Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH Open Access

Transformative synergy: SSEHCET—bridging mobile edge computing and AI for enhanced eHealth security and efficiency

Mamoona Humayun[1*], Amjad Alsirhani[2], Faeiz Alserhani[3], Momina Shaheen[4] and Ghadah Alwakid[2]

Abstract

Blockchain technologies (BCT) are utilized in healthcare to facilitate a smart and secure transmission of patient data. BCT solutions, however, are unable to store data produced by IoT devices in smart healthcare applications because these applications need a quick consensus process, meticulous key management, and enhanced eprivacy standards. In this work, a smart and secure eHealth framework SSEHCET (Smart and Secure EHealth Framework using Cutting-edge Technologies) is proposed that leverages the potentials of modern cutting-edge technologies (IoT, 5G, mobile edge computing, and BCT), which comprises six layers: 1) The sensing layer-WBAN consists of medical sensors that normally are on or within the bodies of patients and communicate data to smartphones. 2) The edge layer consists of elements that are near IoT devices to collect data. 3) The Communication layer leverages the potential of 5G technology to transmit patients' data between multiple layers efficiently. 4) The storage layer consists of cloud servers or other powerful computers. 5) Security layer, which uses BCT to transmit and store patients' data securely. 6) The healthcare community layer includes healthcare professionals and institutions. For the processing of medical data and to guarantee dependable, safe, and private communication, a Smart Agent (SA) program was duplicated on all layers. The SA leverages the potential of BCT to protect patients' privacy when outsourcing data. The contribution is substantiated through a meticulous evaluation, encompassing security, ease of use, user satisfaction, and SSEHCET structure. Results from an in-depth case study with a prominent healthcare provider underscore SSEHCET's exceptional performance, showcasing its pivotal role in advancing the security, usability, and user satisfaction paradigm in modern eHealth landscapes.

Keywords WBAN, IoT, Blockchain, Mobile Edge Computing, eHealth, Smart Agent, AI

Introduction

The timely availability of healthcare services is a fundamental requirement for every individual. A country's healthcare system is a crucial measure of its developmental progress [1–3]. In this aspect, eHealth is highly beneficial asit offers healthcare to everyone, wherever. EHealth exemplifies technological advancements in expanding healthcare locally, nationally, and globally via the use of cutting-edge technologies (CET). It enables individuals who are unable to visit the clinic to access health services through continuous monitoring of vital signs using wearable or implantable IoT (Internet-of-Things) sensors, particularly for chronic and elderly patients. Time

*Correspondence:
Mamoona Humayun
mahumayun@ju.edu.sa
[1] Department of Information Systems, College of Computer and Information Sciences, Jouf University, Sakaka, Al Jouf 72388, Saudi Arabia
[2] Department of Computer Science, College of Computer and Information Sciences, Jouf University, Sakaka, Al Jouf 72388, Saudi Arabia
[3] Department of Computer Engineering & Networks, College of Computer and Information Sciences, Jouf University, Sakaka, Al Jouf 72388, Saudi Arabia
[4] Department of Computing, School of Arts, Humanities and Social Sciences, University of Roehampton, London SW15 5PJ, UK

savings, insight into one's health, and reduced administrative burden are among the primary advantages provided by eHealth [4–7]. According to a report presented by Statista in August 2022 (as shown in Fig. 1), the use of eHealth in various healthcare sectors is also expanding] (https://www.statista.com/outlook/dmo/digital-health/ehealth/worldwide#revenue). However, eHealth services have not developed as much as anticipated, partly due to issues of dependability, fault tolerance, and privacy. In eHealth, biological data collected by IoT devices is transmitted to Cloud entities operated by third parties, which presents challenges for data security and the protection of a patient's privacy [8–12].

In eHealth, the wireless body area network (WBAN) is employed extensively. It is concerned with networks made up of several sensors that are dispersed across or implanted into the human body. These sensors take measurements of the body's important health signals and transmit them to the user's smart device. Using the WBAN to check on a patient's health from afar is one way to help the patient live a normal life and do everyday things without having to live in a hospital or go there often [13–15]. But in a typical IoT design, a single health app running on a smartphone sends data to edge devices and then to cloud servers that are overseen by outside parties that are susceptible to various insider attacks [16, 17]. Furthermore, as explained in [18–20], owing to third-party participation, traditional Edge or Cloud processes cannot provide accountability and traceability of patient data.

With the use of Mobile Cloud Computing (MCC), a smartphone's functionality may be expanded by sending medical records to a remote server for processing and storage [21, 22]. The success of MCC depends on how well network loss and latency can be controlled. Lacking this, the enormous storage and processing capacity of the cloud is rendered useless by transmission delays and unreliable connections. Mobile Edge Computing (MEC) offers an IT service closer to the client to leverage the potential of Cloud computing capabilities. [23, 24]. Content processing in MEC is performed over edge devices. This formed a bridge between IoT devices and the cloud for collection and processing of data. Bringing data collection and processing closer to the client/edges reduces latency and boosts the performance of high-bandwidth applications [25, 26]. Since several parties are responsible for managing edge devices, moving work to remote servers on the network's periphery raises the risk of data theft and privacy violations [27, 28].

The preceding discussion demonstrates that IoT devices, cloud computing, MEC, and WBAN have greatly improved healthcare services by offering timely and low-cost treatment, better-quality care, effective data processing and management, and a number of other benefits. However, security remains a major challenge, as a result of which eHealth services have not evolved to the extent expected. In this article, SSE-HCET (Smart and Secure EHealth Framework using Cutting-edge Technologies) is developed to impart a secure and smart eHealth solution using the above-mentioned cutting-edge technologies. The motivation behind the study and the explicit contributions of the article are discussed in the following subsections.

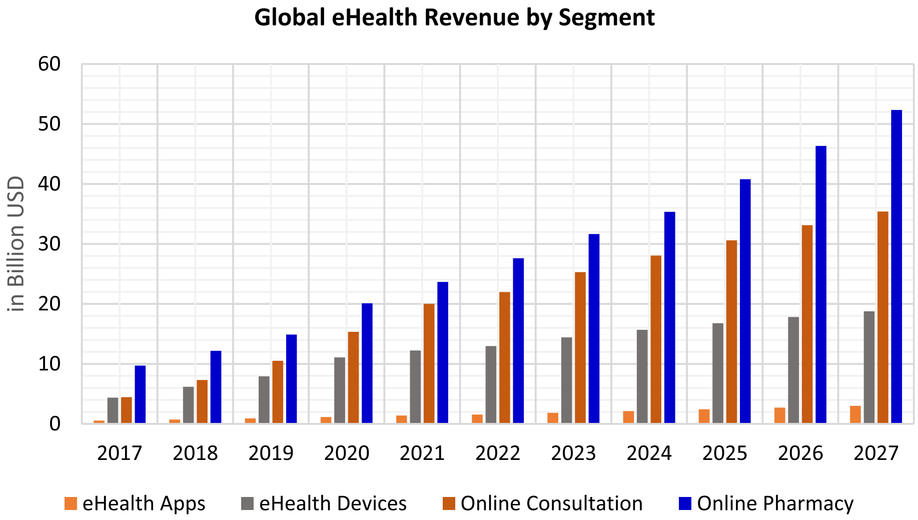

Fig. 1 Global Health revenue estimated till 2027 in billion USD

Motivation of the study

The motivation behind this study is to present a secure eHealth framework using cutting-edge technologies for smart health monitoring that can be applied in a variety of smart healthcare platforms. The SSEHCET leverages the potentials of IoT devices, Edge computing devices, cloud computing, 5G, and BCT to provide an end-to-end secure healthcare system. The IoT devices are helpful in collecting patients' vitals. To improve performance, edge computing devices are placed in the intermediary computing layer between IoT sensor devices and cloud computing. In SSEHCET, the edge layer provides several advantages, including real-time diagnosis services, decreasing the cost of cloud resources, improving the use of computing IoT devices, and minimizing the volume of data carried via networks. Encryption and the Blockchain consensus mechanism (BCM) are used to prevent the disclosure of sensitive healthcare information and potential leakage during the exchange between multiple parties. 5G is incorporated into SSEHCET to enable quick data transfer and job mobility across several tiers. Various smart contracts are deployed to ensure the confidentiality and integrity of healthcare data. Smart agent (SA) is used at various layers to improve task handling and migration.

Contribution of the study

The following is a summary of this article significant contributions:

- Develop SSEHCET with six layers: the sensing layer (WBAN), the edge layer, the communication layer (5G), the storage layer (the cloud), the security layer, and the healthcare community layer. Multiple instances of the SA are deployed at all tiers to handle patient data safely and efficiently.
- The SSEHCET can gather, monitor, and analyze patients' vitals in real-time. Machine learning (ML) approaches based on clustering are used to assess and identify anomaly changes in patients' data. BCT ensures the anonymity of members' sensitive data. The use of 5G technology improves data transfer efficiency.
- To analyze data supplied by medical IoT sensors, a customized Blockchain with a lightweight BCM is built at the edge layer. The healthcare Blockchain's consensus method is conducted on edge devices to make use of those devices' quicker connectivity capability. At the same time, the permanent storage for the Blockchain is controlled in the cloud.
- The evaluation of the SSEHCET is a pivotal aspect of this research paper, as it contributes valuable insights through a real-world case study involving healthcare organizations.

The remaining article is divided into five sections; the study background and the overview of existing related studies are provided in Sect. "Preliminaries and related work". Sect. "Proposed methodology/Framework (SSEHCET)" elaborates on the SSEHCET and its working in detail. Sect. "SSEHCET Evaluation using a Case study" discusses the proposed SSEHCET assessment using a case study. Sect. "Results and discussion" presents the findings and related discussion. Section six concludes the research by providing deeper insights into possible future directions.

Preliminaries and related work

In this part, the literature was evaluated into two categories: explaining the functions of CET in healthcare and giving an overview of the current body of research.

Wireless Body Area Network (WBAN)

WBANs are a specific type of sensor network that enables remote patient monitoring by utilizing IoT sensors to measure physiological indicators. WBANs may also be implanted or wearable, as illustrated in Fig. 2. They are primarily used to monitor people's health by placing sensors on the body to transmit physiological data to medical servers [29, 30]. This enables doctors to comprehend the patient's health. These systems can be very helpful to the medical board and individuals in the circumstances by providing services such as monitoring and delivering medical and pharmaceutical information, improving the processing of patients' data, and exchanging data [30–32]. The WBAN monitors a patient's vital signs and provides a prompt response to the user, enabling them to track the progression of the patient's illness.In this type of network, the efficient use of energy by the sensors is crucial. If the energy supply is depleted, the network's lifespan would be shortened.

WBAN offers many benefits, but it also poses certain overlooked risks. WBAN poses a number of privacy and security problems since it keeps and processes personal sensitive health data [31, 33–35]. There are primarily two categories of dangers: 1) unauthorized access: Unauthorized intruders breach the WBAN and steal user information. Suppose the attacker sells the users' information to an insurance provider, for instance. In that case, such assaults will breach their privacy 2) Modification of the messages: The hacker manipulates WBAN signals to provide the data collector with false user information. Users' safety will be impacted, for instance, if they are patients and the doctor administers the incorrect therapy as a result of receiving inaccurate patient data.

Edge computing

Edge computing is particularly successful in healthcare applications where real-time processing and large data

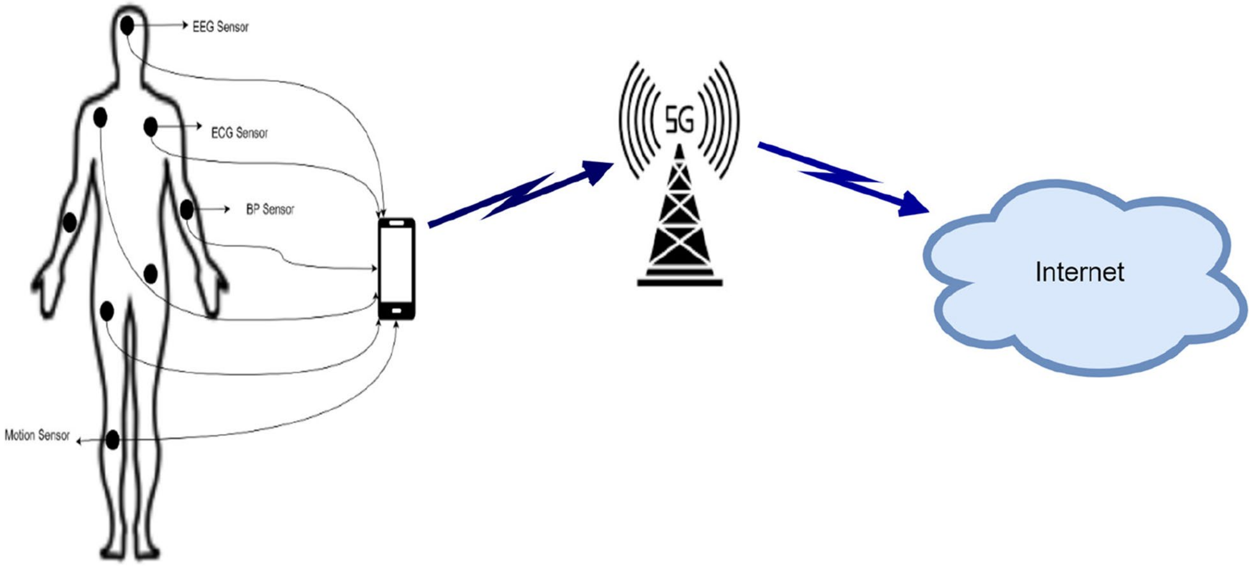

Fig. 2 WBAN Architecture

consumption are critical. In healthcare applications, physiological sensors with limited battery, memory, and channel bandwidth are unable to deliver advanced processing power and huge data transfers to the cloud. Edge computing has the potential to build a new ecosystem that will help the overall increase of information and communication needs [36, 37]. In IoT applications for healthcare, placing edge devices closer to sensing devices helps minimize reaction time and communication overhead, as illustrated in Fig. 3. Several new healthcare applications, such as remote surgery, will need edge computing architecture. The teleoperator requires real-time orders to control the movements and rotation of robotic arms, as well as a voice stream from the surgeon to interact with the surgical team remotely. Additionally, 3D video must be broadcast while physiological measures are sent to the surgeon throughout the procedure [38, 39]. In general, systems with edge computing design may decrease data propagation across network backhaul, improve reaction times, boost privacy and security, and reduce cloud overhead [40, 41].

Blockchain in healthcare

Edge computing is useful for quick access and processing of medical data, but patient security and privacy concerns are still present. Medical data processing on the edge and in the cloud both involve administrators, endangering patient privacy. BCT used in conjunction with the

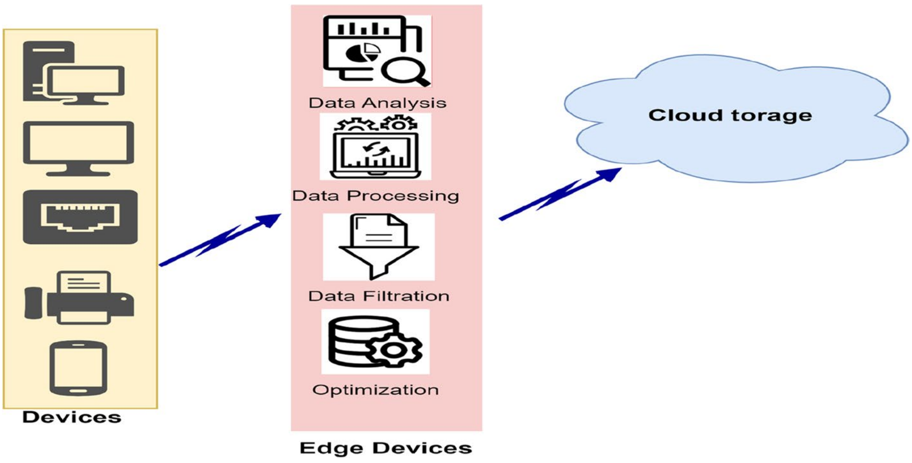

Fig. 3 Edge devices as a bridge between IoT devices and Cloud

cloud and edge devices may make it possible to process and store patient data without depending on centralized cloud management [42, 43]. The BCT's decentralized and distributed nature makes it fundamentally different from conventional databases. Using "blocks," which are collections of data, a BCT may securely store large amounts of data in a distributed ledger (DTL). The basic architecture of Blockchain is depicted in Fig. 4

Researchers have developed various privacy-preserving eHealth solutions as a result of the Blockchain's structure. A framework for remote patient monitoring using Ethereum smart contracts is presented in [44]. WBAN's data is gathered and aggregated using a smart device like a laptop or smartphone. The smart gadget transmits the compiled data to a predetermined smart contract that is kept on Ethereum. The smart contract analyses the data and notifies smart devices and healthcare professionals of the outcome. The cloud stores the data, whereas the blockchain just records the event's occurrence. The smart gadgets, however, are susceptible to denial of service (DoS) attacks and may create a single point of failure. Safe handling of medical data is the sole assurance provided by the design. In a study [45], a framework foraccessing medical data on the blockchain is developed. Cloud platform is used in this system for the storage of medical data while blockchain records every interaction a patient has with a third party. According to Brogan [46], DTL technology may progress the EHRs by preserving the veracity and integrity of patient data. Additionally, the authors demonstrated how to leverage the IoTA protocol's potential to communicate, store, and retrieve encrypted data securely via a DTL that cannot be tampered with. Regarding the accessibility, aggregation, liquidity, identity, and immutability of health data, Gordon spoke about how Blockchain might support patient-driven or patient-mediated data interoperability. Rupasinghe [47] divided the risk factors for falling into two categories: environmental and medical. Based on data and professional judgment, each detected risk factor is assigned one of three strengths: weak, moderate, or strong. To assure the accessibility, and availability of the data to forecast the chance of fall among the elderly, four different categories of users uploaded fall-related data into a blockchain. Incorporating data into the Blockchain, registering users, and predicting falls are all tasks that the smart contract is said to accomplish. Dwivedi et al.[48] introduced a blockchain-focused eHealth framework. They gave consideration to an overlay network that has nodes linked logically or virtually. According to the idea, blocks generated by IoT medical devices are sent to cloud servers after being confirmed by the cluster head. After confirmation, blocks created by IoT medical devices are delivered to cloud servers. The architects of the eHealth system implemented a variety of basic standard security protocols to ensure security and safeguard patient confidentiality. The blockchain's integrity is constantly checked by a static cluster head. However, avoiding a global consensus method may make the blockchain-based eHealth system less resilient. Running a simple BCM on a Fog network helped us improve eHealth. The consensus method is carried out by the cluster leader, who has been chosen for a certain duration depending on the characteristics of the nodes. Additionally, a Patient Agent (PA) that replicates itself in devices at three different levels—the smartphone, the fog, and the cloud—bundles the functional components needed for monitoring a patient. In the context of cloud computing, Gaetani [49] suggested a Blockchain with two levels. The initial layer of the Blockchain avoids the computationally costly Proof of Work and maintains track of all activities performed on the distributed database.

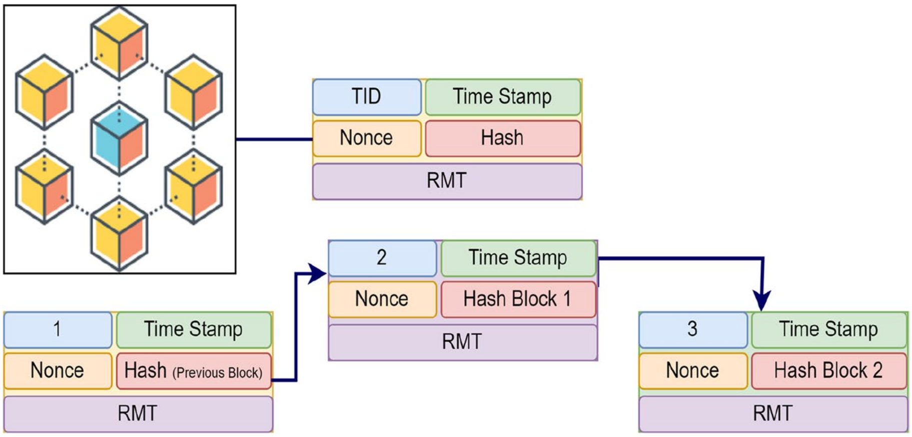

Fig. 4 Blockchain structure

The existing BCT enables eHealth infrastructures examined above to use the potentials of Fog and Cloud for the storage and processing of EHR. However, healthcare research did not progress in the idea of distributing the execution of the blockchain at various levels, such as sensing, communication, edge, and cloud layers. An eHealth system can be made fault-tolerant, dependable, and protected against DoS using a decentralized blockchain controller. Furthermore, current eHealth systems based on blockchain did not progress BCMs or privacy-aware job handling techniques. To fill this gap, our proposed SSEHCET deploys blockchain at different tiers (as outlined in the proposed methodology section) to provide secure eHealth services.

Related work

This section will explore existing studies that used cutting-edge technologies especially Blockchain, edge/fog computing, and Cloud to address eHealth security issues.

In the article [11], the authors suggest a Blockchain-enabled decentralized electronic healthcare architecture that is composed of three layers: 1) The Sensing layer, which consists of several medical sensors that are often placed on or inside a patient's body and transfer data to a smartphone. 2) The Edge Networks are made up of devices that are close to the data-detecting IoT devices. 3) The Core Networks are made up of servers that are high-powered computing clouds or other types. The processing of medical data is handled by a software called Patient Agent (PA), which is duplicated across all three tiers. This helps to guarantee dependable, secure, and confidential communication. In order to illustrate the practicability of the system in the context of the processing and storage of health data, a performance study has been carried out. The findings of the study showed that the suggested eHealth system could handle health data utilizing BCT in almost real-time.

The current research on BCT applied to eHealth are examined and potential research avenues were explored in [50]. Studies from 2010 to 2019 were selected for analysis after a search of well-known scientific resources for blockchain research in the eHealth sector. The search process retrieved 84 papers on blockchain in eHealth, of which 18 were determined to be relevant. Numerous publications outline the benefits of this technology and how it is being developed and utilized in the healthcare industry. The study concludes that the new BCT used by eHealth discovers new methods to share the distributed perspective of health data and advances precision medicine, hence enhancing health and avoiding illness.

A BCT-based eHealth system is suggested in [51] to ensure the auditability of electronic health records (EHR) tampering. In this approach, each valid query manipulation by data consumers and each legitimate outsourced change by hospitals is logged in the blockchain for permanent storage, assuring the traceability of the data. Concurrently, attributes-based proxy re-encryption is employed to ensure access control of medical data, and the auditor will identify any activity that affects the integrity of EHRs. Due to the auditable and tamper-proof nature of BCT, any entity that illegally manipulated EHRs would be held responsible based on the evidence of the proposed Proof-Chain. In conclusion, security evaluation and performance assessment reveal that this technique is both secure and effective.

In [52], the challenges associated with maintaining the privacy and confidentiality of essential medical data are described, and it highlights the benefits of BCT for the implementation of a secure and scalable solution for the exchange of medical data to achieve the best possible potential performance. This article presents an approach that makes use of BCT as a potential solution to problems that are encountered by eHealth application developers. The restricted computational power of sensors and the integrity of data exchange were the two key concerns of the paper. In the proposed approach, the BCT is only used to provide a reference to the data, or a part of it. According to the findings of the study, the eHealth business is poised for expansion provided that this technology is used with suitable instruments, models, protocols, and fully functional systems.

In article [53], an eHealth model based on BCT named BEIM is presented to assure information integrity in eHealth systems. Unlike prior alternatives, the study demonstrates how to enable information removal, which is a legal necessity in many nations. Several blockchain security issues that must be addressed during blockchain usage in eHealth systems are also mentioned. The suggested approach is readily integrated with systems based on service-oriented architectures. The major contribution of the study is a blockchain-based solution to the issue of transactional transparency with the possibility to erase documents or logs.

In the study [54], the authors propose a new scheme that they call EC-ACS for the public verification and auditing of EHRs in the Cloud Server. This is done to protect EHR by utilizing authorized BCT. In this particular investigation, ECC is used to encrypt sensitive medical data, and the CAS is utilized to establish a digital signature for the purpose of data exchange and storage in a cloud-based system. The solution that has been presented protects users' privacy and confidentiality while also preventing illegal access to sensitive data stored in cloud-based healthcare systems. In addition, the BCT ensures the completeness, authenticity, and safety of the cloud-based storage of patient medical data.

In article [55], the authors suggest a new framework for exchanging EHRs by bringing together BCT and the distributed interplanetary file system (IPFS) in a mobile cloud environment. To facilitate the safe transfer of EHRs between patients and their respective healthcare providers, a reliable access control system is developed utilizing smart contracts. The authors put the Ethereum blockchain through its paces in a real-world data-sharing situation, using the Amazon cloud to power a mobile app prototype. The empirical findings validate the effectiveness of the concept in securing private health information during mobile cloud data transfers. Lightweight access control architecture, low network latency, and strong security and privacy levels are only some of the ways in which the evaluated system outperforms conventional methods of data exchange.

In article [56], a method was presented for securing patient data using the BCT to preserve user data and privacy, and cryptographic techniques were utilized to protect the data transmission channel. The findings demonstrated that the suggested system protected the confidentiality, integrity, authenticity, and non-repudiation of patient data, in addition to the privacy of the patients.

The work done in article [57] aims to tackle the difficulties associated with safeguarding patients' sensitive health data in remote health data analysis, particularly in relation to the growing significance of temperature sensor-based respiratory monitoring during the COVID-19 epidemic. The study suggests a method to improve the accuracy of diagnoses on e-Health platforms while maintaining privacy by using blockchain technology, due to the potential dangers of keeping health data on external servers. The proposed strategy utilizes the unchangeability of Blockchain to facilitate safe sharing of health data, with a focus on implementing a robust access control mechanism. The suggested Health-chain has been shown to be suitable for smart healthcare systems via experimental data and security assessments. It has shown efficacy in computing, time consumption, and resistance against security attacks.

A study [58] indicates that the increasing use of deep learning systems in e-healthcare applications has resulted in significant advantages in the areas of diagnosis and treatment. Nevertheless, the presence of significant privacy threats to sensitive patient data highlights the need for strong security measures. An innovative method used in e-healthcare incorporates privacy measures based on several agents into deep learning systems. This strategy involves continuously assessing the levels of confidentiality, integrity, and availability in real-time. The multi-agent system effectively oversees and regulates data access by allocating distinct responsibilities and permissions to each agent. Deep learning integration improves diagnostic precision by using patient symptoms and medical history to forecast outcomes. This strategy guarantees a highly secure e-healthcare system by restricting data access to authorized individuals and facilitating immediate detection of any privacy breaches. Consequently, it results in enhanced patient outcomes.

The study [59] focuses on the difficulties encountered in existing Electronic Health Record (EHR) systems, with a particular emphasis on the shift from traditional paper-based records to EHRs. The research utilizes a methodical examination of existing literature to investigate the current status of electronic health records (EHRs), with a specific emphasis on implementations that use blockchain technology. The study finds compatibility problems in current blockchain-based electronic health record (EHR) frameworks and harmonizes them with established national and international EHR standards, such as HIPAA and HL7. The objective of the suggested interoperable blockchain-based Electronic Health Record (EHR) system is to improve the safe exchange of health information by providing immutability, security, and user control without relying on centralized storage. This study makes a substantial contribution to our knowledge of how Blockchain might be used in EHR frameworks. It highlights the consequences for the healthcare industry, namely in terms of maintaining confidentiality, privacy, and integrity while exchanging and storing electronic health data.

The preceding summary of related work draws attention to the significance of CET for the healthcare industry, particularly BCT and cloud platforms. Despite this, the following issues still exist that need to be solved in order to leverage the potential of eHealth.

- Massive amounts of data that are being exchanged and stored are vulnerable to being hacked and exploited in many ways.
- Healthcare cloud services are negatively impacted by high levels of both latency and reaction time.
- A difficulty lies in the need for faster processing and improved security of healthcare services.
- The movement of tasks across networked devices is difficult.

To address these issues, a framework SSEHCET is proposed in the next section that will use IoT, 5G, edge computing, cloud computing, and blockchain to provide a smart and secure eHealth system.

Proposed methodology/Framework (SSEHCET)

This section provides a thorough explanation of our eHealth framework, SSEHCET. Figure 5 shows the SSEHCET's high-level perspective; it is a sophisticated eHealth solution designed to advance the security, efficiency, and privacy of patient data transmission and processing. This comprehensive framework encompasses six layers: Sensing, Edge, Communication, Storage, Security, and Healthcare Community. At the heart of SSEHCET is the Smart Agent (SA) program, strategically duplicated across all layers, playing a pivotal role in implementing blockchain technology (BCT). The SA program ensures the secure processing of medical data and offers additional functionalities such as task migration management, BCT oversight, and efficient allocation of network resources. The framework seamlessly integrates modern technologies, including IoT, 5G, mobile edge computing, and BCT, addressing critical challenges in data security, consensus processing, key management, and privacy standards within smart healthcare applications. Below, a detailed overview of all six layers is provided.

Sensing layer

The first layer of the SSEHCET is the sensing layer, which consists of wearable or implantable IoT sensors attached to the human body. These IoT sensors collect

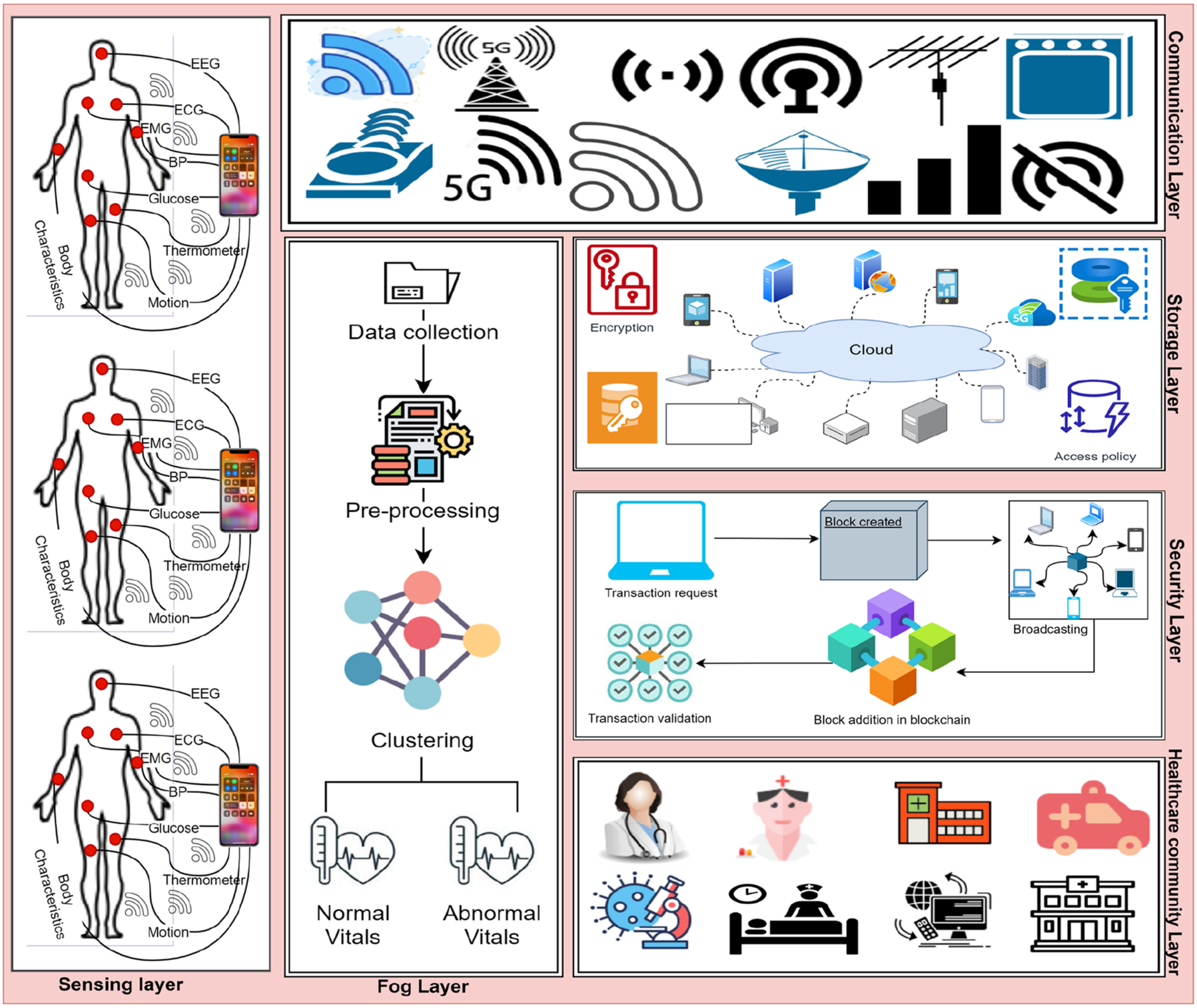

Fig. 5 Proposed Framework SSEHCET

patients' vital signs, which are collected by the smart device connected to these sensors [60–62]. This smart device application monitors the vitals and transmits them to the next layer in case the vitals are not normal. The SA in the SSEHCET helps in task migration from the smart application to the edge layer for further processing and storage. SA works as an intermediary between IoT devices and edge devices; it uses 5G services for migrating tasks to the edge layer.

The working of the sensing layer is modeled in Fig. 6; Algorithm 1 shows the details of tasks to be executed at this layer.

Algorithm 1. Working of physical/sensing layer

```
Let $v = vitals$; $\varsigma = Body\ sensors$; $\Xi\forall$ =Smart App;
$\mathfrak{H} = Smart\ agent$; $n = total\ number\ of\ sensors$; $\Gamma\Upsilon = vitals\ threhold\ values$
Begin
Int count = 0;
for (i = 1 to n)
If (Check(a[i] = true)
count = count + 1
return count;
if count = n
    $Collect(v) \rightarrow \varsigma \rightarrow 5G$
    $Send(v) \rightarrow \Xi\forall \rightarrow 5G$
    $\Xi\forall \rightarrow Send(v) \rightarrow \mathfrak{H} \rightarrow 5G$
    $\mathfrak{H} \rightarrow Analyse(v)$
    $Compare(v, \Gamma\Upsilon)$
else
    $Check(\varsigma, \Xi\forall)$
    $Adjust(\varsigma, \Xi\forall)$
if v = normal
    Go to End
else
    $Transmit(v) \rightarrow 5G$
End
```

Communication layer

The SSEHCET's communication layer makes use of 5G's capabilities to send and receive information across different tiers. Many factors contribute to 5G's popularity, such as its faster speeds, lower latency, increased capacity for remote execution, ability to support more devices simultaneously, and it's potential to implement virtual networks, allowing for more flexible connectivity based on individual requirements. The SA and BCT are envisioned on the 5G network in the proposed framework to manage and distribute logical resources to various healthcare applications, hence enhancing the quality of experience. 5G operates on almost all the layers. In the sensing layer, it transmits data from IoT sensors to the smart device and then from the smart device to the edge layer through SA. In the edge layer, it transmits data between edge devices and finally sends the processed data to the cloud for storage via SA after the execution of BCM. In the cloud layer, 5G helps to transmit data between multiple cloud devices. The healthcare community uses 5G services to fetch data from the cloud and transmit data to the cloud.

Edge layer

IoT devices at the sensing layer gather and evaluate patient data before triggering actions depending on the insights provided. In our instance, these insights are required in real-time; hence, edge computing is required. It will bring computation nearer to the IoT device, as well as data collecting and analytics, to a physically closer area. This reduces network latency since the round trip to the data center, and return is shorter. Thus, the SSEHCET's utilization of edge computing will improve the performance of IoT applications performing real-time tasks. Furthermore, Edge computing allows for the processing and filtering of IoT-produced data closer to the devices, hence optimizing bandwidth. Patients' aberrant medical data will be incorporated into a customized Blockchain to boost security. At this layer, the Blockchain will also keep track of environmental data and event occurrences.

Figure 7 describes the working of the edge layer and the role SA plays in task migration. The details of operations performed at this layer are mentioned in Algorithm 2.

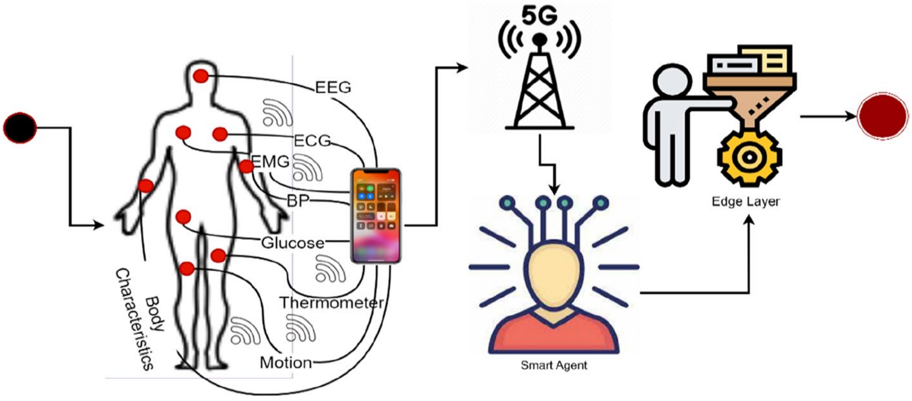

Fig. 6 Working of the physical layer

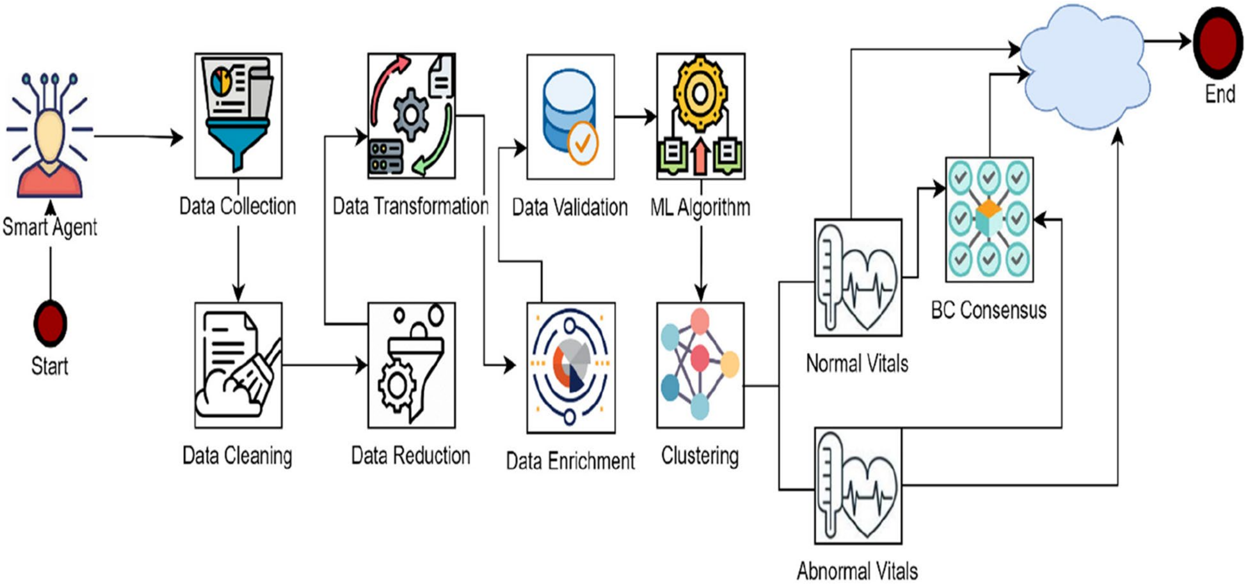

Fig. 7 working of the edge layer

Algorithm 2. Working of Edge layer

```
Let $v$ = vitals; $\mathfrak{H}$ = Smart agent ; $\varpi$ = BlockChain ; $\mathbb{C}\mathcal{M}$ = Consensus mechanism ; $\forall v$ = Abnormal vitals
    Begin
    $\mathfrak{H} \rightarrow Collect(v) \rightarrow 5G$
    $Deploy(\varpi)$
    $Execute\ (\mathbb{C}\mathcal{M})$
    $Store(v)$
    $process(v)$
    $Apply\ clustering(v) \rightarrow (v;\ \forall v)$
    $Insert(\forall v) \rightarrow \varpi$
    $transmit\ (v) \rightarrow 5G$
    End
```

Storage layer

This layer leverages the potential of cloud computing to store healthcare data. The SA also works at this layer to take decisions related to access control policy and the use of encryption standards. Additionally, blockchain maintains a distributed tamper-proof ledger that is duplicated across numerous nodes. A DTL duplicated across numerous servers prevents tampering with a record. Managing big data in health is complicated by the storage in a decentralized DTL. In our approach, cloud servers can handle the huge storage necessary for decentralized DTL for healthcare data. SA deployed in the cloud conducts time-sensitive and high-computing activities with increased availability and flexibility.

As can be seen in Fig. 8, the data is retrieved from edge devices and stored on the cloud via a smart agent. Blockchain keeps records of environmental parameters and event occurrences. The functions performed at this layer are further elaborated in Algorithm 3.

Algorithm 3. Working of Storage layer

```
Let $v$ = vitals; $\mathfrak{H}$ = Smart agent ; $\alpha\gamma\rho$ = Access control policy ; $\mathbb{C}$ = Cloud ; $\varpi\ell$ = Blockchain ledger
    Begin
    $\mathfrak{H} \rightarrow Collect(v) \rightarrow 5G$
    $\mathfrak{H} \rightarrow Encrypt(v)$
    $\mathfrak{H} \rightarrow Store(v) \rightarrow \mathbb{C}$
    $\mathfrak{H} \rightarrow Manage(\varpi\ell)$
    $\mathfrak{H} \rightarrow verify(\alpha\gamma\rho)$
    End
```

Security layer

This layer of the proposed architecture not only ensures the security of EHRs but also expedites the processing of healthcare services by enhancing the patient experience. This layer uses blockchain's capabilities to offer end-to-end security. The edge network performs task movement via Blockchain. The BCM is conducted on the edge layer to give its tenants and customers quicker and more secure processing. SA and Blockchain collaborate on the communication layer to govern the 5G network and assign logical resources to various health apps, hence enhancing QoE. The Blockchain preserves a record of the event's existence, and data is maintained on the EHR, while anomalous patient medical data is added to a tailored Blockchain.

The BCM protects data integrity, and the DTL prevents records from being altered. At the storage layer of SSE-HCET, the execution environment parameters of a distant computer are stored in the Blockchain. The nodes of the blockchain approve the environment settings of possible distant devices that want to participate in the execution of migrating tasks. The local computer obtains these

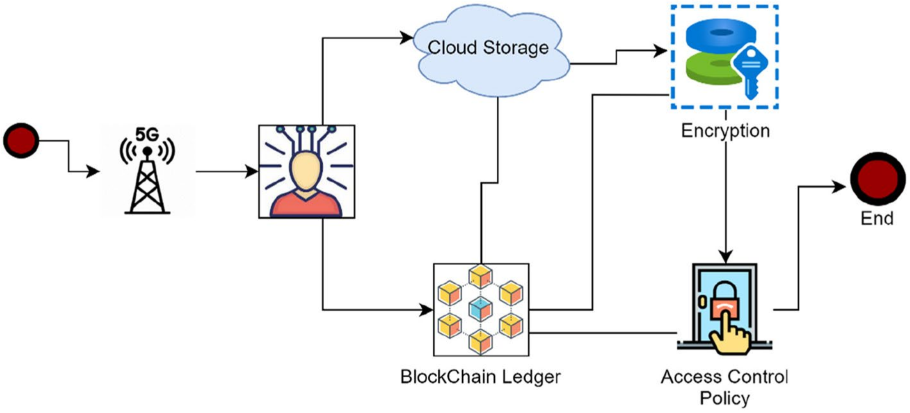

Fig. 8 Working of the storage layer

characteristics from the Blockchain in order to delegate jobs to nearby or distant machines. SA manages and stores performance metrics for transferring jobs via blockchain. Each SA's performance characteristics are recorded on the blockchain. Every node on the blockchain holds the rules for a smart contract's coding. A smart contract is activated when a blockchain network transaction corresponding to that contract is issued. The SA creates many types of intelligent contracts for processing EHRs. Smart contracts for SA registration, data filtration, data categorization, warning creation, task movement, and healthcare professional registration are a few examples of smart contracts.

Algorithm 4. Working of Security layer

```
Let $v$ = vitals; $\mathfrak{H}$ = Smart agent ; $\alpha\gamma\rho$ = Access control policy ; $\mathbb{C}$ = Cloud ; $\varpi\ell$ = Blockchain ledger ;
$\mathcal{TM}$ = Task migration;   $\mathbb{C}\mathcal{M}$ = Consensus mechanism   $\mathcal{SC}$ = Smart Contract;   $\mathcal{EO}$ =
Event Occurence                     ;                      $\mathcal{EP}$ = Environmental Parameters;
$\mathcal{DF}$ = Data Filtration; $\mathcal{DC}$ = Data Classification; $\mathcal{WG}$ = Warning Generation; $\mathcal{NR}$ =
Network Resources

1. Begin
2. Switch (Layers)
   {
       Case 1: Communication Layer
       {
       Manage ($\mathcal{NR}$)
       Allocate($\mathcal{NR}$) $\rightarrow$ Diverse Health Apps
       }
       Case 2: Edge Layer
       {
       Perform($\mathcal{TM}$)
       Execute($\mathbb{C}\mathcal{M}$)
       EnableProcessing($v$)
       EnableStoarge($v$)
       KeepRecord($\mathcal{EO}$)
       Trigger ($\mathcal{SC}$) $\rightarrow \mathfrak{H}$
       Trigger ($\mathcal{SC}$) $\rightarrow \mathcal{DF}$
       Trigger ($\mathcal{SC}$) $\rightarrow \mathcal{DC}$
       Trigger ($\mathcal{SC}$) $\rightarrow \mathcal{WG}$
       Trigger ($\mathcal{SC}$) $\rightarrow \mathcal{TM}$
       Store($\mathcal{EP}$)
       Break
       }
       Case 3: Storage Layer
       {
       Support ($\alpha\gamma\rho$)
       Authorize($\mathcal{EP}$)
       LocalMachines $\rightarrow$ Retrieves($\mathcal{EP}$) $\rightarrow \varpi$
       Maintain ($\mathcal{TM}$) $\Rightarrow$ TamperProof
       Store($\mathcal{EP}$)
       Trigger ($\mathcal{SC}$) $\rightarrow \mathcal{TM}$
       }
   }
3. End
```

The blockchain replicates a unique DTL across several nodes. The ledger is comprised of a series of verified blocks linked in a linked-list way, with each Block containing a certain amount of transactions bundled in a secure Merkle tree. Nodes on a blockchain add a new block to the ledger by executing a consensus method. The smartphone transfers collected health data to the edge layer of our SSEHCET. Edge blockchain activities are executed to handle medical IoT data in near real-time. However, BCT requires expensive computing and storage, and edge devices lack the necessary capabilities to support it. To circumvent this, blockchain activities are partitioned and assigned to three levels of the proposed healthcare architecture, taking into account the capabilities of these layers' devices. For instance, the SA at the sensing layer may establish the transaction structure and begin data flow. The SA at the edge layer is able to perform a lightweight consensus method and save block information. Due to the proximity of edge devices to medical sensors, this minimizes the time required for block's confirmation on the blockchain. SA on the storage layer is capable of providing persistent storage for the Blockchain-based DTL. After the SA at the edge layer certifies the block by executing a consensus procedure, the SA at the storage layer inserts the block into the cloud ledger. The key functions provided by the security layer at various other levels are discussed in Algorithm 4.

Healthcare community layer

Last but not least is the healthcare community layer, which includes healthcare organizations and professionals. This layer is responsible for providing healthcare services to the patients by analyzing their vitals. At this layer, the SA observes the vitals of the patients and sends them to the concerned healthcare community device. The SA fetches the EHR from the cloud, analyses these records, and takes the decision to forward it to the concerned healthcare section. The Blockchain works at this layer as well to check the authenticity of SA. Figure 9 provides the overview of this layer. According to Fig. 9, SA retrieves EHRs from the cloud and forwards them to the concerned section, while Blockchain at this layer keeps track of event occurrences and environmental parameters.

Role of smart agent

The smart agent plays a critical role in the proposed methodology; it is deployed on various layers to provide different services, which include; task migration, data storage and retrieval, access control management, etc. SA, a software module installed on many layers, facilitates the activities of each layer to provide dependable, secure, and confidential communication. The SA implements BCM and leverages a blockchain-enabled algorithm for task-offloading to protect EHRs' privacy while outsourcing duties. On the 5G network, SA and blockchain are anticipated to manage and allocate logical resources for varied health applications in order to enhance QoE. SA is placed in the cloud to handle high-computing and delay-tolerant jobs with improved availability and flexibility. Algorithm 5 shows the functionality of the smart agent.

Algorithm 5. Working of Smart Agent

```
Let $v$ = vitals; $\mathfrak{H}$ = Smart agent; $\alpha\gamma\rho$ = Access control policy; $\mathbb{C}$ = Cloud ; $\varpi\ell$ = Blockchain ledger; $\varkappa$ = logical resources
Begin
$(\mathfrak{H}, \varpi) \rightarrow 5G \Rightarrow Manage(\varkappa)$
$\mathfrak{H} \rightarrow Collect(v) \rightarrow 5G$
$\mathfrak{H} \rightarrow Encrypt(v)$
$\mathfrak{H} \rightarrow Store(v) \rightarrow \mathbb{C}$
$\mathfrak{H} \rightarrow Manage(\varpi\ell)$
$\mathfrak{H} \rightarrow verify(\alpha\gamma\rho)$
End
```

SSEHCET Evaluation using a case study

Case studies are an effective method of examination because they provide sufficient details about the actual world, especially in the healthcare domain [63–66]. The case study methodology is more suitable to evaluate SSEHCET as it was designed for the healthcare industry. SSEHCET was evaluated using a case study with a prominent healthcare provider. The primary goal of the case study was to demonstrate the viability of employing SSEHCET in an actual eHealth setting and to demonstrate the feasibility of implementing SSEHCET.

To preserve the confidentiality of the organization involved in our case study, it was named organization A. Organization A is an ISO 9001:2015 initiative of the renowned group, which offers nationwide eHealth services. It was founded in 2011 to offer healthcare services of an international grade nationwide. It has highly competent and experienced consultants as well as trained paramedical personnel who provide 24/7 healthcare services with distinction. Organization A uses cutting-edge medical and surgical equipment and technology for patient diagnosis, monitoring, and treatment. To effectively meet the ever-evolving demands of eHealth, the business continues to innovate to enhance its systems and procedures.

To conduct the case study, an online training session was conducted with the relevant staff of organization A, and we went over the SSEHCET and all of its layers in detail. After training, the respondents were given the questionnaire, and they were requested to fill it out based on what they had learned about the SSEHCET and how they felt about it. The questionnaire consists of 20 questions (As shown in Table 1), from which ten questions were related to security, four questions were related to usability, three questions were related to user satisfaction, and three questions were related to the structure of SSEHCET. The answers to each question were given on a five-point Likert scale, which lets respondents say

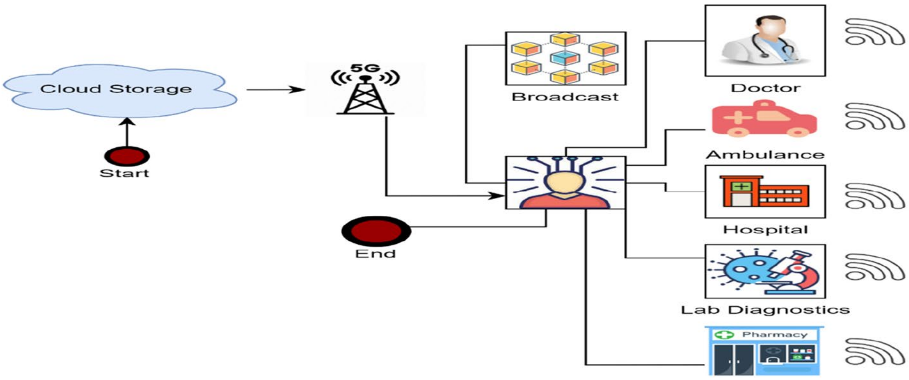

Fig. 9 Working of the healthcare community layer

Table 1 Questions for SSEHCET Evaluation

Security
1. SA replicated in smartphones, edge devices, and the cloud can protect EHR from malicious assault
2. The SSEHCET overcomes the computational constraints of IoT devices using the Edge layer
3. The BCM, which is implemented on the edge layer, provides quicker processing and more security
4. Access control support using Blockchain improves security at the storage layer
5. Inserting aberrant medical data from patients into a customized Blockchain improves security
6. The use of Blockchain to store environmental parameters and event occurrence improves security at several levels
7. BCM ensures data integrity
8. A DTL duplicated across numerous servers prevents tampering with a record
9. Registration of SA performance parameters on the Blockchain improves security
10. Various Smart contracts for processing EHR prevent a record from being tampered with
Ease of learning
1. The practices/technologies recommended for each layer of *SSEHCET* are simple to grasp.
2. *SSEHCET* helps to assess organizations' willingness to secure the transmission of EHR
3. *SSEHCET* is easy to understand and unambiguous
4. Some training is required for the use of *SSEHCET*
User Satisfaction
1. *SSEHCET* is general and can be applied to most healthcare organizations providing eHealth
2. Using *SSEHCET* would identify vulnerabilities in the company regarding the secure transmission of EHR
3. The user will trust on eHealth system more if *SSEHCET* is applied by the healthcare organization
The structure of SSEHCET
1. All the layers of *SSEHCET* are self-explanatory
2. The idea of the *SSEHCET* is applicable in the healthcare industry
3. The distribution of technologies at various layers is useful

how much they agree or disagree with a statement: (1) Strongly disagree; (2) Disagree; (3) Neither agree nor disagree; (4) Agree; and (5) Strongly agree.

The Likert scale was utilized in the survey, and the mean and the degree of agreement for each question were determined. The weighted average was used to calculate the degree of agreement, as shown in Table 2.

The four topics of the questionnaire were examined for validity and reliability (Alpha Cronbach) in order to ensure the accuracy of the assertions included within each theme. A pilot study was done with five professionals to determine the internal consistency of the items/questions within each of the four categories before the survey was given to the respondents of organization A. The survey's reliability was checked by gauging the items' internal consistency using Cronbach's alpha. It measures internal consistency on a standard scale from 0 to 1. It is a common metric used by analysts in the process of developing and validating a new Survey [67–70]. The value of Cronbach's alpha for each category is shown in column 4 of Table 3. The formula in Eq. 1 was used to calculate the values of Cronbach's alpha for each theme of the survey based on the results of a pilot study

Table 2 Degree of agreement for each question based on the weighted average

Weighted average value	Degree of agreement
Less than 2	**Very Low**
From 2 to less than 3	**Low**
From 3 to less than 3.5	**Average**
From 3.5 to less than 4.5	**High**
Greater than or equal to 4.5	**Very High**

$$\propto = \left(\frac{k}{k-1}\right)\left(\frac{s_y^2 - \sum s_i^2}{s_y^2}\right) \tag{1}$$

where k represents the number of questions in a theme, s_y^2 refers to the variance associated with total scores, s_i^2 represents the variance associated with each item/theme.

The process of calculating Cronbach's alpha involves several steps, as given below:

- Item Selection: Choose a set of items or questions that are intended to measure the same underlying construct or trait. These items should be related to each other in concept.
- Data Collection: Administer the items to a sample of participants. Each participant provides responses to all the items.

Table 3 Survey questions reliability testing using Cronbach's alpha

Theme	Titles of the themes of the questionnaire	Number of items in each theme	$\propto$ Cronbach reliability coefficient
First	Security	10	0.90
Second	Ease of learning	4	0.93
Third	User Satisfaction	3	0.87
Fourth	The structure of SSEHCET	3	0.89

- Data Preparation: Organize the responses in a matrix, where each row represents a participant, and each column represents a specific item.
- Compute Average Scores: Calculate the average score for each participant across all items. This will result in a column of average scores.
- Compute Variance: Calculate the variance of the total scores across all participants. This provides an indication of the variability in the responses.
- Compute Covariance: Calculate the covariance between each item and the total score. This represents how each item varies with the overall score.
- Compute Cronbach's Alpha: Use the formula of Eq. (1) to calculate Cronbach's alpha:
- Interpretation: Cronbach's alpha ranges from 0 to 1. A higher alpha value indicates greater internal consistency. Generally, a value above 0.70 is considered acceptable, but the acceptable threshold may vary depending on the context.

It's important to note that while Cronbach's alpha is widely used, it has limitations, and researchers should consider other factors such as item content, scale length, and the specific context of the study when interpreting the results.

Twenty-five people from different areas of healthcare belonging to organization A took part in the case study and filled out the questionnaire. During the online session, the questionnaire was filled out so any questions from the respondents could be answered at the same time. All the responses received were compiled into an excel sheet for analysis. Only the percentage of strongly agree and agree was considered for each question. The weighted average of the agreement percentage was calculated based on Table 2. The individual results of the four themes are presented in Table 3 in the next section.

Results and discussion

This section provides the results of the case study against the four themes mentioned in Table 3. It will also provide the strengths and weaknesses of SSEHCET, as mentioned by the case study participant, along with suggestions for improvement.

Security evaluation of SSEHCET

The questionnaire given to the case study's participants consists of ten questions related to the security of SSEHCET. The respondents were asked to evaluate these questions based on their understanding of SSEHCET. The percentage of strongly agree and agree was considered only to calculate the weighted average of each question. Figure 10 shows the results of the security evaluation of SSEHCET. The weighted average of above 3.5 shows that the percentage of agreement is high. The threshold value was set to 3.5; the results of Fig. 10 show that the weighted average of each security question is above the threshold value. This shows that SSEHCET helps to improve the security of healthcare data transmission and storage.

Ease of learning/usability evaluation of SSEHCET

The questionnaire used in the case study involved four questions related to the ease of learning and usability evaluation of SSEHCET. The weighted average of all four questions was above 3.5, which shows that the proposed model can be learned easily after a few hours of training. The results shown in Fig. 11 highlight the positive elements of the ease of learning connected with SSEHCET. This evaluation was conducted using a well-designed questionnaire consisting of four relevant items. A weighted average score over 3.5 suggests a favorable trend, indicating that users find SSEHCET to be readily learnable, especially after a few hours of training. This favorable evaluation is in accordance with our design principles, which prioritize user-friendly interfaces and intuitive interactions at all levels of the framework. The strong user satisfaction, especially in terms of ease-of-use, confirms SSEHCET's dedication to provide a smooth and easily accessible experience, further affirming its potential for universal acceptance in many healthcare environments. The findings derived from the study of the questionnaire greatly enhance our comprehension of SSEHCET's usability, highlighting its user-centered design and efficacy in practical scenarios.

User satisfaction evaluation of SSEHCET

In this subject of the questionnaire, the respondents were questioned about the degree of user satisfaction and confidence in the eHealth application if SSEHCET is completely implemented by healthcare organizations providing eHealth services. The respondents included in the case study were aware of the shortcomings which hamper the planned adoption of eHealth. According to respondents, financial, legal, societal, and ethical impediments inhibit the proper adoption of eHealth. However, they all agreed that the security of EHR is a critical

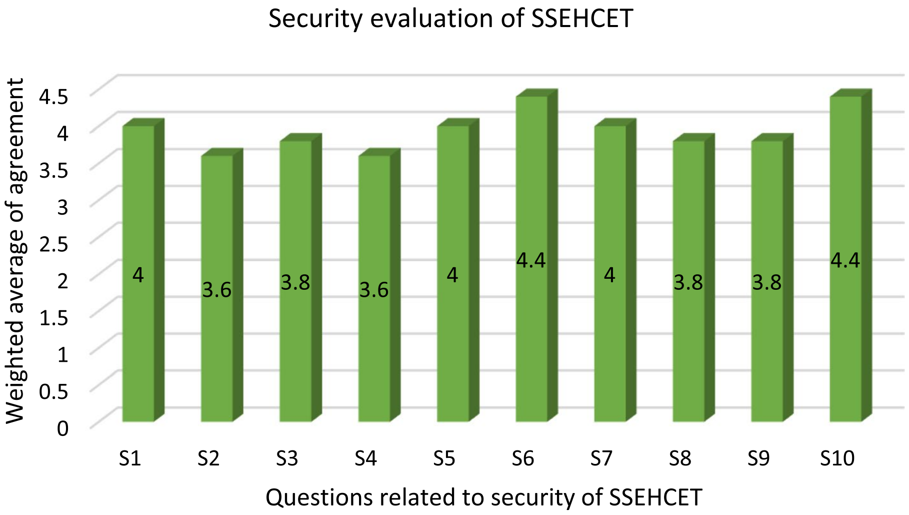

Fig. 10 Security evaluation of SSEHCET

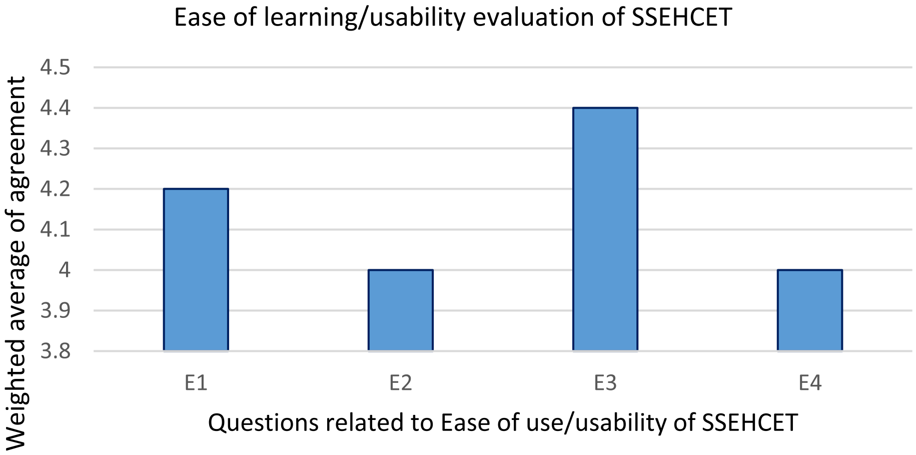

Fig. 11 Ease of learning/usability evaluation of SSEHCET

concern, owing to the low user acceptance of eHealth. The case study results related to user satisfaction for SSEHCET are given in Fig. 12.

According to the statistics of Fig. 12, the weighted average score for each question was more than 3.5. This shows that the successful implementation of SSEHCET will improve users' trust in eHealth.

SSEHCET structure evaluation

The case study allowed us to examine SSDMM's applicability in a real-world setting. The respondents of the case study were also asked to evaluate the structure of SSEHCET. The evaluation of structure involves three dimensions: self-explanatory, applicable, and the distribution of technologies at various layers.

According to the statistics presented in Fig. 13, the weighted average score for each question related to the SSEHCET structure was more than 3.5. This shows that the proposed SSEHCET is self-explanatory and applicable, and the division of technologies at various layers of SSEHCET is useful for the security and adoption of eHealth.

Strengths and weaknesses of the SSEHCET

The respondents involved in the case study were asked to mention the strengths and weaknesses of SSEHCET

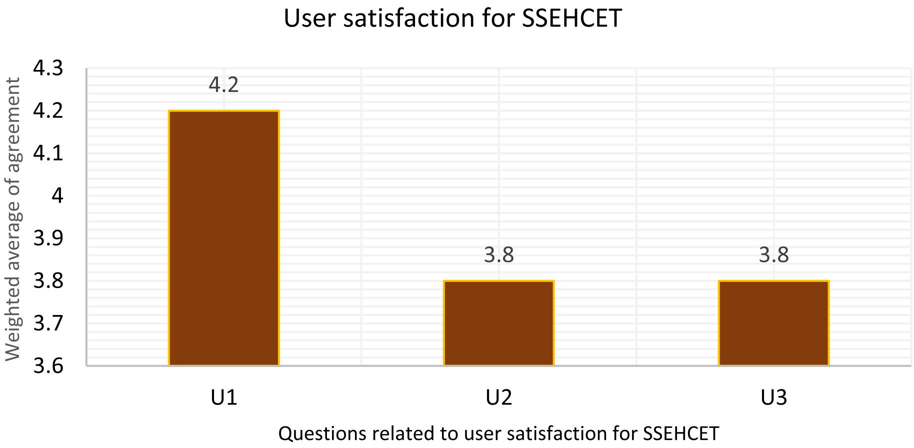

Fig. 12 User satisfaction for SSEHCET

based on their understanding of SSEHCET. According to respondents, SSEHCET is touching the most sensitive areas of security, and it can make a tremendous impact on the eHealth sector and will noticeably help avoid risk beyond accepted thresholds. The explicit strengths and weaknesses mentioned by the respondents are listed below.

Strengths:

- Clarity of the proposed model and ease of implementation
- Highlight the most critical points related to eHealth security
- Efficient and has a very low cost
- Defines and suggests a new way to conduct security assessments of eHealth organizations.
- The large surface of applicability as it can be implemented by different healthcare organizations

Weaknesses:

- 5G service is not accessible nationwide, especially in developing countries
- Although the proposed model addresses various issues faced by eHealth, legal and financial issues still remain an important concern in the growth of eHealth.

Suggestion for improvement of SSEHCET

According to the respondents of the case study, the suggested methodology is a straightforward and trustworthy method for enhancing eHealth security. Still, one of the recommendations that might enhance the model having this model in a word document can be misleading. Consequently, one option that may be improved is to create a prototype of the suggested model via simulation, which

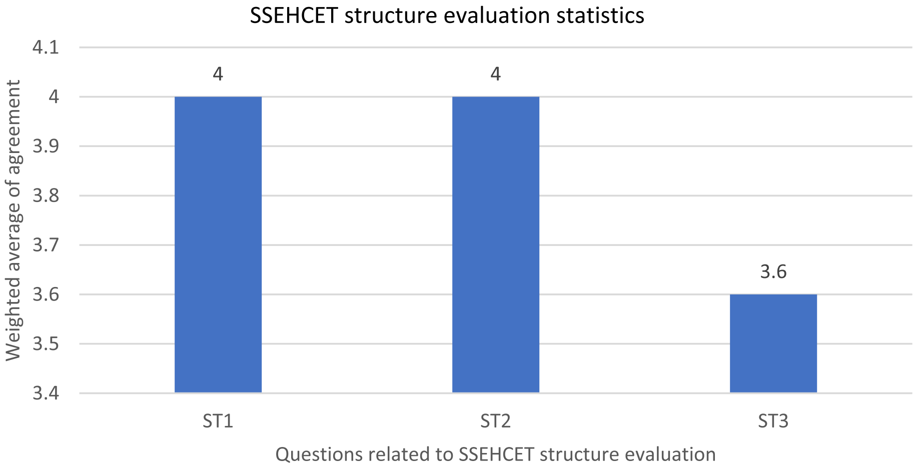

Fig. 13 SSEHCET structure evaluation

may assist eHealth stakeholders in better comprehending the use of SSEHCET.

Comparative analysis with existing studies

The proposed SSEHCET framework introduces a novel and comprehensive approach to address the critical challenges associated with security in eHealth applications. While existing studies often focus on specific aspects of security in healthcare, such as data transmission or storage, SSEHCET stands out by providing end-to-end security across all layers of the framework. The integration of cutting-edge technologies, including IoT, 5G, mobile edge computing, and Blockchain Technologies (BCT), contributes to a holistic and secure ecosystem for the transmission and storage of patient data. Notably, the Smart Agent (SA) program, leveraging the potential of BCT, ensures the protection of patients' privacy during data outsourcing, marking a distinctive feature of the proposed model. The framework's empirical validation through a meticulous evaluation, including security, ease of use, and user satisfaction, along with a real-world case study, further demonstrates its unique and impactful contribution to advancing the security paradigm in modern eHealth landscapes. Below, we provide a comparison of the proposed study with the latest studies to highlight the uniqueness and novelty of the proposed system further.

Comparison with study [57]

Our study and study [57] both focus on the use of advanced technology, including Blockchain, in healthcare applications. Nevertheless, they vary in terms of their emphasis, approaches, and particular implementations within the eHealth field. Here, we provide the similarities and differences between the two studies. We will start by giving a summary of each study and then proceed to compare them.

- The proposed framework (SSEHCET): SSEHCET prioritizes the use of blockchain technology to provide safe transfer of data in the healthcare sector, with a special focus on resolving issues connected to storing data from IoT devices. The proposed SSEHCET integrates advanced technologies such as IoT, 5G, mobile edge computing, and Blockchain. These technologies are structured into six layers to enable safe communication and privacy in healthcare applications. The architecture categorizes many levels, including Sensing, Edge, Communication, Storage, Security, and Healthcare Community, to provide a systematic way for managing medical data. The use of Smart Agent (SA) software replicated at all levels emphasizes a commitment to ensuring patient privacy when data is outsourced.
- The Paper [57]: Privacy-Preserving Diagnostic Enhancement Strategy for e-Health Platforms: The main objective of Paper [58] is to tackle the difficulties related to data privacy in eHealth platforms. It specifically emphasizes the use of blockchain technology to improve diagnostic techniques. The study investigates the capacity of blockchain technology to enable the secure sharing of health data, with a focus on ensuring data integrity and safeguarding privacy. It introduces a robust access control system on the Health-chain, enabling data owners to define access restrictions for their privacy-sensitive medical data. This system empowers users to have more control over managing their information. Thus, article [57] provides a comprehensive empirical analysis, evaluating the Blockchain's efficiency in terms of computation, time efficiency, and resilience against security attacks.

Comparison of the proposed framework with Paper [57]

- Shared Perspective: Both studies acknowledge the significance of blockchain technology in augmenting security and privacy in healthcare applications.
- Differences: Our article presents a comprehensive architecture that ensures safe communication and data management in many healthcare situations. In contrast, article [58] focuses on a single application, namely diagnostic improvement, and highlights the importance of user-controlled access using blockchain technology.

Comparison with study [58]

Commonalities:

- Privacy concerns are recognized by both SSEHCET and Paper [58] as being substantial in healthcare applications. Their objective is to bolster the security of patient data in response to advancing technology.
- Technological Integration: Both studies include state-of-the-art technology in their frameworks. SSEHCET utilizes IoT, 5G, mobile edge computing, and blockchain technology. In contrast, Paper [58] integrates deep learning and multi-agent systems to tackle privacy issues.

- Security measures: Both SSEHCET and Paper [58] use security measures to guarantee the confidentiality, integrity, and availability of patient data. SSEHCET does this by using a replicated Smart Agent program, whereas Paper [58] utilizes privacy measures based on many agents for instantaneous assessment.

Contrasts:

- Focus on technology: SSEHCET prioritizes a complete framework that emphasizes safe communication and data management in many healthcare situations. The focus of the Paper [58] is the amalgamation of deep learning and multi-agent systems, with a special emphasis on enhancing e-healthcare applications and diagnostic accuracy.
- Extent and Usage: SSEHCET offers a comprehensive and all-encompassing structure that may be used in many healthcare situations, with a particular focus on ensuring the secure transfer of data. The Paper [58] discusses the use of deep learning to enhance the process of diagnosing and treating medical conditions. It explores the employment of multi-agent systems to ensure the security of e-healthcare applications.
- Access Control Mechanism: SSEHCET utilizes a replicated Smart Agent software at several levels to ensure the protection of patient confidentiality when data is outsourced. The Paper [58] presents a multi-agent system that is developed to oversee and regulate access to patients' data by assigning distinct roles and permissions.

Main Benefits:

- SSEHCET prioritizes privacy by implementing a well-organized architecture, and the replicated Smart Agent program guarantees the safety of data during transmission and storage. The article [58] emphasizes the benefits of a secure system for e-healthcare applications, the ability to identify possible privacy breaches in real-time, and enhanced accuracy in diagnoses achieved by deep learning.

Although SSEHCET and Paper [58] both address privacy problems in e-healthcare, they vary in terms of their technical focus, extent, and regions of implementation. SSEHCET offers a wide-ranging and inclusive structure, whereas Paper [58] focuses on using deep learning and multi-agent systems to improve diagnostics in e-healthcare applications. The selection between the two options would be contingent upon unique healthcare needs, which span from ensuring the safe transmission of data in various situations (SSEHCET) to incorporating deep learning for enhanced diagnostic precision (Paper [58]).

Comparison of the proposed framework with paper [59]

Commonalities:

- Blockchain Integration: SSEHCET and Paper 64 both aim to use blockchain technology to improve security and governance in healthcare data management. They acknowledge the capacity of blockchain technology to provide immutability, security, and user autonomy in managing stored information.
- Both articles discuss the difficulties faced in the healthcare industry. SSEHCET prioritizes the establishment of secure communication and data management in healthcare applications. At the same time, Paper [59] especially addresses the shift from paper-based medical records to electronic health records (EHRs), with a particular emphasis on the safe storage and administration of data.
- Security and privacy are given high importance in both articles, particularly in relation to healthcare data. SSEHCET integrates Smart Agent software to safeguard privacy. Paper [63] strives to improve the secure exchange and storage of electronic health information while guaranteeing the security, privacy, and accuracy of medical records.

Contrasts:

- Extent and Usage: SSEHCET offers a complete framework that may be used in many healthcare situations, including secure communication and data management. Paper [59] focuses on the difficulties present in existing electronic health record (EHR) frameworks. Its goal is to develop a blockchain-based EHR framework that is compatible with both national and international EHR standards.
- Emphasis on Interoperability: SSEHCET does not prioritize interoperability but instead stresses a comprehensive strategy to ensure the safe management of healthcare data. On the other hand, Paper [59] specifically addresses problems related to the capacity of different blockchain-based electronic health record (EHR) frameworks to function together in accordance with established EHR standards at both national and international levels.
- Approach: SSEHCET's approach entails presenting a comprehensive framework and doing a thorough assessment that covers security, user-friendliness, and user contentment. Paper [59] utilizes a methodical examination of existing literature to investi-

gate the current status of electronic health records (EHRs), specifically focusing on implementations that include blockchain technology. The objective is to identify and outline the challenges and specifications related to interoperability.

SSEHCET and Paper [59] both acknowledge the potential of Blockchain for safeguarding healthcare data, but they have distinct differences in terms of their scope and emphasis. SSEHCET provides a thorough system for securely managing data in different healthcare situations, with Paper [63] notably focusing on the difficulties in electronic health record systems and highlighting the need for interoperability according to national and international standards. The selection between the two options would rely on unique healthcare needs, whether a comprehensive strategy for ensuring data security and management (SSEHCET) or a focused solution for compatible electronic health record systems (Paper [59]).

Conclusion and Future work

The use of cutting-edge technologies in healthcare is rapidly expanding, but eHealth adoption is still below expectations. Lack of security, ineffectiveness, and higher costs are some of the obstacles preventing the general public from adopting eHealth. To overcome these challenges, SSEHCET, a smart and secure eHealth framework that capitalizes on the capabilities of cutting-edge technologies, is proposed. The proposed SSEHCET has six layers: 1) The Sensing layer, which includes IoT sensors that are often situated on or inside patients' bodies and transfer data to smartphones. 2) The edge layer, which comprises components that gather data near IoT devices. 3) The communication layer makes use of the capabilities of 5G technology to send patient data across many levels effectively. 4) Cloud servers or other powerful computers comprise the storage layer. 5) A security layer that uses BCT to transmit and retain patient data securely. 6) Healthcare practitioners and institutions comprise the healthcare community layer. Smart Agent (SA) software was used on layers for the processing of medical data and to provide secure communication. To demonstrate the feasibility of the SSEHCET in improving eHealth security and efficiency, a case study with a well-known eHealth organization was conducted. SSEHCET surpasses previous research by presenting a holistic framework that tackles end-to-end security in eHealth applications. This framework incorporates advanced technologies, including IoT, 5G, mobile edge computing, and Blockchain. The Smart Agent (SA) software, which is unique to this system, guarantees patient privacy when data is outsourced, making it a notable characteristic. The empirical validation and real-world case study provide evidence of the framework's distinctive and significant contribution, distinguishing it from other research that may concentrate on certain components or applications within the eHealth field.

Acknowledgements
This work was funded by the Deanship of Scientific Research at Jouf University through the Fast-track Research Funding Program.

Institutional review board statement
Not applicable.

Informed consent statement
Not applicable.

Authors' contributions
Mamoona Humayun: Conceptualization, data collection & analysis, writing original draft, funding acquisition
Amjad Alserhani: Data collection & analysis, Project adminstration
Faeiz serhani: Writing review & editing, data collection
Momina shaheen: Supervision, visualization
Ghadah Naif Alwakid: Visualization and data analysis.

Funding
This work is funded by the Deanship of Scientific Research at Jouf University.

Availability of data and materials
No datasets were generated or analysed during the current study.

Declarations

Competing interests
The authors declare no competing interests.

Received: 13 December 2023 Accepted: 25 January 2024
Published online: 08 February 2024

References

1. Singh A, Chatterjee K (2023) Edge computing based secure health monitoring framework for electronic healthcare system. Cluster Comput 26:1205–1220
2. Yadav H, Shah D, Sayed S, Horton S, Schroeder LF (2021) Availability of essential diagnostics in ten low-income and middle-income countries: results from national health facility surveys. Lancet Glob Health 9:e1553–e1560
3. Zegeye B, El-Khatib Z, Ameyaw EK, Seidu A-A, Ahinkorah BO, Keetile M et al (2021) Breaking barriers to healthcare access: a multilevel analysis of individual-and community-level factors affecting women's access to healthcare services in Benin. Int J Environ Res Public Health 18:750
4. Penedo FJ, Oswald LB, Kronenfeld JP, Garcia SF, Cella D, Yanez B (2020) The increasing value of eHealth in the delivery of patient-centred cancer care. Lancet Oncol 21:e240–e251
5. Triberti S, Savioni L, Sebri V, Pravettoni G (2019) eHealth for improving quality of life in breast cancer patients: a systematic review. Cancer Treat Rev 74:1–14
6. Schreiweis B, Pobiruchin M, Strotbaum V, Suleder J, Wiesner M, Bergh B (2019) Barriers and facilitators to the implementation of eHealth services: systematic literature analysis. J Med Internet Res 21:e14197
7. Maramba I, Chatterjee A, Newman C (2019) Methods of usability testing in the development of eHealth applications: a scoping review. Int J Med Informatics 126:95–104

8. Bhagyoday R, Kamani C, Bhojani D, Parmar V (2019) Comprehensive study of E-Health security in cloud computing. Int Res J Eng Technol 6(11):1216–1228
9. Sahi A, Lai D, Li Y (2021) A review of the state of the arts in privacy and security in the eHealth cloud. IEEE Access 9:104127–104141. https://doi.org/10.1109/ACCESS.2021.3098708
10. Al-Issa Y, Ottom MA, Tamrawi A (2019) eHealth cloud security challenges: a survey. J Healthc Eng. 2019:7516035
11. Uddin MA, Stranieri A, Gondal I, Balasubramanian V (2020) Blockchain leveraged decentralized IoT eHealth framework. Internet of Things 9:100159
12. Alenoghena CO, Onumanyi AJ, Ohize HO, Adejo AO, Oligbi M, Ali SI et al (2022) eHealth: A survey of architectures, developments in mHealth, security concerns and solutions. Int J Environ Res Public Health 19:13071
13. Hasan K, Chowdhury MJM, Biswas K, Ahmed K, Islam MS, Usman M (2022) A blockchain-based secure data-sharing framework for Software Defined Wireless Body Area Networks. Comput Netw 211:109004
14. Morales-Sandoval M, De-La-Parra-Aguirre R, Galeana-Zapién H, Galaviz-Mosqueda A (2021) A three-tier approach for Lightweight data security of body area networks in E-health applications. IEEE Access 9:146350–146365
15. Majeed JH, Aish Q (2021) A remote patient monitoring based on WBAN implementation with internet of thing and cloud server. Bulletin of Electrical Engineering and Informatics 10:1640–1647
16. Hussain SJ, Irfan M, Jhanjhi N, Hussain K, Humayun M (2021) Performance enhancement in wireless body area networks with secure communication. Wireless Pers Commun 116:1–22
17. Jabeen T, Ashraf H, Ullah A (2021) A survey on healthcare data security in wireless body area networks. J Ambient Intell Humaniz Comput 12:9841–9854
18. Zhang P, White J, Schmidt DC, Lenz G, Rosenbloom ST (2018) FHIRChain: applying blockchain to securely and scalably share clinical data. Comput Struct Biotechnol J 16:267–278
19. Kitanov S, Janevski T (2019) Introduction to fog computing. In: The Rise of Fog Computing in the Digital Era. IGI Global, p 1–35. https://doi.org/10.4018/978-1-5225-6070-8.ch001
20. Naeem RZ, Bashir S, Amjad MF, Abbas H, Afzal H (2019) Fog computing in internet of things: Practical applications and future directions. Peer-to-Peer Networking and Applications 12:1236–1262
21. Puthal D, Mohanty SP, Bhavake SA, Morgan G, Ranjan R (2019) Fog computing security challenges and future directions [energy and security]. IEEE Consumer Electronics Magazine 8:92–96
22. Caprolu M, Di Pietro R, Lombardi F, Raponi S (2019) "Edge computing perspectives: architectures, technologies, and open security issues," in. IEEE International Conference on Edge Computing (EDGE) 2019:116–123
23. Liyanage M, Porambage P, Ding AY, Kalla A (2021) Driving forces for multi-access edge computing (MEC) IoT integration in 5G. ICT Express 7:127–137
24. Maray M, Shuja J (2022) Computation offloading in mobile cloud computing and mobile edge computing: survey, taxonomy, and open issues. Mob Inf Syst 2022:Article ID 1121822. https://doi.org/10.1155/2022/1121822
25. do Prado PF et al (2021) Mobile Edge Computing for Content Distribution and Mobility Support in Smart Cities. In: Mukherjee A, De D, Ghosh SK, Buyya R (eds) Mobile Edge Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-69893-5_19
26. Singh A, Satapathy SC, Roy A, Gutub A (2022) Ai-based mobile edge computing for iot: applications, challenges, and future scope. Arab J Sci Eng 47:9801–9831
27. Fazeldehkordi E, Grønli T-M (2022) A Survey of Security Architectures for Edge Computing-Based IoT. IoT 3:332–365
28. Javed L, Yakubu BM, Waleed M, Khaliq Z, Suleiman AB, Mato NG (2022) BHC-IoT: A Survey on Healthcare IoT Security Issues and Blockchain-Based Solution. International Journal of Electrical and Computer Engineering Research 2:1–9
29. Dhanvijay MM, Patil SC (2019) Internet of Things: A survey of enabling technologies in healthcare and its applications. Comput Netw 153:113–131
30. Qu Y, Zheng G, Ma H, Wang X, Ji B, Wu H (2019) A survey of routing protocols in WBAN for healthcare applications. Sensors 19:1638
31. Dutta Pramanik PK, Nayyar A, Pareek G (2019) Chapter 7 - WBAN: Driving e-healthcare Beyond Telemedicine to Remote Health Monitoring: Architecture and Protocols. In: Jude HD, Balas VE (eds) Telemedicine Technologies. Academic Press, p 89–119. https://doi.org/10.1016/B978-0-12-816948-3.00007-6. ISBN 9780128169483
32. Ren Y, Leng Y, Zhu F, Wang J, Kim H-J (2019) Data storage mechanism based on blockchain with privacy protection in wireless body area network. Sensors 19:2395
33. Asam M, Jamal T, Ajaz A, Haider Z, Butt SA (2019) Security Issues in WBANs. arXiv preprint arXiv: 1911.04330. https://doi.org/10.48550/arXiv.1911.04330
34. Nandikanti A, Sahu KN, Panigrahi S (2023) Security issues and solutions for reliable WBAN-based e-Healthcare systems: a systematic review. The 1st International Conference on International Conference on Ambient Intelligence in Health Care (ICAIHC-2022)
35. Yaghoubi M, Ahmed K, Miao Y (2022) Wireless Body Area Network (WBAN): A Survey on Architecture, Technologies, Energy Consumption, and Security Challenges. J Sens Actuator Netw 11:67
36. Dave R, Seliya N, Siddiqui N (2021) The benefits of edge computing in healthcare, smart cities, and IoT. arXiv preprint arXiv: 2112.01250. https://doi.org/10.48550/arXiv.2112.01250
37. Li X, Huang X, Li C, Yu R, Shu L (2019) EdgeCare: Leveraging edge computing for collaborative data management in mobile healthcare systems. IEEE Access 7:22011–22025
38. Ray PP, Dash D, De D (2019) Edge computing for Internet of Things: A survey, e-healthcare case study and future direction. J Netw Comput Appl 140:1–22
39. Dash S, Biswas S, Banerjee D, Rahman AU (2019) Edge and fog computing in healthcare–A review. Scalable Computing: Practice and Experience 20:191–206
40. Rahmani AM, Gia TN, Negash B, Anzanpour A, Azimi I, Jiang M et al (2018) Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. Futur Gener Comput Syst 78:641–658
41. Unal D, Bennbaia S, Catak FO (2022) Chapter 12 - Machine learning for the security of healthcare systems based on Internet of Things and edge computing. **Qatar National Research Fund. In: Moustafa AA (ed) Cybersecurity and Cognitive Science. Academic Press, p 299–320. https://doi.org/10.1016/B978-0-323-90570-1.00007-3. ISBN 9780323905701
42. Humayun M, Jhanjhi NZ, Niazi M, Amsaad F, Masood I (2022) Securing Drug Distribution Systems from Tampering Using Blockchain. Electronics 11:1195
43. Humayun M, Jhanjhi N, Alamri M (2020) Smart secure and energy efficient scheme for e-health applications using IoT: a review. International Journal of Computer Science and Network Security 20:55–74
44. Griggs KN, Ossipova O, Kohlios CP, Baccarini AN, Howson EA, Hayajneh T (2018) Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J Med Syst 42:1–7
45. Chen Y, Ding S, Xu Z, Zheng H, Yang S (2019) Blockchain-based medical records secure storage and medical service framework. J Med Syst 43:1–9
46. Brogan J, Baskaran I, Ramachandran N (2018) Authenticating health activity data using distributed ledger technologies. Comput Struct Biotechnol J 16:257–266
47. Gordon WJ, Catalini C (2018) Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. Comput Struct Biotechnol J 16:224–230
48. Dwivedi AD, Srivastava G, Dhar S, Singh R (2019) A decentralized privacy-preserving healthcare blockchain for IoT. Sensors 19:326
49. Gaetani E, Aniello L, Baldoni R, Lombardi F, Margheri A, Sassone V (2017) Blockchain-based database to ensure data integrity in cloud computing environments. Italian Conference on Cybersecurity. Venice, 17–20 Jan 2017
50. Alonso SG, Arambarri J, López-Coronado M, de la Torre Díez I (2019) Proposing new blockchain challenges in ehealth. J Med Syst 43(3):64
51. Huang H, Sun X, Xiao F, Zhu P, Wang W (2021) Blockchain-based eHealth system for auditable EHRs manipulation in cloud environments. Journal of Parallel and Distributed Computing 148:46–57
52. Rifi N, Rachkidi E, Agoulmine N, Taher NC (2017) Towards using blockchain technology for eHealth data access management. 2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME); 19–21 October 2017. Beirut, Lebanon. https://doi.org/10.1109/ICABME.2017.8167555
53. Hyla T, Pejaś J (2019) eHealth integrity model based on permissioned blockchain. Future Internet 11:76
54. Benil T, Jasper J (2020) Cloud based security on outsourcing using blockchain in E-health systems. Comput Netw 178:107344

55. Nguyen DC, Pathirana PN, Ding M, Seneviratne A (2019) Blockchain for secure ehrs sharing of mobile cloud based e-health systems. IEEE access 7:66792–66806
56. Dakhel M, Hassan S (2020) A Secure Wireless Body Area Network for E-Health Application Using Blockchain. In: Khalaf M, Al-Jumeily D, Lisitsa A (eds) Applied Computing to Support Industry: Innovation and Technology. ACRIT 2019. Communications in Computer and Information Science, vol 1174. Springer, Cham. https://doi.org/10.1007/978-3-030-38752-5_31
57. Alsuqaih HN, Hamdan W, Elmessiry H, Abulkasim H (2023) An efficient privacy-preserving control mechanism based on blockchain for E-health applications. Alexandria Engineering Journal 73:159–172
58. Dhasarathan C, Shanmugam M, Kumar M et al (2024) A nomadic multi-agent based privacy metrics for e-health care: a deep learning approach. Multimed Tools Appl 83:7249–7272. https://doi.org/10.1007/s11042-023-15363-4
59. Reegu FA, Abas H, Gulzar Y, Xin Q, Alwan AA, Jabbari A, Sonkamble RG, Dziyauddin RA (2023) Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System. Sustainability 15(8):6337
60. Qi L, Liu Y, Zhang Y, Xu X, Bilal M, Song H (2022) Privacy-Aware Point-of-Interest Category Recommendation in Internet of Things. IEEE Internet of Things Journal. 9(21):21398–21408. https://doi.org/10.1109/JIOT.2022.3181136
61. Liu Y, Zhou X, Kou H, Zhao Y, Xu X, Zhang X et al (2023) Privacy-preserving point-of-interest recommendation based on simplified graph convolutional network for geological traveling. AACM Transactions on Intelligent Systems and Technology. https://doi.org/10.1145/3620677. Accepted on August 2023
62. Hussain I, Tahir S, Humayun M, Almufareh MF, Jhanjhi NZ, Qamar F (2022) Health Monitoring System Using Internet of Things (IoT) Sensing for Elderly People. 2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS). Karachi, p 1–5. https://doi.org/10.1109/MACS56771.2022.10023026
63. Yin RK (2011) Applications of Case Study Research. Sage, Newbury Park, CA, USA
64. Cho H, Yen P-Y, Dowding D, Merrill JA, Schnall R (2018) A multi-level usability evaluation of mobile health applications: A case study. J Biomed Inform 86:79–89
65. Mans RS, Schonenberg M, Song M, van der Aalst WM, Bakker PJ (2008) Application of process mining in healthcare–a case study in a dutch hospital. International joint conference on biomedical engineering systems and technologies. p 425–438. Virtual Event, February 9–11, 2022
66. Palos-Sánchez P, Saura JR, Álvarez-García J (2019) Innovation and creativity in the mobile applications industry: a case study of mobile health applications (e-Health Apps) in Cultural and Creative Industries, ed: Springer 121–135
67. Sullivan GM (2011) A primer on the validity of assessment instruments. J Grad Med Educ 3(2):119–120
68. Chan LL, Idris N (2017) Validity and reliability of the instrument using exploratory factor analysis and Cronbach's alpha. International Journal of Academic Research in Business and Social Sciences 7:400–410
69. Alhasan A, Audah L, Ibrahim I, Al-Sharaa A, Al-Ogaili AS, M. Mohammed, J (2022) A case-study to examine doctors' intentions to use IoT healthcare devices in Iraq during COVID-19 pandemic. Int J Pervasive Comput Commun 18(5):527–547. https://doi.org/10.1108/IJPCC-10-2020-0175
70. Vasset F, Marnburg E, Furunes T (2011) The effects of performance appraisal in the Norwegian municipal health services: a case study. Hum Resour Health 9:1–12

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.