposed to be a successful solution to lowering latency, reducing data transmission, and maintaining local data privacy. Table 2 summarizes the main characteristics of edge computing compared to cloud and fog computing.

### 4.2 Edge computing functions

The typical functional architecture of edge computing



**Table 2 Characteristics of cloud, fog, and edge computing.**

Criterion	Cloud computing	Fog computing	Edge computing
Purpose	Long-term analysis	Real-time analysis	Real-time analysis
Latency	High	Low	Very low
Security	Less secure	High security	High security
Storage	High	Low	Low
Response time	Minutes to weeks	Seconds or less	Milliseconds
Bandwidth utilization	High	Low	Very low
Server overhead	Very high	Low	Very low
Scalability	Medium	High	High
Location of data processing	Cloud server	IoT gateway or LAN	Device itself
Geographic coverage	Global	Connected devices	Device
Architecture	Centralized	Distributed	Distributed
Device example	Data center	Car, phone, and computer	Sensor, actuator, and wearables
Application	Big data	Dependable services	M2M communication haptics

is characterized by a three-tier framework, encompassing four layers: perception, connectivity, processing, and performance, i.e., reaction. The layered functional architecture of the computing environment is illustrated in Fig. 2. Firstly, data are received by the perception layer from a variety of sources, including sensors, apps, social networking websites, and electromagnetic devices. Sensors in the intelligent environment collect data from multiple domains, such as pollution monitoring, traffic control, etc. Data can be in different formats and sizes, such as video, audio, or text. Then, using a communication protocol and various technologies, like Wi-Fi<sup>[60]</sup>, Bluetooth<sup>[61]</sup>, Zigbee<sup>[62]</sup>, and Near Field Communication (NFC)<sup>[63]</sup>, all the captured data are sent to the processing layer. The processing layer sends the collected data to the middleware, referred to as the “edge gate”. The essential functions of this layer are data reading, aggregation, management control, etc. In the performance layer, reports are prepared in any intelligent environment after receiving the results from the processing layer. The actuators take actions depending on the data acquired by the sensors. The apps may respond based on the processing outcome<sup>[64]</sup>. This layer does all the essential operations to increase processing speed significantly faster than the cloud.

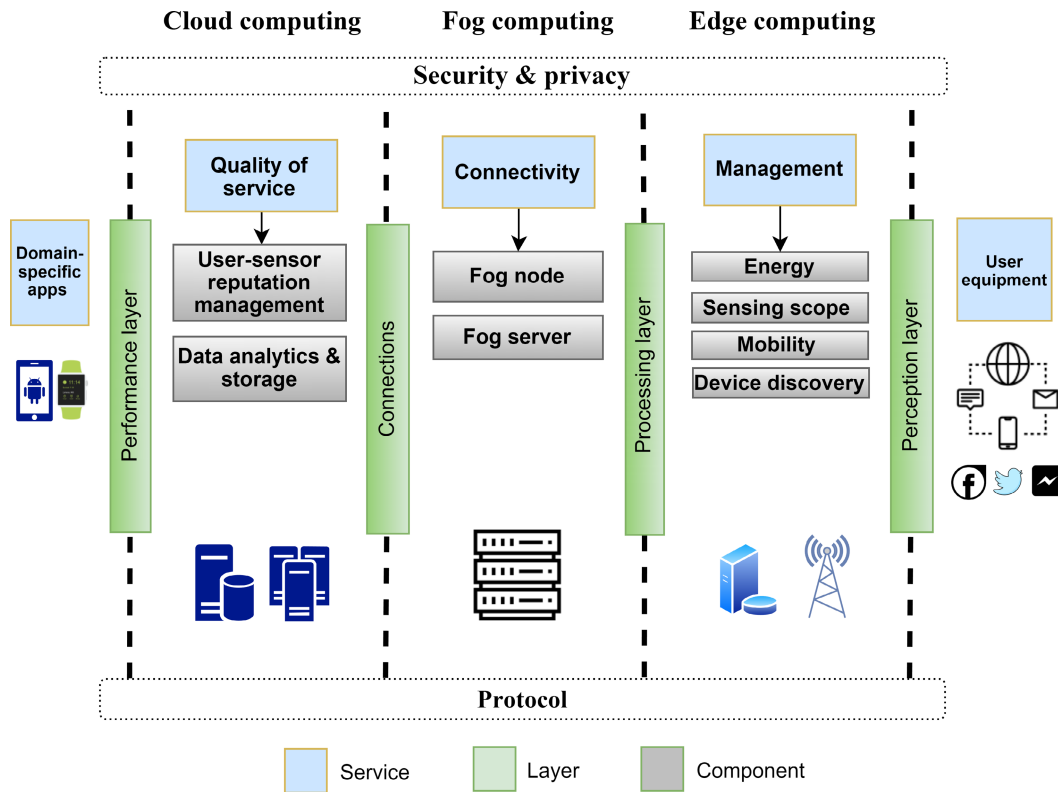
Figure 2 also demonstrates the cloud, fog, and edge environments into three tiers. The cloud level is primarily made up of centralized cloud infrastructure<sup>[65]</sup>. It comprises numerous servers with significant computational and storage capacities that offer a variety of services. In contrast to the traditional cloud computing design, some computation or services in the

fog architecture may be proficiently shifted from the cloud to the fog layer to lessen the burden on cloud resources and boost efficiency. The fog level is made up of many fog nodes. The OpenFog Consortium defines a fog node as “the physical and logical network piece that offers fog computing services”<sup>[66]</sup>. Fog nodes, which can be located anywhere between the cloud and edge devices, can compute, transmit, and temporarily store data. As a result, fog nodes are directly connected to edge devices to supply services. They, on the other hand, are linked to the cloud infrastructure to supply and receive services<sup>[67]</sup>. For example, fog nodes can benefit from cloud storage and computing capabilities while providing context information to users. Finally, the edge level includes edge devices<sup>[68]</sup> situated closer to the network end for data processing, communication, or caching<sup>[69]</sup>, which are the fundamental components of edge computing.

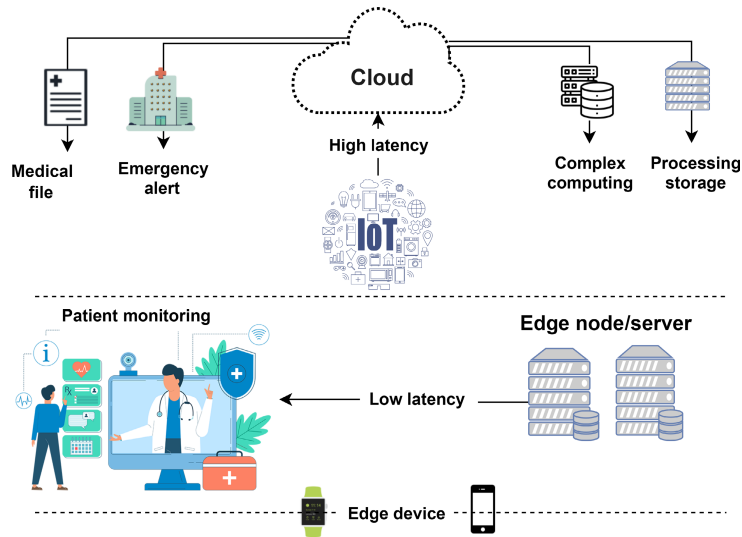
### 4.3 Architectural requirements of edge-based healthcare systems

This section introduces a generic architecture with the main requirements required to deploy healthcare applications in the edge computing environment. Generally, healthcare applications can be classified according to device type, data type, or unique use case<sup>[23]</sup>. The following are the primary healthcare categories based on the use cases: Genuine health monitors, emergency management systems, mental well-being smart applications, and healthcare dissemination of information.

As shown in Fig. 3, edge computing helps to improve healthcare standards by offering more thorough and



**Fig. 2** Layered functional architecture of computing environment.



**Fig. 3** General edge computing architecture in the context of healthcare.

timely treatment anywhere. The widespread use of health sensors, especially those with computing power for disease diagnosis and patient monitoring, can reduce the number of patients who visit hospitals and clinics. Patients can easily keep these edge sensor devices, which leads to new data insights on healthcare through continuous vital sign monitoring. Edge computing can therefore aid in lowering data transit

costs by moving necessary data from servers to the edge, thus reducing latency issues with cloud systems.

Moreover, there are several architectural requirements that should be maintained to achieve the best experience and performance while employing edge technologies in the field of healthcare. As can also be observed in Fig. 3, low latency, location awareness, and high-level privacy are important general requirements that should

be maintained.

In terms of low latency, when compared to standard cloud solutions, edge solutions have reduced latency, and some specialized system design characteristics enable this. With elderly monitoring in homes being the most popular application needing low latency, several edge mining algorithms can help to reduce the amount of time spent transferring data to the cloud or fog/edge nodes for computation or storage<sup>[23]</sup>. Some systems use sensors to gather information on a patient's current physical condition and transmit it to a Personal Digital Assistant (PDA) or mobile phone. The PDA or phone processes the data locally and notifies a patient's family or emergency services if a fall is detected or if their heart rate or blood pressure are outside of the normal range.

Mobile users can get services from the edge server that is closest to them geographically because of edge computing's location-aware capability. Users can use a range of technologies, including wireless access points<sup>[70, 71]</sup>, GPS, and mobile phone infrastructure, to find electronic devices. It might be used by a wide range of edge computing applications, such as fog-based automobile safety systems and disaster management<sup>[72]</sup>. Since it enables the patient to be located in the event of a medical emergency, location awareness is also a crucial requirement for edge computing in the healthcare industry. Greater precision can be attained by adopting localization techniques designed expressly for edge applications rather than costly GPS locating systems. Algorithms can deduce a person's position indoors or outside using a cloud server and a basic infrared sensor.

Health and location-related information are sensitive in terms of high-level privacy, so it is essential to offer users a high level of security. Prior to being sent to other nodes, health information at the edge of the network, frequently on mobile devices, must be secured. This needs to be done effectively but efficiently due to energy restrictions. Many potential computer nodes create new opportunities for obtaining patient data while simultaneously enhancing privacy due to the dispersion of essential data<sup>[39]</sup>. In edge computing applications, authentication protocols and trust ratings are employed to reduce the chance of infiltration.

In addition to the general requirements mentioned, there are a set of specific security and privacy requirements that need to be also maintained in the

domain of edge-based healthcare. Because of the massive volume of health data accessible and communicated over the Internet, security and privacy are now the key concerns of the healthcare business. Because it is an open communication route, network assaults on the data are possible. According to Zhang et al.<sup>[18]</sup>, there are various critical components for measuring system security. Edge computing requires the outsourcing of the patient and doctor's data protection (to high-end data centers, for example), which inevitably results in data loss, data leakage, illegal data operations like copying and publishing, as well as other data security issues, and data confidentiality and integrity cannot be ensured<sup>[73-75]</sup>.

As a result, external data security remains a fundamental issue in the security of edge computing data. In general, there is a demand to maintain the following security and privacy requirements in any edge-based healthcare system:

**(1) Confidentiality:** It aims to stop information from being disclosed without authorization. Confidentiality guards against unauthorized parties from accessing user data while they are transferred and received in the peripheral or core network infrastructure, and stored or processed at the edge. This implies that the data must be encrypted for the user before it is outsourced to edge servers. Many techniques have attracted more attention recently, such as Identity-Based Encryption (IBE)<sup>[76]</sup>, Attribute-Based Encryption (ABE)<sup>[77-79]</sup>, Proxy Re-Encryption (PRE)<sup>[80]</sup>, and Homomorphic Encryption (HE)<sup>[81]</sup>.

**(2) Integrity:** It ensures that data are transmitted correctly and consistently to the authorized user(s) without any observable data changes. Data integration research in edge computing should focus on four functional elements: batch auditing<sup>[82]</sup>, dynamic auditing<sup>[83]</sup>, privacy auditing<sup>[84]</sup>, and low complexity<sup>[85]</sup>.

**(3) Availability:** All authorized parties can access edge and cloud services whenever and wherever they need them. It also means that user data are stored in encrypted text in edge or cloud data centers, and handled according to different operational needs.

**(4) Authentication:** Authentication ensures that a customer's identification is permitted, which implies that there must be a way to verify the user's identity. Furthermore, the edge computing environment mandates identity validation for every entity within a certain trust domain and for entities to reciprocally prove each other throughout those trust domains.

Cross-domain authentication<sup>[86]</sup>, which is a typical identity management technique that authenticates customers for sites that exist in various fields, single-domain authentication<sup>[87]</sup>, and handover authentication<sup>[88]</sup>, are currently acceptable authentication techniques.

**(5) Access control:** Through control laws, access management serves as an improved mechanism for protection and privacy. It determines who has access to the information and what abilities, e.g., reading and writing, can be practiced.

**(6) Privacy requirements:** Sensitive information of end-users is sent to remote servers from edge devices. The privacy issue is exacerbated by the presence of numerous honest but curious adversaries. These attackers typically have authorized entities with the secondary purpose of gaining access to more sensitive information that could be utilized for egotistical purposes. Probabilistic public-key encryption<sup>[89]</sup>, a public-key cryptography system, which varies the ciphertext of a message encrypted with the same public key on each run of a probabilistic Turing machine<sup>[90]</sup>, and pseudo-random permutation<sup>[91]</sup> can all be used to create lightweight data privacy-preserving algorithms. Then, in a dynamic and dispersed computing environment, users must safeguard their credentials using management and authentication operations<sup>[92, 93]</sup>. Finally, since users frequently have relatively constant Points Of Interest (POIs), user location information is highly predictable, suggesting that users would frequently use the same edge servers. In this case, we should be more concerned about protecting our location privacy<sup>[94]</sup>.

## 5 Security and Privacy Challenges of Edge Computing in Healthcare Systems

Recently, the proliferation of smart healthcare systems has created massive amounts of data that are communicated via the Internet between doctors and patients, as the Internet is an open communication route that enables easy attacks on this data. As a result, privacy and security are now the top objectives in the healthcare sector. To protect patient data from unauthorized users, security techniques are utilized to control access to it. It is possible to achieve it through operational controls within a covered entity<sup>[95]</sup>. Personal Health Information (PHI), which is maintained and sent via digital systems, is used worldwide. The protection of a patient's healthcare

data from unauthorized access is defined as privacy in health information. This can be accomplished through the implementation of policies. On the other hand, privacy implies that only authorized individuals have access to a patient's health information and that, under certain conditions, patient information may be accessed, used, and reported to a third party. The HIPAA Act, for example, safeguards patients' health information<sup>[96]</sup>.

IoT-based healthcare systems now face numerous security and privacy challenges because they rely on IoT devices that can connect with other devices. The security and privacy of patients' personal health information acquired by IoT devices is a common worry for medical professionals and IoT device vendors. The major concerns are as follows: (1) When an adversary obtains unauthorized access to patient or healthcare provider data; (2) If a virus infects the device; (3) If a device failure occurs, an opponent steals the devices, copies them, and reprograms them with malicious software that compromises the system; and (4) How soon will the healthcare system restore operations after a device malfunction or network attack? Below, we summarize and discuss the major security and privacy challenges in the context of edge-based smart healthcare.

**(1) Device authentication:** It is challenging to update the various medical devices and determine whether an IoT device sends out misleading information from a rogue node due to the vast number of IoT devices and healthcare providers. The lack of authentication mechanisms on IoT healthcare equipment could jeopardize patient privacy if an attacker accesses the data and uses them inappropriately<sup>[97]</sup>. Kotz<sup>[98]</sup> discussed some additional privacy threats that can affect an IoT-based healthcare system.

**(2) Anonymity:** The patient's privacy may be seriously compromised if an intruder manages to steal their identity. As a result, anonymity is one of the security criteria. The identities of the patient and doctor must be verified during the login request phase<sup>[18]</sup>. However, the symmetric encryption method, DES, is applied to encrypt the identities of patients and doctors, posing a challenge in determining their actual identities.

**(3) Data modification:** The transfer of medical data within the healthcare system can be intentionally intercepted by adversaries, either from the IoT device

node or during data exchange across the network. The adversary can insert false information in the data, prompting the healthcare provider to react and administer treatment using false data. This could be fatal for the patient.

**(4) Compromise of hardware and software:** Adversaries can physically steal healthcare IoT devices, extract patient data and security features, reconfigure the stolen device, and relocate it to the network. Furthermore, bugs or viruses may attack the application's operating system, causing the system to malfunction. As a result, the challenge is in detecting the infection and strategies to debug security incidents.

**(5) Security and privacy vulnerabilities:** Many factors contribute to edge computing network security and privacy vulnerabilities and putting patients' personal data at risk, which are as follows:

- Edge nodes receive a lot of sensitive data because they are located closer to users in edge computing. It could have fatal consequences if any parts of the data are stolen.

- Because edge computing has fewer network resources than cloud computing, it cannot use sophisticated encryption methods.

- The dynamic environment that makes up the edge computing network is always evolving. Attackers can so easily ingratiate themselves into the organization. Additionally, it is difficult to create security rules for such a dynamic network.

**(6) Common edge computing attacks:** The following are the common edge computing attacks:

- **Eavesdropping:** The attackers can view patients' medical data through the communication channel between the sensor node and the edge server.

- **Denial of Service (DoS) attacks:** This enables an attacker or hacker to get access to a system or network, and block authorized users from using it by flooding huge requests.

- **Distributed Denial of Service (DDoS) attack:** This attack takes place when an attacker continuously sends many packets toward the victim's device from compromised distributed devices, depleting the victim's hardware resources to handle any other packet and, as a result, failing to timely fulfil any valid request.

- **Data tampering attack:** The attacker has the ability to change data stored or sent through a communication channel.

- **Service manipulation:** It is an attack in which the adversary takes over the edge data center, enabling it to

alter or misrepresent the services.

- **False data injection:** The attacker introduces fake code onto the system that gathers all database data and transfers them to the attacker.

- **Physical attack:** This attack happens when the edge infrastructure's physical security is inadequate or negligent. As the deployment of edge servers is dispersed, physical attacks will have an impact on services in certain geographical areas<sup>[19, 53]</sup>.

- **Rogue gateway:** It is an assault conducted by attackers that causes the same effects as a man-in-the-middle attack by injecting excessive traffic into the entire edge computing network architecture<sup>[99]</sup>.

**(7) Data protection outsourcing:** Healthcare requires a high level of security and privacy from its IT infrastructure<sup>[100]</sup>. In Healthcare Industry 4.0, The medical industry adopts the design principles of Industry 4.0<sup>[101, 102]</sup>, including interoperability, virtualization, decentralization, real-time capability, service orientation, and modularity. Keeping medical data private and secure is the primary issue<sup>[103]</sup>. Preventing physical and digital assaults on hospitals with IT systems with the intention of using patient data unethically is the main objective of maintaining the security and privacy of IT-based hospitals. Smart healthcare systems can enhance traditional healthcare treatments in a flexible and effective manner. Because medical sensors lack computation, storage, and energy capability. Any IoT security architecture should fulfil the three components of the Confidentiality, Integrity, and Availability (CIA) triad. Because of the massive volume of health data accessible and communicated over the Internet, there are various requirements to ensure the security of the system<sup>[18]</sup>. The protection of patient and physician data must be outsourced, similar to the principles of edge computing, which benefits the healthcare sector in many different aspects:

- **Strong infrastructure:** Healthcare facilities can continue operating normally even when there are network issues by processing data on-site using edge devices.

- **Processing with very low latency:** To ensure safer surgeries, throughput and real-time insights are required for tasks like hand-eye coordination or notifications about the location of critical organs during a procedure. Near-instant feedback is provided through data processing at the edge.

- **Increased security:** Patient health data are maintained secure and less susceptible to multiple

threats and data breaches by keeping data on the device and inference at the edge.

- **Savings in bandwidth:** Processing at the edge avoids the need to send high-bandwidth data over the network or to a remote location, such as video feeds.

## 6 Current Solutions for Secure and Private Edge-Based Healthcare

This section offers an in-depth analysis of cutting-edge data security and privacy-preserving techniques in edge-related paradigms with a particular focus on smart healthcare applications. As shown in Fig. 4, a specific taxonomy includes solutions for data privacy-preserving, data integrity, confidentiality, authorization, authentication, access control system, and core infrastructure.

### 6.1 Privacy-preserving data integrity

#### 6.1.1 Data privacy

It is necessary for the treatment profile to be decentralized, secure, and seamlessly integrated while moving the patient from one medical facility to another. In this regard, Rahman et al.<sup>[26]</sup> described a safe therapeutic framework using blockchain-based MEC that allows patients to own and manage their personal information without the involvement of a permitted third party, such as a therapy center. The treatment data will be unchangeable, anonymized, secure, and available to the public. Full implementation of the framework suggests that it can accommodate enough users without significantly increasing the mean processing time.

Further, IoT technologies raise privacy concerns which are significant for healthcare systems that handle sensitive patient data. It is necessary to provide frameworks for secure and intelligent medical monitoring services based on edge computing platforms. Singh and Chatterjee<sup>[100]</sup> presented an edge computing layer and a middle layer for a smart healthcare system based on edge computing, which oversees controlling network latency and protecting patient data privacy. This edge computing layer handles the patient data’s encryption and privacy with the help of the Privacy-Preserving Searchable Encryption (PPSE) method<sup>[104]</sup>. The access control method also prevents unwanted access to remotely stored patient data. Sample patient monitoring data, including body temperature, pulse rate, respiration rate, blood pressure, and oxygen saturation, are gathered by the authors. The proposed model’s implementation, performance, and security analysis show low latency, low transfer time, low power, and low energy when compared to similar techniques. The computed results show that the edge computing strategy reduces the transfer time by 64.24%, the power consumption by 69.03%, and the energy consumption by 69.56%.

With the rapid advances in machine learning capabilities, the users of mobile devices may transmit specific symptoms for medical evaluation at any time and from any location. However, because ML is dependent on vast amounts of medical data, it is essential to keep the data from leaking. Ma et al.<sup>[45]</sup> introduced a lightweight privacy-preserving XGBoost over encrypted model parameters, known as the LPME,

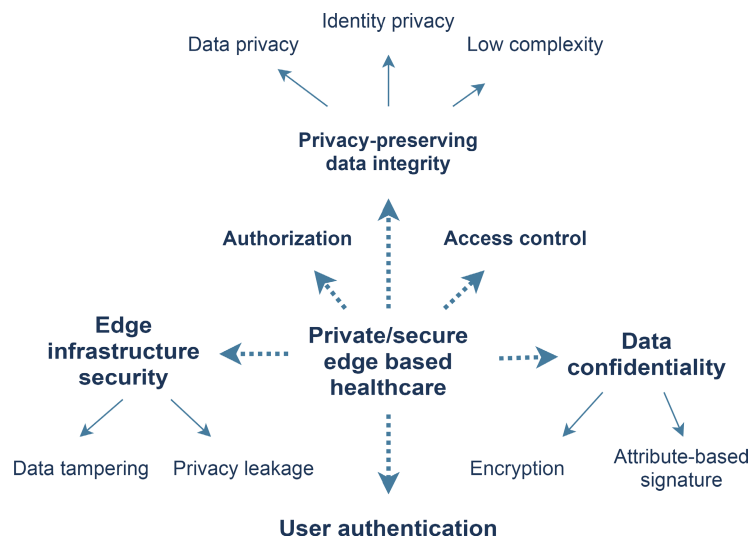


Fig. 4 Generic taxonomy of the discussed solutions.

to drastically lower computational costs when compared to data-sharing-based and privacy-preserving ML. LPME uses the edge model to modify the XGBoost model<sup>[105]</sup>. The authors assessed two public datasets: heart disease and thyroid disease. LPME improves as the K-Tree<sup>[106]</sup> count increases, which results in an accuracy of 97.1% for the thyroid disease dataset and 90.6% for the heart disease dataset.

In a different COVID-19 pandemic-related experience, Vadrevu et al.<sup>[46]</sup> used several applications to protect patient data by broadcasting the information to the public without executing any personal privacy preservation techniques and without violating the privacy of the affected person. However, attackers can take advantage of this public data and provide them to any insurance agency. When an entity in charge uses patient data for any authorized research or analysis, data privacy must be highly maintained. As a case, after completing a COVID-19 test, the government receives information about the infected or non-infected individual. If a person is infected with a virus, such details are shielded using approaches, such as K-anonymity<sup>[107]</sup>, 1-diversity<sup>[108]</sup>, or differential privacy<sup>[109]</sup>. The experiment is carried out using the adult dataset and a sample dataset produced and derived from news articles and published during the pandemic period. If the entire process is automated utilizing robotic and IoT technology, the outputs would be efficient and accurate.

### 6.1.2 Identity privacy

The Internet of Medical Things (IoMT), which leverages IoT in the healthcare business, is the next frontier in the digital revolution<sup>[110]</sup>. This vast volume of medical data created by IoMT is maintained in a centralized storage system. However, centralizing sensitive patient data introduces a single point of failure, along with concerns regarding privacy and security. Kumar and Tripathi<sup>[27]</sup> proposed an IoMT-based solution that employs blockchain and IPFS technology<sup>[111]</sup>. The IoMT network's security mechanism is broken down into two parts: initialization and authentication. To maintain anonymity in the IoMT network, patients and their device data are submitted as a transaction to the blockchain network following registration and authentication. Furthermore, unlike other cloud-based systems, the framework offers authorized agents (peers) equitable service without depending on a third party. The technique is designed and implemented using distributed off-chain storage,

both safe and anonymous. Additionally, it is designed and developed using distributed off-chain storage, which is extremely secure and upholds anonymity. The suggested architecture employs an IPFS cluster, which increases the scalability of IoMT healthcare systems while also facilitating safe access to patient data.

Bosri et al.<sup>[49]</sup> designed the HIDEchain user-centric edge computing architecture, which guarantees secure edge computing for healthcare to retain user data transaction records. A user might monitor how the architecture uses his/her data by saved hashes. Blockchain maintains data transactions, which ensures data integrity, and the user data remain anonymous in the edge node. HIDEchain allows only registered IoT devices to communicate data, thereby preserving device authorization and authentication.

Saha et al.<sup>[29]</sup> developed an e-healthcare framework to deal with Electronic Medical Records (EMRs)<sup>[112]</sup> that addresses privacy concerns within the e-healthcare network. In addition to recording the response time and latency, the authors showed that the algorithm effectively provides privacy while maintaining conventional network settings. The transaction time is statistically 13.84% less than similar algorithms, possessing the required features for any cloud-based healthcare system. IoT intelligent technologies are also employed to secure patients' identification and privacy. For Intelligent Telehealth Systems (ITS) in a multi-server edge computing environment, Wang et al.<sup>[30]</sup> developed an efficient and expandable blockchain-assisted handover approach. It can enable efficient authentication, tight anonymity, and computing load transfer. Furthermore, the authenticated edge server is used to help with handover authentication, thus reducing communication and computing overheads on the user side.

Hossain et al.<sup>[113]</sup> suggested a B5G framework to detect COVID-19 using chest X-ray or Computational Time (CT) scan images by utilizing the low-latency and high-bandwidth capabilities of the 5G network. The framework includes a mass surveillance system that can recognize body temperature, social distance, and mask use. Recent advances in cutting-edge computing analyze hospital test results and crucial human signals at the edge. The proposed COVID-19 diagnostic technique might be used to diagnose any infectious illness. As a result, it will aid in decreasing hospital overcrowding, authenticating patients who do not have COVID-19, and handling sensitive personal

data at the edge to maintain anonymity. Three deep learning models are used to investigate blockchain technology: ResNet50<sup>[114]</sup>, deep tree, and inception v3<sup>[115]</sup>.

### 6.1.3 Low complexity

While maintaining great precision, a low level of complexity can be used for deployment at the edge zone. According to Huong et al.<sup>[116]</sup>, low-complexity cyberattack detection in IoT edge computing (namely LockEdge) is a multi-attack detection technique with low complexity for deployment at the edge zone while maintaining good accuracy. LockEdge is implemented and evaluated in centralized and federated environments. Lin et al.<sup>[85]</sup> proposed a strategy for managing fat clients in an edge computing environment to provide tailored healthcare services. The proposed solution includes a fat-client profile for each fat-client user to operate, such as data source sequences and analysis algorithms. The fat-client manager of the cloud layer controls the fat-client model through the fat-client profile. Each fat-client that belongs to the user is managed by the edge layer's fat-client instance manager. The cloud layer oversees building and managing the fat-client model, which necessitates many computational resources. The fat-client is kept at the edge layer for on-site data processing and includes a number of user interactions. Table 3 summarizes the solutions proposed for preserving data privacy, identity privacy, and low complexity.

## 6.2 Authorization

The system decides whether the user has sufficient credentials to access the requested resources; in this regard, Egala et al.<sup>[39]</sup> presented an SHPI, in which

essential data are handled in edge computing placed within the hospital to decrease connection latency. Blockchain technology and cryptographic techniques are used by SHPI to ensure the confidentiality of patient data and tamper-proof medical records. A data access token system is also created to segregate the group of users depending on their jobs. Logical analysis is performed to define the operating principles, demonstrating that the system can deliver the needed security and privacy. Mistry<sup>[118]</sup> also proposed a system that provides a cost-effective, secure, private, and adaptable solution. The proposed approach uses rule-based beacons for seamless data management, machine-to-machine transmission, and a variety of data processing algorithms to support smart healthcare applications.

## 6.3 Access control

The procedure of gaining access to resources is limited to a small number of users. Nguyen et al.<sup>[119]</sup> suggested a new decentralized healthcare architecture based on blockchain and MEC for spreading EMR sharing among federated hospital services. The focus of the research is on a fully decentralized access control system based on smart contracts, which enables EMR access verification at the network edge without the need for central authority. A decentralized IPFS platform also connects to smart contracts on the MEC network, reducing the time it takes to get data and enhancing security for EMR sharing. The authors conducted several real-world tests to validate the efficacy of the EMR sharing strategy. By reducing data retrieval latency, enhancing blockchain performance, and providing security assurances, the implementation

**Table 3 Summary of approaches on preserving data privacy, identity privacy, and low complexity.**

Reference	Feature	Approach	Aim	Result
[100]	Data privacy	Searchable encryption	Prohibit illegal access	Low time and energy
[26]	Data privacy	Blockchain-based MEC	Patients control personal data	Users scalability
[45]	Data privacy	Lightweight privacy preserving LPME	Reduce computational cost	High accuracy
[46]	Data privacy	K-anonymity, l-diversity, differential privacy	Protected Covid-19 patient details	High accuracy
[27]	Identity privacy	Blockchain and IPFS	Handle security and storage	Scalability increased
[49]	Identity privacy	HIDEchain	Data integrity	Authenticated device
[29]	Identity privacy	E-healthcare framework	Addresses privacy	Low transaction time
[30]	Identity privacy	Blockchain-assisted handover AKA scheme	Verification and strict anonymity	Low communications cost
[113]	Identity privacy	B5G framework	Low latency and high bandwidth	Patients verified
[116]	Low complexity	LockEdge	Low complexity	Maintaining high accuracy
[117]	Low complexity	Fat-client profile	Local data processing	Efficient management



results demonstrate a significant improvement in Quality of Services (QoS) compared to the baselines.

Similarly, Hewa et al.<sup>[32]</sup> created an MEC and blockchain-based secure service architecture for future study that makes use of lightweight Elliptic Curve Qu Vanstone (ECQV) certificate mechanisms<sup>[120]</sup>. The authors handled access control to patients' data using smart contracts. The authors conducted a near-realistic performance assessment, demonstrating that the system can manage large transaction volumes via MEC nodes with little latency. They also optimized blockchain storage by outsourcing it to expandable IPFS storage.

Guo et al.<sup>[121]</sup> introduced a hybrid architecture that controls access to EHR data using edge nodes and blockchain. The identity and access control rules are managed by a blockchain-based controller, which also serves as a tamper-proof log of access events inside the architecture. Additionally, off-chain edge nodes store EHR data and implement attribute-based access control on EHR data in conjunction with Access Control Logs (ACL) based on blockchain technology. The proposed hybrid architecture is evaluated using a hyperledger composer fabric blockchain to determine how well smart contracts and ACL rules executed in terms of transaction processing speed and response time to unauthorized data retrieval. Azaria et al.<sup>[35]</sup> suggested MedRec, a decentralized record management system that uses blockchain technology to manage EMRs. The proposed approach gives patients easy access to their medical records across doctors and treatment locations, and provides a full and immutable track of their medical information. By utilizing special blockchain features, MedRec offers identification, confidentiality, accountability, and data sharing—all of which are crucial issues when working with sensitive information.

Christo et al.<sup>[36]</sup> implemented ECC, a simple authentication method for data exchange. The authors went over two critical data security issues: data authentication and confidentiality. To ensure data validity, they used a method to encrypt and decrypt the data with a 512-bit key. The blockchain ledger system ensures data secrecy by allowing only ethical people to access the data. The experimental findings show that the time required to create the key, encrypt, and decrypt is reduced compared to other current techniques. To effectively analyze data and store it on cloud servers, the suggested infrastructure also includes edge servers on the ground. It ensures data security,

data secrecy, and authenticity by processing and storing the data in the blockchain ledger. Table 4 lists the main characteristics of the access control approaches proposed in this context.

## 6.4 Data confidentiality

### 6.4.1 Encryption

By using specific mathematical techniques and a password or “key” meant to decode the data, encryption tries to protect digital data. Data are converted during the encryption process using an algorithm that makes the original data unreadable. Among the works that use this technique is presented by Alabdullatif et al.<sup>[48]</sup>, in which they developed a safe Edge-of-Things (EoT) framework for smart healthcare monitoring. The system is capable of collecting, observing, and analyzing biosignal data in real time. EoT is a computing paradigm representing an intermediate processing layer between IoT devices and cloud computing. The EoT framework enables early illness identification and treatment, possibly lowering disease-related damage and extending many lives. FHE<sup>[122]</sup> is used in EoT databases stored in the cloud to provide end-to-end data privacy. The authors devised a distributed strategy for applying clustering-based approaches in the context of the EoT paradigm. This method is involved in clustering-based techniques, such as K-KMC clustering and FCM clustering. The authors of Ref. [48] assessed the proposed secure EoT smart healthcare monitoring system using the Google Cloud Platform (GCP), they used a real heart disease dataset from the University of California Irvine's (UCI)

**Table 4 Summary of the recent works handling access control.**

Reference	Aim	Result
[119]	IPFS platform integrated with MEC network	Reduced data retrieval latency, enhanced blockchain performance
[32]	MEC and blockchain-based secure service architecture	Handle transaction volumes with optimized blockchain storage
[120]	Hybrid architecture with blockchain and edge nodes	Store EHR data with access control
[121]	MedRec	Identification, secrecy, accountability, and data sharing
[35]	Elliptic-curve cryptography	Provides data security, data secrecy, and authenticity

machine learning repository<sup>[123]</sup>, together with synthetic datasets that vary in size and distribution to adequately demonstrate the proposed methodology. The collection includes data from 303 patients and 75 characteristics. According to the dataset size, the accuracy increase from 0.29% to 8.90%. When the number of Virtual Machines (VMs) is changed from 1, 2, and 4, the performance measurement shows considerable improvements to the execution time ranging from 49.38% to 76.06% for 8000 data points.

Al Omar et al.<sup>[40]</sup> proposed an alternative for the healthcare system that would guarantee patient privacy and transparency regarding insurance policies. These policies are maintained on the blockchain to make the user's insurance policy transparent. Users can also safely keep personal information on the blockchain and healthcare data, such as test results, prescriptions, and diagnostic reports, in the cloud. The patient's data are kept private by utilizing cryptographic technologies, such as the ECC<sup>[124]</sup> encryption algorithm.

Jan et al.<sup>[125]</sup> introduced SmartEdge, an end-to-end encryption architecture that handles computationally challenging activities at the network edge and cloud data centers, and is used for smart city applications. To provide a secure connection between smart core devices for multimedia streaming to registered and validated edge devices, the authors developed a lightweight symmetric encryption technique. The multimedia streams are encrypted, encoded, and broadcast to the cloud data centers when the edge devices receive the data. Prior to broadcasting, each edge device creates a secure connection with a data center by combining symmetric and asymmetric encryption methods. In SmartEdge, the use of somewhat complex encryption techniques at the network edge and cloud data centers is compensated by the execution of a lightweight encryption approach at resource-constrained smart devices. The suggested system reduces end-to-end encryption delay, response time, security overhead, and computational and communication costs for participating entities. Furthermore, the suggested system is very resistant to a variety of adversarial techniques.

Jan et al.<sup>[41]</sup> also provided a lightweight mutual authentication solution for protecting the privacy of wearable devices and their data in I-CPS. The technique is built on a client-server interaction architecture and offers safe sessions among entities by using symmetric encryption. Following mutual

authentication, an artificial intelligence enabled HMM is employed to anticipate the privacy risk linked to patient data<sup>[126]</sup>. Furthermore, the authors evaluated the scheme's resilience and security using Burrows AbadiNeedham (BAN) logic. This study shows that the suggested method is secure, quick, and robust due to the use of lightweight security primitives for session key exchange. Finally, the proposed method reduces the processing, communication, and storage overhead.

Islam and Shin<sup>[42]</sup> presented a blockchain-based secure outside health monitoring method that employs an Unmanned Aerial Vehicle (UAV) to gather health information from wearables worn by consumers. A user encrypts health data before sending them using a public key of the UAV. After capturing health data, the UAV decrypts and transmits them via UAV to the nearest MEC server. The health data are then encrypted and sent to the nearest MEC server via MEC. MEC decodes and analyses health data to discover health problems in the user. If MEC servers detect any issues with health data, they contact the user and any local hospitals in case of an emergency. The MEC server saves the health data on the blockchain after the diagnostic is complete. The simulation results show that the validation process requires a longer duration and incurs higher energy costs as the number of users increases. Furthermore, when the number of users rises, UAV energy consumption increases, providing security against cyber-attacks.

#### **6.4.2 Attribute-based signature**

Patients must reclaim control over their medical data and prioritize their treatment. Guo et al.<sup>[43]</sup> proposed an approach called ABS with multiple authorities to guarantee the validity of EHRs stored on blockchains. Multiple authorities are incorporated into the ABS and suggest an MA-ABS scheme that ensures the information is immutable and anonymous to protect patient privacy in the blockchain-based EHR system while also meeting the requirements of the blockchain framework.

Guo et al.<sup>[38]</sup> proposed a hybrid blockchain and edge node paradigm that enables multi-authority ABE to encrypt EHR data stored on the edge node and ABMS<sup>[127]</sup> to validate user signatures without disclosing sensitive information. The hyperledger fabric platform is used to construct the blockchain module, while the Hyperledger Ursa Library is used to develop the ABMS module. The authors of Ref. [38] measured the signing and verifying time for the ABMS

module at various attribute lengths. They found that both the signing and verification time metrics are independent of attribute length, with values of time remaining between 32 and 243 ms for each attribute. The overall running time increases in a linear fashion as the number of features increases.

Another secure blockchain-assisted approach for medical IoT devices, based on the LMDS, was proposed by Alzubi<sup>[44]</sup>. The LMDSG approach initially authenticates IoT devices by producing a tree in which the leaves reflect the hash function of sensitive patient medical data. A CHC also employs LMDSV to determine the data source. If the hash of the public key equals the leaf in the verification process, it is considered the tree's root, hence the signature is genuine. As a result, the proposed LMDS technique efficiently identifies harmful user activity while using lower computational overhead which is favorable in medical IoT systems. Table 5 highlights the main attributes of the data confidentiality works presented for healthcare systems.

## 6.5 Edge infrastructure security

### 6.5.1 Privacy leakage

Many research works have used the benefits of blockchain and IPFS technologies to maintain privacy. The IPFS aids the blockchain in resolving the storage restriction issue. IPFS stores decentralized and immutable data. BEdgeHealth, a decentralized health infrastructure that combines MEC and blockchain, was proposed by Nguyen et al.<sup>[128]</sup> for data offloading and sharing in dispersed hospital networks. To enhance the QoS, the authors used a decentralized authentication method with distributed IPFS storage<sup>[129]</sup>.

Baskar et al.<sup>[130]</sup> presented a battery charge

management cell-based energy monitoring approach. It corrects event categorization for an edge computing mobile heart monitor with Wireless Body Area Network (WBAN) engineering using the Digital Signal Processor (DSP) frame compact approach. WBAN detects every element of an Electrocardiogram (ECG) pulse and classifies it as normal or abnormal based on Heart Rate Variability (HRV), the key sign of an arrhythmia. In contrast to previous QRS sensors, the tracker may be adjusted to handle backdrop circling objects while keeping precision with minimal equipment. Wherever peak detection adaptive synthesis is used, the method effectively enhances the slopes of the ideal QRS complex. The ECG detector's application reveals that its proposed system absorbs 0.3 mw of power at the hardware level. Over a large capacity design, transmitting only structured parts in standby mode may preserve approximately 98% of the transmission system. The highest activity level shows that the invention is adequate for the real-time task. The energy is mainly used optimally during both propagation modes.

Yang et al.<sup>[131]</sup> provided another decentralized approach for sharing and controlling private health data. The solution allows for data exchange between Edge Data Hubs (EDHs) and medical institutions while maintaining data privacy and reducing storage space requirements. A Secure Computing Platform (SCP) is utilized to run the executable code given by the service in the EDH without exposing private data to ensure data privacy. Data hash values are recorded on the blockchain to ensure that the data accessed is tamper-proof. The authors employed an off-chain storage technique that uses data sparsity to save storage space. Because the blockchain ledger is tamper-proof, it

**Table 5 Summary of the works dedicated for data confidentiality.**

Reference	Scope	Aim	Approach	Feature
[48]	Encryption	End-to-end data privacy	Fully homomorphic encryption	Improve accuracy and run time
[40]	Encryption	Patient privacy with insurance policies	ECC	Private patients' data
[84]	Encryption	Secure link between smart core devices	SmartEdge	Minimize response time, communication overhead, and end-to-end encryption delay
[125]	Encryption	Protect privacy of data and wearable devices in I-CPS	Lightweight mutual authentication	Low processing, communication, and storage overhead
[42]	Encryption	Secure outdoor health monitoring	Blockchain-based secure outdoor health monitoring	Protect against cyber threats
[43]	ABS	Protect patient privacy	Blockchain-based EHRs	-
[38]	ABS	Validate user signatures without disclosing sensitive information	ABMS	Assure anonymity and immutability
[44]	ABS	Identifies harmful user activity	LMDS	Linear growth with features

maintains an auditable record of medical data access. Furthermore, when the data analysis request is approved, the system can avoid data leaking via SCP and decrease off-chain storage while retaining as much medical data information as feasible. The method can reduce storage costs, making enormous volumes of medical data collection viable. Taking one of the essential characteristics of decentralization, it does not rely on a centralized body but on many participating entities that can avoid a single point of failure.

### 6.5.2 Data tampering

Malicious acts on the patient's records inflict serious damage to the reputations of all parties associated directly or indirectly with the data, thus imposing different hazards to patients' privacy. ElRahman and Alluhaidan<sup>[31]</sup> provided an approach to include a blockchain within an IoT-based edge computing architecture. They specifically targeted the healthcare sector, providing complete patient data protection, secure transmission of examination results, and private and unaltered data transfers. By obtaining and storing data from the source studies, the system can ascertain how quick the edge layer is.

Tripathi et al.<sup>[28]</sup> investigated the various facets of technologically enabled healthcare and suggested a secure and privacy-preserving SMS architecture for the ecosystem of smart cities. This study employs the notion of protected MEC for executing essential time-bound calculations on edge itself to provide real-time analysis and replies. The blockchain concept is used to protect patients' personal and medical data and make it tamper-proof. This technology is designed to detect changes in patients' conditions and provide notifications to physicians and caregivers. Furthermore, information may be used to generate analytics and prediction models with deep learning algorithms that can forecast the patient's future condition based on changes in the patient's vitals.

MeDShare was introduced by Xia et al.<sup>[132]</sup> as a solution to the issue of medical data interchange across big data custodians in a risky setting. The blockchain-based technology makes it possible to control, audit, and establish the provenance of shared medical data amongst huge data institutions. MeDShare checks organizations that access data from a data custodian system for unauthorized usage. It also keeps a tamper-proof record of all data transfers and sharing between entities, as well as any additional activities carried out on the system. When data permissions are violated, MeDShare employs smart contracts and an access control mechanism to effectively trace data activities and revoke access to offending entities. Table 6 lists the main characteristics of the core infrastructure methods discussed above.

### 6.6 User authentication

User authentication entails comparing the credentials given with those in the database. Abou-Nassar et al.<sup>[33]</sup> proposed a blockchain DIT framework for IoT zones. A smart contract ensures budget authentication while the ITIS addresses semantic gaps and improves TF estimates. Semantic annotations for IoHT health edge layers are provided by the robust ecosystem known as the DIT blockchain healthcare-based IoT platform. Cryptographic techniques are employed at various phases of inclusion, exchange, and so on, to authenticate, validate, and preserve data. Scalability, interoperability, availability, mutual authentication, trustworthiness, data integrity, authentication mechanism, secrecy, and privacy are all advantages of the proposed model.

A secure framework for SDN-based edge computing in an IoT-enabled healthcare system was suggested by Li et al.<sup>[34]</sup>. To authenticate IoT devices, it collects data from patients and sends them to edge servers. The edge servers are linked to an SDN controller, which watches

**Table 6 Summary of the core infrastructure approaches.**

Reference	Scope	Aim	Approach	Result
[128]	Privacy leakage	Increase QoS	BEdgeHeal	QoS enhanced
[130]	Privacy leakage	Correct event categorization	Energy monitoring	Power absorbed
[131]	Privacy leakage	Avoid data leakage	Controlling private health data	Storage cost reduced
[31]	Data tampering	Ensure edge data integrity	Blockchain IoT	Data integrity and confidentiality
[28]	Data tampering	Secure patients' information as tamper-proof	SMS	Identify changes in a patient's status
[132]	Data tampering	Avoid tamper of shared data	MeDShare	Track of data activity and revoke access to offending entities

over the healthcare system's load balancing, network optimization, and resource use. Li et al.<sup>[37]</sup> introduced EdgeCare, a safe edge computing technology for mobile healthcare systems, in which data management is decentralized and collaborative. EdgeCare relies on specialized Local Authorities (LA) to function as trustworthy authorities in scheduling edge servers to process healthcare data securely and promote viable data trade. The EMR management scheme and protocol processes have been carefully designed to facilitate healthcare information administration while adhering to security and privacy standards. In addition, the developers of EdgeCare investigate the optimization problem of decentralized data trading.

To meet the contemporary demands of wireless multimedia health sensor networks, Deebak et al.<sup>[133]</sup> suggested a seamless, secure, anonymous authentication approach that enables seamless connectivity/single sign-in by utilizing ECC, a one-way hash function, and a less expensive transaction. Ali et al.<sup>[134]</sup> designed a heterogeneous biometric authentication system that encrypts biometric user templates. The suggested method can be used effectively in the centralized cloud environment owing to the secured templates without being concerned about information escaping in the event of a data breach. It additionally capitalizes on most computer resources by using personal portable devices as edges, easing the load on the cloud. As a result, the person's identity cannot be revealed until decoded with the appropriate secret key. Table 7 lists the main characteristics of the user authentication methods.

## 7 Challenge and Research Direction

Many research issues that act as a deterrent must be addressed to acquire high-level privacy and security in the future with the help of healthcare systems based on edge computing. There are plenty of promising techniques to train EC-based models with sufficient

and diverse datasets without sacrificing data privacy. Although there are numerous examples of successful uses of edge computing technologies, more research is needed before EC-based architectures can be widely adopted for use in smart healthcare applications. We will now go over some of the most important issues in further detail.

### 7.1 Federated learning

Obstacles specific to healthcare data can be imposed which differentiate them from those encountered with other information. Data heterogeneity is one of the main functional challenges that need to be addressed due to its influence on data privacy. Therefore, effective implementation of Federated Learning (FL)<sup>[135, 136]</sup> solutions for healthcare and medical data can significantly reduce privacy concerns<sup>[137]</sup>. While preserving the confidentiality of each client's data, FL enables decentralized training of ML or DL models across several clients. The utilization of federated networks in healthcare entities, e.g., hospitals, is instrumental because medical data have its own distinct characteristics. Multiple healthcare data owners can participate in the whole training process of algorithms or models that are controlled by a central server. Data owners use their local data to train an ML network or algorithm, then share the updated observations with the main server. The server acts as a training manager that gathers all the sub-results and aggregates them into a unified global model. Following the successful training, the final global model is shared with the data owners. This approach permits the use of private data from several clients while retaining sensitive and confidential information stored locally.

FL approaches can be generally categorized based on the mechanism and amount of data exchanged between the clients and the central server. Common FL techniques include Federated Averaging (FedAvg)<sup>[136]</sup> to minimize parameters change among data owners,

**Table 7 Summary of user authentication approaches.**

Reference	Aim	Approach	Result
[33]	Ensure budget authentication	Blockchain DIT	Mutual authentication
[34]	Authenticate IoT devices	SDN-based edge computing	Load balancing, network resources optimization
[37]	Decentralized and collaborative data management	EdgeCare	Secure and efficient data management
[133]	Authenticate wireless medical sensor networks	ECC	Seamless, safe, and anonymous authentication
[134]	Avoid unwanted access	Heterogeneous biometric authentication	Protect identity of patient

Single Weight Transfer (SWT)<sup>[138]</sup> which trains deep models at one client for a specific time period and then passed to the next client, Cyclic Weight Transfer (CWT)<sup>[126]</sup> which trains deep models at each client for a particular time, and then transfers the next client with possible multiple visits to each client, and split learning<sup>[139]</sup> which involves transferring middle layer outputs of a deep neural network that excites various processes, introducing distortions to the input. However, machine learning architectures still enclose some confidential data in the parameters they exchange. On a federated network, the encryption of patients' confidential data would be more feasible to keep only the local training model from clients or data owners<sup>[140]</sup>. This protects the learning models from any possible distortion by malicious parties. Therefore, there is a demand to secure such learning models and to guarantee that adversaries are unable to breach data and models, and cannot employ them in the real world<sup>[141, 142]</sup>.

FL is also effective in securing data over mobile or wearable devices. For instance, Guo et al.<sup>[47]</sup> presented a federated edge learning solution for mobile devices that trains medical machine learning models by effectively and reliably processing distributed private data in parallel. They attempted to address the challenge in mobile medical networks that rely on artificial neural networks. The mobile device offloads essential training and monitoring tasks to the hospital's private server to increase efficiency. The data are then maintained at users' devices, while scattered hospitals combine their models to develop the global model to increase diagnostic quality. To defend against both external and internal security threats, a two-stage differential privacy approach is also used in the interaction. Chen et al.<sup>[143]</sup> also proposed a federated healthcare framework called FedHealth, which is based on a transfer learning mechanism for deep models that have little in common with samples or features. It is designed specifically for wearable healthcare applications.

## 7.2 Data snooping

Data snooping is a commonly used umbrella term that encompasses various forms of inappropriate access to records. It can range from an employee accessing the records of their family or friends to excessive printing of information, to viewing the patient log of another unit. Snooping may be either intentional or accidental,

and it can occur due to curiosity, boredom, or a desire to stay informed. In edge computing applications, authentication mechanisms and trust ratings are commonly employed to reduce the chance of infiltration. Globally, stealing patient information is illegal and the security of health information is regulated; any breach of health data may result in a lawsuit. To overcome this issue, health information at the network's edge must be encrypted before being transmitted to other nodes, commonly done on mobile devices.

Transferring a patient from one medical facility to another necessitates decentralized, safe, and seamless interaction and integration with the treatment profile. For instance, Rahman et al.<sup>[26]</sup> described a secure therapeutic framework based on blockchain-based MEC that permits patients to own and manage their private data without the participation of a third party, e.g., a therapy facility. The treatment data are unchangeable, anonymized, secure, and accessible to the public. The full implementation of the framework indicates that it can support enough users without significantly increasing the mean processing time.

Singh and Chatterjee<sup>[100]</sup> also proposed a smart healthcare system for edge computing environments. The edge computing layer, which controls network latency and protects patient data privacy, is included in this design. Using the PPSE approach, this layer handles the encryption and privacy of patient data. The access control method also prevents unauthorized access to patient data stored remotely. In another situation relating to the COVID-19 pandemic, Vadrevu et al.<sup>[46]</sup> employed multiple applications to maintain the confidentiality of patient information by disseminating the data to the public without adopting any personal privacy preservation techniques, where also the infected individual's privacy is compromised. Attackers can use this public data to provide them to any insurance company. They may approach the patients to issue an insurance policy due to the high risk of death involved. Therefore, authorities must keep patient data secure, especially when it is used for research or analysis purposes.

## 7.3 Infrastructure and deployment

Due to the limited resources of smart devices, most resource-intensive tasks are carried out at smart edges and cloud data centers. To tackle this problem, new developments should be able to determine what data to

encrypt and identify the various sorts of data exchanged (e.g., credit card numbers and customer information) according to sensitivity, usage, and regulatory implications. They should establish only the resources needed for data encryption.

As edge nodes typically have limited resources and lack sufficient intelligence to detect attacks, decentralized edge environment, especially user devices connected to edge nodes, pose a greater vulnerability to assaults compared to centralized systems, where additional privacy concerns arise as they involve the transmission of sensitive data over the network<sup>[144]</sup>. Additionally, existing data security protection mechanisms are not generally applicable to edge computing designs for resource-constrained edge devices, because network edge devices have limited resources. Most countries and cities also have only a limited number of 5G communication networks in place<sup>[145]</sup>. Edge computing often performs well in contexts that can generate massive amounts of data. For instance, when Hossain et al.<sup>[113]</sup> used the B5G framework, the training process requires a sufficient and diverse COVID-19 dataset. To address this issue, more efforts should be put into the use of effective methods for resource allocation. However, raising resource usage to minimize energy consumption may result in an increased failure, latency, and inability to communicate with edge networks. Consequently, optimization factors should be favored according to workload and QoS requirements. For example, Yang et al.<sup>[131]</sup> used data sparsity to decrease off-chain storage costs.

Additionally, the security requirements of extremely diverse edge networks may vary according to the applications and devices deployed<sup>[144]</sup>. While some low-capability devices only need primitive security and delay-sensitive networks, like vehicle networks, and demand highly effective security measures to handle their delay-sensitive applications. One of the attempts to tackle this challenge is the design and implementation of Domain Based Security (DBSy)<sup>[146]</sup>. The DBSy approach represents an organization's security requirements from two different but connected views using basic models: The infosec infrastructure model represents the logical provision of strong boundaries that enforce separation, while the infosec business model represents the security aspects of the business. When combined, they create an infoSec architectural model. This method lays the groundwork

for conducting a complete risk assessment.

#### 7.4 Communication encryption

Sensitive healthcare data are vulnerable to internal and external threats, as well as probable leakage during the exchange between multiple parties, especially under the EoT paradigm. Furthermore, healthcare ML or DL algorithms and models could be accessed by adversaries over non-encrypted networks which enables them to decrypt training models and expose patients' information accurately<sup>[147, 148]</sup>. FHE<sup>[48]</sup>, which may offer full confidentiality for members' data, can handle data privacy. In contrast to previous approaches, FHE protects stored data and performs analytical tasks in an encrypted environment. The volume of data transported from the data source to the cloud may, however, increase dramatically<sup>[149, 150]</sup>. Additionally, the user will not be able to access the encrypted file if the password or key is lost. On the other hand, when data are encrypted using simpler keys, the data are no longer secure, and anyone can access it at any time.

A breach of data integrity also occurs when unintended changes to data occur because of storage, retrieval, or processing operations, including malicious intent, unexpected hardware failure, or mistakes made by humans. If such modifications are the result of unauthorized access, that may also be a sign that data security has been compromised. Data security is at risk if keys fall into the wrong hands. Users must keep track of all your encryption keys, as well as who has access to them, and how and when they have been used. Therefore, it is important to use key management systems which help in storing and managing encryption keys.

Alabdulatif et al.<sup>[48]</sup> presented a distributed strategy adopting clustering-based approaches in the EoT paradigm. The edge layer in this method, which receives data from dispersed IoT devices, may run distinct analytical services. This method is also used in clustering-based approaches, such as KMC and FCM. It may, however, be expanded to numerous machine learning approaches. The system relies on many entities working together to carry out certain analytical tasks, starting with data collection and storage tasks and concluding with analysis responsibilities, while adhering to privacy. The architecture is divided into four major components, which are as follows: (1) Community Members (CM) included within the smart community, which comprises healthy people, geriatric

patients, and hospital patients. The collection of biosignal data from CMs using wired or wireless sensors is followed by its encryption and delivery to cloud-based storage; (2) Smart IoT gateway that performs local analysis within each smart community. Data collected from CMs is examined for local diagnostic feedback within each community. The encrypted data are then sent by each smart gateway to cloud storage for additional processing; (3) Cloud-enabled Database (CD) which is an encrypted cloud-based storage for CM's health data from all smart communities; and (4) the system's analytical engine, called Abnormality Detection Model (ADM), analyses aggregated encrypted data from several smart communities in an encrypted form. In order to gather, store, and analyze biosignal data for anomaly detection, the entities work together. Following the transfer of encrypted data to the CD entity, the ADM safely and autonomously performs encrypted analytical operations on encrypted data. The CD entity can provide encrypted feedback results to the CM, which the CM can decode securely.

Al Omar et al.<sup>[40]</sup> also suggested a blockchain-based smart city solution that protects patient information data, the diagnostic report of the patient, and the prescription of the patient in the cloud for later access while maintaining user IP privacy. There are seven entities included in this platform: users, insurance company, Election Commission (EC) databases, system applications, Health Organization (HO), blockchain, and cloud. The system application communicates with patients, EC database, doctors, health insurance companies, cloud, and blockchain. To register and join the system, a new user must provide the necessary information. Verification Unit (VU) validates the submitted information from the insurance company and the EC repository before authenticating the user. HO registration will be also validated by the governmental healthcare database. This procedure guarantees that only verified HOs are permitted access to the site.

## 8 Conclusion

This study highlights and discusses the importance of maintaining privacy and security in healthcare systems based on edge computing solutions, where patient data protection is critical. An overview of edge computing architecture is provided, including definitions, applications, and architecture. The needs for privacy

and security in healthcare systems are articulated using six fundamental metrics: user privacy, data confidentiality, integrity, availability, access control, and authentication. We do believe that this systematic review is beneficial for those who are interested in marinating data privacy in the healthcare industry that relies on edge computing technologies, as they will be able to rely on many challenges and issues, discussed in this manuscript, to make fresh scientific contributions. As part of future endeavors, the scope of this review study can be broadened to encompass additional specific domains that pertain to emerging technologies. These areas may include addressing confidentiality concerns in federated learning paradigms and implementing cryptography within the context of smart healthcare systems. A potential avenue for further analytical investigation involves exploring the integration of edge and fog computing, laying the groundwork for a new dimension in handling more complex healthcare algorithms.

## References

- [1] A. Singh and K. Chatterjee, Security and privacy issues of electronic healthcare system: A survey, *J. Inform. Optim. Sci.*, vol. 40, no. 8, pp. 1709–1729, 2019.
- [2] R. Wang, J. Lai, Z. Zhang, X. Li, P. Vijayakumar, and M. Karuppiah, Privacy-preserving federated learning for internet of medical things under edge computing, *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 854–865, 2023.
- [3] N. Fernando, S. W. Loke, and W. Rahayu, Mobile cloud computing: A survey, *Future Gener. Comput. Syst.*, vol. 29, no. 1, pp. 84–106, 2013.
- [4] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, Fog computing and its role in the internet of things, in *Proc. first Edition of the MCC Workshop on Mobile Cloud Computing*, Helsinki, Finland, 2012, pp. 13–16.
- [5] K. Gai, M. Qiu, H. Zhao, L. Tao, and Z. Zong, Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing, *J. Netw. Comput. Appl.*, vol. 59, pp. 46–54, 2016.
- [6] Y. Hao and R. Foster, Wireless body sensor networks for health-monitoring applications, *Physiol. Meas.*, vol. 29, no. 11, pp. R27–R56, 2008.
- [7] K. Cao, Y. Liu, G. Meng, and Q. Sun, An overview on edge computing research, *IEEE Access*, vol. 8, pp. 85714–85728, 2020.
- [8] A. Lakhan, M. A. Mohammed, A. N. Rashid, S. Kadry, K. H. Abdulkareem, J. Nedoma, R. Martinek, and I. Razzak, Restricted boltzmann machine assisted secure serverless edge system for internet of medical things, *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 673–683, 2023.
- [9] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W.



- Zhao, A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications, *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, 2017.
- [10] A. Mosenia and N. K. Jha, A comprehensive study of security of internet-of-things, *IEEE Trans. Emerg. Top. Comput.*, vol. 5, no. 4, pp. 586–602, 2017.
- [11] X. Zhou, W. Liang, W. Li, K. Yan, S. Shimizu, and K. I. K. Wang, Hierarchical adversarial attacks against graph-neural-network-based IoT network intrusion detection system, *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9310–9319, 2022.
- [12] A. Algarni, A survey and classification of security and privacy research in smart healthcare systems, *IEEE Access*, vol. 7, pp. 101879–101894, 2019.
- [13] J. J. Hathaliya and S. Tanwar, An exhaustive survey on security and privacy issues in Healthcare 4.0, *Comput. Commun.*, vol. 153, pp. 311–335, 2020.
- [14] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, Security and privacy in the medical internet of things: A review, *Secur. Commun. Netw.*, vol. 2018, p. 5978636, 2018.
- [15] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, Edge computing security: State of the art and challenges, *Proc. IEEE*, vol. 107, no. 8, pp. 1608–1631, 2019.
- [16] Statista—the statistics portal, <https://www.statista.com/>, 2023.
- [17] M. Yahuza, M. Y. I. B. Idris, A. W. B. A. Wahab, A. T. S. Ho, S. Khan, S. N. B. Musa, and A. Z. B. Taha, Systematic review on security and privacy requirements in edge computing: State of the art and future research opportunities, *IEEE Access*, vol. 8, pp. 76541–76567, 2020.
- [18] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, Data security and privacy-preserving in edge computing paradigm: Survey and open issues, *IEEE Access*, vol. 6, pp. 18209–18237, 2018.
- [19] H. S. G. Pussewalage and V. A. Oleshchuk, Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions, *Int. J. Inf. Manage.*, vol. 36, no. 6, pp. 1161–1173, 2016.
- [20] R. Roman, J. Lopez, and M. Mambo, Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges, *Future Gener. Comput. Syst.*, vol. 78, pp. 680–698, 2018.
- [21] Z. Huang, G. Xia, Z. Wang, and S. Yuan, Survey on edge computing security, in *Proc. Int. Conf. Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*, Fuzhou, China, 2020, pp. 96–105.
- [22] F. Y. Rao and E. Bertino, Privacy techniques for edge computing systems, *Proc. IEEE*, vol. 107, no. 8, pp. 1632–1654, 2019.
- [23] M. Hartmann, U. S. Hashmi, and A. Imran, Edge computing in smart health care systems: Review, challenges, and research directions, *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, p. e3710, 2022.
- [24] Q. Jiang, X. Zhou, R. Wang, W. Ding, Y. Chu, S. Tang, X. Jia, and X. Xu, Intelligent monitoring for infectious diseases with fuzzy systems and edge computing: A survey, *Appl. Soft Comput.*, vol. 123, p. 108835, 2022.
- [25] A. Ometov, O. L. Molua, M. Komarov, and J. Nurmi, A survey of security in cloud, edge, and fog computing, *Sensors*, vol. 22, no. 3, p. 927, 2022.
- [26] M. D. A. Rahman, M. S. Hossain, G. Loukas, E. Hassanain, S. S. Rahman, M. F. Alhamid, and M. Guizani, Blockchain-based mobile edge computing framework for secure therapy applications, *IEEE Access*, vol. 6, pp. 72469–72478, 2018.
- [27] R. Kumar and R. Tripathi, Towards design and implementation of security and privacy framework for internet of medical things (IoMT) by leveraging blockchain and IPFS technology, *J. Supercomput.*, vol. 77, no. 8, pp. 7916–7955, 2021.
- [28] G. Tripathi, M. Abdul Ahad, and S. Paiva, SMS: A secure healthcare model for smart cities, *Electronics*, vol. 9, no. 7, p. 1135, 2020.
- [29] R. Saha, G. Kumar, M. K. Rai, R. Thomas, and S. J. Lim, Privacy ensured e-healthcare for fog-enhanced IoT based applications, *IEEE Access*, vol. 7, pp. 44536–44543, 2019.
- [30] W. Wang, H. Huang, L. Xue, Q. Li, R. Malekian, and Y. Zhang, Blockchain-assisted handover authentication for intelligent telehealth in multi-server edge computing environment, *J. Syst. Architect.*, vol. 115, p. 102024, 2021.
- [31] S. A. ElRahman and A. S. Alluhaidan, Blockchain technology and IoT-edge framework for sharing healthcare services, *Soft Comput.*, vol. 25, no. 21, pp. 13753–13777, 2021.
- [32] T. Hewa, A. Braeken, M. Ylianttila, and M. Liyanage, Multi-access edge computing and blockchain-based secure telehealth system connected with 5G and IoT, in *Proc. GLOBECOM 2020–2020 IEEE Global Communications Conf.*, Taipei, China, 2020, pp. 1–6.
- [33] E. M. Abou-Nassar, A. M. Ilyasu, P. M. El-Kafrawy, O. Y. Song, A. K. Bashir, and A. A. A. El-Latif, DITrust chain: Towards blockchain-based trust models for sustainable healthcare IoT systems, *IEEE Access*, vol. 8, pp. 111223–111238, 2020.
- [34] J. Li, J. Cai, F. Khan, A. U. Rehman, V. Balasubramaniam, J. Sun, and P. Venu, A secured framework for SDN-based edge computing in IoT-enabled healthcare system, *IEEE Access*, vol. 8, pp. 135479–135490, 2020.
- [35] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, MedRec: Using blockchain for medical data access and permission management, in *Proc. 2016 2nd Int. Conf. Open and Big Data (OBD)*, Vienna, Austria, 2016, pp. 25–30.
- [36] M. S. Christo, V. E. Jesi, U. Priyadarsini, V. Anbarasu, H. Venugopal, and M. Karuppiah, Ensuring improved security in medical data using ECC and blockchain technology with edge devices, *Secur. Commun. Netw.*, vol. 2021, p. 6966206, 2021.
- [37] X. Li, X. Huang, C. Li, R. Yu, and L. Shu, EdgeCare: Leveraging edge computing for collaborative data management in mobile healthcare systems, *IEEE Access*, vol. 7, pp. 22011–22025, 2019.
- [38] H. Guo, W. Li, E. Meamari, C. C. Shen, and M. Nejad,

- Attribute-based multi-signature and encryption for EHR management: A blockchain-based solution, in *Proc. IEEE Int. Conf. Blockchain and Cryptocurrency (ICBC)*, Toronto, Canada, 2020, pp. 1–5.
- [39] B. S. Egala, S. Priyanka, and A. K. Pradhan, SHPI: Smart healthcare system for patients in ICU using IoT, in *Proc. IEEE Int. Conf. Advanced Networks and Telecommunications Systems (ANTS)*, Goa, India, 2019, pp. 1–6.
- [40] A. Al Omar, A. K. Jamil, M. S. H. Nur, M. M. Hasan, R. Bosri, M. Z. A. Bhuiyan, and M. S. Rahman, Towards a transparent and privacy-preserving healthcare platform with blockchain for smart cities, presented at the 2020 IEEE 19<sup>th</sup> Int. Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 2020, pp. 1291–1296.
- [41] M. A. Jan, F. Khan, R. Khan, S. Mastorakis, V. G. Menon, M. Alazab, and P. Watters, Lightweight mutual authentication and privacy-preservation scheme for intelligent wearable devices in industrial-CPS, *IEEE Trans. Ind. Inform.*, vol. 17, no. 8, pp. 5829–5839, 2021.
- [42] A. Islam and S. Y. Shin, BHMUS: Blockchain based secure outdoor health monitoring scheme using UAV in smart city, in *Proc. 7<sup>th</sup> Int. Conf. Information and Communication Technology (ICoICT)*, Kuala Lumpur, Malaysia, 2019, pp. 1–6.
- [43] R. Guo, H. Shi, Q. Zhao, and D. Zheng, Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems, *IEEE Access*, vol. 6, pp. 11676–11686, 2018.
- [44] J. A. Alzubi, Blockchain-based Lamport Merkle digital signature: Authentication tool in IoT healthcare, *Comput. Commun.*, vol. 170, pp. 200–208, 2021.
- [45] Z. Ma, J. Ma, Y. Miao, X. Liu, K. K. R. Choo, R. Yang, and X. Wang, Lightweight privacy-preserving medical diagnosis in edge computing, *IEEE Trans. Serv. Comput.*, vol. 15, no. 3, pp. 1606–1618, 2022.
- [46] P. K. Vadrevu, S. K. Adusumalli, and V. K. Mangalapalli, Personal privacy preserving data publication of COVID-19 pandemic data using edge computing, *J. Crit. Rev.*, vol. 7, no. 19, pp. 8103–8111, 2020.
- [47] Y. Guo, F. Liu, Z. Cai, L. Chen, and N. Xiao, FEEL: A federated edge learning system for efficient and privacy-preserving mobile healthcare, in *Proc. 49<sup>th</sup> Int. Conf. Parallel Processing*, Edmonton, Canada, 2020, p. 9.
- [48] A. Alabdulatif, I. Khalil, X. Yi, and M. Guizani, Secure edge of things for smart healthcare surveillance framework, *IEEE Access*, vol. 7, p. 31010–31021, 2019.
- [49] R. Bosri, A. R. Uzzal, A. Al Omar, M. Z. A. Bhuiyan, and M. S. Rahman, HIDEchain: A user-centric secure edge computing architecture for healthcare IoT devices, in *Proc. IEEE INFOCOM 2020-IEEE Conf. Computer Communications Workshops*, Toronto, Canada, 2020, pp. 376–381.
- [50] F. Wang, L. Wang, G. Li, Y. Wang, C. Lv, and L. Qi, Edge-cloud-enabled matrix factorization for diversified APIs recommendation in mashup creation, *World Wide Web*, vol. 25, no. 5, pp. 1809–1829, 2022.
- [51] X. Zhou, X. Xu, W. Liang, Z. Zeng, and Z. Yan, Deep-learning-enhanced multitarget detection for end-edge-cloud surveillance in smart IoT, *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12588–12596, 2021.
- [52] L. Qu, Y. Zhou, P. P. Liang, Y. Xia, F. Wang, E. Adeli, F.-F. Li, and D. Rubin, Rethinking architecture design for tackling data heterogeneity in federated learning, in *Proc. IEEE/CVF Conf. Computer Vision and Pattern Recognition*, New Orleans, LA, USA, 2022, pp. 10051–10061.
- [53] X. Zhou, X. Yang, J. Ma, and K. I. K. Wang, Energy-efficient smart routing based on link correlation mining for wireless edge computing in IoT, *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14988–14997, 2022.
- [54] I. A. Elgendy, A. Muthanna, M. Hammoudeh, H. Shaiba, D. Unal, and M. Khayyat, Advanced deep learning for resource allocation and security aware data offloading in industrial mobile edge computing, *Big Data*, vol. 9, no. 4, pp. 265–278, 2021.
- [55] M. Hammoudeh, G. Epiphaniou, S. Belguith, D. Unal, B. Adebisi, T. Baker, A. S. M. Kayes, and P. Watters, A service-oriented approach for sensing in the Internet of Things: Intelligent transportation systems and privacy use cases, *IEEE Sens. J.*, vol. 21, no. 14, pp. 15753–15761, 2021.
- [56] M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, The case for VM-based cloudlets in mobile computing, *IEEE Pervasive Comput.*, vol. 8, no. 4, pp. 14–23, 2009.
- [57] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, Edge computing: Vision and challenges, *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, 2016.
- [58] S. Wang, Edge computing: Applications, state-of-the-art and challenges, *Adv. Netw.*, vol. 7, no. 1, pp. 8–15, 2019.
- [59] S. B. Calo, M. Touna, D. C. Verma, and A. Cullen, Edge computing architecture for applying AI to IoT, in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Boston, MA, USA, 2017, pp. 3012–3016.
- [60] B. R. Behera and P. Suraj, Rectangular microstrip patch antenna for wireless fidelity application: Design of a Wi-Fi antenna using the concept of metamaterials, in *Proc. IEEE Int. Conf. Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, India, 2016, pp. 1933–1937.
- [61] C. Bisdikian, An overview of the Bluetooth wireless technology, *IEEE Commun. Mag.*, vol. 39, no. 12, pp. 86–94, 2001.
- [62] S. Safaric and K. Malaric, ZigBee wireless standard, in *Proc. ELMAR 2006*, Zadar, Croatia, 2006, pp. 259–262.
- [63] V. Coskun, B. Ozdenizci, and K. Ok, A survey on near field communication (NFC) technology, *Wirel. Pers. Commun.*, vol. 71, no. 3, pp. 2259–2294, 2013.
- [64] B. Panchali, Edge computing-background and overview, in *Proc. Int. Conf. Smart Systems and Inventive Technology (ICSSIT)*, Tirunelveli, India, 2018, pp. 580–582.
- [65] H. El-Sayed, S. Sankar, M. Prasad, D. Puthal, A. Gupta, M. Mohanty, C. T. Lin, Edge of things: The big picture on the integration of edge, IoT and the cloud in a distributed computing environment, *IEEE Access*, vol. 6,

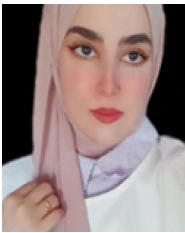
- pp. 1706–1717, 2018.
- [66] OpenFog Consortium Architecture Working Group, OpenFog architecture overview, White Paper, <https://site.ieee.org/denver-com/files/2017/06/OpenFog-Architecture-Overview-WP-2-2016.pdf>, 2016.
- [67] K. Dolui and S. K. Datta, Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing, in *Proc. Global Internet of Things Summit (GloTS)*, Geneva, Switzerland, 2017, pp. 1–6.
- [68] X. Masip-Bruin, E. Marin-Tordera, A. Jukan, and G. J. Ren, Managing resources continuity from the edge to the cloud: Architecture and performance, *Future Gener. Comput. Syst.*, vol. 79, pp. 777–785, 2018.
- [69] M. De Donno, K. Tange, and N. Dragoni, Foundations and evolution of modern computing paradigms: Cloud, IoT, edge, and fog, *IEEE Access*, vol. 7, pp. 150936–150948, 2019.
- [70] T. A. A. Alsoubi, M. Hammoudeh, Z. Bandar, and A. Nisbet, An overview and classification of approaches to information extraction in wireless sensor networks, in *Proc. 5<sup>th</sup> Int. Conf. Sensor Technologies and Applications & 1<sup>st</sup> Int. Workshop on Sensor Networks for Supply Chain Management*, Nice/Saint Laurent du Var, France, 2011, pp. 255–260.
- [71] M. Hammoudeh, R. Newman, C. Dennett, S. Mount, and O. Aldabbas, Map as a service: A framework for visualising and maximising information return from multi-modal wireless sensor networks, *Sensors*, vol. 15, no. 9, pp. 22970–23003, 2015.
- [72] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, Edge computing: A survey, *Future Gener. Comput. Syst.*, vol. 97, pp. 219–235, 2019.
- [73] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, Fog computing for the internet of things: Security and privacy issues, *IEEE Internet Comput.*, vol. 21, no. 2, pp. 34–42, 2017.
- [74] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, Security and privacy challenges in mobile cloud computing: Survey and way ahead, *J. Netw. Comput. Appl.*, vol. 84, pp. 38–54, 2017.
- [75] T. Bhatia and A. K. Verma, Data security in mobile cloud computing paradigm: A survey, taxonomy and open research issues, *J. Supercomput.*, vol. 73, no. 6, pp. 2558–2631, 2017.
- [76] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, *SIAM J. Comput.*, vol. 32, no. 3, pp. 586–615, 2003.
- [77] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, and W. Xie, An efficient file hierarchy attribute-based encryption scheme in cloud computing, *IEEE Trans. Inform. Forensics Secur.*, vol. 11, no. 6, pp. 1265–1277, 2016.
- [78] S. Moffat, M. Hammoudeh, and R. Hegarty, A survey on ciphertext-policy attribute-based encryption (CP-ABE) approaches to data security on mobile devices and its application to IoT, in *Proc. Int. Conf. Future Networks and Distributed Systems*, Cambridge, UK, 2017, p. 34.
- [79] S. Belguith, N. Kaaniche, and M. Hammoudeh, Analysis of attribute-based cryptographic techniques and their application to protect cloud services, *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, p. e3667, 2022.
- [80] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, Y. Yu, and A. Yang, A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing, *Future Gener. Comput. Syst.*, vol. 52, pp. 95–108, 2015.
- [81] M. R. Baharon, Q. Shi, and D. Llewellyn-Jones, A new lightweight homomorphic encryption scheme for mobile cloud computing, in *Proc. IEEE Int. Conf. Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, Liverpool, UK, 2015, pp. 618–625.
- [82] D. Eckhoff and I. Wagner, Privacy in the smart city—applications, technologies, challenges, and solutions, *IEEE Commun. Surv. Tutor.*, vol. 20, no. 1, pp. 489–516, 2018.
- [83] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, Enabling public auditability and data dynamics for storage security in cloud computing, *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 5, pp. 847–859, 2011.
- [84] K. Yang and X. Jia, An efficient and secure dynamic auditing protocol for data storage in cloud computing, *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 9, pp. 1717–1726, 2013.
- [85] C. Lin, Z. Shen, Q. Chen, and F. T. Sheldon, A data integrity verification scheme in mobile cloud computing, *J. Netw. Comput. Appl.*, vol. 77, pp. 146–151, 2017.
- [86] D. S. Touceda, J. M. S. Cámara, S. Zeadally, and M. Soriano, Attribute-based authorization for structured Peer-to-Peer (P2P) networks, *Comput. Stand. Interfaces*, vol. 42, pp. 71–83, 2015.
- [87] H. Liu, H. Ning, Q. Xiong, and L. T. Yang, Shared authority based privacy-preserving authentication protocol in cloud computing, *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 1, pp. 241–251, 2015.
- [88] X. Yang, X. Huang, and J. K. Liu, Efficient handover authentication with user anonymity and untraceability for mobile cloud computing, *Future Gener. Comput. Syst.*, vol. 62, pp. 190–195, 2016.
- [89] M. Bahrami and M. Singhal, A light-weight permutation based method for data privacy in mobile cloud computing, in *Proc. 3<sup>rd</sup> IEEE Int. Conf. Mobile Cloud Computing, Services, and Engineering*, San Francisco, CA, USA, 2015, pp. 189–198.
- [90] S. K. Pasupuleti, S. Ramalingam, and R. Buyya, An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing, *J. Netw. Comput. Appl.*, vol. 64, pp. 12–22, 2016.
- [91] I. S. Park, Y. D. Lee, and J. Jeong, Improved identity management protocol for secure mobile cloud computing, in *Proc. 46<sup>th</sup> Hawaii Int. Conf. System Sciences*, Wailea, HI, USA, 2013, pp. 4958–4965.
- [92] I. Khalil, A. Khreishah, and M. Azeem, Consolidated Identity Management System for secure mobile cloud computing, *Comput. Netw.*, vol. 65, pp. 99–110, 2014.
- [93] M. Chen, W. Li, Z. Li, S. Lu, and D. Chen, Preserving location privacy based on distributed cache pushing, in

- Proc. IEEE Wireless Communications and Networking Conf. (WCNC)*, Istanbul, Turkey, 2014, pp. 3456–3461.
- [94] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, Enhancing privacy through caching in location-based services, in *Proc. IEEE Conf. Computer Communications (INFOCOM)*, Hong Kong, China, 2015, pp. 1017–1025.
- [95] N. H. Hassan and Z. Ismail, A conceptual model for investigating factors influencing information security culture in healthcare environment, *Procedia Soc. Behav. Sci.*, vol. 65, pp. 1007–1012, 2012.
- [96] D. Box and D. Pottas, Improving information security behaviour in the healthcare context, *Procedia Technol.*, vol. 9, pp. 1093–1103, 2013.
- [97] P. Kumar and H. J. Lee, Security issues in healthcare applications using wireless medical sensor networks: A survey, *Sensors*, vol. 12, no. 1, pp. 55–91, 2011.
- [98] D. Kotz, A threat taxonomy for mHealth privacy, in *Proc. Third Int. Conf. Communication Systems and Networks (COMSNETS 2011)*, Bangalore, India, 2011, pp. 1–6.
- [99] I. Butun, N. Pereira, and M. Gidlund, Security risk analysis of LoRaWAN and future directions, *Future Internet*, vol. 11, no. 1, p. 3, 2018.
- [100] A. Singh and K. Chatterjee, Securing smart healthcare system with edge computing, *Comput. Secur.*, vol. 108, p. 102353, 2021.
- [101] L. Qi, Y. Yang, X. Zhou, W. Rafique and J. Ma, Fast anomaly identification based on multiaspect data streams for intelligent intrusion detection toward secure industry 4.0, *IEEE Trans. Ind. Inform.*, vol. 18, no. 9, pp. 6503–6511, 2022.
- [102] X. Zhou, Y. Hu, J. Wu, W. Liang, J. Ma, and Q. Jin, Distribution bias aware collaborative generative adversarial network for imbalanced deep learning in industrial IoT, *IEEE Trans. Ind. Inform.*, vol. 19, no. 1, pp. 570–580, 2023.
- [103] T. Javid, M. Faris, H. Beenish, and M. Fahad, Cybersecurity and data privacy in the cloudlet for preliminary healthcare big data analytics, in *Proc. Int. Conf. Computing and Information Technology*, Tabuk, Saudi Arabia, 2020, pp. 1–4.
- [104] P. Chaudhari and M. L. Das, Privacy preserving searchable encryption with fine-grained access control, *IEEE Trans. Cloud Comput.*, vol. 9, no. 2, pp. 753–762, 2021.
- [105] T. Chen and C. Guestrin, XGBoost: A scalable tree boosting system, in *Proc. 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, San Francisco, CA, USA, 2016, pp. 785–794.
- [106] L. Minder and A. Sinclair, The extended  $k$ -tree algorithm, *J. Cryptol.*, vol. 25, no. 2, pp. 349–382, 2012.
- [107] L. Sweeney,  $k$ -anonymity: A model for protecting privacy, *Int. J. Unc. Fuzz. Knowl.-Based Syst.*, vol. 10, no. 5, pp. 557–570, 2002.
- [108] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkatasubramanian,  $L$ -diversity: Privacy beyond  $k$ -anonymity, *ACM Trans. Knowl. Discov. Data*, vol. 1, no. 1, p. 3–es, 2007.
- [109] C. Dwork, Differential privacy: A survey of results, in *Proc. 5th Int. Conf. Theory and Applications of Models of Computation*, Xi'an, China, 2008, pp. 1–19.
- [110] S. Vishnu, S. R. J. Ramson, and R. Jegan, Internet of medical things (IoMT)-An overview, in *Proc. 5th Int. Conf. Devices, Circuits and Systems (ICDCS)*, Coimbatore, India, 2020, pp. 101–104.
- [111] M. Steichen, B. Fiz, R. Norvill, W. Shbair, and R. State, Blockchain-based, decentralized access control for IPFS, in *Proc. IEEE Int. Conf. Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, NS, Canada, 2018, pp. 1499–1506.
- [112] R. C. Wasserman, Electronic medical records (EMRs), epidemiology, and epistemology: Reflections on EMRs and future pediatric clinical research, *Acad. Pediatr.*, vol. 11, no. 4, pp. 280–287, 2011.
- [113] M. S. Hossain, G. Muhammad, and N. Guizani, Explainable AI and mass surveillance system-based healthcare framework to combat COVID-19 like pandemics, *IEEE Netw.*, vol. 34, no. 4, pp. 126–132, 2020.
- [114] ResNet-50 convolutional neural network-MATLAB resnet50-mathworks.com, <https://www.mathworks.com/help/deeplearning/ref/resnet50.html>, 2023.
- [115] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, Rethinking the inception architecture for computer vision, in *Proc. IEEE Conf. Computer Vision and Pattern Recognition*, Las Vegas, NV, USA, 2016, pp. 2818–2826.
- [116] T. T. Huong, T. P. Bac, D. M. Long, B. D. Thang, N. T. Binh, T. D. Luong and T. K. Phuc, Lockedge: Low-complexity cyberattack detection in IoT edge computing, *IEEE Access*, vol. 9, pp. 29696–29710, 2021.
- [117] D. Kim, J. Mun, Y. Park, J. Choi, and J. Choi, Planning system architecture of fat-client management for customized healthcare services in edge computing environment, in *Proc. 2020 5th Int. Conf. Intelligent Information Technology*, Hanoi, Vietnam, 2020, pp. 91–96.
- [118] M. Mistry, Softwarization of the infrastructure of Internet of Things for secure and smart healthcare, *Ann. Rom. Soc. Cell Biol.*, vol. 25, no. 6, pp. 6680–6701, 2021.
- [119] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, Blockchain and edge computing for decentralized EMRs sharing in federated healthcare, in *Proc. GLOBECOM IEEE Global Communications Conf.*, Taipei, China, 2020, pp. 1–6.
- [120] M. Campagna, SEC 4: Elliptic curve Qu-Vanstone implicit certificate scheme (ECQV), Standards for Efficient Cryptography, <https://www.secg.org/sec4-1.0.pdf>, 2013.
- [121] H. Guo, W. Li, M. Nejad, and C. C. Shen, Access control for electronic health records with hybrid blockchain-edge architecture, in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Atlanta, GA, USA, 2019, pp. 44–51.
- [122] J. Fan and F. Vercauteren, *Somewhat Practical Fully*

- Homomorphic Encryption*. Cryptology ePrint Archive, <https://eprint.iacr.org/2012/144>, 2012.
- [123] A. Frank, UCI machine learning repository, <http://archive.ics.uci.edu/ml>, 2010.
- [124] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. New York, NY, USA: Springer, 2004.
- [125] M. A. Jan, W. Zhang, M. Usman, Z. Tan, F. Khan, and E. Luo, SmartEdge: An end-to-end encryption framework for an edge-enabled smart city application, *J. Netw. Comput. Appl.*, vol. 137, pp. 1–10, 2019.
- [126] S. R. Eddy, Hidden Markov models, *Curr. Opin. Struct. Biol.*, vol. 6, no. 3, pp. 361–365, 1996.
- [127] X. Liu, J. Ma, Q. Li, J. Xiong, and F. Huang, Attribute based multi-signature scheme in the standard model, in *Proc. Ninth Int. Conf. Computational Intelligence and Security*, Emeishan, China, 2013, pp. 738–742.
- [128] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, BEdgeHealth: A decentralized architecture for edge-based IoMT networks using blockchain, *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11743–11757, 2021.
- [129] K. Kritikos, B. Pernici, P. Plebani, C. Cappiello, M. Comuzzi, S. Benrroun, I. Brandic, A. Kertész, M. Parkin, and M. Carro, A survey on service quality description, *ACM Comput. Surv.*, vol. 46, no. 1, p. 1, 2013.
- [130] R. Baskar, R. Dhanagopal, K. Elangovan, and K. Gunasekaran, VLSI based architecture in ECG monitoring for adaptive power management in wireless bio signal acquisition network, *Journal of Physics: Conference Series*, vol. 1964, no. 6, p. 062090, 2021.
- [131] Q. Yang, Q. Liu, and H. Lv, A decentralized system for medical data management via blockchain, *J. Internet Technol.*, vol. 21, no. 5, pp. 1335–1345, 2020.
- [132] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, MeDShare: Trust-less medical data sharing among cloud service providers via blockchain, *IEEE Access*, vol. 5, pp. 14757–14767, 2017.
- [133] B. D. Deebak, F. Al-Turjman, and L. Mostarda, Seamless secure anonymous authentication for cloud-based mobile edge computing, *Comput. Electr. Eng.*, vol. 87, p. 106782, 2020.
- [134] Z. Ali, M. S. Hossain, G. Muhammad, I. Ullah, H. Abachi, and A. Alamri, Edge-centric multimodal authentication system using encrypted biometric templates, *Future Gener. Comput. Syst.*, vol. 85, pp. 76–87, 2018.
- [135] L. Witt, M. Heyer, K. Toyoda, W. Samek, and D. Li, Decentral and incentivized federated learning frameworks: A systematic literature review, *IEEE Internet Things J.*, vol. 10, no. 4, pp. 3642–3663, 2023.
- [136] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, Communication-efficient learning of deep networks from decentralized data, in *Proc. 20<sup>th</sup> Int. Conf. Artificial Intelligence and Statistics*, Fort Lauderdale, FL, USA, 2017, pp. 1273–1282.
- [137] M. Ali, F. Naeem, M. Tariq, and G. Kaddoum, Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey, *IEEE J. Biomed. Health Inform.*, vol. 27, no. 2, pp. 778–789, 2023.
- [138] K. Chang, N. Balachandar, C. Lam, D. Yi, J. Brown, A. Beers, B. Rosen, D. L. Rubin, and J. Kalpathy-Cramer, Distributed deep learning networks among institutions for medical imaging, *J. Am. Med. Inform. Assoc.*, vol. 25, no. 8, pp. 945–954, 2018.
- [139] M. G. Poirot, P. Vepakomma, K. Chang, J. Kalpathy-Cramer, R. Gupta, and R. Raskar, Split learning for collaborative deep learning in healthcare, arXiv preprint arXiv: 1912.12115, 2019.
- [140] Y. Zhang, R. Jia, H. Pei, W. Wang, B. Li, and D. Song, The secret revealer: Generative model-inversion attacks against deep neural networks, in *Proc. IEEE/CVF Conf. Computer Vision and Pattern Recognition*, Seattle, WA, USA, 2020, pp. 250–258.
- [141] R. Tomsett, K. Chan, and S. Chakraborty, Model poisoning attacks against distributed machine learning systems, in *Proc. Volume 11006, Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications*, Baltimore, MD, USA, 2019, pp. 481–489.
- [142] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, Deep learning with differential privacy, in *Proc. 2016 ACM SIGSAC Conf. Computer and Communications Security*, Vienna, Austria, 2016, pp. 308–318.
- [143] Y. Chen, X. Qin, J. Wang, C. Yu, and W. Gao, FedHealth: A federated transfer learning framework for wearable healthcare, *IEEE Intell. Syst.*, vol. 35, no. 4, pp. 83–93, 2020.
- [144] G. Carvalho, B. Cabral, V. Pereira, and J. Bernardino, Edge computing: Current trends, research challenges and future directions, *Computing*, vol. 103, no. 5, pp. 993–1023, 2021.
- [145] R. Dave, N. Seliya, and N. Siddiqui, The benefits of edge computing in healthcare, smart cities, and IoT, arXiv preprint arXiv: 2112.01250, 2021.
- [146] A. Pekar, J. Mocnej, W. K. G. Seah, and I. Zolotova, Application domain-based overview of IoT network traffic characteristics, *ACM Comput. Surv.*, vol. 53, no. 4, p. 87, 2020.
- [147] M. Fredrikson, S. Jha, and T. Ristenpart, Model inversion attacks that exploit confidence information and basic countermeasures, in *Proc. 22<sup>nd</sup> ACM SIGSAC Conf. Computer and Communications Security*, Denver, CO, USA, 2015, pp. 1322–1333.
- [148] L. Kong, G. Li, W. Rafique, S. Shen, Q. He, M. R. Khosravi, R. Wang, and L. Qi, Time-aware missing healthcare data prediction based on ARIMA model, *IEEE/ACM Trans. Comput. Biol. Bioinform.*, doi: 10.1109/TCBB.2022.3205064.
- [149] J. Saleem, B. Adebisi, R. Ande, and M. Hammoudeh, A state of the art survey-Impact of cyber attacks on SME's, in *Proc. Int. Conf. Future Networks and Distributed Systems*, Cambridge, UK, 2017, p. 52.
- [150] S. Khanagha, S. Ansari, S. Paroutis, and L. Oviedo, Mutualism and the dynamics of new platform creation: A study of Cisco and fog computing, *Strateg. Manag. J.*, vol. 43, no. 3, pp. 476–506, 2022.



**Ahmad Alzu'bi** received the PhD degree in computer science from University of the West of Scotland (UWS), Paisley, UK in 2016. He is currently an associate professor at Department of Computer Science, Jordan University of Science and Technology, Jordan. He has many research publications in reputable journals and conferences. He is a member of several professional scientific organizations and councils. His research interests include computer vision, deep learning, healthcare technologies, and medical imaging.



**Ala'a Alomar** received the BEng degree in computer science from Yarmouk University, Irbid, Jordan in 2020. She is currently a master student in computer science at Jordan University of Science and Technology, Jordan. Her research interests include machine learning and edge computing.



**Shahed Alkhaza'leh** received the BEng degree in computer science from Yarmouk University, Irbid, Jordan in 2019. She is currently a master student in computer science at Jordan University of Science and Technology, Jordan. Her research interests include machine learning and edge computing.



**Abdelrahman Abuarqoub** received the PhD degree in computer science from the Manchester Metropolitan University, UK in 2014, and the MEng degree (Distinction) in data telecommunications and networks from University of Salford, UK in 2011. He is currently a senior lecturer in computer security at Cardiff School of Technologies, Cardiff Metropolitan University, UK. His research interests are in distributed algorithms, ubiquitous and mobile computing, communication, authentication techniques, and privacy issues in IoT.



**Mohammad Hammoudeh** received the MEng degree in advanced distributed systems from University of Leicester in 2006, and the PhD degree in computer science from the University of Wolverhampton in 2008, both in UK. He is currently the Saudi Aramco Cybersecurity Chair Professor at King Fahd University of Petroleum and Minerals, Kingdom of Saudi Arabia. His research interests are in the areas of cybersecurity, IoTs, and complex highly decentralised systems.