IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received June 24, 2021, accepted July 6, 2021, date of publication July 20, 2021, date of current version July 30, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3098708

A Review of the State of the Art in Privacy and Security in the eHealth Cloud

AQEEL SAHI, DAVID LAI, AND YAN LI, (Member, IEEE)
University of Southern Queensland, Toowoomba, QLD 4350, Australia

Corresponding author: Aqeel Sahi (u1050771@usq.edu.au)

This work was supported by the University of Southern Queensland.

ABSTRACT The proliferation and usefulness of cloud computing in eHealth demands high levels of security and privacy for health records. However, eHealth clouds pose serious security and privacy concerns for sensitive health data. Therefore, practical and effective methods for security and privacy management are essential to preserve the privacy and security of the data. To review the current research directions in security and privacy in eHealth clouds, this study has analysed and summarized the state of the art technologies and approaches reported in security and privacy in the eHealth cloud. An extensive review covering 132 studies from several peer-reviewed databases such as IEEE Xplore was conducted. The relevant studies were reviewed and summarized in terms of their benefits and risks. This study also compares several research works in the domain of data security requirements. This paper will provide eHealth stakeholders and researchers with extensive knowledge and information on current research trends in the areas of privacy and security.

INDEX TERMS Cloud security, cloud privacy, eHealth cloud.

I. INTRODUCTION

The official definition of cloud computing, according to the National Institute of Standards and Technology (NIST) is: *cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction* [1]. Over the last decade, cloud computing has gained popularity within the health sector, as it offers several advantages such as low costs and flexible processes [2]. Cloud-based health services allow physicians, patients, and owners of health data (health departments or health organizations) to control and share their data easily. However, eHealth cloud computing poses a range of challenges, such as data security and privacy for both clients and cloud service providers (CSPs) [3]–[5]. Security and privacy issues undermine confidence in an open network and semi-trusted servers which may lose, leak, or disclose data [6]. These can allow breaches in users' privacy when sharing data in a public cloud.

A great deal of research has been done to target the security and privacy issues associated with eHealth clouds, and many solutions have been suggested. To obtain a clear picture of the security and privacy problems that can affect eHealth clouds, this study has reviewed and summarized the current state of the art in eHealth security and privacy studies from the year of 2013 to 2021. The aim of this study is to deliver a clear and complete picture of eHealth security and privacy issues and their proposed solutions through reviewing the relevant recent research studies. As shown in Figure 1, we divide our literature study into five main categories: security and privacy, security controls, effective encryption, data security requirements, and disaster recovery plans.

Although cloud computing is widely used in the health sector, numerous issues remain unresolved [7]–[10]. Several studies have been reported to review the research work in security and privacy in eHealth clouds [4], [11]–[14]. However, some of these studies are now rather outdated, and others do not cover certain vital aspects such as access control, revocation and data recovery plans, in cloud security and privacy. In addition, some of the existing review papers focus on either the privacy of the cloud or the security of the cloud, but not both. In this paper we review most of the recent studies in both security and privacy areas.

A. REVIEW PAPERS SELECTION

In this research, the review papers were collected from research databases and search engines, including IEEE

The associate editor coordinating the review of this manuscript and approving it for publication was Fan-Hsun Tseng.

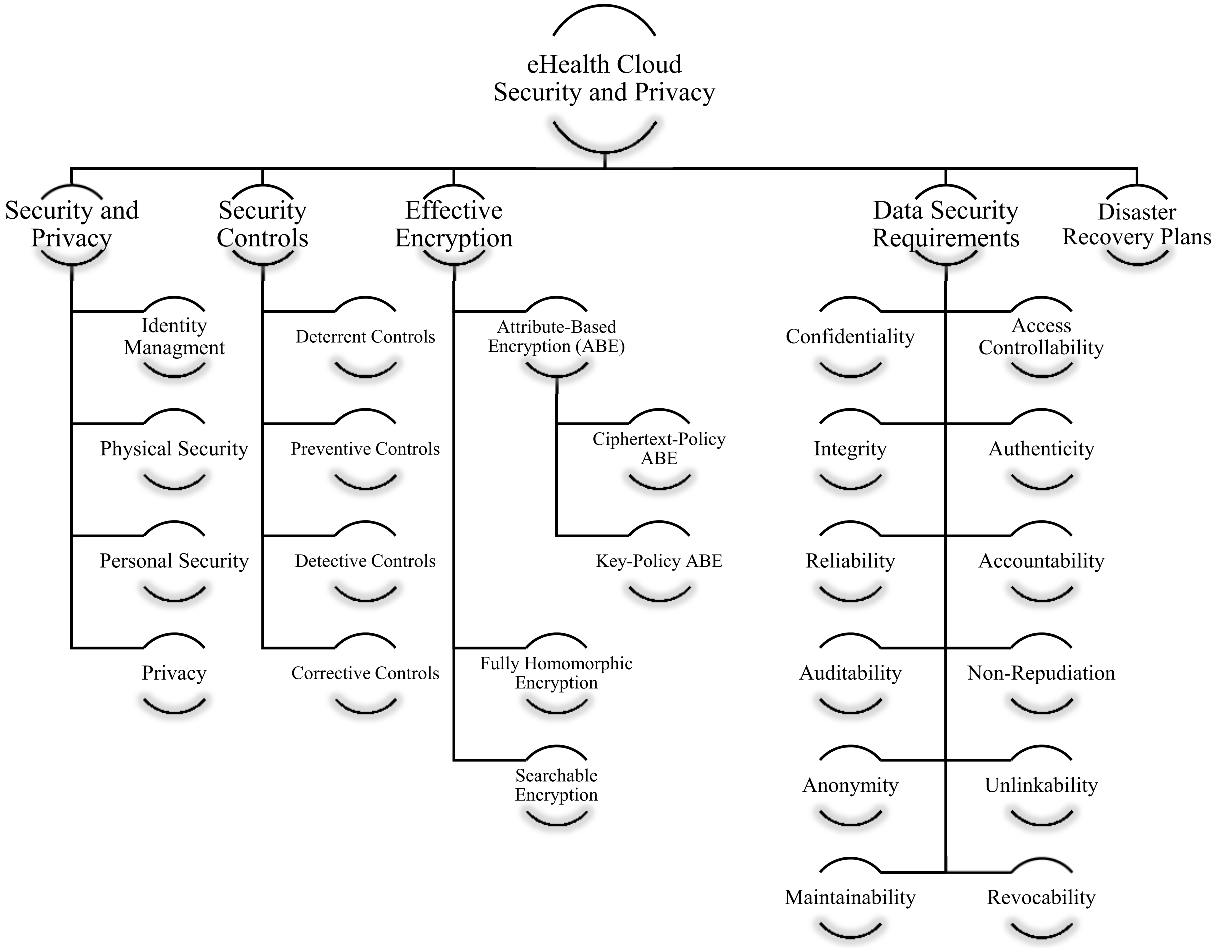


FIGURE 1. Security and privacy literature taxonomy for the eHealth cloud research.

Xplore, Springer, Elsevier Science Direct, and Google Scholar. Those databases contain large amounts of studies from journals and conferences that are relevant to security and privacy in eHealth clouds. The review papers were selected from the period of 2013 to 2021, with some exceptions such as very well-known older articles that couldn't be ignored, such as [15]. We used search terms such as "eHealth cloud security and privacy", "*eHealth cloud access control", "eHealth cloud encryption", "eHealth cloud security requirements", and "eHealth cloud recovery plans".* The function words AND, OR, and NOT were also used to perform advanced searches, such as "*eHealth cloud revocation"* AND ("*integrity*" OR "*access control*"). Finally, we reviewed the selected papers according to their titles, abstracts, keywords and conclusions to include the most relevant papers and to exclude irrelevant ones from the study. Figure 2 shows the inclusion and exclusion processes, and Figure 3 shows the distribution of the selected articles over the years.

The key contributions of this study are as follows: we conducted an extensive literature review, and summaries the state of the art in eHealth security and privacy schemes. We classify the papers into five categories, as shown in Figure 1. We discuss the advantages and limitations covered in the reviewed papers to facilitate better security and privacy in eHealth clouds. This study will benefit eHealth decision makers and researchers with advanced knowledge and information on current research trends in the areas of privacy and security to make better-informed decisions.

The remainder of this paper is organized as follows, using a structure similar to that of Figure 1. Section 2 describes the proposed schemes with regard to the security and privacy of eHealth clouds. Section 3 describes the proposed schemes with regard to security controls. Section 4 describes effective encryption of eHealth clouds. Section 5 discusses the data security requirements of the eHealth cloud. Section 6 describes disaster recovery plans, and Section 7 concludes this study.

II. KEY SECURITY AND PRIVACY ASPECTS IN THE CLOUD

Cloud computing is a model commonly used to save money and effort in many sectors, and particularly in the health sector. However, despite the benefits of eHealth clouds, there

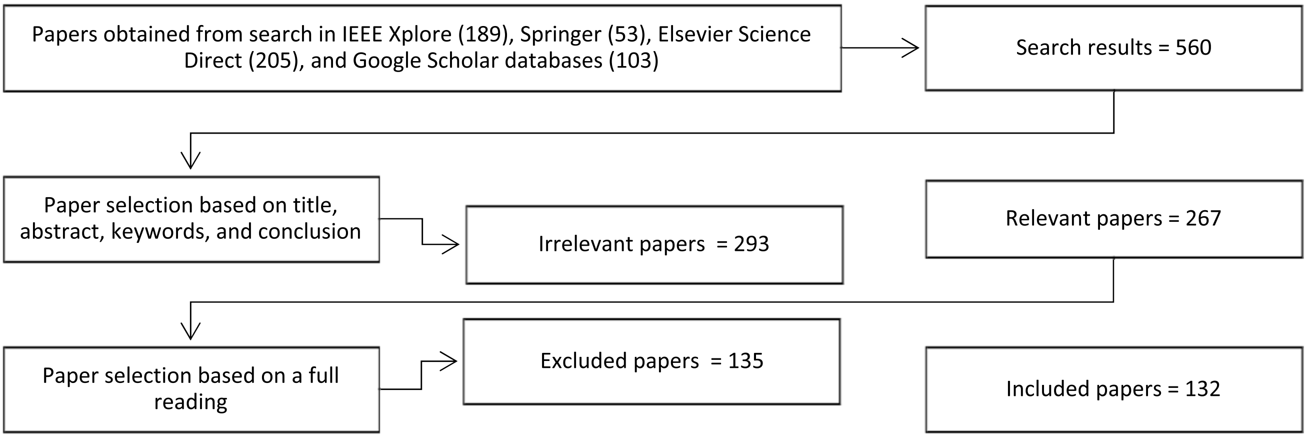

Papers obtained from search in IEEE Xplore (189), Springer (53), Elsevier Science Direct (205), and Google Scholar databases (103)
Search results = 560
Paper selection based on title, abstract, keywords, and conclusion
Irrelevant papers = 293
Relevant papers = 267
Paper selection based on a full reading
Excluded papers = 135
Included papers = 132

FIGURE 2. The inclusion/exclusion process.

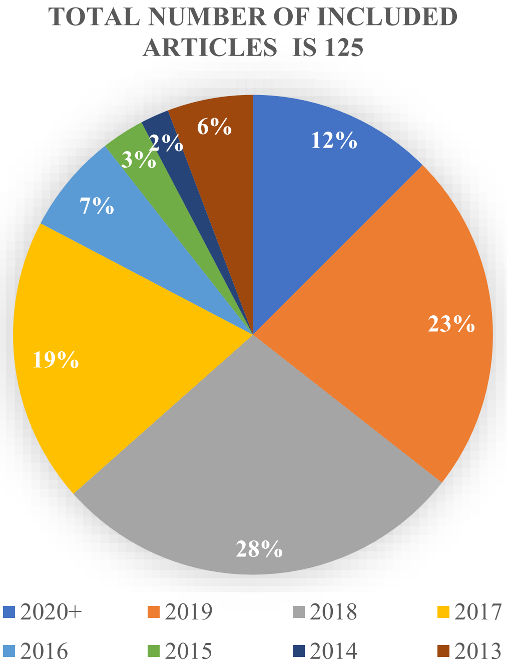


FIGURE 3. Distribution of the selected articles by year.

are many unresolved issues regarding security and privacy which require a great deal of research to be resolved [16].

A. IDENTITY MANAGEMENT

An Identity Management System (IMS) is a comprehensive organizational system used to identify entities in a cloud project. Access to information and resources in the project is managed by linking client privileges and constraints with a proven identity. The main aim of an IMS is to determine what clients can do within a cloud project and under what conditions [17]. In addition, an IMS is utilized to improve the security and privacy of a cloud system, and to reduce the running costs and effort. Many studies have reported on identity management [15], [18]–[26].

To manage the access to data and resources, cloud service providers (CSPs) use either their own IMS (such as CloudID [18]), or incorporate the client's IMS into their infrastructure [18], for example using a biometric-based IMS to preserve the privacy of the cloud project's information [18]. A biometric-based IMS is used to connect the private data of the clients to their biometrics, which are saved as ciphertexts. To ensure that the CSPs or any possible attackers cannot obtain any type of access to private information, the proposed biometric-based IMS is implemented in an encrypted domain using a searchable cryptographic system.

In 2017 Wang *et al.* proposed a cost-effective secure eHealth cloud system using an Identity Based Encryption (IBE) method [19]. In that system, there are four parties with different roles: the cloud, the health community, physicians, and patients. The system works as follows. Firstly, the system sets up public and private keys for all parties according to their published identities (e.g. email addresses). Those identities are considered public keys, and are used to generate private keys using an IBE algorithm. Secondly, the Electronic Health Records (EHRs) are encrypted by the parties using a block cipher algorithm such as AES, and the keys are encrypted using the IBE and sent to the cloud. Following that, the parties can receive the encrypted EHRs from the cloud, and decrypt them using their identity keys.

According to a survey conducted in [20], more than 66% of users' identities are stored in unsafe places. Khalil *et al.* [20], therefore, proposed an IMS system called the Consolidated Identity Management (CIDM) system, which they claimed was resistant to certain attacks such as server compromise attacks, mobile device compromise attacks, and traffic interception attacks [20]. The CIDM structure was a public key cryptosystem. It split permission identifications and spread them between the parties at the IMS to prevent traffic interception attacks. In order to mitigate mobile device compromise attacks, a challenge-response approach was adopted. Finally, the security of the communication channels between the CIDM and the CSPs was addressed to reduce the possibility of any effective compromise of that channel [20]. However, further investigation is required to resolve the problem of insufficiently dynamic federated identities and privacy in most current IMS systems [21]. This is an architectural problem and must be considered at the design level.

Haufe *et al.* proposed a framework named the Information Security Management System (ISMS) [22], consisting of many vital security procedures for eHealth clouds. The proposed security management framework was implemented based on the ISO 27000 family of standards. The ISMS was able to identify the most frequent cloud computing threats and the information they aimed to collect were from the cloud system [22]. One drawback is that the ISMS needs specific details from processes, such as input, output, and interfaces, to facilitate communication and interaction between processes.

In a different study, the concept of Identity Management as a Service (IDaaS) was discussed [23]. In that work, the authors proposed an IMS called BlindIdM which preserved the privacy of data and delivered them as IDaaS. Specifically, the authors described how a system based on the Security Assertion Markup Language (SMAL) was employed with proxy encryption to enhance the security of the cloud projects with respect to the CSPs [23]. To improve the proposed system, extending the IDaaS from a single domain to a cross-domain approach has been suggested, as in the System for Cross-domain Identity Management (SCIM) [24], [25].

Xiong *et al.* proposed a scheme named Privacy Reserving Identity and Access Management (PRIAM) [26] that has five components of registration, token withdrawal, tenant pre-authorization, access control, and token spending. PRIAM is described as being able to fulfill all the requirements of cloud security. The proposed scheme used a hash function, signature, and mutual authentication to ensure the privacy of clients. In order to deliver the secured access control for clients and CSP, it utilized a service-level agreement. Burrows Abadi Needham (BAN) logic was finally used to confirm the correctness of the scheme [15].

B. PHYSICAL SECURITY

Physical security is the concept of securing and controlling access to servers, storage, and workstations. In other words, the aim of physical security is to prevent intruders from accessing cloud physical facilities [27]. Cloud hardware, such as servers, switches etc., are also physically secured by the CSPs from any unusual activities such as attacks, threats, and floods [28], and is provided with the necessary power supplies to reduce any potential interruptions. Typical research was reported in [28]–[31].

Mxoli *et al.* showed that to protect Personal Health Records (PHRs) from any physical intrusion, system hardware must have a physical security border [29]. For example, physical access control, offices and rooms must be secured, and resistance against natural disasters and other environmental situations must be available. All of these security borders must be in place to ensure that the cloud and network equipment are not readily accessible to the public. The equipment and applications used by the CSPs, which may contain PHRs, must not be moved out of the site or repositioned without the administrator's authorization [29].

The IT equipment building, or the site where data centres and other cloud hardware are located, must be properly secured. Rodrigues *et al.* highlighted that these buildings must be secured by security staff members, video surveillance systems and Intrusion Detection Systems (IDS). In addition, only authorized people should be allowed to enter the building using authenticated access controls [30].

Carlson stated that CSPs should adopt Federal Information Security Management Act (FISMA) standards to ensure the physical security of their records. Since physical entrances to the physical machines and storage devices are a possible route for data compromise, FISMA must be implemented at client sites as well as server sites [31].

C. PRIVACY

CSPs use encryption and other techniques to preserve the privacy of clients' critical information, such as credit card numbers, and only authorized clients have the right to access this kind of information [32]–[34]. Security is about the protection of unauthorized data access, while privacy is about the protection of user identity. The specific differences are, however, more complex, and there can certainly be areas of overlap between the two. A lot of research have been done in eHealth cloud privacy [32], [35]–[44].

Abbas *et al.* reviewed the state of the art in eHealth cloud privacy in 2014 [14]. Here, in this study we aim to cover not only the issues regarding privacy, but also other security concerns, such as storage security, access controls, and disaster recovery plans etc. In this section, we will therefore first review some of the proposed approaches with regard to eHealth privacy. Earlier studies on privacy preservation approaches can be found in Abbas *et al.*'s paper [14].

A three-factor authentication protocol based on Elliptic Curve Cryptography (ECC) was proposed by Yeh *et al.* in 2013 [35]. The protocol had certain disadvantages such as a vague procedure, impractical IDs, and no shared key [36]. In addition, the protocol could not prevent spoofing attacks [36]. Another authentication protocol based on a fingerprint was proposed by Khan *et al.* [37]. However, this protocol could not mitigate impersonation or desynchronization attacks [36]. To overcome the weaknesses of these protocols, Wu *et al.* proposed a new biometrics-based three-factor authentication protocol that can overcome all those drawbacks as well as ensuring the privacy of clients [36]. This protocol used the ECC and mobile devices, and adopted a fuzzy extractor to deal with inadequate biometric inputs. The protocol proposed by Wu *et al.* was formally proved using random oracles and Elliptic Curve Gap Diffie–Hellman (ECGDH) problem assumption to demonstrate the low probability of success of these attacks [36]. However, this protocol is vulnerable to other attacks such as impersonation and offline password guessing attacks if the mobile device falls into the wrong hands. In addition, the user revocation procedure was not included in that protocol [38]. Therefore, another three-factor authentication protocol that can resist these attacks and offers more security features was proposed by Jiang *et al.* in 2016 [38].

Yang *et al.* presented a privacy preservation approach for health records in eHealth clouds [39]. This approach was based on the classification of health record attributes. It collected these attributes vertically from the health dataset in order to ensure that those were collected from all areas of the dataset with different privacy aspects. Their approach consisted of four steps: (1) vertical data collection, (2) data merging, (3) integrity checks and (4) plain and cipher text searches. Cryptography and statistical analysis were combined to create multiple approaches which can strike a balance between the use of health records and privacy preservation [39]. However, this approach did not consider the situation where several users would use the service at the same time.

Another scheme proposed by Sahi *et al.* aimed to preserve the privacy of the PHRs [40]. This scheme adopted a three-party password-based authenticated key exchange protocol (3PAKE) based on the computational Diffie–Hellman assumption proposed by Khader and Lai [41]. The scheme used a different generator and primitive root in each session to ensure that only the specific client has complete access to his/her PHR and clients are revoked at the end of the session. This can ensure that old session keys cannot be used to access a client's PHRs. A disaster recovery plan and a break-glass technique are also addressed in that scheme.

According to Wang *et al.*, cryptography can be very expensive when it is used to preserve the privacy of health records in the cloud [42]. As a result, they proposed a privacy preserving scheme that transferred sensitive health information to a trusted private cloud and the remaining non-sensitive part to a public one. Two protocols were involved in the scheme. The first was used to preserve the privacy of the clients, and the second was used to resist any potential collusion between user records and the public CSPs. To ensure the privacy of sensitive information, the dataset was divided into several parts. The fragmented information was distributed among clouds and could be re-joined [42].

Based on the HireSome-I method, an improved history record-based service optimization method (HireSome-II) was proposed by Dou *et al.* in 2015 [43]. HireSome-II was proposed to ensure the privacy of big data such as health records in cloud computing. The cloud rejects requests that can reveal transaction information for privacy reasons, and the proposed method can efficiently support the cloud service structure to complete transactions securely [43].

Another framework to ensure the privacy of patient data was proposed by Page *et al.* [44]. This framework combined monitoring and analytic methods to deliver secure and authenticated health records. This framework was based on fully homomorphic encryption (FHE). However, FHE was known as a slow technique. To measure the practicality of the proposed framework, therefore, the authors developed a proof of concept and prototype system [44].

III. CLOUD SECURITY CONTROLS

Security approaches are effective in cloud environments when an excellent protection mechanism is adopted. This mechanism must identify the potential problems that may arise during the management process. These problems are addressed and considered by security controls, thus preserving the security of the system from its own weaknesses and reducing the number of attacks [11], [45]. There are many cloud security controls which can be categorized as follows [46]–[61].

A. DETERRENT CONTROLS

Deterrent controls aim to reduce the number of attacks on a cloud project. A "No Trespassing" sign can alert security personnel to watch out for intruders as well as highlighting the consequences of intrusion. Deterrent controls serve to warn attackers that there will be penalties and punishments if they proceed with attacks [46], [47].

B. PREVENTIVE CONTROLS

Preventive controls aim to secure cloud projects by preventing or decreasing vulnerabilities. For example, an effective authentication protocol can ensure the security of the cloud's clients and prevent any unauthorized access to that cloud. Preventive controls can, therefore, help the cloud system to confidently identify its clients [46], [47]. A preventive control could be writing a piece of code that disables inactive ports to ensure that there are no available entry points for hackers. Maintaining a strong user authentication system is another way of reducing vulnerability to attack.

C. DETECTIVE CONTROLS

Detective controls aim to detect and respond appropriately to attacks which could threaten the cloud system. During an attack, the detective control will notify the preventive control or the corrective control to report the problem. An intrusion detection system (IDS) is typically used as a detective control [2], [3].

D. CORRECTIVE CONTROLS

Corrective controls aim to reduce the damage of an attack. These controls are usually initiated during or after attacks. Restoring a cloud system from a backup to ensure the availability of services is an example of a corrective control [46], [47].

Generally, access controls are linked to security policies delivered to clients while accessing the service [62], [63]. A company typically has its own security controls which allow staff members access to a set of data rather than giving them full data access. This control limits the access of a staff member to a particular group of data. These kinds of security controls need to be put in place in cloud projects to avoid unauthorized access. The Software as a Service (SaaS) model must be sufficiently elastic to combine the set of controls offered by the company [48].

Recently, much research has been done on cloud security controls. We discuss some of these studies in the following paragraphs.

Many stakeholders attempt to access PHRs without authorization. Access control is therefore a major problem for the privacy of data when health records are stored and shared in the cloud. Thus, a dynamic access control is necessary to ensure the privacy of the stored health records. Son *et al.* [49] propose a dynamic access control scheme for securing the privacy of the PHRs in cloud projects [49]. Their scheme can detect unauthorized access dynamically by altering the context information, meaning that even if the subject has the same role, access authorization will not be defined in the same way, according to the conditions and the context information. The proposed scheme was tested using a real-life health system.

Tong *et al.* proposed an access control architecture which was designed to ensure the privacy of data [50]. The proposed architecture has several features, including key exchange, storage data privacy, emergency retrieval, and auditability to overcome any misuse of health records. A pseudorandom number generator was used as a key exchange to ensure unlinkability, and a redundancy-based secure indexing feature was proposed to preserve the privacy of the data by hiding the search and access patterns. Finally, in order to mitigate any potential misbehaviour, an attribute-based encryption was integrated with threshold signing to be used in emergency and normal situations as an access control with auditability.

Based on a two-stage keyed access control and a zero-knowledge protocol, Kahani *et al.* proposed a security control method [49]. Their method aimed to facilitate access control and authentication in electronic health cloud systems. When a user requests access to a health record, a limited amount of access is allowed based on the user's rights. To connect two parties in the system securely, two-stage key management is used. This two-stage key management is a combination of public key encryption and Derived Unique Key Per Transaction (DUKPT)

Fernando *et al.* proposed an approach that aimed to reduce leaks of patient information using unlinkability [52]. Their approach provided the health data owner with the ability to make decisions in terms of access control. To fulfill the policies of the service provider, the proposed approach utilized a personal information management protocol which could improve the privacy of the patients. This approach depended on a scenario in which patient EHRs were stored on a Health Information Exchange (HIE) cloud service. The approach demonstrated the communication techniques between EHR consumers, EHR owners, EHR creators, and the HIE service. The authors claimed that the privacy of the EHR was ensured by the unlinkability of consumers' sessions with the HIE service. In addition, the HIE service could not reach the consumer classes even when they had access policies. The proposed approach works as follows. A patient consults a doctor and the doctor prescribes a medical test. The patient goes to a laboratory with the doctor's instructions, and the laboratory carries out the test. The results of the test are sent by the laboratory to the HIE. Finally, the patient provides access to the doctor and the HIE [52].

In 2015, Wand *et al.* proposed a scheme called Constant-Size Ciphertext Policy Comparative Attribute-Based Encryption (CCP-CABE). This method inserts similar characteristics from all attributes into a key, and combines the restrictions of these attributes into a single chunk of a ciphertext. The procedure is carried out during the encryption process to apply flexible access control rules with a variety of relationships. The authors showed that the CCP-CABE scheme was efficient, as it produced keys and ciphertexts of the same size each time for any number of attributes, as well as reducing the cost of the computation to a trivial amount. To ensure access privacy, the authors extended CCP-CABE to different attribute domains [53].

Younis *et al.* proposed a model named Access Control for Cloud Computing (AC3) [54]. The model utilized the role and task principles, and used clients' jobs as a categorizing factor. Based on clients' job roles, security domains are created to restrict each client to a particular security domain. Each role within the AC3 is given a group of related and required tasks for performing those roles. For access to data and resources, security classification is done for each task, and an authentic permission is required to complete the task. The authors employed a risk engine to interact with unpredictable client behaviours. However, an authentication protocol that can deal with massive storage complexity and high performance is required.

In 2014, Yang and Jia proposed a multi-authority access control scheme [55]. In that scheme, the authors presented a Ciphertext-Policy Attribute-based Encryption (CP-ABE) scheme. It was an extension to a single-authority scheme proposed by Lewko and Waters in [56]. Yang and Jia adopted Chase's multi-authority scheme [57] in which all generated secret keys were combined together for the same client. CP-ABE also used a revocable scheme and could mitigate collusion attacks. More specifically, the functionality of a single authority was divided into a certificate authority and multiple attribute authorities.

Li *et al.* adopted Semantic-Based Access Control (SBAC) techniques to propose an architecture called IntercroSsed Secure Big Multimedia Model (2SBM) for securing accesses between different cloud systems [58]. In addition, the 2SBM architecture can be summarized in three steps:

- To relate attributes to each other, the proposed architecture formats the data by linking the attributes in a matrix;
- Based on their relationships, the architecture creates interrelations between attributes in the matrix; and
- To improve the efficiency of access control, the architecture builds a tree of attributes and sorts the attributes according to their frequency.

Choi et al proposed an ontology-based Access Control Model (Onto-ACM) in 2014 [59]. Onto-ACM is a model of analysis which recognizes and presents the differences between providers and clients. Based on ontology cognitive and context-aware technologies, the proposed model can decide whether data access would be allowed. The model can be considered as a detailed access control, which can be used to establish cloud feature boundaries.

Yu *et al.* proposed a scheme that claimed to achieve secure, scalable, and fine-grained access policies for cloud projects [60]. The proposed scheme used an attribute-based encryption (ABE), proxy re-encryption (PRE), and lazy re-encryption. Specifically, it allows the data owner to pass the operations of computation to the servers without revealing the original data. In that scheme, the data owner is therefore responsible for the accessibility of the data, which is particularly suitable for cloud projects.

Ruj *et al.* proposed a different form of access control in 2014 [61]. There are three types of clients: creator, reader, and writer in their method. For example, Alice is the client and a trusted party gives her a token (general feature). The trusted party could be any government office controlling health records. When submitting a claim, Alice presents her identification (e.g., a health card), and the trusted party provides her with the token. In this scheme, there are two key distribution centres (KDCs) which are responsible for distributing the keys to the clients. Based on the information in the token and the keys from one or two of the KDCs, a creator makes a decision on the claim, ensuring the identity of Alice and authenticating and encrypting the messages under this claim. The signed ciphertext is then sent to the cloud. The cloud system authenticates the signature of the ciphertext and keeps it on the cloud servers. When the reader requests to read a message, the cloud system will send the ciphertext. Without the appropriate keys, the user will not be able to retrieve the plaintext; however, the access control manager has full access to all client information and can decrypt the ciphertexts.

IV. EFFECTIVE ENCRYPTION

Several advanced encryption algorithms have been reported in cloud computing research to protect the security and privacy of eHealth data. Encryption schemes such as public key encryption (PKE) and symmetric key encryption (SKE) have been frequently used to protect data in eHealth cloud projects [14], [64]–[66]. Other encryption schemes are also used to ensure the security and privacy of eHealth records including attribute-based encryption (ABE), fully homomorphic encryption (FHE), and searchable encryption (SE).

A. ATTRIBUTE-BASED ENCRYPTION ALGORITHMS

The first ABE algorithms were presented by Sahai and Waters in 2005 [67], and by Goyal *et al.* in 2006 [68].

ABE is a type of PKE where the ciphertext and shared key of a client depend on attributes. In ABE systems, retrieving a plaintext from ciphertext is applicable for clients who have a group of key attributes that match ciphertext attributes. One of the most important features of the ABE system is that it is collusion resistant. An attacker who has many keys can only access the system when at least one key has an approved access. Many researchers have proposed various ABE algorithms. Some of which are discussed in the following paragraphs.

Fabian *et al.* proposed an ABE-based scheme for secure data sharing in eHealth clouds [69]. The proposed scheme aimed to preserve the security and privacy of patients' records in partly trustworthy cloud servers. It uses the ABE algorithm to manage users' accessibility to health records and shared keys, and to distribute information and health records among several clouds. If a patient visiting three different Health Centres (HCs), such as HC A, HC B and HC C. His/her health record is updated at each of the three centres. When a patient visits HC C, the doctors at HC C can request the full health record for that patient from HCs A and B through the multi-cloud proxy. However, the key management process needs to be reconsidered and solved. In addition, the key authority of the ABE algorithm has to be distributed, and security responsibilities must be separated.

Li *et al.* proposed an ABE-based framework for secure sharing of PHRs in eHealth clouds [2]. The authors assumed that the cloud servers were semi-trusted, and they also argued that the PHR records had to be encrypted to ensure the privacy of the patients. They used the ABE algorithm to encrypt PHRs, and patients can delegate others from public domains to access their PHR records. Their work involved verifying key management complexity reduction and privacy enhancement. The proposed framework involves multiple data owners, clients, attribute authorities (AAs), and SDs. The framework can use one of two ABE algorithms: the revocable key policy ABE system proposed by Yu et al for each public and personal domain (PSD) [60], and their own revocable MA-ABE system for each personal and public domain (PUD) [2].

Outsourced ABE (OABE) approaches can significantly decrease the computational cost of encryption by moving large computation to a CSPs. However, large encrypted files which are saved on the cloud are likely to affect query processing in a negative way. Li *et al.*, therefore, proposed a keyword search function (KSF-OABE) approach that aimed to solve the problem [70]. KSF-OABE offers key issuing, decryption and keyword search functions. It retrieves part of the ciphertext according to a particular keyword. In that approach, operations that consume a large amount of time will be moved to the CSPs, while users who need less processing time would go ahead with their operations. Thus, the processing time can be reduced on both the CSPs and user sides. However, the proposed KSF-OABE approach does not offer verifiability features. The proposed approach was tested only for a replayable chosen-ciphertext attack (RCCA) and was not tested for a chosen-ciphertext attack (CCA). CCA-secure approaches are RCCA-secure, although RCCA-secure approaches are not CCA-secure. Therefore, testing under both CCA and RCCA conditions is suggested.

A PHR system based on the ABE algorithm was presented by Xhafa *et al.* for secure sharing and storing of PHRs in the cloud [71]. The system permits users to share their PHRs and personal information selectively with health service providers. The proposed system is practical as it provides searchability, revocation, and local decryption. Based on their operations, ABEs can be classified as ciphertext-policy or key-policy ABEs.

1) CIPHERTEXT-POLICY ABES

In the ciphertext-policy (CP-ABE) approaches, the encryptor normally manages the access operation. The public key process is more complex due to the complexity of the access operation and tightens the system [72]. Most CP-ABE research concentrates on the access control design [73].

Liu *et al.* proposed an approach based on CP-ABE with a signature (SignCryption), called CP-ABSC. It delivers PHR authentication, encryption, and access control [74]. The proposed approach permits a patient to sign the PHR record using a secret key and a group of personal attributes. CP-ABSC has two features: access control and signature encryption (SignCryption). The authors claim that a combination of these two features could deliver the authenticity, unforgeability, confidentiality and collusion prevention required by a PHR system. However, a revocation process was not considered. In addition, according to Rao [75], that approach couldn't provide verifiability for a public ciphertext property, which is necessary to resist any invalid ciphertext decryption in order to decrease the redundant load on the decryptor [75].

As a result, in 2017, Rao proposed another CP-ABSC approach for PHR cloud projects, which claimed to be verifiable for a public ciphertext [75]. Their approach satisfies the important security properties of the attribute-based signature (ABS) and ABE. Furthermore, it uses communication links to a lesser extent than other approaches. The CP-ABSC has two assumptions: existential unforgeability in selective signing predicate and adaptive chosen message attack (EUF-sSP-CMA) and the resistance of the computational Diffie–Hellman Exponent (cDHE) problem, and decisional Bilinear Diffie–Hellman Exponent (dBDHE) problem [75]. Those assumptions can prevent the ‘‘indistinguishability of ciphertext in selective encryption predicate and adaptive chosen ciphertext’’ attack (IND-sEP-CCA2).

Wang *et al.* [76] introduced another cloud-based PHR (CB-PHR) system. CB-PHR permits the owners of PHRs to safely store their records in a partly trustworthy CSPs, and to share them with several clients of their choice. PHR clients were divided into public and personal domains to decrease the complexity of key management. In their approach, health records are encrypted by the owner of the PHRs using CP-ABE for presentation to the public domain, whereas health records are encrypted using a nameless multi-receiver identity-based encryption algorithm for the personal domain. Therefore, only accredited clients whose identification can meet the CP specifications can decrypt health records [76]. It should be mentioned that the CB-PHR has a high computational cost, as it encrypts the same record twice.

Motivated by cloud security requirements, Xu *et al.* modified the CP-ABE scheme to propose a Verifiable Delegation CP-ABE (VDCPABE) [77]. The cloud computing scheme is based on verifiable technology and multilinear maps. Hybrid encryption is used to encrypt data by its owner. For each ciphertext block, a verifiable message authentication code (MAC) is generated privately, and the full ciphertext is then uploaded to the cloud. When the data owner is not online, the client who requested the data can ask the cloud server directly [77].

Health records are usually represented using a multilayer hierarchical structure. However, according to Wang *et al.*, this hierarchical characteristic of health records has not been investigated thoroughly in terms of CP-ABE [78]. As a result, they propose a data hierarchy ABE approach for such cloud projects. They use a single access control method rather than levelled access control methods, and the hierarchical data are encrypted using a single access control method. As the parts of the ciphertext which were related to attributes were distributed by the records, the proposed scheme was shown to reduce storage and time costs [78].

A PHR privacy preserving approach based on a multi-authority CP-ABE which offers revocation features and ensures fine-grained access was proposed by Qian *et al.* [79]. The authors report that their approach can be implemented in a partly trustworthy server and encrypted PHRs with multiple owners can be stored on that server. The proposed approach was able to work in public cloud PHR systems [2]. Once PHRs encryption is complete, to achieve a fine-grained access, a patient can combine ciphertext with multilayer access attributes. A key exchange scheme was used to preserve the privacy of the PHRs. This key exchange scheme ensured that if cracked, authorities would expose zero information regarding the client's global identifier (GId). As a result, the tracing of a GId by an attacker yielded no information about the client's attributes. The revocation of lazy client and on-demand services are features provided by this approach that decrease the computational overhead [79].

An approach based on CP-ABE was proposed by Guo *et al.* to secure EHRs in health cloud environments [80]. The approach uses a CP-ABE algorithm to encrypt tables published by healthcare providers, such as EHRs. The patient's identification number is used as a primary key to store these records in a database. It permits multiple clients with multiple constraints to search multiple database columns. The authors highlighted that their work differed from others in terms of securing outsourcing records, as the search management of columns in the database was emphasized [80].

Xhafa *et al.* presented a multi-authority CP-ABE approach with a patient accountability feature to secure PHR sharing in a health cloud project [81]. In the proposed work, patient privacy was secured by hiding the access control policy. The reduction of authority and PHRs trust assumptions were ensured through the accountability feature.

2) KEY-POLICY ABE

In the Key-Policy Attribute-Based Encryption (KP-ABE) schemes, ciphertext has a group of attributes, and the access regulations are controlled by the client's private key. Ciphertext can be decrypted only when these groups of attributes match the structure of access to the client's private key [82], [83].

Based on the Decisional Bilinear Deffie-Hellman (DBDH) assumption, a privacy-preserving KP-ABE (PP KP-ABE) approach was proposed for secure data sharing in a cloud system [84]. This approach permits clients to retrieve data from the cloud and then decrypt it, without exposing any attribute information to a third party. The issue of collusion attacks has been resolved in that research, as PP KP-ABE is collusion resistant. The authors of PP KP-ABE utilized a key management scheme to strengthen the connection between the client and the secret key. Thus, multiple clients cannot use their secret keys to produce a secret key for an unapproved client [84].

Another KP-ABE-based scheme named access policy re-definable ABE (APR-ABE) was proposed by Qin *et al.* for securing EHRs in cloud environments [85]. In APR-ABE, attribute vectors were used to implement access control. This access control was linked to clients' secret keys. Higher level clients can easily redefine their access control to be commensurate with their roles, and can then provide lower level clients with a secret key that has more limitations.

B. FULLY HOMOMORPHIC ENCRYPTION (FHE)

The FHE is a type of encryption that has a special feature permitting operations to be done on a ciphertext as well as on plaintext [86], [91]. The feature is important, especially for the modern ICT systems as it enables the possibility of chaining several services together without leaking information. There are several schemes which secure health records using the FHE, and we discuss some of these in the following paragraphs.

An FHE-based scheme was proposed to secure computations for the Genome-Wide Association Study (GWAS) [87]. The proposed scheme aimed to preserve the privacy of patients' genomic data. It adapts the FHE to encrypt genotype and phenotype data for all patients to implement meaningful operations on a ciphertext. However, the authors do not consider the computational complexity of the FHE in their proposed scheme, which was a major issue for the proposed FHE scheme [88].

A different approach based on the FHE was proposed to preserve the privacy of health data in a public cloud [89], [90]. A detailed analysis was provided based on heart rate (average), heart rate (max/min), and the automated detection of irregular heartbeats. The authors provided a set of experimental results over 24 hours using an electrocardiogram (ECG) signal dataset and a homomorphic encryption library (HElib). The results showed that the proposed approach could be adapted for a health cloud system to secure data from those issues [89], [90]. However, the proposed scheme does not solve the problem of computational complexity in the FHE. The implementation of that approach in a real-time parallel system also needs to be considered to reduce the processing time.

Zhao *et al.* proposed a different FHE-based system to solve the issue of lack of data safety in a health cloud [92]. The authors claimed that the proposed method was suitable for both retrieving and processing ciphertext for a secure storage of health data on cloud servers and the transmission of data between the cloud and the clients. The method was able to offer search date for a third party. However, in the same way as the previous methods, this method also suffers from high computation requirements.

C. SEARCHABLE ENCRYPTION (SE)

SE is a cryptographic scheme that provides safe search in a ciphertext. For enhanced effectiveness [93], SE typically constructs keyword indexes to verify client requests. SE schemes can be based either on a public key or secret key. Many proposals have been investigated to deliver secure search over encrypted text, and some of these are described below [94]–[100].

Yang and Ma proposed a time-dependent SE approach with a designated tester and timing enabled proxy re-encryption function (Re-dtPECK) [94]. The approach allowed patients to give limited access privileges to others, which helps control search procedures over the health records within a certain timeframe. People who are given access privileges by patients can search and decrypt health records within this limited timeframe. In addition, Re-dtPECK offers a linked word search, and can prevent guessing attacks [94]. However, the revocation feature is not considered in this approach, as the patient holds the same key most of the time, meaning that Re-dtPECK needs to consider redistributing secret keys among authorized clients.

A scheme named secure channel-free searchable encryption (SCF-PEKS) has been proposed to offer a secure search over encrypted EHR [95]. This version of SCF-PEKS was shown to be able to reduce storage and computational costs when compared to the previous SCF-PEKS. Moreover, it could resist keyword guessing attacks. However, despite reductions in storage and computational costs, ranked and fuzzy keyword searches were not provided, and integrity checks were missing.

Another proposed scheme uses a Bloom filter tree index to permit accredited users to retrieve data from ciphertext in a cloud [96]. In addition to the proposed scheme, the authors introduced a ranking method based on keyword membership, to retrieve only vital keywords. The authors argued that their work was the first to be able to retrieve fully encrypted text from a large cloud storage database. However, a collusion attack could possibly threaten the proposed scheme.

Liu *et al.* proposed a novel EHR cloud project which aimed to safely share and store EHR records in a cloud environment [97]. The proposed approach is based on binary trees for saving EHR ciphertext, and the ABE algorithm was adopted for efficient encryption of the shared keys. The authors claimed that the proposed project was designed to secure EHRs, and these were encrypted using a symmetric algorithm. With fewer cryptographic operations, a searchable encryption scheme might improve the system further. However, integrity checks were not offered by the proposed system.

Since the security of data sharing is an important factor for any cloud-based system, especially health cloud systems, Liang and Susilo defined a notation searchable attribute-based proxy re-encryption (ABPRE) scheme to address the issue [98]. However, the authors did not state how they might reduce the search token size, and how a key holder could create tokens. A modified scheme was recommended to address the issues.

In addition, Li *et al.* introduced two fine-grained multi-keyword search (FMS) schemes, FMS_I and FMS_II [99]. FMS_I was designed to provide an accurate search by considering common keyword factors and related scores. FMS_II was built to offer a secure complex search, which might contain several keywords connected with logical operations such as "AND" and "OR" operations. Finally, to enhance the efficiency of the proposed schemes, FMS classified support (FMSCS) sub-dictionaries were proposed. However, the proposed method cannot deal with a multi-user cloud.

Finally, a multi-keyword SE method was proposed to safely search over encrypted text on a cloud [100]. This method was able to offer dynamic operations such as insert and delete operations. The authors designed their own tree-based index, as well as a "greedy depth-first search" method to enhance the ranked search using multiple keywords. They chose the KNN algorithm to encrypt the query and the index. In addition, the algorithm was chosen to compute the score of the connections between the query and the index. Shade terms are inserted into the index to prevent statistical attacks. However, a revocation feature is not offered by the proposed approach, as the patient holds the same key most of the time, as in Re-dtPECK, that was discussed above.

V. DATA SECURITY REQUIREMENTS

Several security issues are related to cloud systems, such as EHR cloud-based systems. The issues include not only common concerns such as DDoS attacks [101], but also specific issues in the cloud such as side channel attacks, etc. [6], [102], [103]. Thus, setting security requirements for any cloud system is essential and needs to be included in our review. From an eHealth cloud perspective, the security requirements (R) of cloud systems are included in Table 1.

Table 2 shows a comparison of security approaches for eHealth clouds in terms of data security requirements.

VI. DISASTER RECOVERY PLANS

The CSPs should establish continuity and recovery plans to ensure that services will remain available, and can recover all lost data even after disasters such as floods, earthquakes, bushfires, or electricity power failures [121]. The data recovery plan may be established solely by CSPs, or in consultation with clients.

Several suggestions have been made to facilitate disaster recovery, and some of these are discussed below [40], [122], [123].

Sahi *et al.* developed a disaster recovery plan to ensure the availability of PHRs and HERs in a health cloud environment [40]. The authors assumed that a cloud storage consisted of three or more data centres. Distributing signals called heartbeats were used between data centres and the CSPs in order to keep track of the status of these data centres. Each health record was divided into several parts, and multiple copies of each part were stored in different data centres. In the case of a disaster, the heartbeat from a data centre would stop if the data centre machine was damaged, which would alert the manager. The manager would recover or retrieve the records from the other data centres, without accessing access the damaged one. The authors reported that the data centres must be physically located in different geographic locations (for example in different countries) to ensure the availability of the data and the services [40].

Another disaster recovery plan was proposed based on three different techniques: TCP/IP, VM snapshots, and replication [122]. The plan was reported to achieve 99.94% data recovery in the event of a disaster. The proposed approach was implemented with real data and was tested with the backup data from all the sister site records in London, Southampton, and Leeds. However, the data centres in the proposed approach were not integrated with any existing data centres. In addition, all data centres are located within one country, in the same geographical area, which could be considered a major drawback.

Gu *et al.* proposed backup and recovery models for implementing a disaster recovery plan [123]. In terms of the backup model, clients are provided with accounts with limited rights. The CSPs is responsible for sending and receiving data to/from clients. A client is able to request a backup from the CSPs within a certain timeframe. The CSPs will hold this request, make three copies of the data and store those copies in different locations. In the recovery model, the client can request a data recovery from the CSPs. The CSPs can retrieve the data from the stored three copies and send it back to the client. However, storing the data in full at three different locations can significantly increase the backup data size.

Mansoori *et al.* presented a disaster recovery plan based on two servers, a local server and a disaster recovery server [124]. The proposed plan considers four scenarios to provide availability and continuity of services. The authors implemented the proposed plan within a university hospital health system to ensure constant access to the picture archiving and communication system (PACS) application and its controlled radiology images. However, the authors did not consider a scenario in which a disaster would affect a relatively wide geographic area leading to damage to the backup images.

TABLE 1. Data security requirements.

R		Description
R1	Confidentiality	The confidentiality of data in a health cloud system means that unauthorized clients cannot decrypt or retrieve health records. The data owner, for example a patient, does not control the health records stored in the cloud [2]. Authorized clients are the only users who can access the records, with even CSPs are not allowed to access any information regarding the data. Furthermore, patients expect a full control over their health records in the cloud, without any leakage to other legitimate system users or attackers.
R2	Access Controllability	Access controllability means that a data owner controls his/her record data by implementing certain carefully constructed rules in order to ensure the security and privacy of records, and by allowing only legal users to have controlled access [6, 104]. Other users cannot access health records without permission. Users have different access rights to access different parts of the data. This is called fine-grained access control. In an untrusted cloud system, the data owner is the only one permitted to grant access.
R3	Integrity	Integrity is a security feature that ensures the completeness and accuracy of data. In other words, data must stay complete and must not be altered or deleted. Users normally expect their data to be kept safe in a cloud storage [105]. Furthermore, users must be able to rectify any unsolicited modification, loss, or corruption of this data, and to retrieve lost pieces.
R4	Authenticity	Authenticity means that only an authentic user can request access [14]. In the health sector, EHR service providers must provide verified information to ensure the authenticity of the cloud.
R5	Reliability	Reliability means that the system performs as users expect [106]. One of the main factors of reliability is availability, which means the continuity of services provided. In other words, availability means how long the system is expected to serve users without interruption [106].
R6	Accountability	As cited in [107], "defining what exactly accountability means in practice is complex". One definition is that the controller of the data must be responsible for acting in accordance with procedures that affect the privacy of data.
R7	Auditability	Auditability means monitoring security, privacy, and all access activities on an eHealth cloud [14]. From time to time, auditing must be done to ensure that no errors occur.
R8	Non-Repudiation	Non-repudiation means that no one can falsely deny any unethical behaviour [108, 109]. In the eHealth cloud environment, patients and physicians cannot deny any misuse or mishandling of health records.
R9	Anonymity	The anonymity of the user means preventing a third party from obtaining valid user information that leads to server access [110, 111]. As the attacker is unable to learn any personal information, anonymity ensures the privacy of legitimate users in the cloud. A lack of anonymity means an attacker can fake an identity as an authenticated user.
R10	Unlinkability	Unlinkability means that in order to ensure a user's privacy, associating information with a particular user must be difficult [112]. Although sometimes a group of words needs to be used for a particular function, this group of words should be different each time. Thus, a random word generation function is required [113].
R11	Maintainability	Maintainability means the ability to perform fast maintenance on a project, as the development of very large projects is often not fully complete [114]. Maintainability can therefore ensure the delivery of services without error for different parties. In addition, a testing method is needed to decrease the time of maintenance.
R12	Revocability	Revocability means that users' access rights should be revoked after a period of time so they cannot access specific data later on using old keys [115]. Revocability is a vital feature for eHealth cloud systems and needs to be well implemented to ensure the privacy of users and the secrecy of the contents [116]. Once a manager chooses to revoke a particular user's rights, the corresponding keys need to be eliminated from the system.

TABLE 2. Comparison of security approaches for the eHealth cloud.

Ref.	Technique(s)	Aim(s)	Limitation(s)	Server assumption(s)	Data Security Requirements											
					R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12
[115]	Proxy re-encryption, El-Gamal encryption	In-home monitoring	Invalid assumption, usability tests not available	Proxy re-encryption, El-Gamal encryption	√	√	X	X	–	X	X	X	X	X	X	√
[117]	Least Significant Bit	Secure 3D images, limited power	Unparalleled, missing many requirements	Least Significant Bit	√	√	√	√	X	X	X	X	X	X	√	X
[69]	ABE, cryptographic secret sharing	Multiple distribution, reduction in attackers' abilities	Key authority, security duties, usability	ABE, cryptographic secret sharing	√	√	√	√	√	–	√	√	√	√	√	√
[118]	Internet of Things (IoT) medical sensor	Secure monitoring, resource reduction	Inefficient, missing revocation	Internet of Things (IoT) medical sensor	√	√	√	√	√	X	X	√	X	X	X	X
[2]	ABE	Access control, multiple clouds, key complexity reduction	Inefficient	ABE	√	√	√	√	√	√	X	–	X	X	–	√
[119]	Multiple hashes	Preventing DoS, dissemination protocol	Unparalleled, assumptions, revocation	Multiple hashes	√	√	√	√	–	X	X	√	X	X	√	X
[120]	IoT, Body Sensor Network (BSN)	Secure healthcare, computationally efficient	Revocation	IoT, Body Sensor Network (BSN)	√	√	√	√	–	X	X	√	√	√	X	X
[112]	Bilinear pairing, Authenticated key Exchange	Secure anonymous authentication, computationally efficient	Impersonation attack	Bilinear pairing, Authenticated key Exchange	√	√	√	√	–	X	X	√	√	√	X	X
[110]	Elliptic curve cryptosystem (ECC), bilinear pairing	Secure anonymous authentication, computationally efficient	Revocation	Elliptic curve cryptosystem (ECC), bilinear pairing	√	√	√	√	–	X	X	√	√	√	X	X
[109]	Symmetric encryption, MAC, RFC 2631	Anywhere anytime access	Anonymity and unlinkability	Symmetric encryption, MAC, RFC 2631	√	√	√	√	–	X	X	√	X	X	X	√
[111]	Quantum key distribution	Resist all attacks, generate keys over distance of 100km of optical fibre	Revocation	Quantum key distribution	√	√	√	√	√	√	X	√	√	X	X	X
[116]	ABE, SE, bilinear pairing	Ciphertext retrieval, fine-grained access control	Anonymity and unlinkability	ABE, SE, bilinear pairing	√	√	√	X	X	X	X	√	X	X	X	√

Note: √ = Valid (requirement been satisfied) X = Invalid (requirement not been satisfied) – = Not specified

Some of the existing review papers focused on either the privacy of the cloud or the security of the cloud, but not both. There were few examples of research papers that considered reviewing security and privacy at the same time within the health sector such as [66], [125]–[130]. In this paper we have reviewed most of the recent studies in both security and privacy areas. To sum up, the main contribution of this study is to help eHealth decision makers and researchers to make a better decision by picking up their preferred requirements for: (1) identity management / physical security / privacy; (2) cloud security control; (3) encryption; (4) data security, and (5) disaster recovery. Then, they can start to look for providers offering services matching the desirable requirements.

VII. CONCLUSION

The security and privacy of health data in the cloud requires secure solutions that are capable of controlling security and privacy while keeping all features of eHealth under consideration. In this paper, we review the state of the art on security and privacy research in eHealth clouds from five main perspectives: security and privacy, security controls, effective encryption, data security requirements, and disaster recovery plans. This paper, therefore, provides a clear overall picture for the current security and privacy development in eHealth to stakeholders in order to facilitate better understanding, designs and decisions. In summary, this paper reviews, evaluates, and classifies the state-of-the-art eHealth security and privacy schemes. It covers the most recent studies in this research area, and discusses the benefits and drawbacks of most important literature to help improve the security and privacy of eHealth clouds.

REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," *Nat. Inst. Standards Technol.*, vol. 53, no. 6, p. 50, 2011.

[2] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131–143, Jan. 2013.

[3] Y. Yu, A. Miyaji, M. H. Au, and W. Susilo, "Cloud computing security and privacy: Standards and regulations," *Comput. Standards Interfaces*, vol. 54, pp. 1–2, Nov. 2017.

[4] B. Yüksel, A. Küpçü, and Ö. Özkasap, "Research issues for privacy and security of electronic health services," *Future Gener. Comput. Syst.*, vol. 68, pp. 1–13, Mar. 2017.

[5] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in Healthcare 4.0," *Comput. Commun.*, vol. 153, pp. 311–335, Mar. 2020.

[6] J. Tang, Y. Cui, Q. Li, K. Ren, J. Liu, and R. Buyya, "Ensuring security and privacy preservation for cloud data services," *ACM Comput. Surv.*, vol. 49, no. 1, p. 13, 2016.

[7] S.-Y. Jing, S. Ali, K. She, and Y. Zhong, "State-of-the-art research study for green cloud computing," *J. Supercomput.*, vol. 65, no. 1, pp. 1–24, Jul. 2013.

[8] A. Sahi, D. Lai, and Y. Li, "Parallel encryption mode for probabilistic scheme to secure data in the cloud," in *Proc. 10th Int. Conf. Inf. Technol. Appl. (ICITA)*, 2015, pp. 1–4.

[9] V. Vijayakumar, M. K. Priyan, G. Ushadevi, R. Varatharajan, G. Manogaran, and P. V. Tarare, "E-health cloud security using timing enabled proxy re-encryption," *Mobile Netw. Appl.*, vol. 24, no. 3, pp. 1034–1045, Jun. 2019.

[10] Y. Zhang, D. Zheng, and R. H. Deng, "Security and privacy in smart health: Efficient policy-hiding attribute-based access control," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 2130–2145, Jun. 2018.

[11] A. Sajid and H. Abbas, "Data privacy in cloud-assisted healthcare systems: State of the art and future challenges," *J. Med. Syst.*, vol. 40, no. 6, pp. 1–16, 2016.

[12] J. L. Fernández-Alemán, I. C. Señor, P. A. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review," *J. Biomed. Inform.*, vol. 46, no. 3, pp. 541–562, 2013.

[13] J. A. González-Martínez, M. L. Bote-Lorenzo, E. Gómez-Sánchez, and R. Cano-Parra, "Cloud computing and education: A state-of-the-art survey," *Comput. Educ.*, vol. 80, pp. 132–151, Jan. 2015.

[14] A. Abbas and S. U. Khan, "A review on the state-of-the-art privacy-preserving approaches in the e-health clouds," *IEEE J. Biomed. Health Informat.*, vol. 18, no. 4, pp. 1431–1441, Apr. 2014.

[15] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proc. Roy. Soc. London A, Math., Phys. Eng. Sci.*, vol. 426, pp. 233–271, Dec. 1989.

[16] O. Ali, A. Shrestha, J. Soar, and S. F. Wamba, "Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review," *Int. J. Inf. Manage.*, vol. 43, pp. 146–158, Dec. 2018.

[17] C. Anilkumar and S. Sumathy, "Security strategies for cloud identity management—A study," *Int. J. Eng. Technol.*, vol. 7, no. 2, pp. 732–741, 2018.

[18] M. Haghighat, S. Zonouz, and M. Abdel-Mottaleb, "CloudID: Trustworthy cloud-based and cross-enterprise biometric identification," *Expert Syst. Appl.*, vol. 42, no. 21, pp. 7905–7916, Nov. 2015.

[19] X. A. Wang, J. Ma, F. Xhafa, M. Zhang, and X. Luo, "Cost-effective secure E-health cloud system using identity based cryptographic techniques," *Future Gener. Comput. Syst.*, vol. 67, pp. 242–254, Feb. 2017.

[20] I. Khalil, A. Khreishah, and M. Azeem, "Consolidated identity management system for secure mobile cloud computing," *Comput. Netw.*, vol. 65, no. 2, pp. 99–110, Jun. 2014.

[21] R. Sanchez, F. Almenares, P. Arias, D. Diaz-Sanchez, and A. Marin, "Enhancing privacy and dynamic federation in IdM for consumer cloud computing," *IEEE Trans. Consum. Electron.*, vol. 58, no. 1, pp. 95–103, Feb. 2012.

[22] K. Haufe, S. Dzombeta, and K. Brandis, "Proposal for a security management in cloud computing for health care," *Sci. World J.*, vol. 2014, pp. 1–7, Jan. 2014.

[23] D. Nuñez and I. Agudo, "BlindIdM: A privacy-preserving approach for identity management as a service," *Int. J. Inf. Secur.*, vol. 13, no. 2, pp. 199–215, Apr. 2014.

[24] *System for Cross-Domain Identity Management*. Accessed: Jul. 2018. [Online]. Available: https://www.simplecloud.info/

[25] P. Hunt, K. Grizzle, E. Wahlstroem, and C. Mortimore, "System for cross-domain identity management: Core schema," Internet Eng. Task Force, Fremont, CA, USA, Sep. 2015.

[26] J. Xiong, Z. Yao, J. Ma, X. Liu, Q. Li, and J. Ma, "Priam: Privacy preserving identity and access management scheme in cloud," *Trans. Internet Inf. Syst.*, vol. 8, no. 1, pp. 282–304, 2014.

[27] A. M. Canedo, L. Dalloro, D. Wei, and B. Collar, "Siemens corp, system and method for cyber-physical security," U.S. Patent 10 044 749, Aug. 7, 2018.

[28] N. Regola and N. V. Chawla, "Storing and using health data in a virtual private cloud," *J. Med. Internet Res.*, vol. 15, no. 3, p. e63, Mar. 2013.

[29] A. Mxoli, M. Gerber, and N. Mostert-Phipps, "Information security risk measures for cloud-based personal health records," in *Proc. Int. Conf. Inf. Soc. (i-Society)*, Nov. 2014, pp. 187–193.

[30] J. J. P. C. Rodrigues, I. de la Torre, G. Fernández, and M. López-Coronado, "Analysis of the security and privacy requirements of cloud-based electronic health records systems," *J. Med. Internet Res.*, vol. 15, no. 8, p. e186, Aug. 2013.

[31] F. R. Carlson, "Security analysis of cloud computing," 2014, *arXiv:1404.6849*. [Online]. Available: https://arxiv.org/abs/1404.6849

[32] M. A. Sahi, H. Abbas, K. Saleem, X. Yang, A. Derhab, M. A. Orgun, W. Iqbal, I. Rashid, and A. Yaseen, "Privacy preservation in e-healthcare environments: State of the art and future directions," *IEEE Access*, vol. 6, pp. 464–478, 2017.

[33] A. T. Lo'ai and G. Saldamli, "Reconsidering big data security and privacy in cloud and mobile cloud systems," *J. King Saud Univ.-Comput. Inf. Sci.*, pp. 1–10, May 2019.

[34] O. Kocabas and T. Soyata, "Towards privacy-preserving medical cloud computing using homomorphic encryption," in *Virtual and Mobile Healthcare: Breakthroughs in Research and Practice*. Hershey, PA, USA: IGI Global, 2020, pp. 93–125.

[35] H.-L. Yeh, T.-H. Chen, K.-J. Hu, and W.-K. Shih, "Robust elliptic curve cryptography-based three factor user authentication providing privacy of biometric data," *IET Inf. Secur.*, vol. 7, no. 3, pp. 247–252, Sep. 2013.

[36] F. Wu, L. Xu, S. Kumari, and X. Li, "A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client–server networks," *Comput. Electr. Eng.*, vol. 45, pp. 274–285, Jul. 2015.

[37] M. K. Khan and S. Kumari, "An improved biometrics-based remote user authentication scheme with user anonymity," *BioMed Res. Int.*, vol. 2013, pp. 1–9, Nov. 2013.

[38] Q. Jiang, M. K. Khan, X. Lu, J. Ma, and D. He, "A privacy preserving three-factor authentication protocol for e-health clouds," *J. Supercomput.*, vol. 72, no. 10, pp. 3826–3849, 2016.

[39] J.-J. Yang, J.-Q. Li, and Y. Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment," *Future Gener. Comput. Syst.*, vols. 43–44, pp. 74–86, Feb. 2015.

[40] A. Sahi, D. Lai, and Y. Li, "Security and privacy preserving approaches in the eHealth clouds with disaster recovery plan," *Comput. Biol. Med.*, vol. 78, pp. 1–8, Nov. 2016.

[41] A. S. Khader and D. Lai, "Preventing man-in-the-middle attack in Diffie-Hellman key exchange protocol," in *Proc. 22nd Int. Conf. Telecommun. (ICT)*, Apr. 2015, pp. 204–208.

[42] W. Wang, L. Chen, and Q. Zhang, "Outsourcing high-dimensional healthcare data to cloud with personalized privacy preservation," *Comput. Netw.*, vol. 88, pp. 136–148, Sep. 2015.

[43] W. Dou, X. Zhang, J. Liu, and J. Chen, "HireSome-II: Towards privacy-aware cross-cloud service composition for big data applications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 2, pp. 455–466, Feb. 2015.

[44] A. Page, O. Kocabas, T. Soyata, M. Aktas, and J.-P. Couderc, "Cloud-based privacy-preserving remote ECG monitoring and surveillance," *Ann. Noninvasive Electrocardiol.*, vol. 20, no. 4, pp. 328–337, Jul. 2015.

[45] M. K. Kundalwal, K. Chatterjee, and A. Singh, "An improved privacy preservation technique in health-cloud," *ICT Exp.*, vol. 5, no. 3, pp. 167–172, Sep. 2019.

[46] T. Rajamani and S. P. PrabuSevugan, "An investigation on the techniques used for encryption and authentication for data security in cloud computing," *Inst. Integrative Omics Appl. Biotechnol.*, vol. 7, pp. 126–138, May 2016.

[47] B. Nedelcu, M.-E. Stefanet, I.-F. Tamasescu, S.-E. Tintoiu, and A. Vezeanu, "Cloud computing and its challenges and benefits in the bank system," *Database Syst. J.*, vol. 5, no. 1, pp. 45–58, 2015.

[48] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, 2011.

[49] J. Son, J.-D. Kim, H.-S. Na, and D.-K. Baik, "Dynamic access control model for privacy preserving personalized healthcare in cloud environment," *Technol. Health Care*, vol. 24, no. 1, pp. S123–S129, Dec. 2015.

[50] Y. Tong, J. Sun, S. M. Chow, and P. Li, "Cloud-assisted mobile-access of health data with privacy and auditability," *IEEE J. Biomed. Health Informat.*, vol. 18, no. 2, pp. 419–429, Mar. 2014.

[51] N. Kahani, K. Elgazzar, and J. R. Cordy, "Authentication and access control in e-health systems in the cloud," in *Proc. Big Data Security Cloud (BigDataSecurity), IEEE Int. Conf. High Perform. Smart Comput. (HPSC) IEEE Int. Conf. Intell. Data Secur. (IDS)*, Apr. 2016, pp. 13–23.

[52] R. Fernando, R. Ranchal, B. An, L. B. Othman, and B. Bhargava, "Consumer oriented privacy preserving access control for electronic health records in the cloud," in *Proc. IEEE 9th Int. Conf. Cloud Comput. (CLOUD)*, Jun. 2016, pp. 608–615.

[53] Z. Wang, D. Huang, Y. Zhu, B. Li, and C.-J. Chung, "Efficient attribute-based comparable data access control," *IEEE Trans. Comput.*, vol. 64, no. 12, pp. 3430–3443, Dec. 2015.

[54] Y. A. Younis, K. Kifayat, and M. Merabti, "An access control model for cloud computing," *J. Inf. Secur. Appl.*, vol. 19, no. 1, pp. 45–60, 2014.

[55] K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 7, pp. 1735–1744, Jul. 2014.

[56] A. Lewko and B. Waters, "New proof methods for attribute-based encryption: Achieving full security through selective techniques," in *Advances in Cryptology*. Berlin, Germany: Springer, 2012, pp. 180–198.

[57] M. Chase, "Multi-authority attribute based encryption," in *Proc. Theory Cryptogr. Conf.*, 2007, pp. 515–534.

[58] Y. Li, K. Gai, Z. Ming, H. Zhao, and M. Qiu, "Intercrossed access controls for secure financial services on multimedia big data in cloud systems," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 12, p. 67, Sep. 2016.

[59] C. Choi, J. Choi, and P. Kim, "Ontology-based access control model for security policy reasoning in cloud computing," *J. Supercomput.*, vol. 67, no. 3, pp. 711–722, Mar. 2014.

[60] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.

[61] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 384–394, Feb. 2014.

[62] K. Riad, R. Hamza, and H. Yan, "Sensitive and energetic IoT access control for managing cloud electronic health records," *IEEE Access*, vol. 7, pp. 86384–86393, 2019.

[63] T. Kanwal, A. Anjum, and A. Khan, "Privacy preservation in e-health cloud: Taxonomy, privacy requirements, feasibility analysis, and opportunities," *Cluster Comput.*, vol. 24, pp. 1–25, Mar. 2020.

[64] K. Abouelmehdi, A. Beni-Hssane, H. Khaloufi, and M. Saadi, "Big data security and privacy in healthcare: A review," *Procedia Comput. Sci.*, vol. 113, pp. 73–80, Jan. 2017.

[65] I. Masood, Y. Wang, A. Daud, N. R. Aljohani, and H. Dawood, "Towards smart healthcare: Patient data privacy and security in sensor-cloud infrastructure," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–23, Nov. 2018.

[66] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, "Security and privacy-preserving challenges of e-Health solutions in cloud computing," *IEEE Access*, vol. 7, pp. 74361–74382, 2019.

[67] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2005, pp. 457–473.

[68] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS)*, 2006, pp. 89–98.

[69] B. Fabian, T. Ermakova, and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds," *Inf. Syst.*, vol. 48, pp. 132–150, Mar. 2015.

[70] J. Li, X. Lin, Y. Zhang, and J. Han, "KSF-OABE: Outsourced attribute-based encryption with keyword search function for cloud storage," *IEEE Trans. Services Comput.*, vol. 10, no. 5, pp. 715–725, Sep. 2017.

[71] F. Xhafa, J. Li, G. Zhao, J. Li, X. Chen, and D. S. Wong, "Designing cloud-based electronic health record system with attribute-based encryption," *Multimedia Tools Appl.*, vol. 74, no. 10, pp. 3441–3458, May 2015.

[72] H. Cui, R. H. Deng, B. Qin, and J. Weng, "Key regeneration-free ciphertext-policy attribute-based encryption and its application," *Inf. Sci.*, vol. 517, pp. 217–229, May 2020.

[73] J.-S. Su, D. Cao, X.-F. Wang, Y.-P. Sun, and Q.-L. Hu, "Attribute-based encryption schemes," *J. Softw.*, vol. 22, no. 6, pp. 1299–1315, Jun. 2011.

[74] J. Liu, X. Huang, and J. K. Liu, "Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute-based signcryption," *Future Generat. Comput. Syst.*, vol. 52, pp. 67–76, Nov. 2015.

[75] Y. S. Rao, "A secure and efficient ciphertext-policy attribute-based signcryption for personal health records sharing in cloud computing," *Future Gener. Comput. Syst.*, vol. 67, pp. 133–151, Feb. 2017.

[76] C. Wang, X. Xu, D. Shi, and J. Fang, "Privacy-preserving cloud-based personal health record system using attribute-based encryption and anonymous multi-receiverIdentity-based encryption," *Informatica*, vol. 39, no. 4, pp. 1–8, 2015.

[77] J. Xu, Q. Wen, W. Li, and Z. Jin, "Circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation in cloud computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 1, pp. 119–129, Jan. 2016.

[78] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, and W. Xie, "An efficient file hierarchy attribute-based encryption scheme in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1265–1277, Jun. 2016.

[79] H. Qian, J. Li, Y. Zhang, and J. Han, "Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation," *Int. J. Inf. Secur.*, vol. 14, no. 6, pp. 487–497, Nov. 2015.

[80] C. Guo, R. Zhuang, Y. Jie, Y. Ren, T. Wu, and K.-K.-R. Choo, "Fine-grained database field search using attribute-based encryption for E-healthcare clouds," *J. Med. Syst.*, vol. 40, no. 11, p. 235, Nov. 2016.

[81] F. Xhafa, J. Feng, Y. Zhang, X. Chen, and J. Li, "Privacy-aware attribute-based PHR sharing with user accountability in cloud computing," *J. Supercomput.*, vol. 71, no. 5, pp. 1607–1619, 2015.

[82] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. Ràfols, "Attribute-based encryption schemes with constant-size ciphertexts," *Theor. Comput. Sci.*, vol. 422, pp. 15–38, Mar. 2012.

[83] J. Priyanka and M. Ramakrishna, "Performance analysis of attribute based encryption and cloud health data security," in *Proc. 4th Int. Conf. Intell. Comput. Control Syst. (ICICCS)*, May 2020, pp. 989–994.

[84] Y. Rahulamathavan, S. Veluru, J. Han, F. Li, M. Rajarajan, and R. Lu, "User collusion avoidance scheme for privacy-preserving decentralized key-policy attribute-based encryption," *IEEE Trans. Comput.*, vol. 65, no. 9, pp. 2939–2946, Sep. 2016.

[85] B. Qin, H. Deng, Q. Wu, J. Domingo-Ferrer, D. Naccache, and Y. Zhou, "Flexible attribute-based encryption applicable to secure e-healthcare records," *Int. J. Inf. Secur.*, vol. 14, no. 6, pp. 499–511, Nov. 2015.

[86] V. Maral, S. Kale, K. Balharpure, S. Bhakkad, and P. Hendre, "Homomorphic encryption for secure data mining in cloud," *Int. J. Eng. Sci.*, vol. 2016, pp. 4533–4536, Jan. 2016.

[87] W.-J. Lu, Y. Yamada, and J. Sakuma, "Privacy-preserving genome-wide association studies on cloud environment using fully homomorphic encryption," *BMC Med. Informat. Decis. Making*, vol. 15, no. S5, pp. 1–8, Dec. 2015.

[88] H. Kumarage, I. Khalil, A. Alabdulatif, Z. Tari, and X. Yi, "Secure data analytics for cloud-integrated Internet of Things applications," *IEEE Cloud Comput.*, vol. 3, no. 2, pp. 46–56, Mar. 2016.

[89] O. Kocabas and T. Soyata, "Utilizing homomorphic encryption to implement secure and private medical cloud computing," in *Proc. IEEE 8th Int. Conf. Cloud Comput.*, Jun. 2015, pp. 540–547.

[90] A. Page, O. Kocabas, S. Ames, M. Venkitasubramaniam, and T. Soyata, "Cloud-based secure health monitoring: Optimizing fully-homomorphic encryption for streaming algorithms," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2014, pp. 48–52.

[91] B. Alaya, L. Laouamer, and N. Msilini, "Homomorphic encryption systems statement: Trends and challenges," *Comput. Sci. Rev.*, vol. 36, May 2020, Art. no. 100235.

[92] F. Zhao, C. Li, and C. F. Liu, "A cloud computing security solution based on fully homomorphic encryption," in *Proc. 16th Int. Conf. Adv. Commun. Technol.*, Feb. 2014, pp. 485–488.

[93] X. Zhang, Y. Tang, S. Cao, C. Huang, and S. Zheng, "Enabling identity-based authorized encrypted diagnostic data sharing for cloud-assisted E-health information systems," *J. Inf. Secur. Appl.*, vol. 54, Oct. 2020, Art. no. 102568.

[94] Y. Yang and M. Ma, "Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 4, pp. 746–759, Apr. 2016.

[95] Y. Wu, X. Lu, J. Su, and P. Chen, "An efficient searchable encryption against keyword guessing attacks for sharable electronic medical records in cloud-based system," *J. Med. Syst.*, vol. 40, no. 12, p. 258, Dec. 2016.

[96] W. Song, B. Wang, Q. Wang, Z. Peng, W. Lou, and Y. Cui, "A privacy-preserved full-text retrieval algorithm over encrypted data for cloud storage applications," *J. Parallel Distrib. Comput.*, vol. 99, pp. 14–27, Jan. 2017.

[97] Z. Liu, J. Weng, J. Li, J. Yang, C. Fu, and C. F. Jia, "Cloud-based electronic health record system supporting fuzzy keyword search," *Soft Comput.*, vol. 20, pp. 3243–3255, Aug. 2016.

[98] K. Liang and W. Susilo, "Searchable attribute-based mechanism with efficient data sharing for secure cloud storage," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1981–1992, Sep. 2015.

[99] H. Li, Y. Yang, T. H. Luan, X. Liang, L. Zhou, and X. S. Shen, "Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data," *IEEE Trans. Depend. Sec. Comput.*, vol. 13, no. 3, pp. 312–325, May/Jun. 2016.

[100] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 2, pp. 340–352, Jan. 2016.

[101] A. Sahi, D. Lai, Y. Li, and M. Diykh, "An efficient DDoS TCP flood attack detection and prevention system in a cloud environment," *IEEE Access*, vol. 5, pp. 6036–6048, 2017.

[102] M. Yaseen, K. Saleem, M. A. Orgun, A. Derhab, H. Abbas, J. Al-Muhtadi, W. Iqbal, and I. Rashid, "Secure sensors data acquisition and communication protection in eHealthcare: Review on the state of the art," *Telematics Informat.*, vol. 35, no. 4, pp. 702–726, Jul. 2018.

[103] A. Majeed, "Attribute-centric anonymization scheme for improving user privacy and utility of publishing e-health data," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 31, no. 4, pp. 426–435, Oct. 2019.

[104] Y. Al-Issa, M. A. Ottom, and A. Tamrawi, "EHealth cloud security challenges: A survey," *J. Healthcare Eng.*, vol. 2019, pp. 1–15, Sep. 2019.

[105] C. Liu, C. Yang, X. Zhang, and J. Chen, "External integrity verification for outsourced big data in cloud and IoT: A big picture," *Future Gener. Comput. Syst.*, vol. 49, pp. 58–67, Aug. 2015.

[106] W. Lehr, "3 Reliability and the internet cloud," *Regulating the Cloud: Policy for Computing Infrastructure*. Cambridge, MA, USA: MIT Press, 2015, p. 87.

[107] M. Felici and S. Pearson, "Accountability for data governance in the cloud," in *Accountability and Security in the Cloud*. Cham, Switzerland: Springer, 2015, pp. 3–42.

[108] A.-E. Mihaita, C. Dobre, F. Pop, C. X. Mavromoustakis, and G. Mastorakis, "Secure opportunistic vehicle-to-vehicle communication," in *Advances in Mobile Cloud Computing and Big Data in the 5G Era*. Cham, Switzerland: Springer, 2017, pp. 229–268.

[109] C.-L. Chen, Y.-Y. Chen, C.-C. Lee, and C.-H. Wu, "Design and analysis of a secure and effective emergency system for mountaineering events," *J. Supercomput.*, vol. 70, no. 1, pp. 54–74, Oct. 2014.

[110] Q. Jiang, X. Lian, C. Yang, J. Ma, Y. Tian, and Y. Yang, "A bilinear pairing based anonymous authentication scheme in wireless body area networks for mHealth," *J. Med. Syst.*, vol. 40, no. 11, p. 231, Nov. 2016.

[111] G. Sharma and S. Kalra, "Identity based secure authentication scheme based on quantum key distribution for cloud computing," *Peer-to-Peer Netw. Appl.*, vol. 11, no. 2, pp. 1–15, 2016.

[112] L. Wu, Y. Zhang, L. Li, and J. Shen, "Efficient and anonymous authentication scheme for wireless body area networks," *J. Med. Syst.*, vol. 40, no. 6, pp. 1–12, Jun. 2016.

[113] H. Li, D. Liu, Y. Dai, T. H. Luan, and S. Yu, "Personalized search over encrypted data with efficient and secure updates in mobile clouds," *IEEE Trans. Emerg. Topics Comput.*, vol. 6, no. 1, pp. 97–109, Jan. 2018.

[114] S. Biswas, Anisuzzaman, T. Akhter, M. S. Kaiser, and S. A. Mamun, "Cloud based healthcare application architecture and electronic medical record mining: An integrated approach to improve healthcare system," in *Proc. 17th Int. Conf. Comput. Inf. Technol. (ICCIT)*, Dec. 2014, pp. 286–291.

[115] D. Thilakanathan, S. Chen, S. Nepal, R. A. Calvo, and L. Alem, "A platform for secure monitoring and sharing of generic health data in the cloud," *Future Gener. Comput. Syst.*, vol. 35, pp. 102–113, Jun. 2014.

[116] Y. Yang, "Attribute-based data retrieval with semantic keyword search for e-health cloud," *J. Cloud Comput.*, vol. 4, no. 1, p. 10, Dec. 2015.

[117] A. Castiglione, R. Pizzolante, A. De Santis, B. Carpentieri, A. Castiglione, and F. Palmieri, "Cloud-based adaptive compression and secure management services for 3D healthcare data," *Future Gener. Comput. Syst.*, vols. 43–44, pp. 120–134, Feb. 2015.

[118] 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," *J. Sensors*, vol. 2017, pp. 1–11, Jan. 2017.

[119] D. He, S. Chan, Y. Zhang, and H. Yang, "Lightweight and confidential data discovery and dissemination for wireless body area networks," *IEEE J. Biomed. Health Inform.*, vol. 18, no. 2, pp. 440–448, Mar. 2014.

[120] P. Gope and T. Hwang, "BSN-care: A secure IoT-based modern healthcare system using body sensor network," *IEEE Sensors J.*, vol. 16, no. 5, pp. 1368–1376, Mar. 2016.

[121] J. Rangras and S. Bhavsar, "Design of framework for disaster recovery in cloud computing," in *Data Science and Intelligent Applications*. Singapore: Springer, 2021, pp. 439–449.

[122] V. Chang, "Towards a big data system disaster recovery in a private cloud," *Ad Hoc Netw.*, vol. 35, pp. 65–82, Dec. 2015.

[123] Y. Gu, D. Wang, and C. Liu, "DR-cloud: Multi-cloud based disaster recovery service," *Tsinghua Sci. Technol.*, vol. 19, no. 1, pp. 13–23, Feb. 2014.

[124] B. Mansoori, B. Rosipko, K. K. Erhard, and J. L. Sunshine, "Design and implementation of disaster recovery and business continuity solution for radiology PACS," *J. Digit. Imag.*, vol. 27, no. 1, pp. 19–25, Feb. 2014.

[125] P. Vimalachandran, H. Liu, Y. Lin, K. Ji, H. Wang, and Y. Zhang, "Improving accessibility of the Australian my health records while preserving privacy and security of the system," *Health Inf. Sci. Syst.*, vol. 8, no. 1, pp. 1–9, Dec. 2020.

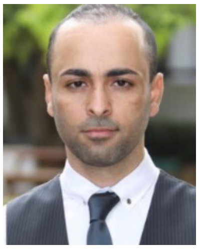
[126] C. Butpheng, K.-H. Yeh, and H. Xiong, "Security and privacy in IoT-cloud-based e-health systems—A comprehensive review," *Symmetry*, vol. 12, no. 7, p. 1191, Jul. 2020.

[127] R. Sivan and Z. A. Zukarnain, "Security and privacy in cloud-based E-health system," *Symmetry*, vol. 13, no. 5, p. 742, Apr. 2021.

[128] I. Ahmad, S. Jimmy, and J. Kaiser, "Security and privacy of E-health data," in *Multimedia Security*. Singapore: Springer, 2021, pp. 199–214.

[129] Z. Hollo and D. E. Martin, "An equitable approach to enhancing the privacy of consumer information on my health record in Australia," *Health Inf. Manage. J.*, vol. 2021, Jun. 2021, Art. no. 183335832110197.

[130] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K.-K.-R. Choo, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey," *Comput. Secur.*, vol. 97, Oct. 2020, Art. no. 101966.



AQEEL SAHI received the bachelor's degree in computer science from the University of Thi-Qar, Iraq, in 2007, the master's degree in information technology from Universiti Utara Malaysia, in 2010, and the Ph.D. degree from the School of Sciences, University of Southern Queensland, Toowoomba, QLD, Australia, in 2018. He is currently working as a Lecturer and a Professional Software Engineer with the University of Southern Queensland. His current research interests include cryptography, data security, and parallel processing, with a focus on block cipher modes of operation and key exchange protocols.

DAVID LAI received the B.Sc., P.G.Dip.Ed., and M.Phil. degrees from The Chinese University of Hong Kong, the G.Dip.Comp.Sc. degree from Victoria University of Technology, the MIT degree from Queensland University of Technology, and the Ph.D. degree from the University of Southern Queensland, Australia. He is currently a Senior Lecturer with the School of Sciences, University of Southern Queensland. His research interests include networks, cyber security, and penetration testing.

YAN LI (Member, IEEE) received the Ph.D. degree from Flinders University, Australia. She is currently a Professor in artificial intelligence with the School of Sciences, University of Southern Queensland, Australia. Her research interests include artificial intelligence, machine learning, big data technologies, internet technologies and security, and signal/image processing.