


## Review Article

# Towards Smart Healthcare: Patient Data Privacy and Security in Sensor-Cloud Infrastructure

Isma Masood <sup>1</sup>, Yongli Wang,<sup>1</sup> Ali Daud,<sup>2</sup> Naif Radi Aljohani,<sup>3</sup> and Hassan Dawood<sup>4</sup>

<sup>1</sup>School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210000, China

<sup>2</sup>Department of Computer Science and Software Engineering, International Islamic University, Islamabad 44000, Pakistan

<sup>3</sup>Faculty of Computing and Information Technology, King Abdulaziz University Jeddah, 21432, Saudi Arabia

<sup>4</sup>Department of Software Engineering, University of Engineering and Technology, Taxila 47070, Pakistan

Correspondence should be addressed to Isma Masood; [isma\\_masood@njust.edu.cn](mailto:isma_masood@njust.edu.cn)

Received 16 July 2018; Revised 13 October 2018; Accepted 22 October 2018; Published 4 November 2018

Guest Editor: Georgios Kambourakis

Copyright © 2018 Isma Masood et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Nowadays, wireless body area networks (WBANs) systems have adopted cloud computing (CC) technology to overcome limitations such as power, storage, scalability, management, and computing. This amalgamation of WBANs systems and CC technology, as sensor-cloud infrastructure (S-CI), is aiding the healthcare domain through real-time monitoring of patients and the early diagnosis of diseases. Hence, the distributed environment of S-CI presents new threats to patient data privacy and security. In this paper, we review the techniques for patient data privacy and security in S-CI. Existing techniques are classified as multibiometric key generation, pairwise key establishment, hash function, attribute-based encryption, chaotic maps, hybrid encryption, Number Theory Research Unit, Tri-Mode Algorithm, Dynamic Probability Packet Marking, and Priority-Based Data Forwarding techniques, according to their application areas. Their pros and cons are presented in chronological order. We also provide our six-step generic framework for patient physiological parameters (PPPs) privacy and security in S-CI: (1) selecting the preliminaries; (2) selecting the system entities; (3) selecting the technique; (4) accessing PPPs; (5) analysing the security; and (6) estimating performance. Meanwhile, we identify and discuss PPPs utilized as datasets and provide the performance evolution of this research area. Finally, we conclude with the open challenges and future directions for this flourishing research area.

## 1. Introduction

The advancement and application of Wireless Body Area Networks (WBANs) are considered key research areas for improving healthcare quality [1]. Pervasive healthcare monitoring provides rich contextual information to handle the odd conditions of chronically ill patients. Constant monitoring and an early medical response not only increase the life quality of elderly and chronically ill people but also help families and parents by providing high-quality healthcare to their young babies and paralyzed children [1–6]. The importance of the WBANs cannot be very promising, as many applications and prototypes are already in progress. For example, some WBANs are dedicated to continuous observation of cognitive diseases such as Alzheimer's, epilepsy, and Parkinson's disease. Another significant advancement in WBANs is the formation of tiny sensors implanted in the human body or integrated into fabric.

While the importance of WBANs in healthcare is indubitable, the amount of data generated by these sensors is huge and demands more resources in terms of computation, memory, communication power, massive storage infrastructure, energy-efficient performance for processing, real-time monitoring, and data analysis [5, 7–18]. Cloud computing shows very promising progress in hosting the aforementioned resources as services over the Internet [10, 19, 20]. At present, IT professionals extend cloud computing to reduce the complexity and utilization of WBANs' resources. This extension is called S-CI [8, 21–24]. Figure 1 shows a typical S-CI for PPPs monitoring and access.

In S-CI, a large amount of patient data are collected from WBANs and transmitted to cloud servers for scalability, real-time accessibility, storage, and processing capability. Therefore, patient data privacy and security are more challenging due to the distributed environment [25–27]. The motivation

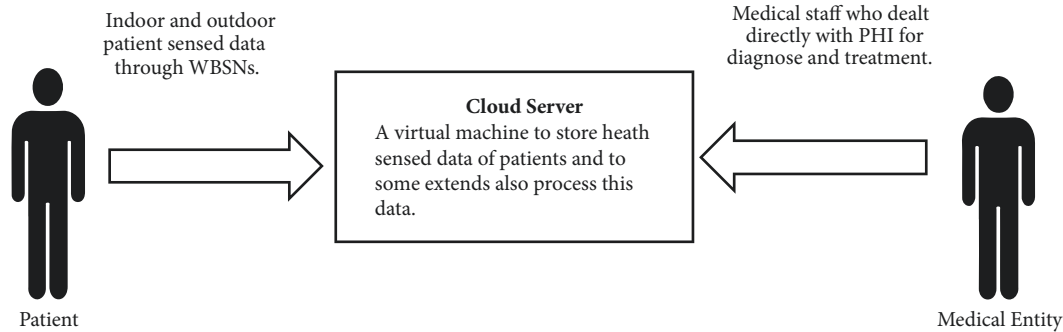


FIGURE 1: S-CI for PPPs monitoring.

for this study is to investigate and organize the existing techniques of S-CI so that the research community can address the vulnerabilities and limitations of PDPS and to identify the need for further work in this domain. Significantly, a number of studies have utilized patient physical parameters (PPPs) as their dataset. However, other studies refer to their dataset as medical data, personal health information (PHI), or electronic health records (EHRs), not clearly mentioning which are PPPs. In this review, we will identify and organize existing solutions to patient data privacy and security in S-CI.

Nowadays, the use and significance of the S-CI in the healthcare domain cannot be denied [28]. At a commercial level, large numbers of applications [8, 29] are already in service: ubiquitous healthcare, Google health, Microsoft Health Vault, and so on. However, the distributed environment of S-CI opens new challenges for patient data privacy and security: data integrity, confidentiality, patient participation in data control, data purpose specification for use limitation, audit control, availability, scalability, data transmission security, network security, source authentication, and so on [30–35]. In 2010, Almedar et al. [1] evaluated the literature to show the state of the art regarding how wireless sensor technology is improving healthcare conditions for patients at home and highlighted issues to bear in mind for future development. Similarly, in 2012, two studies were published. Kumar et al. [32] reviewed the literature to identify security and privacy issues in medical sensor-based applications, while Ameen et al. [36] reviewed the literature on wireless sensor networks and raised major concerns relating to social implications such as security and privacy. Furthermore, in 2013, Alamri et al. [8] investigated sensor-cloud architecture in several applications and discussed the emerging opportunities to handle more complex scenarios in the real world through S-CI. Presently, no comprehensive and organized study is available to address patient data privacy and security in S-CI. The literature shows some significant solutions in different application areas such as mobile healthcare [37–41], electronic healthcare [42–45], health data management [2], and health data aggregation [46]. Hence, the following are the major contributions summarized in this study:

- (1) Detailing the state-of-the-art existing techniques, which gives a roadmap for this innovative research area.

- (2) Providing a classification scheme for existing techniques in order to identify in-depth investigation and limitations of each application domain for better future extension.
- (3) Providing a generic six-step framework for privacy and security of PPPs in S-CI.
- (4) Highlighting future directions, with useful recommendations.

The rest of the paper is organized as follows: Section 2 presents the basic concepts and terminologies, Section 3 explained the method, Section 4 presents the results, Section 5 gives the performance estimation of the techniques, finally, Section 6 highlights the future directions and useful recommendations for this area of interest, and Section 7 concludes this study.

Table 1 provides a list of the abbreviations and notations used in the study.

## 2. Basic Concepts and Terminologies

In this section, we will discuss some important concepts and terminologies relating to patient data privacy and security in S-CI. The concepts and terminologies have evolved according to their level of complexity.

**2.1. UBUNTU Enterprise Cloud.** The general concept of cloud computing is that it is an Internet-based service provided by a third party. This is true for a public cloud, yet there is another type of cloud computing known as private cloud computing whereby an enterprise or an organization hosts its own private cloud. The UBUNTU enterprise cloud is a cloud computing technology that allows an enterprise to build a private cloud on their environment. UBUNTU allows a centrally managed resource pool behind a firewall on a local network. The chief benefits of this technology are as follows: (1) better use of server resources; (2) provision of new cloud images in a short period of time; (3) allowing bursting to public cloud (e.g., Amazon EC2), giving an added level of flexibility and also driving down building and maintenance costs [56].

**2.2. Amazon EC2 IaaS Platform.** The Amazon Elastic Compute Cloud EC2 is an Amazon web service used to access software, servers, and storage resources across the Internet

TABLE I: List of Abbreviations and Notations.

Sr. no	Abbreviations	Description
1	CC	Cloud Computing
2	WBANs	Wireless Body Area Networks
3	S-CI	Sensor Cloud Infrastructure
4	PPPs	Patient Physiological Parameters
5	PDPS	Patient Data Privacy and Security
6	PHI	Personal Health Information
7	EHRs	Electronic Health Records
8	AWS	Amazon Web Services
9	Eucalyptus	Elastic Utility Computing Architecture Linking Your Programs to Useful Systems
10	SP	Social Point
11	CS	Cloud Server
12	WBSs	Wireless Body Sensors
13	TA	Trusted Authority
14	HA	Healthcare Authority
15	$SK_p$	Secret Key
16	$AR_p$	Access Structure
17	CSP	Cloud Service Provider
18	AES	Advanced Encryption Standard
19	DES	Data Encryption Standard
20	IDEA	International Data Encryption Algorithm
21	MD5	Message Digest 5
22	SHA	Secure Hashing Algorithm
23	ECG	Electrocardiograms
24	PR	Pulse Rate
25	RR	Respiratory Rate
26	BT	Body Temperature
27	$SpO_2$	Oxygen Saturation
28	GL	Hyperglycemia
29	BP	Blood Pressure
30	PS	Personal Server

on a self-service basis. Amazon EC2 provides scalability, pay-per-use computing capacity, and an elastic scale in both directions [11].

**2.3. Eucalyptus System.** “Eucalyptus” stands for “Elastic Utility Computing Architecture Linking Your Programs to Useful Systems.” Eucalyptus is free and open-source software for developing Amazon web services (AWS) compatible with the hybrid and private cloud-computing environment. Eucalyptus facilitates storage, pooling the computing and network resources dynamically. The Eucalyptus system announced a formal agreement with AWS in March, 2012. The main objectives are to provide (1) a vehicle to extend the utility model of cloud computing; (2) an experimentation vehicle for development and a debugging platform for public clouds before buying original software; (3) a homogenized IT environment for public clouds; and (4) a basic platform for the open-source community (e.g., Linux) [57].

**2.4. SNIA’s Cloud Data Management Interface.** SNIA’s [58] cloud data management interface is a standard for cloud

data storage. This standard proposed an interface for managing and accessing data cloud storage. The “cloud data management interface” is broadly acceptable architecture that specifies a framework for data access, data management operations, data object definitions, access control, and logging specifications for cloud environment. However, this standard lacks specifications for security and privacy [59].

**2.5. Social Spot.** According to Zhang et al. [46], a social spot (SP) is a predeployed local gateway that is fully equipped for high storage and powerful communication. The PHDA [46] scheme proposed for cloud-assisted WBANs used these social spots for the collection of outdoor PPPs. The total L numbers of SP are located at intersections or ‘spots’ where patients frequently visit. These spots are located according to their behaviour. SP is responsible for collecting PPPs directly sensed data from each patient via a cloud-assisted WBAN. Finally, SPs upload this aggregated data at cloud servers.

**2.6. Cloud Server.** A cloud server (CS) is a virtual machine that stores large amounts of health-sensed data from patients

and, to some extent, processes that data. For example, this could be ECG data to produce useful information that can be accessed by doctors or other medical staff, through query, for diagnosis [7].

**2.7. Outdoor and Indoor Patient.** The term ‘outdoor’ refers to those patients who are equipped with wireless body sensors (WBSs) for healthcare monitoring and to transmit PPPs to CS through social spots or social networks (explained below). Similarly, ‘indoor’ patients are those who are equipped with WBSs and monitored in their home, hospital, and so on. PPPs are transmitted to CS by personal handheld devices or laptops [60].

**2.8. Trusted Authority.** A trusted authority (TA) is a trusted, powerful, and rich storage entity. A TA bootstraps the whole system in the initialization phase. According to Zhang et al. [46], a TA can be a certified hospital in the real world that is responsible for the management of health data. In the PHDA [46] scheme, initially a TA generates a secret key for legitimate users and certificates for further authorization. After authorization of legitimate users and health data aggregation, a TA can decrypt data for diagnosis. In addition, a TA repels malicious user attacks in PHDA. In ESPAC [42], a TA generates public and secret key parameters. A TA is responsible for issuing keys and revoking, updating, and granting authorization rights to individuals based on their roles and attributes. For storage, a TA maintains an index table to store the location of the distributed storage server. Lounis et al. [2] introduced a healthcare authority (HA) as a TA in their scheme for healthcare data management. An HA generates a secret key  $SK_p$  and builds an access structure  $AR_p$  that patients use for health data encryption.

**2.9. Medical Entity.** Medical entities cover those staff who dealt directly with PPPs and PHI for patient diagnosis and treatment, for example, doctors, nurses, and medical assistants. These entities access PHI primarily to perform some operation or transfer to third party for secondary use [48, 61].

**2.10. Encryption Technology in Cloud Computing.** The hassle-free management and encouragement attract a large number of users towards untrusted servers. A CS may leak information to unauthorized parties. Therefore, all data needs to be transmitted in ciphertext mode to ensure data confidentiality and integrity against untrusted cloud service providers (CSP) [62]. The transmitted data are encrypted so that authorized bodies understand it. The three main encryption technologies that are utilized and used in cloud computing [63] are set out as follows.

Symmetric encryption, also known as “private key cryptography” [63], is a basic and the most trustworthy method to secure online transmission. A private key preserves arbitrarily created words or mix of letters connected as a secret key to change the message particularly. For example, let the password be ABC and for the encryption, algorithm advances this password by five places; then, the new password will be

EFG, which is obviously simple, like the ABC password, but difficult to hack. This encryption technique can be used as a “stream cipher” [63] or “block cipher” [63], directly proportional to the quantity of data encrypted or decrypted over time. A “stream cipher” [63] performed encryption character by character at a time, while a “block cipher” [63] processed a fixed amount of information. Traditional algorithms for symmetric encryption are “Advanced Encryption Standard (AES)” [63], “Data Encryption Standard (DES)” [63], and “International Data Encryption Algorithm (IDEA)” [63].

The asymmetric method, or simply “public key cryptography” [63], is that two paired keys are used together to encrypt and decrypt messages to keep them secure during transmission. When talking about data transfer for large businesses or organizations, this method is considered to be more enhanced than symmetric encryption. According to Microsoft, “you do not have to worry about passing public keys over the Internet (the keys are supposed to be public). However, asymmetric encryption is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message” [63].

The generation of special fixed-length passwords for a message, signature, or set of data is called hashing encryption. In this type of encryption, hash functions are used to protect information. The main advantage of this method is that the slightest change in information makes a completely new hash function that is incredibly difficult to hack and, once the message is secured, it cannot be read or altered by any process: “This means that even if a potential attacker were able to obtain a hash, he or she would not be able to use a decryption method to discover the contents of the original message. Some common hashing algorithms are Message Digest 5 (MD5) and Secure Hashing Algorithm (SHA) [64].”

**2.11. Pairing-Based Cryptography.** The basic concept of pairing-based cryptography is pairing between elements of two cryptographic groups and mapping this pairing to a third group  $e: G_1 \times G_2 \rightarrow G_T$ , for the construction or analysis of cryptographic systems. According to academic research [65], the common definition used for pairing-based cryptography is as follows: Let  $G_1, G_2$  be additive cyclic groups of prime order  $q$  and  $G_T$  another order of prime  $q$  for multiplicativity. The pairing map of  $e: G_1 \times G_2 \rightarrow G_T$  satisfies the following properties:

Bilinearity:

$$\forall \mathcal{P}, \mathcal{Q} \in \mathcal{G}_1, \forall \alpha, \beta \in \mathcal{Z} * q, \quad e(\alpha \mathcal{P}, \beta \mathcal{Q})^{ab} \quad (1)$$

Nondegeneracy:

$$\begin{aligned} P \in G_1, P \neq 0 &\implies e(P, P) \neq 1 \\ &= G_2 \quad (e(P, P) \text{ generates } G_2) \quad (2) \\ \mathcal{P} \neq 0 \quad e(\mathcal{P}, \mathcal{P}) &\neq 1 \end{aligned}$$

Computability:

$$e \text{ is efficiently computable.} \quad (3)$$



If the first two groups use the same group (i.e.,  $G_1=G_2$ ), then this type of pairing is known as symmetric. This classification of pairing can be further divided into three types: (1)  $G_1=G_2$ ; (2)  $G_1 \neq G_2$ , with efficient computable homomorphism  $\phi: G_2=G_1$ ; and (3)  $G_1 \neq G_2$  nonefficient computable homeomorphisms between  $G_1$  and  $G_2$  [66].

### 3. Method

In this study, we have conducted a literature review to find techniques proposed for PPPs privacy and security in S-CI. We categorized and organized these techniques according to the applications of the healthcare domain. The outcome of the study will be beneficial for the research community who are involved for the betterment of patient data privacy and security in S-CI.

**3.1. Inclusion and Exclusion Criteria.** Literature addressed large number of studies on privacy and security of images, cloud storage-based patient data, sensor networks, wireless communication, cloud-assisted wireless body area network, and in-home patient monitoring. This study only included those empirical published studies, which have been peer-reviewed in journals, conferences, and workshops published up to two quarters of 2018. This inclusion criterion is based upon the evidence provided by the pilot study. Those studies not explicitly providing techniques for the privacy and security of PPPs or supporting any other area of wireless body sensors rather than cloud-assisted wireless body area network were excluded. We also excluded books, technical reports, and project thesis studies based on expert and physiological opinions.

**3.2. Search String.** Literature addressed large number of studies on privacy and security of images, cloud storage-based patient data, sensor networks, wireless communication, and in-home patient monitoring. We used these results in finalizing the pilot study. Initial search by applying general string at selected databases for pilot study was as follows:

*Patient AND Medical AND Wireless Body Sensors  
AND Cloud Computing (Privacy OR Security)*

There are many diversified terms used to address patient data privacy, security, and body sensors for patients in literature. It was a challenge to generate a valid string for targeting relevant studies. Therefore, we used the major terms of our selected primary studies search from the aforementioned string to formalize a search string for our final study. As a result, the following search string was produced:

*((Healthcare" OR "Patient" OR "Medical" OR "eHealth" OR "mHealth" OR "Health data" OR "Mobile Computing" OR "Mobile Device" OR "Medical Care System" OR "Mobile Cloud" OR "E-Healthcare System") AND ("Wireless Body Area Network" OR "WSN" OR "Wireless Sensor Network") AND ("Cloud" OR "Cloud Computing" OR "Cloud-assisted" OR "Private Cloud"*

*OR "Sensor Cloud" OR "Cloud Storage") AND ("Privacy" OR "Security"))*

**3.3. Data Extraction and Analysis.** At this stage of conducting phase, data of selected primary studies from previous phase was extracted. To carry out data extraction more efficiently, forms were designed in MS word. These forms also help in consistency of data extraction. These data extraction forms were evaluated in our pilot study. It is difficult to set values of all properties prior to data extraction. These properties are totally dependent on the papers and their contents. However, the extracted properties with relevant questions are mentioned. Data synthesis involves collecting and summarizing the results of the included primary studies. Synthesis can be descriptive (nonquantitative). However, it is sometimes possible to complement a descriptive synthesis with a quantitative summary. The extracted data from data extraction forms were recorded on Excel sheets. This really helped us to find trends, consistency, and relevant similarities for analysis of data.

## 4. Results

**4.1. S-CI Process for Patient Data Privacy and Security.** In this section, we outline our six-step generic framework for S-CI to achieve PPPs privacy and security. This framework does not follow any particular research method of a study. We give the basic steps that we adopted to ensure patient data security and privacy in S-CI. The main purpose of our framework is to help readers to understand the process more clearly and easily. Figure 2 is a block diagram showing patient data privacy and security in S-CI. Firstly, particular techniques identify relevant system entities before defining method. Meanwhile, PPPs were accessed as dataset and utilized to validate the technique. Finally, security and performance analysis of the selected parameters was performed for evaluation of PDPS.

**4.1.1. Selecting the Preliminaries.** Almost all studies define a set of preliminaries before proposing a technique. These preliminaries are the basic concepts of the proposed solution. Preliminaries serve as the baseline, and the entire technique for PPPs security and privacy stems from them. For example, bilinear pairing [42], pairing-based cryptography [55], hash function [38], attribute-based encryption [38], and access tree [39] are some important preliminaries in S-CI.

**4.1.2. Identify the System Entities.** The majority of studies have identified system entities before proposing a solution or technique. The system entities are those such as trusted authority, cloud service provider, registered user, data-access requester, health cloud, social cloud, data owner, user, healthcare provider, healthcare analyzer, hospital, key generation centre, IoT medical sensor, mobile device, emergency family contacts, key management centre, doctor, medical staff, body sensor, patient, and social spot, which are some significant entities identified for different techniques. One should identify the relevant set of system entities based on the relevant application area and technique.

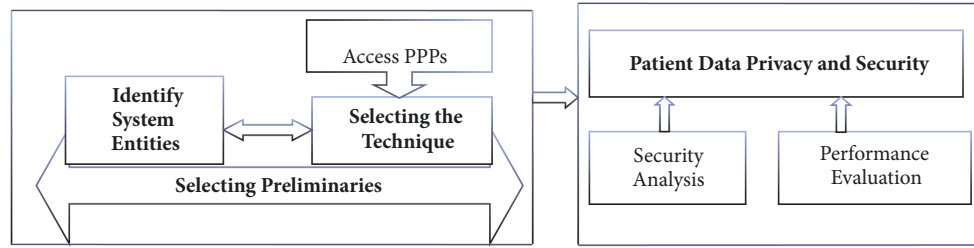


FIGURE 2: Patient data privacy and security in S-CI.

**4.1.3. Selecting the Technique.** In this study, we categorized S-CI-based technique for patient data privacy and security into 10 types: (1) multibiometric key generation; (2) pairwise key establishment; (3) hash function; (4) attribute-based encryption; (5) chaotic maps; (6) hybrid encryption; (7) Number Theory Research Unit; (8) Tri-Mode Algorithm; (9) Dynamic Probability Packet Marking; and (10) Priority-Based Data Forwarding. All techniques were proposed for specific application areas such as m-healthcare, e-healthcare, health data aggregation, and health data management. The primary purpose of all the techniques is to ensure PPPs privacy and security for S-CI. Every technique has its pros and cons, and before selecting one, all possible alternatives should be borne in mind. However, attribute-based encryption is the most widely adopted technique for this area of interest.

**4.1.4. Access PPPs.** The core of this study is to organize the techniques available for PPPs privacy and security in S-CI. Therefore, every study concerns PPPs through WBANs or medical sensors. Common PPPs, accessed for real-time monitoring and early diagnosis, are Electrocardiograms (ECG), pulse rate (PR), respiratory rate (RR), body temperature (BT), oxygen saturation ( $SpO_2$ ), hyperglycemia (GL), blood pressure rate (BP), and so on. One should access PPPs according to the needs of the solution and based on the condition and type of the patient (indoor or outdoor).

**4.1.5. Security Analysis.** Almost every study had performed security analysis to show the strength of the techniques against security attacks. For example, analyses of some common security requirements include data confidentiality, fine-grained access control, collusion resistance, patient-centered access control, message integrity, denial of service (DoS) attack, prevention of ciphertext-only attack, patient privacy, patient control, source authentication, dynamic data operation, audit control, attribute revocation, cloud reciprocity problem, availability, scalability, identity privacy, impersonation attack, resistance to forgery attack, replay attack, man-in-the-middle attack, nonrepudiation, known-key security, signature unforgeability and anonymity, transmission continuity, authorization, and network security.

**4.1.6. Performance Evaluation.** Many different ways have been adopted to evaluate the performance of the techniques. The most common parameters for evaluation are

communication cost, computation cost, storage cost, encryption/decryption time, and key generation time.

**4.2. Patient Data Privacy and Security in the Sensor-Cloud Infrastructure.** In this section, we discuss the various application areas of healthcare in which patient data privacy and security for S-CI have been addressed. Next, we list the pros and cons of existing techniques to ensure patient data privacy and security in S-CI. Lastly, we follow the taxonomical details of these techniques to provide a comprehensive summary of each.

Figure 3 shows the evolution of the types of techniques used to handle patient data privacy and security in S-CI in chronological order. We can see that attribute-based encryption (ABE) is the most used technique in three main application areas: mobile healthcare, e-healthcare, and health data management [6].

The three chief application areas of S-CI in which patient data privacy and security are addressed are set out as shown in Figure 3.

**4.2.1. Mobile Healthcare.** Mobile healthcare, or m-health, technology [67, 68] is a rapidly emerging factor facilitating healthcare for better and more efficient services. M-health with cloud computing includes offloading benefits such as reliability improvement, performance improvement, energy savings, ease of software development, and better exploitation of contextual information [24, 69]. For instance, Figure 4 shows tremendous achievements by m-health to aid healthcare services through technology in bidirectional perspective (customers and providers): mobile-enabled EHRs, patient portals, secure text messaging, patient monitoring devices, and telemedicine. While adopting S-CI in mobile computing, new vulnerabilities affect patient data privacy and security. The following nine techniques are proposed for mobile healthcare to solve issues for patient data privacy and security in S-CI.

**Multibiometric Key Generation (M-BKG).** A secure cloud-based framework is proposed for mobile healthcare using WBANs [37]. In this framework, the author presented a two-fold solution: (1) intersensor communication secured by a multibiometric key generation scheme; (2) secure storage of EMRs on a hospital community cloud to preserve patient privacy. The framework adopted dynamic reconstruction of metadata [70] to secure patient privacy. It is claimed to not

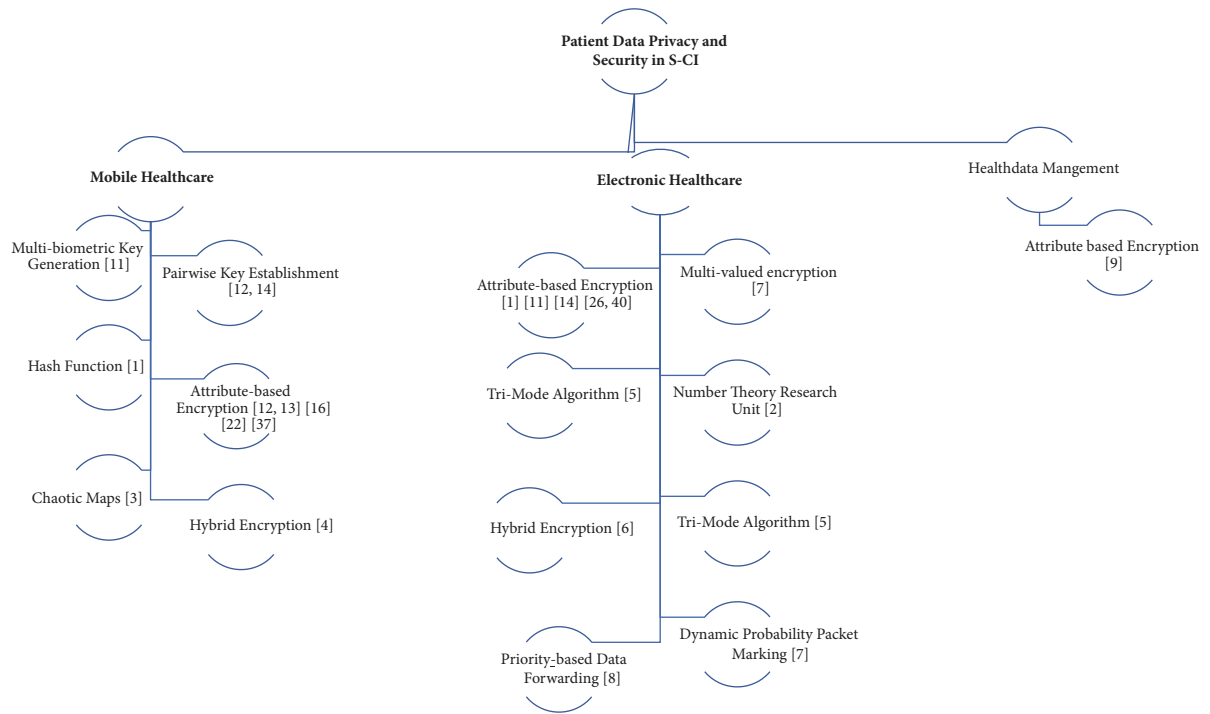


FIGURE 3: Taxonomy of the study.

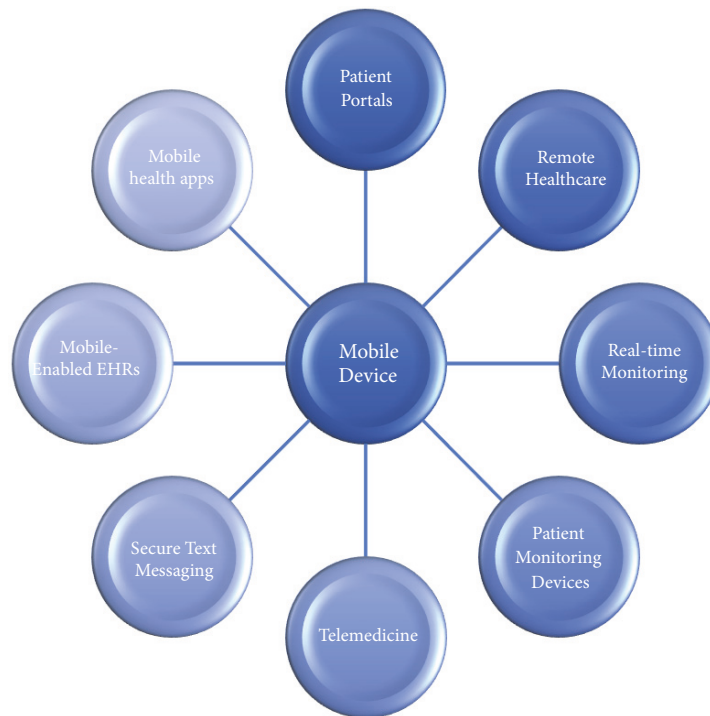


FIGURE 4: M-healthcare services to aid healthcare.

only serve as guidance on privacy and security specifications for SNIA but also assist designers in developing privacy-preserving database schemas in order to store cloud metadata. A fair balance between user privacy, administration rights and roles, limiting the modification requirement in order to make the privacy technique fast and error-free, and cost efficiency in terms of computational resources without any compromise regarding information loss is one of the worthy research goals of this framework. To protect the metadata items of users in clouds, first the metadata items are segregated and stored in the cloud's database. The multibiometric scheme of this framework used a fusion of biometric and two PPPs values, ECG and EEG.

The purpose of the multibiometric scheme is to generate a long key to obtain a secure and random key. First, the scheme performs feature selection for secure intersensor communication. The features are extracted and quantized from EEG and ECG signals using discrete wavelet transform (DWT). WBSs and personal servers (PS) communicate at a sample rate of 125Hz within 5 seconds. In the second step, a key is generated on receiving data blocks of ECG and EEG sensors signals by applying a KeyGen algorithm. Two keys of 160 bits are generated by KeyGen. These keys are concatenated horizontally to generate a 320-bit long key. On receiving compressed blocks from each sensor, common blocks are extracted. The construction of the matrix uses extraction. The Hamming distance is used to measure the elements of the matrix from the  $i$ th block of sensor 1 to the  $j$ th block of sensor 2. When sensor node 'a' ( $SN_a$ ) wishes to communicate with sensor node 'b' ( $SN_b$ ),  $SN_a$  sends a 'Hello' message to  $SN_b$  with its ID in m1:

$$\begin{aligned} m1 : \forall SN_a e (SNIA) : SN_a \\ \rightarrow SN_b : (IDSNa, Hello, nonce). \end{aligned} \quad (4)$$

For calculating pairwise keys of ECG and EEG,

$$\begin{aligned} K1SN_a, SN_b \\ = HMAC (Calculated ECG values |IDSna| IDSNa) \end{aligned} \quad (5)$$

$$\begin{aligned} K2SN_a SN_b \\ = HMAC (Calculated EEG values |IDSNa| IDSNa). \end{aligned} \quad (6)$$

Finally, in m2,  $SN_b$  sends its ID with encrypted data and MAC to  $SN_a$ :

$$\begin{aligned} m2 : \forall SN_b \rightarrow SN_a : IDSNa, EKSNa, \\ SN_b \{IDSnb, Data\}, MACksna, SN_b \\ (IDS_{SN_b}, Data, nonce). \end{aligned} \quad (7)$$

This process consists of the following steps:

- (a) Vertical segregation: In a cloud database, metadata items are stored by vertical segregation according to level, for example, context level, purpose level, and attribute level as first, second, and third, respectively.

- (b) Attribute association: In this step, the individual attributes are associated with one member of attribute-type segregation level.
- (c) Sensitivity parameterization: The segregated attributes are categorized according to the sensitivity parameterization (SP) classes as exclusively private (XP), partially private (PP), or nonprivate (NP).

Exclusively private data items are kept confidential in all circumstances. The sensitivity class XP is divided into two (ascending from 1 to 2) sensitivity levels. An XP class data item is said to be at level 2 if it fails to preserve a cloud user's privacy when disclosed alone, while XP data items are said to be at level 1 if they are disclosed with other attributes of SP classes XP/PP. However, partially private data is not confidential, yet it needs to protect integrity. Like exclusively private data items, private data items are divided into two levels (ascending from 1 to 2). Table 2 is a summary of the multibiometric key generation technique.

*Pairwise Key Establishment.* In contrast with the previous technique, Zhou et al. [40] proposed a scheme utilizing the body symmetric structure with Bloom's symmetric key construction (Table 2). Due to the symmetrical structure of the body, WBANs such as ECG and EEG are deployed symmetrically for patients. Patients with the same disease can create a social group, for communication. However, patients with a different disease are not allowed to communicate, for the preservation of privacy.

Members of a social group of patients with the same WBANs have the same sensor placement on their body. For  $N$  number of patients  $P_s$  ( $s = 1, 2, \dots, N$ ) with the same disease in a social group, their connected data sinks are  $D_s$  ( $s = 1, 2, \dots, N$ ). Pairwise key establishment for privacy key management is carried out in three steps. In step 1, a set of body sensors  $BSR_{s,k}$  ( $k \in \{1, \dots, N_s\} [23]$ ) is deployed on the patient body for a specific disease. The physician uses a symmetric matrix  $Dp_s$  to store information of the symmetrical body sensors' positions. For example, the ECG for position 'CHEST' to pair in symmetric elements in private matrix  $Dp_s$  is

$$Dp_s(j; i) = \frac{1}{4} H0 (LocBSRs; k) \quad (8)$$

where  $LocBSNs; k$   $Dp_s(i; j)$  ( $i \neq j$ ;  $i, j \in \{1; \dots; \lambda + 1\}$ ) denotes each body sensor position at patient body  $P_s$  and the items on the matrix are located at the intersection of  $i$ -th row and  $j$ -th column  $D_s$ .

In step 2, the patient  $P_s$ 's block location for each data sink  $D_s$  is accessed by GPS. The location information of the patient is represented as

$$Dp_s(i; j) (i = j^i; j \in [1; \lambda + 1]) = H1 (LocPs). \quad (9)$$

In step 3, the data sink is calculated with initial key material matrix as  $UP_s = (Dp_s G_{P_s})^T$ .



TABLE 2: Summary of Multibiometric Key Generation Technique in m-health.

Technique Ref. No. Year	M-BKG [37] 2014
<b>Main Idea</b>	Patient data privacy and communication security would increase users' confidence at remote healthcare systems.
<b>PPPs</b>	ECG, EEG
<b>Findings</b>	A framework for cloud-based technique for mobile healthcare that securely perform intersensor communication with patient data privacy and security
<b>Controller</b>	Server
<b>Patient Mode</b>	Indoor/outdoor
<b>Emergency Management</b>	No
<b>Limitation</b>	Only key generation based on ECG and EEG signals.

TABLE 3: Summary of Pairwise Key Establishment Technique in m-Health.

Technique Ref. No. Year	4S [40] 2015
<b>Main Idea</b>	A cloud-assisted m-healthcare social network to facilitate security and privacy of patient's data in location- and time-based attacks.
<b>PPPs</b>	ECG, EEG
<b>Findings</b>	A secure cloud-assisted WBANS-based privacy-preserving key management scheme, pliant to mobile attacks in m-healthcare for patients with the same diseases in social group.
<b>Controller</b>	Patient
<b>Patient Mode</b>	Indoor/outdoor
<b>Emergency Management</b>	No
<b>Limitation</b>	Pairwise key establishment is limited to a group of patients sharing the same disease.

In step 4, the private key  $rs \in \mathcal{G}_p(s = 1; 2; \dots; N)$  is selected for each data sink  $DS_s$  for computing blinded key matrix:

$$U^{rs} p_s \text{ as } U^{res} P_s (UP_s (s = 1; 2; \dots; N)). \quad (10)$$

In step 5, the  $i$  and  $j$  intersection of sensor data implements pairwise key establishment with respect to Bloom's symmetric key construction as

$$K(I, j) = U^{res} p_s(i) GP_s(j) = U^{res} p^s(j) GP_s(i) = K(j; i). \quad (11)$$

The summary of pairwise key establishment in m-health is given in Table 3.

**Hash Function.** In the same year, wireless sensor networks and cloud computing (WSNCC) [47] were proposed to help, manage, and access sensor data in a cloud-computing environment by efficient processing, communication, and security. The conceptual architecture used Secure Hash Algorithms such as *SHA-224*, *SHA-256*, *SHA-384*, and *SHA-512* for message integrity. Symmetric key cryptography is used to provide data confidentially and to maintain the availability of data at all times. Meanwhile, cloud computing supports data with redundancy techniques. Furthermore, the framework is claimed to reduce transmission traffic bandwidth requirements, promote data security, efficient cloud storage, and processing, and reduce cost. Table 4 is a summary of hash function-based techniques.

**Attribute-Based Encryption.** In 2015, Guan et al. [38] proposed a Mask-Certificate attribute-based encryption (MC-ABE) scheme for secure data transfer. The aim of the study was to perform secure transmission and storage of PPPs (ECG, EEG) with fine-grained policies, privacy, and access control. This novel outsourcing encryption scheme provides patient data privacy and security in S-CI. This consists of a total of seven algorithms: *Setup*, *KeyGen*, *CerGen*, *Encrypt<sub>DO</sub>*, *Encrypt<sub>ESP</sub>*, *Decrypt<sub>DSP</sub>*, and *Decrypt<sub>DR</sub>*. The data owner (DO) encrypts  $M$  with algorithm (*Encrypt<sub>DO</sub>* ( $PK, M, K$ )  $\rightarrow MM$ ) for outsourcing, in which a signature is used to mask  $M$ . Then, the encryption service provider (ESP) with algorithm (*Encrypt<sub>ESP</sub>* ( $PK, s, T, MM$ )  $\rightarrow CT$ ) completes the encryption phase. The encrypted data is stored with a storage service provider (SSP). The requester's data access request is sent to the TA for verification by generating a key with algorithm (*KeyGen* ( $MK, S$ )  $\rightarrow SK$ ). The TA selects a unique value to mask the certificate for the data requester (DR). Then, the TA computes SA with algorithm (*KeyGen* ( $MK, S$ )  $\rightarrow SK$ ), using the DR attribute set. After this, the certificate is sent to DR and the SK is sent to DSP. Meanwhile, DP receives CT from SSP. Once DR has the certificate, it performs decryption to get  $M$  with algorithms (*Decrypt<sub>DSP</sub>* ( $SK, CT$ )  $\rightarrow MM$ ) and (*Decrypt<sub>DR</sub>* ( $M, signature, MCert$ )  $\rightarrow M$ ).

In 2016, Guant et al. [39] extended their own MC-ABE scheme into another novel mechanism to secure access control. The mobile-based scheme collects PPPs from S-CI in large amount. To maintain privacy and security for mobile

TABLE 4: Summary of Hash Function Techniques in m-Health.

Technique Ref. No. Year	WSNCC [47] 2015
<b>Main Idea</b>	Fast and reliable transmission required for cloud-based WSN data.
<b>PPPs</b>	BP, HR, ECG, EGG, medical images
<b>Findings</b>	A model to manage and access sensor data efficiently in processing, communication, and security perspective.
<b>Controller</b>	Server
<b>Patient Mode</b>	Indoor/outdoor
<b>Emergency Management</b>	No
<b>Limitation</b>	Only conceptual architecture, need real case scenarios validation.

computing is a big challenge. In this mechanism, a specific signature is designed to mask the plain text. This masked data is securely outsourced on cloud servers. For access control, an authorization certificate, based upon signature and related privilege items, is constructed. A unique value is selected to mask the authorization certificate of each data receiver. MC-ABE-based system provided access control for S-CI. Meanwhile, the proposed scheme had lower computational and storage costs than other models.

Recently, in 2017, Huang et al. [41] preserved the data privacy and security of health and social data with fine-grained access control. The authors claimed that fusion of health data with social data in smart cities is challenging patient data privacy and security. The mobile healthcare social network (MHSN) scheme is based on attribute-based encryption and identity-based broadcast encryption. The basic aim in the system setup phase is that the central authority runs a setup algorithm to select a bilinear pair map  $e: G_1 \times G_2 \rightarrow G_T$  and chooses a maximum number of receivers,  $N$ . Meanwhile, in this cryptographic phase, a hash function selects a public key, PK, and a master key, MK, is selected. In the key generation phase, a central authority *AKeyGen* algorithm makes a random selection of a unique key against each user. A secure health and social data sharing collaboration scheme is proposed to preserve patient data privacy. For secure sharing of health and social data, the data is encrypted and decrypted with independent algorithms. Performance analysis and comparison show that MHSN is more efficient and secure than other schemes.

Similarly, He et al. [48] proposed a fine-grained and lightweight data access control (FLAC) scheme for WSN-integrated cloud computing (WCC). In the WCC environment, sensors and mobile devices are weaker nodes in terms of data storage and computing capacity. The aforementioned weakness of the WCC challenge is patient data confidentiality, integrity, and access control, as handling ciphertext policy attribute-based encryption (CP-ABE) and attribute-based encryption (ABS) is a tough job for lightweight devices. To facilitate the computation overheads, FLAC provides secure outsourcing computation of CP-ABE and ABS operations. First, the network controller (NC) generates PK, MK, and system attributes. Then, a sensor node generates intermediate ciphertext parameters and an encryption signature and sends it to the Encryption-Signature Proxy Server (ESPS). The ESPS

performs the intensive operations and generates ciphertext CT and signature  $\alpha$ . Finally, the ESPS uploads CT and  $\alpha$  to the cloud server. Meanwhile, FLAC claims standard security assumptions, collusion resistance, and anonymity in WCC. Table 5 is a summary of the attribute-based encryption technique in m-health.

*Chaotic Maps.* Furthermore, in 2016, Li et al. [49] proposed an architecture for secure continuous monitoring of patients, based upon chaotic maps. This has five roles for participation in the system: the patient (P), the doctor (D), the healthcare centre (HC), the medical caregiver (MC), and a trusted medical cloud centre (C). Before accessing system, every participant has to register with C to get Chebyshev chaotic map-based specific certificates.

In the first scenario, patient (P) visits HC for a health check, and HC is responsible for uploading P's medical report at C. In the second scenario, P uploads his/her PPPs from WBANs to C using a personal mobile device. In the emergency monitoring application, the MC is allowed to access the uploaded data in order to treat the patient at that time while, in normal situations, when P visits hospital for treatment, D can download his/her data from C. The security analysis of attack model suggests that an attacker may guess such a low entropy password easily. However, to guess a secret parameter such as a certificate is not computationally feasible in polynomial time. Table 6 is a summary of the chaotic map technique.

*Hybrid Encryption (Asymmetric/Symmetric Encryption).* Recently, Hu et al. [50] proposed an intelligent and reliable IoT scheme for the sensor and cloud computing environment to secure elderly patients' privacy. The proposed scheme collects PPPs through their mobile devices. Seven entities are used in this scheme: elder (E), cloud (C), hospital (H), key generation centre (KGC), IoT medical sensor (MS), mobile device (MD), and emergency family contacts (EFC). Initially, the elderly people and the hospital need to register themselves in KGC via a secure communication channel. The elderly people visit hospital for a medical inspection and medical staff uploads their inspection report to the cloud. IoT-based medical sensors collect PPPs and send to the medical device after a set period. The mobile device is responsible for uploading the PPPs to the cloud. The cloud

TABLE 5: Summary of Attribute-Based Encryption Technique in m-Health.

Technique Ref. No. Year	MC-ABE [38] 2015	MC-ABE [39] 2016	MHSN [41] 2017	FLAC [48] 2017
<b>Main Idea</b>	Secure data transfer from data owners to the cloud servers, secure data storage and patient data privacy with authorized access control and fine-grained policies.	As mobile computing collects large amount of data from cloud integrated body sensor network, it is a challenging issue to keep data privacy and security.	The fusion of health data and social data may pose series of privacy and security issues in smart cities.	WCC environment brings new challenges to data confidentiality, data integrity, and access control.
<b>PPPs</b>	ECC, EGG,	ECC, EGG,	Blood pressure, Heart Rate, Pulse	Medical data
<b>Findings</b>	A novel encryption outsourcing scheme MC-ABE for patient data privacy and security in C-BSN.	A novel MC-ABE-based mechanism for access control in C-BSN.	A secure health and social data sharing collaboration scheme to preserve patient data privacy.	A fine-grained and light-weight access control scheme for WCC in order to control access and data confidentiality and to support diverse access policies
<b>Controller</b>	Trusted Authority	Data owner	Trusted Authority	Trusted Authority
<b>Patient Mode</b>	Indoor /outdoor	Indoor	Indoor/outdoor	Indoor
<b>Emergency Management</b>	No	No	No	No
<b>Limitation</b>	Total computational cost is proportional to the number of privileges and storage space is proportional to the number of DRs. Need to improve scalability.	No validation for real access of PPPs available.	Storage cost is not evaluated.	Real PPPs and access scenarios are not evaluated for performance measurements.

TABLE 6: Summary of Chaotic Map Technique in m-Health.

Technique Ref. No. Year	CAA [49] 2016
<b>Main Idea</b>	Patient medical data security in public and insecure communication channels for cloud-assisted WBAN in order to save patients' lives.
<b>PPPs</b>	ECG, EEG, Electromyography, Pulse, oximetry, Body pulse, Heartbeat, Blood pressure
<b>Findings</b>	A secure mobile emergency-based cloud-assisted WBAN system for real-time monitoring of patients. It protects patient privacy and also reduces the burden of system overhead.
<b>Controller</b>	Trusted Authority
<b>Patient Mode</b>	Indoor
<b>Emergency Management</b>	Yes
<b>Limitation</b>	Evaluation of average communication cost and access time ignored.

TABLE 7: Summary of Hybrid Technique Encryption in m-Healthcare.

Technique Ref. No. Year	IoT [50] 2017
<b>Main Idea</b>	Embedded devices with cloud servers can provide flexible medical aid to elderly people. However, this environment has various security issues.
<b>PPPs</b>	ECG, oxygen saturation, blood pressure, body temperature
<b>Findings</b>	A secure IoT-based sensor cloud scheme for continuous monitoring of elderly people.
<b>Controller</b>	Trusted Authority
<b>Patient Mode</b>	Indoor/outdoor
<b>Emergency Management</b>	Yes
<b>Limitation</b>	The scheme is not easy to use for elderly people.

server compares the received PPPs with standard values of parameters on the database. In the event of an emergency, EFC approached and notified within an acceptable time. If the collected PPPs from IoT-based medical sensors are normal, the cloud sends a report to the patient. This whole process and the medical data are shared between the various entities in the scheme in asymmetric/symmetric or hybrid encryption. Meanwhile, the scheme is claimed to reduce the wastage of medical resources. Table 7 is a summary of this technique in m-health.

#### 4.3. E-Healthcare

*Attribute-Based Encryption.* Efficient and secure Patient-Centric Access Control (ESPAC) scheme [42] consists of four main entities: (1) trusted authority, (2) cloud service provider, (3) registered users, and (4) data-access requester in two phases (A and B). In phase A, secure data communication is arranged between different e-health users, while in phase B a traditional cryptographic system data-access request is controlled. The encrypted data is stored in a central health cloud for access. An analysis of the security and performance of ESPAC demonstrated the desired security requirements with only a reasonable delay in communication.

Privacy and security for PHI in IoT cloud-based systems always represent a challenge. Another technique, by Yeh et al. [43] in 2015, proposed e-health as a cloud-based framework for fine-grained access control to address the challenge. A variant of ciphertext, policy attribute-based encryption, is

used with Merkle hash trees and dual encryption to handle fine-grained access control for lightweight devices such as wireless body sensors. Meanwhile, the fine-grained access control framework also provides efficient dynamic auditing, batch auditing, and attribute revocation. An analysis of the security and performance showed that the scheme is excellent as a cloud-based PHI system.

Similarly, the AYA model of K. Martin et al. [44] solves data accountability issues by introducing a new concept of trusted logical agent as a private cloud with data owner control. The data owner is responsible for the processing and storage of his/her data on an outsourced private cloud. The focus of the proposed solution is on an efficient authentication service on a public cloud with a 'one-time token' algorithm and secure access granted on the private cloud by using  $C_{p-ABE}$ . First, a data owner selects a service ( $\Omega$ , PKI) from the public cloud. Secondly, the data owner gives an instruction to the trusted point (TP) to generate a private key. Then, the service requests access to the private cloud for successful authentication.

In 2017, Shynu et al. [51] proposed an e-health cloud storage system to handle multiple users for sensitive data sharing. The system consists of four major entities: CS, key management centre (KMC), DO, data user (DU), a non-patient-centric approach adopted in which the health service provider (HSP) plays the role of DO. The patients were monitored through WBANs continuously and health data were collected in electronic health records (EHR). First, users registered with CS and obtained their pair of cryptographic



keys and smartcard. In the next step, a mutual authentication process takes place. HSP is responsible for the secure connection between DO and DU. HSP issues an attribute certificate to the trusted entities. After this, the HSP enforces access policies (read, write) for data access and enforces data encryption. Here, the system utilized is the attribute-based searchable encryption (ABE) technique. During the whole process, a trapdoor function is calculated for every patient. Table 12 is a summary of the ABE technique in e-healthcare. Table 8 shows the summary of attribute-based techniques in e-healthcare domain.

*Number Theory Research Unit (NTRU).* Compared to earlier studies in 2016, Chen et al. [52] proposed a trustable scheme to maintain patient privacy while sharing PPPs from wearable devices to cloudlet technology. The content sharing and privacy protection are maintained by NTRU [71]. The encryption scheme uses NTRU to encrypt PPPs (ECG, heart rate, blood pressure, and so on) before transmitting to a smartphone or any other personal handheld device. Data collected from smart cloths are usually unsigned and stored integer vectors. Table 9 is a summary of NTRU technique in e-healthcare.

*Tri-Mode Algorithm.* Antony et al. [3] proposed an innovative application, the Integrated Secure Authentication (ISA), by negating all traditional cryptographic approaches. ISA is a cloud-based e-health system to solve the authentication problem by proposing Tri-Mode Algorithm. The e-health system received signal strength (RSS) value from the located device and stored authentication list using the SetUp algorithm. Then, a CheckUp algorithm verifies the authentication of the user for data access to the cloud. However, this technique is limited to authorizing a single medical entity. Table 10 presents the Tri-Mode technique in e-healthcare.

*Hybrid Encryption.* The security model proposed [53] uses layers of security at different levels. For example, integrity and confidentiality at WBAN data collection level; network security and confidentiality at transmission level; integrity, availability, and data confidentiality at storage level; and authentication and authorization at data access level. A double-layer encryption technique is used for control of access in this model. The symmetric encryption technique is used due to its efficiency, as the same key is used to both encrypt and decrypt data. While an asymmetric encryption technique is preferred due to pairs of keys (public, private) and easiness of key distribution during transmission, this process is quite slow. Taking advantage of both the aforementioned encryption techniques, double-layer hybrid encryption is used for data confidentiality and integrity. Table 11 is a summary of the hybrid encryption technique.

*Dynamic Probability Packet Marking.* Latif et al. [54] claimed that existing Probabilistic Packet Marking (PPM) for sensor networks is limited to fixed making probability  $\tau_i$ , which results in high convergence time, uncertainty, and additional overhead due to 'Key Issues in Selecting Probability'. Its main cause is the assignment of uneven probability  $\phi_i$  to  $n_i$  (sensor

node), along with the attack path, whereas Dynamic Probability Packet Marking (DPPM) uses the Time-to-Live (TTL) to determine the travelling time of each packet passing by the router. By using this concept of DPPM, an Efficient Trackback Technique (ETT) is proposed to handle Distributed Denial of Service Attack (DDOS) for S-CI. Table 12 is a summary of the PPM technique in e-healthcare.

*Priority-Based Data Forwarding.* To aggregate different types of health data in S-CI and priorities data according to need and availability is a big challenge. Zhang et al. proposed a 'priority-based health data aggregation' scheme (PHDA) [46] to establish a secure and reliable connection between WBANs and CS, with some security requirements. The network model is responsible for secure and reliable connection, with the assumption that S-CI is a trusted entity. Four entities, TA, SP, cloud server (CS), and mobile users, are utilized in the network model. The security model of PHDA is intended to reduce the communication overhead with security goals such as data privacy, identity privacy, and resistance to forgery attack. The PHDA protocol is able to aggregate health sensing data efficiently, based on data-forwarding strategies. Health data are classified into (1) emergency calls, (2) PPPs, and (3) normal health data. These types of data are prioritized according to their significance and size. Mobile users'  $u_i$  prioritized data has a data priority detection module. PHDA proceeds with (1) an initialization phase, (2) health data generation, (3) priority-based forwarding, (4) data aggregation, and (5) data decryption. Table 13 is a summary of the PHDA technique in health data aggregation.

#### 4.4. Health Data Management

*Attribute-Based Encryption.* Lounis et al. [2] proposed a cloud-based secure architecture for the data management of large-scale data collected from WBANs. In this architecture, the mechanism of CP-ABE is used for effective and flexible security in order to achieve confidentiality and integrity with fine-grained access control for outsourced EHRs. The system is composed of three main entities: patients, cloud servers, and healthcare professionals. For communication security, the SSL protocol is assumed to be the communication channel. Medical data are encrypted at user level, as cloud servers are considered an untrusted entity. Therefore, the health authority (HA) is introduced as the trusted authority for key assurance and access policies. Each party has a public/private key pair, which can be obtained easily through Public Key Infrastructure (PKI). Extensive simulation has shown that the proposed scheme allows for efficiency and scalability with fine-grained access control in both emergency and normal scenarios. Table 14 is a summary of the ABE technique in health data management.

*4.5. Security Services in S-CI.* In this section, we discuss the extracted security services provided by the various techniques, according to their application areas. We observe that areas such as m-healthcare and e-healthcare are the most addressed in terms of security services. In m-healthcare, the most addressed security services are data confidentiality

TABLE 8: Summary of the Attribute-based Technique in e-Healthcare.

Technique Ref. No. Year	ESPAC [42] 2011	e-Health framework [43] 2015	AYA [44] 2015	ABE scheme [51] 2017
<b>Main Idea</b>	Patient self-controlled privileges to PHI for cloud storage at anytime, anywhere, and remote access.	IoT devices for pervasive personal health information (PHI) system facing privacy and security challenges in cloud-based environment.	A new paradigm 'Cloud of Things' rises some new challenges at outsourced data in terms of access control, privacy protection, and data integrity, as patient ownership.	The existing techniques are patient centric and do not provide security with fine-grained access control.
<b>PPPs</b>	e-Healthcare service provider provides health data	PDA based PHI	Medical data	EHR
<b>Findings</b>	A secure and an efficient and patient-centric access control scheme for real-time monitoring and remote access from cloud storage.	E-healthcare-based lightweight framework to achieve fine-grained access control with efficient revocation and dynamic revocation.	A security architecture for patient owner controlled at outsourced data in public cloud environment.	An ABE technique with trapdoor function to avoid unauthorized access control for cloud-based health data.
<b>Controller</b>	Trusted Authority	Trusted Authority	Patient	Trusted Authority
<b>Patient Mode</b>	Indoor/outdoor	Indoor/outdoor	Indoor	Indoor
<b>Emergency Management</b>	No	No	No	No
<b>Limitation</b>	PPPs in dataset and storage cost is not analysed; patient participation and control are not considered.	Log auditing is missing	No support for keyword similarity mechanism	Need to improve efficiency of ABE-based access control for e-health clouds.

TABLE 9: Summary of Number Theory Research Unit Technique in e-Healthcare.

<b>Technique Ref. No. Year</b>	NTRU [52] 2016
<b>Main Idea</b>	Medical data sharing from wearable devices to cloudlet is critical, as it involves sensitive patient data.
<b>PPPs</b>	EEG, Pulse, EMG, ECG
<b>Findings</b>	To protect patient privacy of medical data, a cloudlet-based data sharing system.
<b>Controller</b>	Trusted Authority
<b>Patient Mode</b>	Indoor/outdoor
<b>Emergency Management</b>	No
<b>Limitation</b>	Computation and network cost is not evaluated

TABLE 10: Summary of Tri-Mode Technique in e-Healthcare.

<b>Technique Ref. No. Year</b>	ISA [3] 2016
<b>Main Idea</b>	In WBANs cryptographic authentication is desirable due to their computational complexity for spoofing attacks.
<b>PPPs</b>	RSS value
<b>Findings</b>	ISA application for e-healthcare using cloud computing to prevent spoofing attacks in sensor network.
<b>Controller</b>	Trusted authority
<b>Patient Mode</b>	Indoor
<b>Emergency Management</b>	No
<b>Limitation</b>	Technique is limited to handling just one healthcare authority.

TABLE 11: Summary of Hybrid Encryption Technique in e-Healthcare.

<b>Technique Ref. No. Year</b>	WSN [53] 2016
<b>Main Idea</b>	In S-CI, medical information needs strong privacy and security protection mechanism against unauthorized access.
<b>PPPs</b>	Medical data
<b>Findings</b>	A security framework for S-CI by separating data control to third party to provide fast and reliable security requirements.
<b>Controller</b>	Trusted authority
<b>Patient Mode</b>	Indoor/outdoor
<b>Emergency Management</b>	No
<b>Limitation</b>	Storage and computation cost are not evaluated.

TABLE 12: Summary of Probability Packet Marking in e-Healthcare.

<b>Technique Ref. No. Year</b>	ETT [54] 2016
<b>Main Idea</b>	One of the critical attacks in WBANs environment is DDOS attack, which increases resource utilization and also affects data privacy and security.
<b>PPPs</b>	Body temperature, Pulse oxygen, body temperature, blood pressure, EEG
<b>Findings</b>	An efficient trace back technique for cloud-assisted WBANs environment to avoid DDOS attacks.
<b>Controller</b>	Server
<b>Patient Mode</b>	Indoor
<b>Emergency Management</b>	No
<b>Limitation</b>	This scheme is limited to number of bytes for nodes upon network topology. This scheme uses WBANs and MAC header. Furthermore, this scheme can use IPv6 header for deployment and is evaluated by IPv6 header.

TABLE 13: Summary of the Priority-Based Data Forwarding Technique in Health Data Aggregation.

Technique Ref. No. Year	PHDA [46] 2014
<b>Main Idea</b>	Different types of health data aggregation are challenges in S-CI with security and privacy paramount during communication between WBAN and Cloud.
<b>PPPs</b>	ECG, medical images
<b>Findings</b>	PHD scheme for S-CI to improve health data aggregation efficiently by reserving data identity and privacy.
<b>Controller</b>	Trusted Authority
<b>Patient Mode</b>	Indoor/outdoor
<b>Emergency Management</b>	Yes
<b>Limitation</b>	Computation and computation overheads

TABLE 14: Attribute-Based Encryption Technique in Health Data Management.

Technique Ref. No. Year	CP-ABE [2] 2016
<b>Main Idea</b>	Lack of data management in WSN due to which medical data is facing challenges like scalability, availability, and security.
<b>PPPs</b>	Medical, health data
<b>Findings</b>	Reduce data management and processing overhead in sensor cloud-based scalable architecture to guarantee the integrity, confidentiality, and fine-grained access control of medical data in emergency situations without involving patients and doctors.
<b>Controller</b>	Trusted Authority
<b>Patient Mode</b>	Indoor
<b>Emergency Management</b>	Yes
<b>Limitation</b>	Patient participation and control for data access are not concerned and it is not clearly mentioned which PPPs are accessed

( $n=5$ ) and fine-grained access control ( $n=3$ ). Similarly, there is much on collusion resistance, message integrity, replay attack, and man-in-the middle with ( $n=2$ ). By contrast, patient privacy, source authentication, attributes revocation, availability, impersonation attack, know-key security, non-repudiation, and transmission continuity with ( $n=1$ ) are the least addressed security services in this area. Moreover, patient access controls, denial of attack, ciphertext-only attacks, patient participation, dynamic data operation, cloud reciprocity problems, scalability, resistance to forgery attack, identity attack, authorization, and network security services are totally ignored in m-healthcare.

In the area of e-healthcare, the security services that are commonly addressed are patient control with ( $n=2$ ), source authentication, audit control, data confidentiality, message integrity, and DOS with ( $n=1$ ). Meanwhile, services such as signature unforgeability or anonymity, transmission continuity, man-in-the middle attack, known-key security, nonrepudiation, replay attack, impersonation attack, resistance to forgery attack, and scalability are still answered. The least-addressed application areas in terms of security services are health data management and health data aggregation.

We can clearly observe from Table 14 that data confidentiality, fine-grained access control, collusion resistance message integrity, and availability and scalability with ( $n=1$ ) are a few services that are provided in the area of health data aggregation. Similarly, there is plenty of scope for research in

health data aggregation: patient privacy, identity privacy, and resistance to forgery attack are covered by a single technique. Table 15 is an overview of the extracted security services and the proposed techniques.

*4.6. Patient Physiological Parameters as Dataset.* We observed that studies did not adopt any particular dataset from the existing literature to propose their techniques for patient data privacy and security in S-CI. Most studies utilized common PPPs [72] as a dataset, sensed through body sensors. Table 16 shows the common set of PPPs used as a dataset. The following are some important PPPs sensed through body sensors in S-CI for patient data privacy and security.

*4.6.1. Electrocardiography.* Electrocardiography, or ECG, is a medical process in which electrodes are placed on the human body. In this process, the electric heart activity is recorded over a period of time. In short, the overall purpose of ECG is to obtain information about the function and structure of the heart. In patients, ECG sensors are usually placed for the timely detection of heart attacks, chest pain, shortness of breath, cardiac stress, and so on [37–40, 46, 47, 49, 50, 54].

*4.6.2. Electroencephalography.* Electroencephalography, or EEG, is a medical method to monitor brain activity. In this process, electrodes are placed on the human scalp to measure



TABLE 15: Extracted Security Services from Proposed Techniques.

Security Services	m-Healthcare	e-Healthcare	Health Data Management	Health Data Aggregation
Data Confidentiality	[41, 47, 48, 50, 55]	[44, 53]	[2]	
Fine-grained Access Control	[41, 47, 48]	[43, 51]	[2]	
Collusion Resistance	[41, 48]	[42, 43]	[2]	
Patient-centric Access Control		[42]		
Message integrity	[47, 50]	[42, 53]	[2]	
Denial of Service (Dos) Attack		[42, 54]		
Prevention of Ciphertext-only attack		[42]		
Patient Privacy	[50]	[42]		[46]
Patient Control		[43, 44, 53]		
Source Authentication	[37]	[43, 44]		
Dynamic Data operation		[43]		
Audit Control		[43, 44]		
Attribute revocation	[39]	[43]		
Cloud Reciprocity Problem		[43]		
Availability	[47]	[53]	[2]	
Scalability			[2]	
Identity Privacy		[42]		[46]
Resistance to Forgery Attack				[46]
Impersonation Attack	[55]			
Man-in-the middle Attack	[50, 55]			
Nonrepudiation	[55]			
Signature Unforgeability and Anonymity	[48]			
Replay Attack	[50, 55]			
Transmission Continuity	[50]			
Authorization		[53]		
Known-key Security	[55]			
Network Security		[53]		

TABLE 16: Common Set of PPPs used as Dataset.

Symbol	Description	Frequency	References
ECG	Electrocardiogram	8	[37, 38, 40, 46, 47, 49, 50, 52]
EEG	Electroencephalography	8	[37–40, 47, 49, 50, 52]
HR	Heart Rate	5	[41, 47, 49, 50, 54]
BP	Blood Pressure Rate	5	[41, 47, 49, 50, 54]
PR	Pulse Rate	5	[41, 49, 50, 52, 54]
EMG	Electromyography	2	[52, 54]
Oximetry	Oximetry Technology	1	[49]
BT	Body Temperature	1	[50]
RP	Respiratory Rate	1	[46]
SpO <sub>2</sub>	Oxygen Saturation	1	[46]

voltage fluctuations in the neuron of the brain produced in the form of an ionic current. EEG sensors are usually placed to record epileptic seizures and psychiatric syndromes in patients [37–40, 47, 49].

**4.6.3. Blood Pressure.** The flow of blood circulation in blood vessels for oxygen supply is directly affected by strain at heart arteries. The blood pressure of the body recorded to measure this strain. Smart sensors using microprocessors are used to sense the flow and send the data remotely to medical staff for real-time monitoring [41, 47, 49, 50, 54].

**4.6.4. Body Temperature.** Normal body temperature ranges from 36.5 to 37.5°C according to age, sex, infection, exertion, reproductive status, and so. Medical sensors are placed in patients with a serious disease to diagnose changes in body temperature in order to aid the medical facility in time [50, 54].

**4.6.5. Heartbeat Rate.** The rate of the human heartbeat is measured in the form of contractions, or beats, in bpm. The amount of contraction varies due to the physical need for oxygen in the body. Sensors such as the Polar H10 are placed to monitor the heartbeat rate during the various physical activities that are performed during the day [41, 47, 49, 50].

**4.6.6. Electromyography.** Electromyography, or EMG, is a medical process in which the skeletal muscles' movements are evaluated and recorded in terms of electrical activity. Usually, it is patients with neuromuscular disease who are implanted with EMG sensors to evaluate the muscle activity in real time [54].

**4.6.7. Oximetry.** Oximetry is a medical technology to measure the level of oxygen in the blood with the heart rate. Patients, usually with asthma or respiratory issues, are implanted with oximetry-based sensors in order to aid medical service in case of emergency [49].

**4.6.8. Oxygen Saturation.** In medicine, the term oxygen saturation refers to the amount of oxygen-saturated hemoglobin compared to total hemoglobin. For example, patients suffering from severe anemia usually suffer from reduced arterial oxygen saturation with  $\text{SaO}_2 < 90\%$ .

## 5. Performance Estimation

A number of ways are adopted to evaluate the techniques. Most studies have adopted simulations of the techniques to evaluate the performance of the patient data privacy and security in S-CI. Simulation encryption with operation analysis [2], simulation with NS-2 simulator [3, 52, 54], and implantation with Jpair library and Netbeans for algorithm [44, 53] are other common methods.

The emergency case scenario is evaluated as the highest communication cost, with  $45,760/20 * 10^{-6} = 0.9152$  ms at 20Mbps bandwidth [50]. For the computation cost, AES symmetric encryption, SHA-256 hash function, Menezes-Vanstone cryptosystem, and signature of ECDSA are used in [50]. Similarly, the privacy authentication scheme [55] is compared to existing techniques in terms of computation and communication cost. This scheme also uses AES symmetric encryption, SHA-256 hash function, Menezes-Vanstone cryptosystem, and signature of ECDSA by ECDSA. The average time for health data request is assumed ( $m_{\text{HC}}$ ,  $m_{\text{BS}}$ , or  $m_{\text{D}}$ ) with X.509 certificate with 8192 bits and with 245760 bits. The treatment phase, with 1,230,316 bits as 3G telecommunication cost is 2Mbps/384 kbps/144 kbps, is evaluated and as the worst in terms of communication cost while, in the simulation of experiments in the ABE scheme [51], the computation time for encryption process is 28ms (milliseconds), quite low compared to other existing techniques (39ms). However, a complexity comparison with traditional encryption schemes [46] and the timing cost of operations used in ESPAC [42], evaluated by varying number of attributes [42], are commonly used to calculate time and cost complexity. Furthermore, high communication cost is evaluated on the basis of an emergency scenario, transmitting time of message in Mbps bandwidth network, in [50].

One study also used the SPSS tool to calculate function complexity, whereby an experimental setup created in Ubuntu 14.04 LTS 64-bit system [51] and ABE is compared to other existing encryption techniques in terms of computational time. Another study evaluated data sharing time with cloudlet, based on a trust model, analysed and categorized at three different levels as 'bad, average, and good.' These levels were assigned whereby individual repute ( $r$ ) was set to [0, 1], ranges with ([0, 0.2], [0.2, 0.6], [0.6, 1]) were 'bad,' 'average,'

TABLE 17: Summary of Performance Metrics.

Techniques	Performance Metrics
Multibiometric Key Generation [37]	(1) Entropy
Pairwise Key Establishment [40, 43]	(1) Encryption and decryption measured through Pairing-based Key generation = Pair (ADK), $\text{Exp}_G$ (Share Key) (2) Probability compromise for data sink = $\text{Prob}_{DS}(\alpha)$ , Probability compromise for body sensors = $\text{Prob}_{Bsr}(\gamma)$
Hash Function [47]	(1) Data transfer rate at quality factor= 0.1
Attribute-based Encryption [2, 11, 38, 39, 41-43, 43, 44, 48, 51]	(1) Computational complexity = $O( I )$ , Time Complexity = $O( S )$ (2) Computation cost = $O(n)$ , $O(m)$ (3) Sensor Data encryption = $5T_0 = T_r$ , Data decryption = $T_r$ , Key generation = $3T_0 + T_t$ (4) Key generation complexity = $O(n)$ , Encryption complexity = $O(1) \text{ mod}$ ,
Chaotic Maps [49]	(1) $T_{\text{Hash}}$ = Time of execution per hash function, $T_{\text{Sig}}$ = Time of execution for signature, $T_{\text{sym}}$ = Time of symmetric encryption/decryption
Hybrid Encryption [50]	(1) Key generation = $3T_0 + T_r$ , Data decryption = $T_r$ ,
2014 Multivalued encryption [20]	(1) Coverage time= $\text{CTFBT} \geq 1 \tau 1 - \tau \delta_P N - 1$

and ‘good,’ respectively [52]. In AYA [44], the efficiency analysis of  $C_{p\text{-ABE}}$  algorithms is by comparison, using the Jpair library in terms of set time (ms), encryption time, and decryption time.

The quantitative measurement entropy of multibiometric-based scheme compared with ECG- and EEG-based schemes shows a high entropy, meaning high security [37]. Similarly, the efficiency of the authentication system [3] is evaluated as false positive rate (FPR), false negative rate (FNR), sensitivity, specificity, and accuracy. The FPR is the ratio of negative cases reported as positive, and vice versa for FNR. However, in this analysis, 20% of nodes are assumed to be attackers:

$$\text{“FPR} = \frac{\text{False Positive}}{\text{False Positive}} + \text{True Negative”} \quad (12)$$

$$\text{“FNR} = \frac{\text{False Negative}}{\text{False Negative}} + \text{True Positive”}. \quad (13)$$

The sensitivity of the system (true positive rate) measures the negatives correctly identified:

$$\text{“Sensitivity} = \frac{\text{True Positive}}{\text{True Positive}} + \text{False Negative”}. \quad (14)$$

The accuracy of the system shows the number of accurate results in both positive and negative cases:

$$\text{“Accuracy} = \frac{\text{True Result}}{\text{True Result}} + \text{False Result”}. \quad (15)$$

In WSN [53], a hybrid encryption technique is implemented in Java and run-time patient keys are generated for transmission. The total time required for encryption and decryption varies with file size and key size. For example, key file size with 168 bytes involves encryption in 88ms and decryption in 105ms. Similarly, a data file of 1.5MB is encrypted in 421ms and decrypted in 468ms. Meanwhile, CP-ABE [4] is compared with ABE in terms of encryption and decryption

time. The comparison shows that the proposed solution, with 256 bits, is much faster than ABE. However, CP-ABE performance evolution does not show any significant gain in terms of access control. Furthermore, the ETT [54] technique is evaluated for coverage time, uncertainty, and node overhead. Coverage time is calculated with respect to packet numbers for a successful reconstruction path. The most prominent coverage time is given in  $\text{CT}_{\text{FBT}} \tau (1 - \tau)^{N-1} \geq 1$ . Similarly, the maximum uncertainty is evaluated as  $(m = (1/\tau) - 1)$ . For nodes overhead, every node selects a marking probability of  $1/d$  (for  $d = 1, 2, \dots, N$ ) for each packet, so the overhead at each is  $\text{OH}_{\text{ETT}} = n/d$ . Summary of the performance estimation metrics of the selected techniques is given in Table 17.

## 6. Future Directions and Challenges

The distributed nature of S-CI highlighted a unique set of challenges for the research community in this flourishing area. This snapshot of the domain shows the following future challenges for research opportunities.

**6.1. Lack of Standard Architecture.** There is no standard architecture available for S-CI to ensure patient data privacy and security. Most studies follow a hierarchical architecture and introduce a separate TA entity [50] for key generation and security parameters, yet other studies take the hospital as the TA entity [2] to force access policies. Therefore, there is a great need to propose a standard architecture to access PPPs in S-CI whilst maintaining patient privacy and security.

**6.2. Lack of Policy Compliance.** It has been observed that no single study follows any comprehensive policy to address patient data privacy and security rights. For example, some studies address data confidentiality [47] and fine-grained access control [41] with collision resistance [41, 48], while others totally ignore these security services and focus on DOS [54] and man-in-the-middle attack [28] with anonymity [28]. Furthermore, there have been few studies focusing on

patient participation and control [38, 53]. Similarly, just two studies have focused on auditing [43, 44]. Therefore, there is a great need for privacy and security policy compliance, such as HIPPA [73].

*6.3. Lack of Standard Dataset.* It has been observed that many studies have not used a properly defined dataset for their proposed solutions. Most of the studies have randomly utilized some common PPPs such as ECG, EGG, blood pressure, and pulse rate [10, 43, 47] as their dataset. Others just refer to it as medical data [51] or medical images [46], without specifying particular PPPs. Therefore, there is a great need to adopt some standard or 'golden' dataset.

*6.4. Lack of Handling of Patient Behaviour and Intentions.* It has been observed that how patient behaviour and intentions are handled to stimulate collaboration in social network is totally ignored [40]. Proper strategies and a trust model should be proposed to resolve this issue.

*6.5. Lack of Emergency Management.* Another important area, the emergency management, an important aspect of S-CI for PPPs real-time monitoring and access, is ignored while handling patient data privacy and security. Only a few studies handle emergencies [2, 46, 49, 50] in their solutions. There is a great need to handle emergency management using real scenarios of access.

*6.6. Lack of Data Management in Multiple Accesses.* We also observed that studies follow typical and traditional encryption techniques for S-CI for patient data monitoring and access. There is a great need to design new scenarios of data management for the distributed environment and multiple access of PPPs among various medical entities [2].

*6.7. Lack of Search Encrypted Medical Terms and Similarity Semantics.* It has been observed that no single study has reported any mechanism to search for encrypted key words of medical terms [42] and to support key word similarity semantics [44] in S-CI. Therefore, there is a great need for a search mechanism for encrypted and similarity semantics of key words in S-CI.

*6.8. Non-User-Friendly Applications.* The techniques and processes using S-CI applications should be user-friendly, from the patient perspective, especially for elderly or paralyzed patients to make it easy to follow the process [50].

*6.9. Lack of Data Public Sharing and Data Publication.* As S-CI processes a huge volume of PPPs, the sensitivity and significance of this data cannot be denied for health, technology, and government sectors. Research communities should focus on a secure design for public sharing and data publication [3].

*6.10. Scalable and Efficient Data Access Control.* It is observed that there is a need for improvement in the efficiency and scalability of techniques such as MC-ABE- and ABE- [51] based data access control in S-CI.

*6.11. Innovative Designs for Network and Transmission Security.* It is observed that network and transmission security is also ignored for S-CI. There must be improved techniques and methods for patient data privacy and security to give efficient, reliable, and continuous transmission [54].

*6.12. Unreliability and Quality of PPPs.* It is observed that no single study has proposed any technique to check the reliability and the quality of PPPs. As PPPs are very sensitive medical data [7], for the timely diagnosis and response to provide medical aid, there must be techniques to trace PPPs' quality and reliability with PPPs' privacy and security in S-CI.

*6.13. Real-Time Implementation and Integration.* It is observed that techniques are simulated in artificial environment for experiment in this research area. Therefore, techniques [70] should be implemented and integrated as real time in UEC-Eucalyptus platform to help with future enhancement.

## 7. Conclusion

This study has provided a detailed literature review of patient data privacy and security in S-CI. So far, we can clearly see that many techniques are proposed for mobile healthcare and e-healthcare and that there is much scope in the areas of research into health data management and health data aggregation. Meanwhile, this research area lacks in standard architecture, policy compliance, standard dataset, handling patient behaviour, search of encrypted medical terms, data sharing, data publication, and emergency and multiple access data management. Similarly, S-CI needs special attention in terms of user-friendly applications, non-user-friendly applications, efficient access control, network security, real-time implementation, and improved quality of patient data access. We also propose a generic framework, extracted from the available literature. Our framework is quite innovative and applicable to the research community. We have discussed performance estimation measures and various security services of the techniques proposed for patient data privacy and security in S-CI. Finally, we believe that our roadmap of this flourishing and innovative research area will be beneficial to highlight future enhancement.

## Conflicts of Interest

The author declares that there are no conflicts of interest regarding the publication of this paper.

## Acknowledgments

This article has been awarded by the National Natural Science Foundation of China (61170035, 61272420, 81674099), the Fundamental Research Fund for the Central Universities (30916011328, 30918015103), and Nanjing Science and Technology Development Plan Project (201805036).



## References

- [1] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2688–2710, 2010.
- [2] A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal, "Healing on the cloud: secure cloud architecture for medical wireless sensor networks," *Future Generation Computer Systems*, vol. 55, pp. 266–277, 2016.
- [3] A. A. V. Rani and E. Baburaj, "An efficient secure authentication on cloud based e-health care system in WBAN," *Biomedical Research (India)*, vol. 2016, pp. S53–S59, 2016.
- [4] A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal, "Secure and scalable cloud-based architecture for e-Health wireless sensor networks," in *Proceedings of the 2012 21st International Conference on Computer Communications and Networks, ICCCN 2012*, Germany, August 2012.
- [5] R. Negra, I. Jemili, and A. Belghith, "Wireless body area networks: applications and technologies," *Procedia Computer Science*, vol. 83, pp. 1274–1281, 2016.
- [6] A. Grady, S. Yoong, R. Sutherland, H. Lee, N. Nathan, and L. Wolfenden, "Improving the public health impact of eHealth and mHealth interventions," *Australian and New Zealand Journal of Public Health*, vol. 42, no. 2, 2018.
- [7] S. M. S. K. Dash and P. K. Pattnaik, "A survey on applications of wireless sensor network using cloud computing," *International Journal of Computer Science & Emerging Technologies*, vol. 1, pp. 50–55, 2010.
- [8] A. Alamri, W. S. Ansari, M. M. Hassan, M. S. Hossain, A. Alelaiwi, and M. A. Hossain, "A survey on sensor-cloud: architecture, applications, and approaches," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 917923, 18 pages, 2013.
- [9] A. Tewari and P. Verma, "Security and privacy in e-healthcare monitoring with WBAN: a critical review," *International Journal of Computer Applications*, vol. 136, no. 11, pp. 37–42, 2016.
- [10] A. Sajid and H. Abbas, "Data privacy in cloud-assisted healthcare systems: state of the art and future challenges," *Journal of Medical Systems*, vol. 40, no. 155, pp. 1–16, 2016.
- [11] A. Celesti, F. Celesti, M. Fazio, P. Bramanti, and M. Villari, "Are next-generation sequencing tools ready for the cloud?" *Trends in Biotechnology*, vol. 35, no. 6, pp. 486–489, 2017.
- [12] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," *Egyptian Informatics Journal*, vol. 180, no. 2, pp. 113–122, 2016.
- [13] H.-P. Chiang, C.-F. Lai, and Y.-M. Huang, "A green cloud-assisted health monitoring service on wireless body area networks," *Information Sciences*, vol. 284, pp. 118–129, 2014.
- [14] I. Masood, *Patient Data Privacy and Security in Sensor-Cloud Infrastructure: Past Present Future*, vol. 35, ACM Computing Surveys, 4 edition, 2018.
- [15] A. D. I. Bisio, F. Lavagetto, and A. Sciarrone, "EHealth in the future of medications management: personalisation, monitoring and adherence," *IEEE Internet of Things Journal*, vol. 4, pp. 135–146, 2017.
- [16] F. Firouzi, A. M. Rahmani, K. Mankodiya et al., "Internet-of-Things and big data for smarter healthcare: From device to architecture, applications and analytics," *Future Generation Computer Systems*, vol. 78, pp. 583–586, 2018.
- [17] T. Péteri, N. Varga, and L. Bokor, "A Survey on Multimedia Quality of Experience Assessment Approaches in Mobile Healthcare Scenarios," in *eHealth 360°*, vol. 181 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp. 484–491, Springer International Publishing, Cham, 2017.
- [18] E. Klaoudatou, E. Konstantinou, G. Kambourakis, and S. Gritzalis, "A survey on cluster-based group key agreement protocols for WSNs," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 3, pp. 429–442, 2011.
- [19] R. Hummen, M. Henze, D. Catrein, and K. Wehrle, "A Cloud design for user-controlled storage and processing of sensor data," in *Proceedings of the 2012 4th IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2012*, pp. 233–240, Taiwan, December 2012.
- [20] N. D. Han, L. Han, D. M. Tuan, H. P. In, and M. Jo, "A scheme for data confidentiality in cloud-assisted wireless body area networks," *Information Sciences*, vol. 284, no. 5, pp. 157–166, 2014.
- [21] M. Yuriyama and T. Kushida, "Sensor-cloud infrastructure—physical sensor management with virtualized sensors on cloud computing," in *Proceedings of the 13th International Conference on Network-Based Information Systems (NBIS '10)*, pp. 1–8, September 2010.
- [22] M. Chen, "NDNC-BAN: supporting rich media healthcare services via named data networking in cloud-assisted wireless body area networks," *Information Sciences*, vol. 284, no. 10, pp. 142–156, 2014.
- [23] S. Sharma, K. Chen, and A. Sheth, "Towards practical privacy-preserving analytics for IoT and cloud based healthcare systems," *IEEE Internet Computing*, vol. 22, pp. 42–51, 2018.
- [24] C. Ernsting, S. U. Dombrowski, M. Oedekoven et al., "Using smartphones and health apps to change and manage health behaviors: A population-based survey," *Journal of Medical Internet Research*, vol. 19, no. 4, article no. e101, 2017.
- [25] T. Amjad, M. Sher, and A. Daud, "A survey of dynamic replication strategies for improving data availability in data grids," *Future Generation Computer Systems*, vol. 28, no. 2, pp. 337–349, 2012.
- [26] I. Masood, Y. Wang, A. Daud, N. R. Aljohani, and H. Dawood, "Privacy management of patient physiological parameters," *Telematics and Informatics*, vol. 35, no. 4, pp. 677–701, 2018.
- [27] G. Kambourakis, E. Klaoudatou, and S. Gritzalis, "Securing medical sensor environments: The CodeBlue framework case," in *Proceedings of the 2nd International Conference on Availability, Reliability and Security, ARES 2007*, pp. 637–643, Australia, April 2007.
- [28] C.-T. Li, T.-Y. Wu, C.-L. Chen, C.-C. Lee, and C.-M. Chen, "An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system," *Sensors*, vol. 17, no. 7, 2017.
- [29] R. S. Ponmagal, N. Dinesh, and U. Rajaram, "Design and development of secure cloud architecture for sensor services," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*, vol. 8956, pp. 339–344, 2015.
- [30] M. Henze, L. Hermerschmidt, D. Kerpen, R. Häußling, B. Rumpe, and K. Wehrle, "A comprehensive approach to privacy in the cloud-based Internet of Things," *Future Generation Computer Systems*, vol. 56, pp. 701–718, 2016.
- [31] Q. Jiang, M. K. Khan, X. Lu, J. Ma, and D. He, "A privacy preserving three-factor authentication protocol for e-Health clouds," *The Journal of Supercomputing*, vol. 72, no. 10, pp. 3826–3849, 2016.

- [32] 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, 2012.
- [33] E. Bertino, "Data security and privacy," in *Proceedings of the in IEEE 40th Annual Computer Software and Applications Conference*, 2016.
- [34] A. Abbas and S. U. Khan, "E-health cloud: Privacy concerns and mitigation strategies," *Medical Data Privacy Handbook*, pp. 389–421, 2015.
- [35] W. Khan, A. Daud, J. A. Nasir, and T. Amjad, "A survey on the state-of-the-art machine learning models in the context of NLP," *Kuwait Journal of Science*, vol. 43, no. 4, pp. 95–113, 2016.
- [36] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *Journal of Medical Systems*, vol. 36, no. 1, pp. 93–101, 2012.
- [37] F. A. Khan, A. Ali, H. Abbas, and N. A. H. Haldar, "A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks," in *Proceedings of the 9th International Conference on Future Networks and Communications, FNC 2014 and the 11th International Conference on Mobile Systems and Pervasive Computing, MobiSPC 2014*, pp. 511–517, Canada, August 2014.
- [38] Z. Guan, T. Yang, and X. Du, "Achieving secure and efficient data access control for cloud-integrated body sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2015, 2015.
- [39] Z. Guan, T. Yang, X. Du, and M. Guizani, "Secure data access for wireless body sensor networks," in *Proceedings of the 2016 IEEE Wireless Communications and Networking Conference, WCNC 2016*, Qatar, April 2016.
- [40] J. Zhou, Z. Cao, X. Dong, N. Xiong, and A. V. Vasilakos, "4S: a secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks," *Information Sciences*, vol. 314, pp. 255–276, 2015.
- [41] Q. Huang, L. Wang, and Y. Yang, "Secure and privacy-preserving data sharing and collaboration in mobile healthcare social networks of smart cities," *Security and Communication Networks*, vol. 2017, pp. 1–12, 2017.
- [42] M. Barua, X. Liang, R. Lu, and X. Shen, "ESPAC: enabling security and patient-centric access control for ehealth in cloud computing," *International Journal of Security & Networks*, vol. 6, no. 2-3, pp. 67–76, 2011.
- [43] L.-Y. Yeh, P.-Y. Chiang, Y.-L. Tsai, and J.-L. Huang, "Cloud-based fine-grained health information access control framework for lightweight IoT devices with dynamic auditing and attribute revocation," *IEEE Transactions on Cloud Computing*, no. 99, 2015.
- [44] K. Martin and W. Wang, "Aya: An efficient access-controlled storage and processing for cloud-based sensed data," in *Proceedings of the 12th International Computer Conference on Wavelet Active Media Technology and Information Processing, ICCWAMTIP 2015*, pp. 130–134, China, December 2015.
- [45] J. Zhou, Z. Cao, X. Dong, and X. Lin, "PPDM: A privacy-preserving protocol for cloud-assisted e-Healthcare systems," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 7, pp. 1332–1344, 2015.
- [46] K. Zhang, X. Liang, M. Baura, R. Lu, and X. Shen, "PHDA: a priority based health data aggregation with privacy preservation for cloud assisted WBANs," *Information Sciences*, vol. 284, pp. 130–141, 2014.
- [47] S. Saha, "Secure sensor data management model in a sensor-cloud integration environment," in *Proceedings of the 2015 2nd International Conference on Applications and Innovations in Mobile Computing, AIMoC 2015*, pp. 158–163, India, February 2015.
- [48] H. He, J. Zhang, J. Gu, Y. Hu, and F. Xu, "A fine-grained and lightweight data access control scheme for WSN-integrated cloud computing," *Cluster Computing*, vol. 20, no. 2, pp. 1457–1472, 2017.
- [49] C.-T. Li, C.-C. Lee, and C.-Y. Weng, "A secure cloud-assisted wireless body area network in mobile emergency medical care system," *Journal of Medical Systems*, vol. 40, no. 5, Article ID 117, 2016.
- [50] J.-X. Hu, C.-L. Chen, C.-L. Fan, and K.-H. Wang, "An intelligent and secure health monitoring scheme using IoT sensor based on cloud computing," *Journal of Sensors*, vol. 2017, Article ID 3734764, 11 pages, 2017.
- [51] P. G. Shynu and K. J. Singh, "An enhanced ABE based secure access control scheme for E-health clouds," *International Journal of Intelligent Engineering and Systems*, vol. 10, no. 5, pp. 29–37, 2017.
- [52] M. Chen, Y. Qian, J. Chen, K. Hwang, S. Mao, and L. Hu, "Privacy protection and intrusion avoidance for cloudlet-based medical data sharing," *IEEE Transactions on Cloud Computing*, vol. PP, no. 9, pp. 1–9, 2016.
- [53] S. Saha, R. Das, S. Datta, and S. Neogy, "A cloud security framework for a data centric WSN application," in *Proceedings of the 17th International Conference*, pp. 1–6, Singapore, Singapore, January 2016.
- [54] R. Latif, H. Abbas, S. Latif, and A. Masood, "Distributed denial of service attack source detection using efficient traceback technique (ETT) in cloud-assisted healthcare environment," *Journal of Medical Systems*, vol. 40, no. 161, pp. 1–13, 2016.
- [55] C.-L. Chen, T.-T. Yang, M.-L. Chiang, and T.-F. Shih, "A privacy authentication scheme based on cloud for medical environment," *Journal of Medical Systems*, vol. 38, article no. 143, 2014.
- [56] F. Nadeem and R. Qaiser, "An early evaluation and comparison of three private cloud computing software platforms," *Journal of Computer Science and Technology*, vol. 30, no. 3, pp. 639–654, 2015.
- [57] J. Araujo, R. Matos, V. Alves et al., "Software aging in the eucalyptus cloud computing infrastructure: Characterization and rejuvenation," *ACM Journal on Emerging Technologies in Computing Systems*, vol. 10, no. 1, 2014.
- [58] SNIA, "CloudDataManagementInterface(CDMI)Version1.0.1/," <http://cdmi.sniacloud.com/S>, 2011.
- [59] G. Galante, L. C. Erpen De Bona, A. R. Mury, B. Schulze, and R. da Rosa Righi, "An analysis of public clouds elasticity in the execution of scientific applications: a survey," *Journal of Grid Computing*, vol. 14, no. 2, pp. 193–216, 2016.
- [60] T. Chippendale, P. A. Gentile, M. K. James, and G. Melnic, "Indoor and outdoor falls among older adult trauma patients: A comparison of patient characteristics, associated factors and outcomes," *Geriatrics & Gerontology International*, vol. 17, no. 6, pp. 905–912, 2017.
- [61] G. N. Boysen, M. Nyström, L. Christensson, J. Herlitz, and B. W. Sundström, "Trust in the early chain of healthcare: Lifeworld hermeneutics from the patient's perspective," *International Journal of Qualitative Studies on Health and Well-being*, vol. 12, no. 1, 2017.

- [62] M. B. M. Nateghizad and M. A. Maarof, "Secure searchable based asymmetric encryption in cloud computing," *International Journal of Advances in Soft Computing and Its Applications*, vol. 6, no. 1, pp. 1–13, 2014.
- [63] N. Saini, N. Pandey, and A. P. Singh, "Enhancement of security using cryptographic techniques," in *Proceedings of the 4th International Conference on Reliability, Infocom Technologies and Optimization, ICRITO 2015*, India, September 2015.
- [64] J. Patel, "Secure hashing algorithm and advance encryption algorithm in cloud computing," *International Journal of Computer and Information Engineering*, vol. 11, pp. 754–758, 2017.
- [65] N. Koblitz and A. Menezes, "Pairing-based cryptography at high security levels," in *Cryptography and Coding*, vol. 3796 of *Lecture Notes in Computer Science*, pp. 13–36, Springer Berlin Heidelberg, Berlin, Heidelberg, 2005.
- [66] N. El Mrabet, J. J. Fournier, L. Goubin, and R. Lashermes, "A survey of fault attacks in pairing based cryptography," *Cryptography and Communications*, vol. 7, no. 1, pp. 185–205, 2015.
- [67] Z. Lv, J. Chi, M. Zhang, and D. Feng, "Efficiently attribute-based access control for mobile cloud storage system," in *Proceedings of the 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2014*, pp. 292–299, China, September 2014.
- [68] S. Saleh, A. Farah, H. Dimassi et al., "Using mobile health to enhance outcomes of noncommunicable diseases care in rural settings and refugee camps: randomized controlled trial," *JMIR mHealth and uHealth*, vol. 6, no. 7, p. e137, 2018.
- [69] L. Liu, H. Zhang, X. Yu, Y. Xin, M. Shafiq, and M. Ge, "An efficient security system for mobile data monitoring," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 9809345, 10 pages, 2018.
- [70] A. Waqar, A. Raza, H. Abbas, and M. K. Khan, "A framework for preservation of cloud users' data privacy using dynamic reconstruction of metadata," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 235–248, 2013.
- [71] D. Nuñez, I. Agudo, and J. Lopez, "NTRUREncrypt: An efficient proxy re-encryption scheme based on NTRU," in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, ASIACCS 2015*, pp. 179–189, Singapore, April 2015.
- [72] T. Schradi and G. Tivig, "Representation of a review of a patent's physiological parameters," *Google Patents*, 1999.
- [73] W. B. Lee and C. D. Lee, "A cryptographic key management solution for HIPAA privacy/security regulations," *IEEE Transactions on Information Technology in Biomedicine*, vol. 12, no. 1, pp. 34–41, 2008.





**Hindawi**

Submit your manuscripts at  
[www.hindawi.com](http://www.hindawi.com)

