Privacy Preservation of Electronic Health Records in the Modern Era: A Systematic Survey

RAZA NOWROZY, Victoria University, Melbourne, Australia
KHANDAKAR AHMED, Victoria University, Melbourne, Australia
A. S. M. KAYES, La Trobe University, Bundoora, Australia
HUA WANG, Victoria University, Melbourne, Australia
TIMOTHY R. MCINTOSH, Cyberoo Pty Ltd, Surry Hills, Australia

Building a secure and privacy-preserving health data sharing framework is a topic of great interest in the healthcare sector, but its success is subject to ensuring the privacy of user data. We clarified the definitions of privacy, confidentiality and security (PCS) because these three terms have been used interchangeably in the literature. We found that researchers and developers must address the differences of these three terms when developing electronic health record (EHR) solutions. We surveyed 130 studies on EHRs, privacy-preserving techniques, and tools that were published between 2012 and 2022, aiming to preserve the privacy of EHRs. The observations and findings were summarized with the help of the identified studies framed along the survey questions addressed in the literature review. Our findings suggested that the usage of access control, blockchain, cloud-based, and cryptography techniques is common for EHR data sharing. We summarized the commonly used strategies for preserving privacy that are implemented by various EHR tools. Additionally, we collated a comprehensive list of differences and similarities between PCS. Finally, we summarized the findings in a tabular form for all EHR tools and techniques and proposed a fusion of techniques to better preserve the PCS of EHRs.

CCS Concepts: • **Security and privacy → Usability in security and privacy**; *Social aspects of security and privacy;*

Additional Key Words and Phrases: Block chain, data sharing, confidentiality, electronic health records, privacy, security

ACM Reference Format:
Raza Nowrozy, Khandakar Ahmed, A. S. M. Kayes, Hua Wang, and Timothy R. McIntosh. 2024. Privacy Preservation of Electronic Health Records in the Modern Era: A Systematic Survey. *ACM Comput. Surv.* 56, 8, Article 204 (April 2024), 37 pages. https://doi.org/10.1145/3653297

1 INTRODUCTION

Electronic Health Records **(EHRs)** contain data on a patient's medical history in digital form hence it is extremely important that EHRs are secure, with privacy and confidentiality being its

Authors' addresses: R. Nowrozy, K. Ahmed, and H. Wang, Victoria University, 295 Queen Street, Melbourne, VIC, 3000, Australia; e-mails: raza.nowrozy@live.vu.edu.au, Khandakar.Ahmed@vu.edu.au, hua.wang@vu.edu.au; A. S. M. Kayes, La Trobe University, 360 Plenty Rd &, Kingsbury Dr, Bundoora, VIC, 3086, Australia; e-mail: a.kayes@latrobe.edu.au; T. R. McIntosh, Cyberoo Pty Ltd, 81-83 Campbell Street, Surry Hills, NSW 2010, Australia; e-mail: tim.mcintosh@cyberoo.au.

ACM 0360-0300/2024/04-ART204
https://doi.org/10.1145/3653297

key goals. The literature indicates the many benefits of EHRs over traditional paper-based records, such as cost savings, increased quality of healthcare, advancement of evidence-based medicine, data collection and flexibility [9, 12, 16, 38, 39, 50, 69, 77, 90, 129, 138, 143, 149]. To realise these benefits, EHR systems need to satisfy certain requirements and follow several criteria with respect to data completeness, resilience to failure, high availability and the consistency of security policies [2]. Studies describe EHR systems as unreliable, resulting in patients' privacy being compromised [7, 12, 91]. In the past, data and privacy breaches in the healthcare sector exposed 112 million records [79]. In 2018, a survey found that health breaches, compared with other types, were the most costly, surpassing sectors like business, banking, and government [149]. Many privacy and security acts have also addressed and emphasized the importance of ensuring the privacy of EHRs [9, 46, 77, 79, 114, 130, 142]. Many research studies have discussed the lack of security in current EHR frameworks, the lack of patient privacy and unreliable methods of health data transmission, especially in urgent cases [65, 149]. Australian healthcare authorities raised concerns about the recently introduced ***My Health Record*** **(MHR)** system and demanded improvements due to data and privacy breaches [140]. The UK also faced a similar problem with their ***National Health Service*** **(NHS)** system where nearly 150K British people were affected by ***Personally Identifiable Information*** **(PII)** breaches [129]. Hence, in the era of virtualization, the privacy of data is being protected using various traditional techniques, such as encryption and blockchain. In the recent literature, researchers have highlighted the newly evolved techniques and tools to achieve privacy, security and authentication of electronically stored health data [33, 142].

This paper presents a systematic literature review of the tools and methodologies used to protect EHR privacy. The literature review was carried out using the Kitchenham methodology [74] and examines around 130 publications from 2012 to 2022. The literature review was guided by five survey questions, each of which had corresponding dimensions. This paper contributes to the literature on the privacy preserving of EHR for researchers who are interested in this domain. First, it shows how EHR privacy can be breached. Second, it helps in understanding the concepts of ***privacy, confidentiality, and security*** **(PCS)** as separate terms. Third, it presents how different technologies can be implemented to ensure data privacy. Fourth, it identifies areas for future study that require greater attention so that practitioners and scholars can generate ideas to improve EHR privacy. However, further research is needed to clarify the understanding of the terms PCS in relation to EHR.

The rest of this survey is structured as follows. The motivation and background for the survey is explained in Section 2. The information in Section 3 describes the survey plan and conduct. Section 4 covers reporting and analyzing the results. Section 5 contains survey findings, discussion and limitations. Section 6 concludes the paper.

2 BACKGROUND

The conceptual terms used in the literature review, namely EHRs, privacy preservation of EHR are introduced in this section. At the end, literature reviews on different technologies and privacy preserving of EHR to explain the motivation behind this research are briefly reported. Table 1 lists the key words and Glossary used in this article.

2.1 Electronic Health Records

EHRs comprise patient data in digital form that are stored and exchanged securely and are accessible by multiple authorized users to support the continuous and efficient management of integrated healthcare [16, 27, 65]. EHRs comprise details of patient medical histories, including diagnosis, laboratory findings, information about hospital admissions, surgical procedures, and medicines. They describe the patient's condition, allowing for a more detailed diagnosis and treatment of the

Table 1. PCS: Privacy, Confidentiality, and Security

Glossary	Description
Privacy	In the context of EHR, privacy is defined as the right of individuals to keep their health information confidential and control over the access and use of this data. It is a fundamental patient right under various health laws and regulations.
Confidentiality	Refers to the ethical and legal duty of healthcare professionals to protect personal health information from unauthorized disclosure. It is critical to maintain trust between patients and healthcare providers.
Security	Encompasses the technical and organizational measures to protect EHR data from unauthorized access, use, disclosure, disruption, modification, or destruction. Security practices are crucial for maintaining the integrity and availability of health data.
EHR Management	Involves the systematic approach to handling and governing EHR systems, focusing on efficient and secure data handling, storage, and exchange, ensuring compliance with legal and ethical standards.
EHR Systems and Technologies	Refers to the hardware, software, and methodologies used in EHR systems. This includes traditional and emerging technologies like cloud computing, blockchain, and AI-driven analytics used for enhancing EHR functionalities.
PCS Framework	Represents the integrated approach of Privacy, Confidentiality, and Security in EHR systems. It underscores the interrelatedness of these aspects in ensuring holistic protection and governance of health information.

patient [67]. EHRs can be shared with other healthcare providers when required. However, EHRs are prone to various types of security and privacy attacks during transmission [67, 101]. In light of its widespread use, developing a safe EHR sharing environment has gained a lot of interest in the healthcare sector. The most recent literature [11, 25, 127] indicate that there are many benefits to using EHR software including cost savings, increased quality of healthcare, advancement of evidence-based medicine, more comprehensive data collection and flexibility. Accordingly, the term EHR in this article refers not only to an electronic database for storing and retrieving health information but also a system that can be used to enforce and maintain data completeness, resilience to failure, high availability and the consistency of security policies. Last, we acknowledge the different nature of health information such as ***Personal Health Records*** **(PHRs)** and ***Electronic Medical Records*** **(EMRs)** and their privacy but, in this article, we focus specifically on EHRs.

2.2 EHR Privacy

EHR privacy refers to the protection of patients' rights over their data, encompassing both data protection and physical privacy. It involves ensuring patients' control over their health-related data, maintained under stringent privacy and security policies [46]. Privacy in EHRs also includes mechanisms for tracking data access and transmission, safeguarding against social or economic discrimination and fostering trust in healthcare systems.

A patient's privacy rights encompass both their data and physical privacy. Trust between healthcare workers and patients is fundamental to the practice of medicine. A patient must trust the physician sufficiently to share personal details that may be stressful, embarrassing, or potentially damaging. A physician must trust that a patient is sharing enough information to make an accurate diagnosis, and that a patient is able to give informed consent about treatments that may pose significant risks [37]. An essential component of the trust between doctor and patient is privacy. Over two thousand years ago, Hippocrates emphasized the importance of privacy, and the practice of medicine has recognized and valued the importance of privacy ever since [53, 58]. Privacy is one

of the core cybersecurity challenges nowadays and privacy concerns are regularly addressed in pervasive healthcare system by researchers and end users. Patients who use EHR systems should have control over their health-related data and this data should be maintained by stringent EHR privacy and security policies at national and global levels. This must include actions for compensation for data breaches that have occurred, not simply for those at risk. By doing this, protection from social or economic discrimination and building trust in the health care system can be achieved. However, it is necessary to ensure that critical health data remains accessible at the point of care, and systems must be in place to manage privacy protection. Patients' control of their own data requires appropriate privacy preserving systems which may also help to track who has viewed a record and to whom it has been transmitted [46]. As per information privacy, it is a patient's right to be aware of the personal health data that has been collected on them and the way it has been used.

Software systems handling user's personal and important data like EHRs are facing difficulties in ensuring a high level of data privacy [65]. Health-related information should only be accessed or used by authorized and approved users, such as medical practitioners, as it is confidential and sensitive data. To ensure the safety and protection of users' data, extensive rules and standards have been proposed. Strict security measures are in place to govern the transmission of health data which will result in severe penalties for non-compliance [65]. In many countries around the world, health information is centralized at a national level, for example, with the National Health Scheme in the UK. Whenever a ***General Physician*** **(GP)** updates patient registration information on their clinical system**,** ***Primary Care Support England*** **(PCSE)** uses this information to update the ***National Health Application and Infrastructure Services*** **(NHAIS)** which holds the National Patient Register. But NHAIS is different to GP clinical systems and PCSE cannot see the data on the systems that GPs operate due to privacy concerns [53]. The ***Royal Australian College of General Practitioners*** **(RACGP)** also created a sample registration form for new patients. To ensure the privacy of health information as required by federal and state privacy laws, the form complies with the RACGP standards for general practices (5th edition) [58]. If patients have any privacy concerns, they may discuss these with their GP and leave the form blank. But it is not considered a good practice to let the patient leave the form blank as the information may be required at any phase of their treatment and missing data may result in an incorrect treatment.

2.3 EHR Confidentiality

Confidentiality in EHRs pertains to the protection of identifiable personal health information, shared only with explicit, informed consent. It ensures that sensitive data is shielded from unauthorized disclosure [24]. Measures like data encryption and adherence to privacy laws are key to maintaining confidentiality in EHR systems [26]. It is an agreement and informed consent procedure which guarantees that an individual's identity and personal data will only be shared with another individual or department with their express informed consent [19, 24, 57, 82]. One should be made aware of the fact that data confidentiality is unavoidable. Allowing access to data may put one's confidentially at risk therefore to ensure the confidentiality of electronic data, it must be encrypted [24]. Confidentiality is one of the core concepts of cybersecurity and ensures that private information is protected from unauthorized disclosure [26].

2.4 EHR Security

EHR security focuses on protecting health information from unauthorized access, misuse, or breaches. It encompasses authentication, authorization, and access control measures [48, 155]. Security in EHRs involves both technical and administrative strategies, with compliance to standards

like HIPAA and HITECH being crucial [36]. Security ensures the integrity, confidentiality, and availability of health information.

EHRs are shared among different systems which raises concern about patient privacy due to the possibility of unauthorized access or misuse owing to improper security implementation including authentication, authorization, and access control [48, 100, 155]. Defining access control strategies and policies is imperative in securing EHR systems. Data security involves the protection of personal information against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access. Ensuring the security of EHR systems has been an important aspect in designing, implementing and managing the shared care paradigm, the requirements for such security and privacy of EHRs need to be identified to be applicable in EHR systems. To ensure the security and privacy of EHRs while providing shared and interoperable EHR services, healthcare organizations have highlighted the importance of standards [60, 148]. Examples of such standard developers and publishers include: ***Health Level Seven*** **(HL7)**, ***Health Insurance Portability and Accountability Act*** **(HIPAA)** and ***Health Information Technology for Economic and Clinical Health Act*** **(HITECH)** in the USA; *Canada Health Infoway* in Canada; HEASNET in Japan; and ISO/TC 215, CEN/TC in Europe [36]. ISO 27799 focuses specifically on the information security management perspective for EHR security compared to the technical perspective. EHR needs interoperability, which requires information security, including the restriction of unauthorized access, use, disclosure and modification of data to ensure confidentiality, integrity and availability [115]. EHR connects through wireless communication protocols which can generate a massive amount of data at regular intervals which opens the doors for attackers to launch various security attacks. An insecure technique for Healthcare 4.0 [76] may lead to a breach of healthcare records where hackers can gain full access to patients' email accounts, messages, and reports [110]. Security procedures are used to control access to patients' data to protect it from unauthorized users. This can be achieved with operational controls within a privacy preserved entity [100, 131].

2.5 The Distinction between EHR Privacy, Confidentiality and Security

Understanding the distinctions between EHR privacy, confidentiality and security is crucial for comprehensive protection of patient data. These concepts are intimately related yet distinct in their application and the point of compromise in the event of a cyber attack, as described by the **Cyber Kill Chain (CKC)** model[1].

- **EHR Privacy:** This refers to the patient's ability to control their health information and protect it from unauthorized access. Privacy is compromised when attackers gain unauthorized access to EHR systems, which can occur at the CKC's Installation phase. However, privacy is directly breached when attackers have the capability to read private patient information, which may happen during *Exploitation*, but privacy breach is fully realized in the *Installation* phase if the data is accessed.
- **EHR Confidentiality:** Refers to the ethical and legal duty to keep health information accessible only with the patient's explicit consent. A potential breach of confidentiality occurs during the *Command & Control* phase when attackers have the capability to exfiltrate sensitive data. However, confidentiality is definitively compromised in the *Actions on Objectives* phase if the data is actually extracted from the EHR system.
- **EHR Security:** This involves the technical and administrative safeguards that protect EHR systems from unauthorized access, data breaches, and cyber threats. Security is first compromised at the *Delivery* phase of the CKC when the attack vector is successfully deployed into the healthcare system.

[1] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

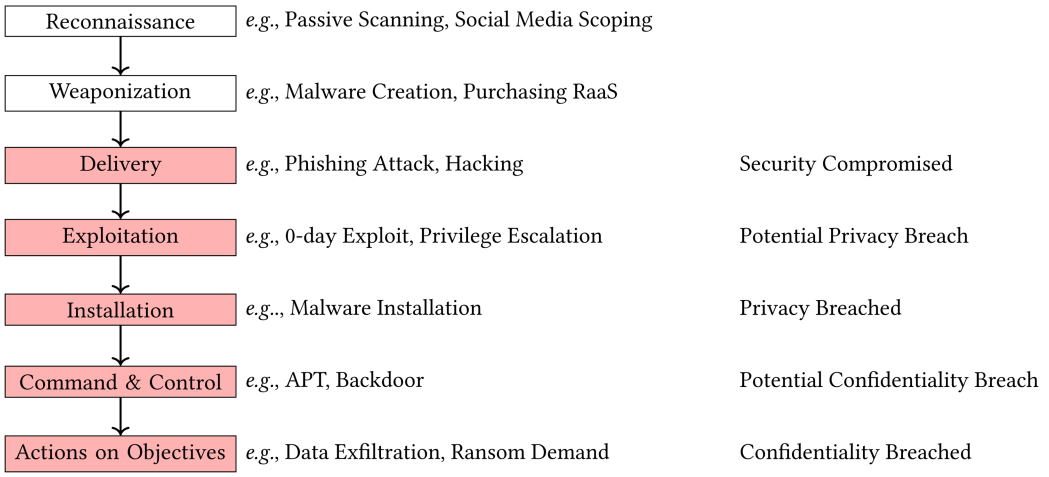

Fig. 1. The Cyber Kill Chain illustrating the points of compromise for security, privacy, and confidentiality in EHR systems.

This alignment with the CKC phases (Figure 1) illustrates that while security can be compromised by the mere success of a delivery mechanism, privacy is specifically breached when unauthorized viewing of patient information occurs, and confidentiality is breached when information is extracted and possibly used for malicious intent such as blackmail or public disclosure.

3 THE SURVEY PLAN AND CONDUCT

We used a systematic, comprehensive, reproducible strategy to survey the articles on methods and technologies related to EHR privacy to identify and categorize them. We perform the survey using three stages, i.e., plan, conduct, report [74]. This section discusses the planning of the survey and how it was conducted.

3.1 Planning the Survey

Planning included the following activities:

3.1.1 Constructing the Survey Questions. The survey aims to explore the current state of privacy preservation in EHR systems. The breakdown into five specific **survey questions (SQs)** serves to provide a comprehensive understanding by covering various aspects: the methods of EHR data sharing, the role of privacy in stakeholder engagement, the strengths and weaknesses of EHR systems in privacy preservation, the distinction between privacy, confidentiality, and security in EHRs, and the technologies available for maintaining EHR privacy.

SQ1: What EHR data sharing methods are currently available?
Justification: This question is intended to catalog existing EHR data sharing methods, setting a foundational understanding of the mechanisms through which privacy must be maintained.

SQ2: What role does privacy play when sharing EHRs with different stakeholders?
Justification: By examining the role of privacy in stakeholder engagement, this question seeks to highlight the privacy expectations and requirements from various perspectives within the healthcare ecosystem.

SQ3: What are the main strengths and weaknesses of EHR systems in terms of privacy preservation?

Justification: Identifying the strengths and weaknesses of current EHR systems provides insights into their privacy preservation capabilities and the areas needing enhancement.

SQ4: What is the difference between EHR privacy, confidentiality, and security?
Justification: Clarifying the distinctions between these concepts is crucial, as each has unique implications for the design of privacy-preserving measures within EHR systems.

SQ5: What different technologies are available to preserve the privacy of EHR?
Justification: This question aims to explore the spectrum of technologies that can be or are being implemented to uphold the privacy of EHR, thus informing future research and development in this area.

Through five targeted questions, the survey's main goal is to delve into EHR data sharing, stakeholder privacy roles, and the strengths and weaknesses of EHR systems, thereby providing a thorough insight into privacy concerns in EHR data sharing.

3.1.2 The Search Keywords. Following a preliminary analysis of some of the most widely read works on the topic of protecting the privacy of EHRs, as well as our own expertise, we selected a number of search keywords. First, the majority of articles in this field were retrieved using the acronym EHR. We also selected EMR [16], PHR, security, privacy, confidentiality, secrecy, sharing, access and breach as significant terms, since they are often used in relation to EHRs. Moreover, as this review focuses on the privacy of EHRs, the difference between various terms which are used interchangeably (e.g., PCS) is also mentioned to limit the focus and elucidate the confusion among them. The following are the important terms used in this paper.

— ***Electronic Medical Record* (EMR):** An EMR is an application environment comprising the clinical data repository, clinical decision support, controlled medical vocabulary, order entry, computerized provider order entry, pharmacy, and clinical documentation applications that may be confidential in different ways to different stakeholders [152].
— ***Personal Health Record* (PHR):** A PHR is a collection of an individual's medical documentation maintained by the individual themselves or a caregiver in cases where patients are unable to do so themselves [16].
— *Privacy*: Privacy refers to an individual's control over how much, when, and under what circumstances they may share details of their physical, behavioral, or intellectual life with others, and their right to restrict other people's access to their personal information [98].
— *Security*: Security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle.
— *Confidentiality*: Data confidentiality means to protect data against unintentional, unlawful, or unauthorized access, disclosure, or theft [98].
— *Secrecy*: Data secrecy means that data is completely unknown and untraceable by anyone other than the owner and those with whom it has been explicitly shared.
— *Sharing*: Data sharing is the ability to make a data resource available at various points.
— *Access*: Data access is a user's ability to access or retrieve data stored within a database or other repository.
— *Breach*: A data breach exposes confidential, sensitive, or protected information to an unauthorized person. It is important to note that several spellings (such as 'behaviour/behavior' and 'modelling/modeling') were also used in the searches to ensure no relevant publications were overlooked.

3.1.3 Data Collection. Data was collected via three sources, i.e., digital libraries namely, Google Scholar, Elsevier Science Direct, Springer Link, ACM Digital Library, and IEEE Xplore, journals and conference proceedings. We found that the most well-known scientific libraries' search engines

Table 2. List of Target Journals and Conferences

Journal/Conference	Selection Criteria
ACM Conference on Health Informatics	Leading conference in healthcare technology
Blockchain in Healthcare	Innovative applications of blockchain technology in healthcare
Digital Health and Telemedicine	Advances in digital health and telemedicine practices
Emerging Technologies in Healthcare	Exploration of new and emerging technologies in healthcare
Health Informatics and Data Analysis	Developments in health informatics and medical data analysis
Healthcare Policy and Management	Studies on healthcare policy, management, and regulatory compliance
IEEE Journal of Biomedical and Health Informatics	Notable for biomedical informatics research
International Conference on Medical Data Privacy	Focus on medical data privacy laws and practices
Journal of Healthcare Privacy and Security	Specialized in EHR privacy and security
Journal of Medical Internet Research	High impact factor, focus on digital health
Medical Data Security and Encryption	Research in data security and encryption for medical data
Patient Privacy and Rights	Research on patient privacy, rights, and ethical considerations

performed differently when the search string was specified. Depending on the library, multiple methods had to be used to undertake the same search (i.e., using different syntax). There were a variety of alternatives in each library to find content, for instance by keywords in the title, in the abstract or in the whole article. As the technologies for data sharing and privacy research are multidisciplinary, therefore, all searches were carried out comprehensively. Conference proceedings and articles pertinent to the survey and studies in the reference lists of selected articles were also examined.

3.1.4 Approach to Gathering Data. For our research, data was amassed from a trio of primary sources, notably digital repositories including Google Scholar, Elsevier Science Direct, Springer Link, ACM Digital Library, and IEEE Xplore, alongside journals and symposium records. The selection of journals and conference papers was intentionally narrowed to those significantly contributing to the domain of EHR privacy and security. This encompassed authoritative sources in the realms of healthcare informatics, data protection, and privacy legislation. A detailed enumeration of these essential journals and symposia is explained in Table 2.

The exploration revealed varied responses from the search engines of prominent scientific databases when specific search queries were inputted. The necessity to adapt methodologies for identical queries across different databases became apparent (*i.e.*, modifying search syntax). Each database offered a spectrum of search options, like pinpointing keywords in titles, abstracts, or throughout the entire text. Given the interdisciplinary nature of data sharing and privacy in research, our search strategy was exhaustive. We also meticulously reviewed conference papers and journal articles that were relevant to our study, including those cited in the bibliographies of the primary articles selected.

3.2 Conducting Survey

The survey was carried out after the planning phase. The literature review and data synthesis are discussed in Sections 3.2.1 and 3.2.2 sequentially.

3.2.1 Executing Survey.

(1) Searching digital libraries: the digital libraries detailed in Section 3.1.3 were searched using the search keywords (Section 3.1.2).
(2) Searching conferences and journals: all the conferences and journals (Section 3.1.3) were searched using the search keywords (Section 3.1.2).
(3) Searching backward snowballing: to identify relevant papers, we looked for references and citations in the publications which were identified in the first two rounds.

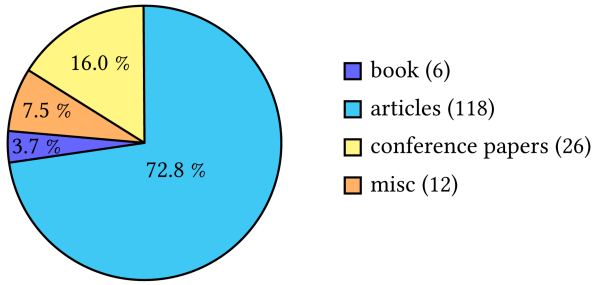

Fig. 2. Numbers and percentages of publication types.

3.2.2 Data Synthesis. The publications were listed on an Excel spreadsheet. The search of the digital libraries yielded 513 relevant publications in four categories, namely journal papers, conference papers, review articles and case studies. We only selected articles that had been published from 2012 onward by taking into consideration the more practical and accurate analysis of publications. We examined each publication carefully and categorized it into one of the four categories along with its publication year. We removed any duplicate studies which resulted in a total of 162 publication (Figure 2). Against each category, we made further three subcategories based on the main topics: (a) EHR, (b) EHR privacy, (c) EHR security, and (d) EHR confidentiality hence reducing the results to 130 publications. The selected publications for comparative review were based on access control, blockchain, cloud-based techniques and cryptography.

4 SURVEY RESULTS

The analysis of the survey results is based on the survey questions (Section 3.1.1).

4.1 What EHR Data Sharing Methods are Currently Available?

4.1.1 Cloud-based Sharing. Cloud-based platforms offer advantages for delivering electronic health services by providing ubiquitous network access, scalability, and cost savings [142, 147]. However, transferring EHRs to the cloud poses major threats to privacy, data integrity, and confidentiality and additional techniques are required to ensure data secrecy. Wang and Song [142] proposed a cloud-based EHR system which uses an attribute-based cryptosystem and blockchain technology to solve these security problems, achieving confidentiality, authentication, integrity of medical data, and supporting the sharing of confidential data [105, 142, 147]. The researchers used ***Attribute-Based Encryption*** **(ABE)** and ***Identity-Based Encryption*** **(IBE)** to encrypt data, ensuring fine-grained access control for encrypted data, and used an ***Identity-Based Signature*** **(IBS)** to implement digital signatures. To achieve different functions of attribute and identity-based encryption and identity-based signature in one cryptosystem, they introduced a new cryptographic primitive, called combined ***Attribute-Based/Identity-Based Encryption and Signature*** **(C-AB/IB-ES)** which eliminates the need for different cryptographic systems for different security requirements. In addition, they use blockchain technology to ensure that medical data cannot be tampered with and the data sources can be traced. Their technique is a well-defined and encrypted data sharing method but its scope is limited to only patients and hospitals and does not accommodate the needs of various other health workers such as pharmacists, clinicians, researchers and the like, but this can easily be extended because of the helpful property of blockchain to trace data sources.

4.1.2 Attribute-based Access Control (ABAC). ABAC enables attribute-based encryption for secure access to cloud-based EHR systems [67]. ABE guarantees tight data security and records every

patient visit as a separate node in the knowledge graph which facilitates easy querying and faster data access.

4.1.3 Role-based Access Control (RBAC). RBAC [114] in cloud storage gives various types of users different access privileges. This policy transformation approach enables EHR data to be transferred from a private cloud to a public cloud with the corresponding transformation in the access control policy. Conditional or emergency access and authorization are delegated.

4.1.4 Encryption-based Sharing. Keyword searchable encryption and proxy re-encryption technology is combined in [143] for privacy-preserving and secure data sharing for EHR sharing based on consortium blockchain technology and cloud storage. Proxy re-encryption (a safe cryptographic method) is used to ensure effective access control on confidential data [133]. The re-encryption of cyphertext by the cloud is a relatively good opportunity to enhance the security of data in the technique proposed by [143]. But keyword searchable encryption is not clearly described from the user point of view. A privacy-preserving framework for access control and interoperability of EHRs using blockchain technology [33] is a blockchain-based framework for secure, interoperable, and efficient access to medical records by patients, providers, and third parties, while preserving the privacy of patients' sensitive information. Keyword searchable encryption and proxy re-encryption technology [143], consortium blockchain technology, cloud storage proxy re-encryption cloud technology ensures users are able to find the relevant EHRs and protects data security with a searchability guarantee that only authorized entities can access the EHRs. It indicates that the challenging problem of private searching on encrypted data is of independent interest and deserves further study.

Attribute-based cryptosystems [85, 86, 108, 143, 149, 151] encrypt data, ensuring fine-grained access control for encrypted data and use an IBS to implement digital signatures. It introduces a new cryptographic primitive, called combined attribute-based/identity-based encryption and signature. The cloud server may not be fully trusted. A general verification mechanism that can be applied to all search schemes is also lacking in the current literature. There is also no effective countermeasure to penalize a misbehaving server or user. Security techniques for data sharing may include but are not limited to items such as firewalls, virus checking, encryption and decryption, as well as authentication measures.

4.1.5 Blockchain-based Sharing. The blockchain-based [6, 9, 31, 79, 85, 86, 103, 108, 123, 133, 151] data sharing mechanism [39] offers a secure distributed research data-sharing network. It provides a way to specify/control the parameters of sharing and provides full accountability of access to such data. The Ancile privacy-preserving framework [33] utilizes smart contracts in an Ethereum-based blockchain using cryptographic techniques, by implementing six separate contracts, thereby improving the efficiency of the patient experience and reduces privacy threats. The patient can be the only node expressly given the location of their information. Blockchain-based searchable encryption [28] guarantees that users can receive accurate search results without additional verification. It allows cryptographic algorithms to be built to ensure data integrity, standardized auditing, and some formalized contracts for data access. Zaghloul et al. [149] proposed a decentralized and hierarchical data-sharing method using smart contracts which offers a secure, private and efficient electronic record-sharing scheme that utilizes smart contracts deployed over a blockchain. It empowers patients to have control over their records, allowing them to selectively share these with data users that satisfy their privacy preferences. It also provides patients with access control over their records and eliminates the need for management services provided by record-generating parties.

4.1.6 HIPPA/Privacy Act-based Sharing. The HIPAA Security Rule incorporates three safeguards, namely administrative, physical and technical [78] which encompass a vast array of security techniques that are implemented by healthcare organizations to protect the health information in EHRs [54, 143]. HIPPA focuses on compliance with security policies and procedures and the protection of physical access to protect health information through hardware and software access. In Europe, sharing health data and access to data is subject to the ***General Data Protection Regulation*** **(GDPR)** [113] which provides subject data rights to EU citizens and is much broader in scope [9].

4.1.7 Current Australian MyHR (My Health Record) Sharing. The lack of interaction between health care practitioners and across various settings in the healthcare sector has been widely observed. Hence, it is possible that a patient's history will not be easily available at the entry of care. The implementation of My Health Record in ***Emergency Departments*** **(EDs)** was undertaken by The Australian Digital ***Health Agency and the Australian Commission on Safety and Quality in Health Care*** **(ACSQHC)** which will empower the use of My Health Record by medical professionals in EDs in Australia.

4.1.8 Model-based Sharing. To promote the sharing and integration of patients' records, healthcare institutions usually follow three models: push, pull and display [79]. Medical data is sent from one supplier to the other in a push model (e.g., from an emergency room physician to a chief care doctor). A provider questions another vendor for data in a pull model (e.g., a cardiothoracic specialist consults with a primary care doctor). A vendor looks at the registry of another company in the display model. For example, a cardiologist reviews the X-ray of a patient that was obtained at an emergency clinic. A significant downside to these is that evidence is not inspected in a structured manner. In comparison, in the push model, a new hospital might not be able to view the information that was "pushed" to the first hospital if a patient is moved to another hospital. The absence of an independent audit (such as ***Hippocratic Databases*** **(HDB)** compliance auditing [3, 48]) means that data accuracy from the perspective of data generation to the perspective of data usage is not assured. Permission is also given on an informal and ad-hoc level in the pull model. The procedures and guidelines regulating HDB differ significantly throughout territories, depending, *inter alia*, on local experience and the national implementation of privacy policies [58]. This approach helps companies to record past information in metadata format recorded in a log database. Auditors make use of these records with the help of queries to extract information such as the identity of a user who accessed a specific record, the time and date of the query, the access purpose, and the results of the query. This HDB approach uses relevance ranking auditing disclosures that depend on sensitive data tracking. This can lead to misuse compared to the results of the previous queries stored in the backlog. The work in [87] investigated database compliance issues and improved database system accountability by saving previous data events to ensure compliance with the companies' top-level policies. The adoption of such methods includes high human-based validation to perform compliance-validation tasks. This is due to the incompatibility of proposed mechanisms to determine the fine-grained requirements automatically.

4.2 What Role does Privacy Play when Sharing EHR with Different Stakeholders?

Data privacy emerges as a paramount concern in the realm of EHR sharing among various stakeholders. The intricacies of data privacy in distributed medical research and healthcare systems pivot around policies shaped by legislative and jurisdictional directives [43, 99, 128]. These policies necessitate stringent enforcement at the program level, yet, they often fall short of providing an ironclad guarantee of privacy protection [20, 83].

The societal acceptance of healthcare systems heavily depends on the scrutiny and enhancement of privacy agreements. Implementing health mechanisms that fortify privacy can substantially allay Australian public concerns regarding their data's privacy [121]. This necessitates the adoption of robust mechanisms safeguarding patient data privacy. However, despite technological advances and automation, privacy risks in healthcare data persist [48, 142].

EHRs, being readily accessible and necessary for improved patient care, pose unique challenges. The access to EHR must be balanced with the utmost respect for privacy and confidentiality [120]. Additionally, these systems are susceptible to cyber security risks, including threats from hackers and system failures, underscoring the need for rigorous governance and audit mechanisms in healthcare applications [71, 151].

Effective governance involves user guidelines and adherence to initial test conformance during access control runtime. This includes reviewing past data-sharing events and permissions granted to each user. Automated solutions for such reviews, while beneficial, are often challenging and costly [3].

EHR comprises various elements like personal, sensitive, private, and historical health information. Streamlining EHR systems for privacy assurance may benefit from standard protocols, such as the EU's General Data Protection Regulation (GDPR), which imposes stringent data protection requirements and penalties for non-compliance [107].

Patient care involves a holistic approach, respecting individual patient preferences and values in clinical decisions [80]. Healthcare systems utilize sensitive patient data, which are subject to privacy laws due to their personal nature. Balancing a patient's data autonomy and privacy with the public benefit derived from this data is a pivotal concern for healthcare policymakers and security developers [57].

Access to a patient's EHR is typically granted to various medical professionals, necessitating complex access control mechanisms. The use of pseudonymized or anonymized records for research purposes introduces challenges, especially regarding genetic data and the necessity of fine-grained access rules [79].

Protecting sensitive data from unauthorized third-party access calls for intelligent audit systems. The **UK National Health Service (NHS)**, for example, employs networks for auditing but faces challenges in ensuring complete and separate audits [83]. Continuous internal and external audit trials are essential to align operational processes with high-level policies and to track regulation breaches effectively.

Under GDPR, personal information is broadly defined, encompassing a wide range of data that could identify an individual [33]. Sensitive data requires extra safeguards due to potential risks of discrimination if mishandled.

4.2.1 Differentiation of Health Record Sets. The categorization of EHR data into distinct sets plays a crucial role in understanding the complexities of data privacy and access control. We define several Health Record Sets as follows:

- *Health Record Set A = {Personal health information}*
- *Health Record Set B = {Personal health information, Private health information}*
- *Health Record Set C = {Personal health information, Sensitive health information, Private health information, Historical health information}*
- *Health Record Set D = {Personal health information, Historical health information}*
- *Health Record Set X = {Health Record A, Health Record B, Health Record C, Health Record D}*

These categorizations are pivotal in understanding how various types of information intersect and combine within the healthcare system. For instance, the intersection of Health Record Sets A

and B can be represented as:

$$\text{Health Record Set A} \cap \text{Health Record Set B} = \{x : (x \epsilon \text{Personal health information}) \wedge (x \epsilon \text{Personal health information, Private health information})\}$$

which simplifies to the set of all Personal health information. Similarly, the union of Sets B and C can be expressed as:

$$\text{Set B} \cup \text{Set C} = \{x : (x \epsilon \text{Set B}) \vee (x \epsilon \text{Set C})\} \quad = \{\text{PHI, SHI, PriHI, HistHI}\}$$

This mathematical representation aids in visualizing the overlap and unique aspects of different types of health information, highlighting the complexity of managing privacy across various data sets.

4.2.2 Case Studies in EHR Data Security. Professionals and Respective Roles - Support Professionals, Nursing Professionals, Medical Practitioners, Diagnosis Professionals, Medical Scientists; Receptionist, Chemist, Nurse, Nurse Manager; Doctor, Specialist, Psychiatrists; Radiologist, Psychologists; Researcher, Senior Researcher, Junior Researcher. Health Record Set A, Health Record Set B, Health Record Set C, Health Record Set D, Health Record Set X. In a hybrid way, the combination of healthcare and information technology, is an ongoing process, which can bring many changes to the healthcare discipline. These developments impact the recovery process of patients, therefore requiring diligent data collection. Healthcare is entirely based on data for service, which poses some questions regarding data access and privacy preservation. The word secrecy is about allowing someone to access patients' PII and it also ensures that private data can only be obtained by authenticated individuals. Ensuring that such sensitive data is kept secure from eavesdroppers or trespassers relates to the term protection, which ensures that the device is capable of protecting the private data of users from strangers [12]. Hence, the privacy risks and attack possibilities that EHR data of patients may encounter and the various techniques used to handle these attacks are discussed below.

Case I: EHR is accessed by an Intruder: The authentication server will control the intruder. This authentication server uses the RADIUS (Remote Authentication Dial-In User Service) protocol, based on server/client service. The protocol is designed in a way that the users' information is passed by clients to RADIUS servers and it acts based on a returned response. In this RADIUS protocol, it first receives the connection requests of users, followed by user authentication, and the necessary information is processed to the client to offer service delivery. Several methods are supported by the RADIUS server for user authentication. After the user logs in to this server with their user-id and password, the users are offered many authenticated mechanisms such as UNIX, CHAP, PAP or PPP login. In general, an Access-Request query of the NAS and the server response (Access Reject/Accept) constitutes the user login. The RADIUS server searches for the username from the database after the NAS access request has been received. It loads the default profile or an Access-Reject message is sent when the RADIUS server does not find the required username from the database. The Access-Reject message is simply a text message that provides the refusal reasons.

Case II: X tries to masquerade as Y: The permissions list is maintained by the **Access Control List (ACL)** server that combines the EHR data on of patients such as drug-related data, neonatal data, sexual health data, and so on. The ACL specifies what data access is granted to system processes or users and their operations. The operation and a subject are specified by all the entries of the ACL. For example, an ACL file has been read and Alice is given permission to read a specific EHR type. When an EHR type operation is requested by subject X, ACL is checked by the operating system to decide its legitimacy. However, there are certain challenges with the ACL model such

as how to edit the control access lists for example, what access is granted to processes and users. An alert will be generated by the system and the relevant personnel are informed when subject X does not have data access.

Case III: Unauthorized Access to Patient EHR via ACL Server: In this scenario, the subject X attempts to bypass the **Access Control List (ACL)** server to illicitly obtain specific patient EHR data. The protocol mandates robust authorization mechanisms, where X is required to procure a legitimate authorization key from the authorization server to access any EHR data. This key is a critical component in safeguarding patient information, as it enables only authorized personnel to retrieve EHR data. The underlying principle emphasizes the importance of strict access controls in preventing unauthorized data breaches, aligning with the security frameworks. In this context, the ACL server functions as a gatekeeper, ensuring that access to sensitive EHR data is tightly regulated and complies with HIPAA guidelines.

Case IV: System operators try to abuse patients' EHRs: The proposed model uses homomorphic encryption in its database server which encrypts the patient's EHR data. The advantage of this type of encryption is that patients can modify their information and system operators do not need to have knowledge about this. The operators also do not know in what profiles this modification has occurred.

Case V: Restriction on Patients Accessing Other Patients' EHRs: This case delves into the scenario where a patient attempts to access or permit access to another patient's EHRs. The system's authentication server plays a pivotal role in this context, rigorously authenticating each patient upon entry into the system. Each patient is assigned a unique, private EHR decryption key, fundamentally preventing them from accessing or decrypting other patients' EHR data. This design principle adheres to the concept of 'Least Privilege' ensuring that individuals have the minimum level of access or permissions necessary to perform their functions. The architecture of this system inherently safeguards against the possibility of patients compromising other patients' EHR data, thereby reinforcing the security protocols recommended in the healthcare data protection guidelines.

Case VI: Man in the Middle Attack: There is no possibility for a man-in-the-middle attack to occur in this proposed framework. For instance, consider cases where patients' EHR data has been used or updated. (i) Update in the cloud server: The consent of patients, the ACL server and the authentication server is in place to ensure access and authentication right for updating the patients' profile by any EHR user. A session mechanism is maintained by these servers to protect them from man-in-the-middle attacks. (ii) Display and update at the doctor's end: If the patients' EHR data is accessed by doctors/specialists, it is assumed that the patients are available for the session. The encrypted EHR data from the server is used by doctors. Then, the private key provided by patients is used to decrypt and use the EHR information. If any updates need to be made with this information, the doctors will use the patients' private key to encrypt the data and then they save this on the server. Hence, there is no possibility for a man-in-the-middle attack as the EHR data are encrypted.

4.3 What are the Main Strengths and Weaknesses of EHR?

The implementation of EHR represents a transformative shift in healthcare management and patient care across the globe. Moving away from conventional paper-based records, EHRs offer a more dynamic, efficient, and accurate way of handling patient health information. The integration of EHR systems is a response to the growing need for coordinated, patient-centric care, reliant on the prompt and accurate exchange of health data. In this section, we will undertake a detailed examination of the strengths and weaknesses of EHRs, addressing the multifaceted impact they have on the healthcare sector. The analysis is structured into two distinct parts: the first part explores

the various advantages EHRs offer, such as enhanced patient care, improved data management, and the overall efficiency of healthcare services. The second part critically assesses the challenges and limitations faced by EHR systems, focusing on privacy concerns, operational complexities, and the integration hurdles with existing healthcare frameworks. This structured approach ensures a comprehensive evaluation of EHRs, highlighting their significant role in modern healthcare while also acknowledging the complexities involved in their application.

4.3.1 Strengths of EHR:. The EHR system, distinct from the Electronic Medical Record (EMR), offers a more comprehensive patient information repository [8]. Its strengths lie in its capacity to support detailed analyses of clinical care and subgroups of patients, particularly those requiring palliative care [10, 30, 51, 70, 92, 132]. The integration of social determinants in EHR enhances the delivery of high-quality, accountable care [30, 35, 69]. Benefits include improved care levels, patient safety enhancement, streamlined processes, and cost reduction [69]. EHRs facilitate better health policy creation, decision making, and lifestyle promotion [81]. The continuous use of EHR improves communication, quality of care, reduces medical errors and waste, and transforms the healthcare industry into an information-rich sector [5, 72]. EHRs' support for **Decision Support Systems (DSS)** and **Intelligent Systems (IS)** is notable [90]. The HITECH Act significantly boosted EHR adoption, enhancing care quality in the NHS [4, 49, 69]. EHRs have led to early disease diagnosis, reduced medication errors, compliance with care adherence, and decreased costs [44, 104]. Other specific advantages include managing epidemics, informed decision-making, care coordination, patient satisfaction, and evidence-based care advancement [69]. Strengths in SWOT analysis highlight the timely access and storage capacity of information [120].

4.3.2 Weaknesses of EHR:. Despite its strengths, EHR implementation has encountered challenges. Initial stages faced issues in data input, security, and resource allocation, with cost issues and ROI concerns [59]. Key weaknesses include lack of system harmony, patient matching problems, data security and privacy issues, and clinician burden due to complex EHR workflows and insecure data storage [69]. EHRs also face limitations in reflecting actual care given versus documented treatment, and in capturing critical outcomes for quality disease treatment [30]. The section Table 3 discusses potential solutions to these drawbacks.

4.4 What is the Difference between EHR Privacy, Confidentiality and Security?

Every health care organization (e.g., hospitals) is responsible for protecting patients' privacy by ensuring that their EHRs are secure and confidential [97]. The terms privacy, confidentiality and security tend to be used interchangeably in the existing literature, however they refer to different individual protections which may overlap but they are not quite the same [14, 26, 52, 122, 124, 134, 144, 150]. Guaranteeing that personal information will be safeguarded is one of the most important components of securing someone's data. This entails safeguarding one's privacy, maintaining data privacy and/or enabling data to remain anonymous [52]. Often, security breaches occur not as the result of a sophisticated technical failure but as the result of a mistake made by someone with authorized access to information [26]. It is also an individual's choice as to whether they want to disclose their matter in front of people [150].

Privacy is sometimes confused with confidentiality and security. The right to confidentiality is based on the fundamental rights to privacy and to "informational self-determination", which relate to personal data protection [107]. An operational definition of privacy is the fair and authorized processing and access of personal information [38]. However, confidentiality is a different concept and comprises more than data protection rights (Figure 4). Firstly, confidentiality works downstream of privacy and for confidentiality to be legally "triggered", privacy must have already been disclosed. Furthermore, the right to privacy is what is called a "negative" right because it claims

Table 3. EHR Complications and Potential Solutions

Key Issues	Potential Solutions
Redundant credentials	Streamline documentation by identifying and focusing on clinically relevant data points that offer the highest utility in patient care management. Consider the adoption of standardized templates that have been recognized for their efficiency in various healthcare settings.
Multiple steps and complicated EHR workflows	Re-engineer process flows to align with best practices for clinical workflow optimization. Employ user-centered design principles to create interfaces that reduce cognitive load and administrative burden on clinicians. Delegate appropriate data entry tasks to support staff trained for this purpose.
Need for automation with new technologies	Leverage emerging technologies such as natural language processing and machine learning to automate routine tasks. Explore the integration of voice-to-text functionalities and interoperable devices to streamline data capture and entry.
Closed EHR software platforms	Advocate for open-platform approaches that allow for customization and integration of third-party applications. Embrace models that foster a collaborative ecosystem, prioritizing the enhancement of the clinician's user experience and specialty-specific functionalities.
Information resting in silos	Promote the development and adoption of industry-wide standards for Application Programming Interfaces (APIs) to facilitate robust data exchange. Emphasize the importance of interoperability as a means to achieve a more holistic patient record and improve continuity of care.
Poor user experience	Prioritize the simplification of user interfaces and enhance mobile optimization. Recognize the increasing prevalence of mobile device usage and the need for responsive design that adapts to various screen sizes and user contexts.

non-interference with information belonging to the private sphere [39]. Privacy and confidentiality are among the inalienable rights of every human being that contribute to preservation of a sense of reverence and dignity [82]. Privacy refers to an individual's control over how much, when, and under what circumstances they may share details of their physical, behavioral, or intellectual life with others, and their right to restrict other people's access to their personal information [98]. Privacy requirements typically arise in two forms. First, many organizations adopt privacy policies based on their own ethical sense of proper information handling. Second, a variety of laws and regulations impose privacy requirements on institutions and organizations [26]. Data security is the use of logical, technical, administrative, physical safeguards to ensure that the confidentiality, integrity, and availability of data is maintained. But confidentiality prevents authorized access to non-public information that two or more parties have agreed to restrict [38]. Thus, confidentiality means that providing information to another person will result in a commitment on their part not to reveal it to anyone else [98]. In clinical contexts, hospitalized patients have limitations that may jeopardize their privacy and thus result in serious consequences [9]. Moreover, a commitment to confidentiality provides the basis for trust in therapeutic communication.

The issue of privacy is one that often applies to patients' right to safeguard their information from any other person. It involves the protection of vulnerable data such as personal data, demographic data, disease illness, medical history, tests reports, medication record, and so on from being openly disseminated to others (specialists, radiologists, pharmacists, researchers etc.). In general, privacy is the individuals' right to keep their data to themselves. Confidentiality is a

Table 4. Clarifying the Components of Information Security

Component	Definition	Role in Information Security
Confidentiality	The principle that information should not be made available or disclosed to unauthorized individuals, entities, or processes.	Confidentiality is a key aspect of information security that involves restricting access to information to protect personal privacy and proprietary knowledge.
Integrity	The assurance that information is trustworthy and accurate, and has not been tampered with or altered by an unauthorized party.	Integrity is crucial for maintaining the trustworthiness of information systems and ensuring that data is not altered in an unauthorized manner.
Availability	The guarantee that authorized users have reliable and timely access to information and associated assets when needed.	Availability is essential for ensuring that information systems operate effectively and that data can be accessed when required.
Security	A broader term encompassing the practices and procedures designed to protect information from unauthorized access, use, disclosure, disruption, modification, or destruction.	Security as a whole is built on the principles of confidentiality, integrity, and availability, often referred to as the CIA triad. Each component plays a distinct role in the protection of information assets.

similar idea, but with a slightly different component. Confidentiality agreements are often applied to situations where someone trusted with personal data must safeguard this data from being released. Alternately, some studies define confidentiality as issues about the data that gets collected, where privacy issues have to do, again, with the core principle of an individual not being recorded or monitored. Security is a different term that's applied to organizational systems. Security may include the idea of customer privacy, but the two are not synonymous. Likewise, security may provide for confidentiality, but that is not its overall goal. The overall goal of most security systems is to protect the healthcare organization, which may or may not house a lot of patients' data. Sometimes, the objectives for privacy and security are the same. In other cases, security may not automatically provide for privacy concerns. One example is where a healthcare organization may be able to keep its data safe from outside attackers, but where staff (doctors, nurses) may be able to view patients' information. Another scenario might involve situations where an organization (e.g., hospital), doesn't face any liability by releasing patients' data, and so chooses to do so. Here, the hospital's security is not jeopardized, but patient privacy is violated. The studies in [38, 102] describe three areas of overlap between privacy and information security:

— Integrity (information security) and accuracy (privacy): Information security's integrity requirement overlaps with privacy's accuracy requirement in that both aim to ensure that data are not altered without both authentication and authorization.
— Availability (information security) and access (privacy): Information security's availability requirement supports privacy's access requirement because if the data are not available, it cannot be accessed.
— Accountability (both): Both information security and privacy doctrines require data owners and custodians to be responsible for protecting data in accordance with the respective protection regimen, which is a form of accountability.

Between privacy and confidentiality, privacy is about personal or private i.e., while security and privacy are interdependent, security can be achieved without privacy but privacy cannot be achieved without security. Security protects confidentiality, integrity and availability of information, whereas privacy is more granular about privacy rights with respect to personal information.

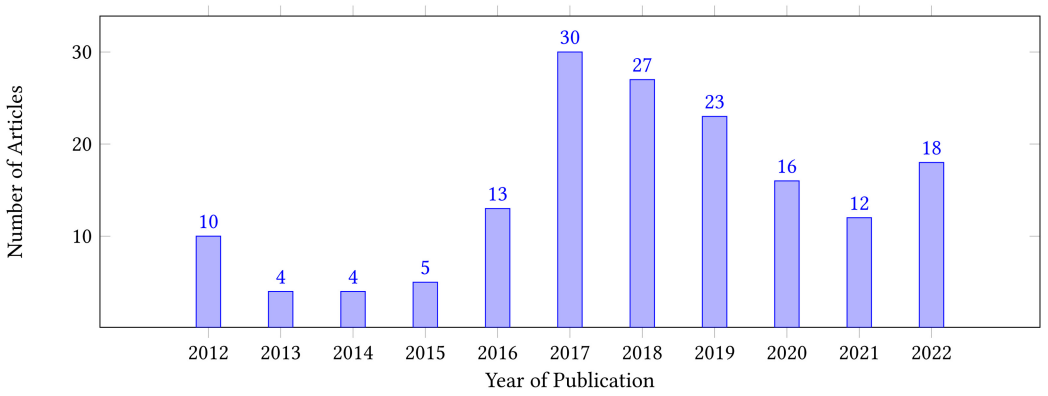

Fig. 3. Distribution of research articles from 2013 to 2022.

Privacy prevails when it comes to processing personal data, while security means protecting information assets from unauthorized access. Personal data may refer to any information concerning any individual such as names, addresses, credentials, financial accounts information, social security numbers, and the like [102].

To ensure a high degree of privacy and to protect user data in the EHR system, various criteria must be met. Privacy advocates and regulators have devised viable strategies that promote privacy protection, similar to the GDPR which is a collection of rules that gives EU citizens more control over their personal data. Under the GDPR, organizations are obligated to ensure that personal data is collected legally and under strict conditions. Furthermore, those who collect data can be held legally liable for any resulting misuse or exploitation in the event of any negligence. The Data Protection Act 2019 works similarly in the USA [21]. Healthcare data have value and are attractive to cyber criminals who wish to inflict data extortion attacks. The overall performance of healthcare systems is impaired by this unauthorized access [7, 12, 85].

Many researchers and policy acts have addressed and emphasized the privacy of patients' EHRs [9, 46, 77, 79, 114, 130, 142, 149]. The work in [149] illustrates that there is a lack of security in current EHR frameworks, a lack of privacy for patients, and an unreliable method of transmitting their health data, especially in urgent situations. Due to the high need for data privacy, the HIPAA and the HITECH have implemented many EHR safety protections in the US [78]. The GDPR guidelines have been implemented to ensure data protection and subsequent rights to EU citizens [113]. In Australia, 13 privacy principles have been implemented in relation to the use, disclosure and sharing of personal information [23, 56]. Despite having local and international privacy policies, EHR systems have encountered many data breaches which resulted in a lack of trust in using existing health record systems.

4.5 What Different Technologies are Available to Preserve the Privacy of EHRs?

A range of information (sharing) security and privacy strategies have been introduced and implemented, but the cloud, NLP, cryptography and blockchain are seen as the most effective [78, 106, 114, 143, 154]. We divided the various techniques and technologies for preserving EHR privacy into the following four categories: for our review as ABC i.e., Access Control Techniques, Blockchain Techniques, Cloud-based Techniques, Cryptography Techniques.

4.5.1 Access Control Techniques. A number of EHR services are either blockchain based, cryptography base or cloud based (Table 5). The majority of the proposed approaches do not provide an attribute-based access control and encryption mechanism. Various access control models have

Table 5. Categorization of Technologies, ABC (Access Control, Blockchain, Cloud-Based, Cryptography)

Strengths	Limitations	Included papers	References
Access control			
1. Limits access rights to unauthorized users 2. Gives patients greater control 3. Reduces adminis- trative overheads 4. Provides granularity of system privilege management	1. Reliance on manual input 2. Constant need for maintenance 3. Too many roles assigned to a person may lead to role explosion causing security holes	Papers that focus on allowing role-based access to handle various types of users who possess different access privileges. Papers that discuss a hierarchical access structure to grant access to authorized users and limit access rights to other users in the public domain, smart contracts for decentralized data sharing and providing patients with access control over their records and eliminating the need for management services provided by the record-generating parties.	[4, 14, 18, 38, 39, 63, 64, 68, 86, 119, 146, 153]
Blockchain			
1. Immutability 2. Transparency 3. Reliability 4. Interoperability 5. Data provenance	1. Block timestamp dependency 2. Re-entrancy problem 3. Unchecked and failed send 4. No restricted transfer	Papers that focus on blockchain-based strategies for healthcare, the mitigation of problems associated with the privacy and integrity of patient information, the features of blockchain, such as immutability, transparency and reliability, and other factors. Papers also include blockchain- based framework for storing EHRs, aiming to tackle problems such as response time in data access, interoperability, and better data quality.	[27, 32, 38, 41, 46, 49, 50, 71, 87, 88, 91, 97, 134, 136, 139]
Cloud-based Techniques			
1. Large scale and on-demand storage 2. Easy Data recovery 3. Syncing and updating 4. Mobility 5. Quick deployment	1. Downtime due to power failure 2. Provider login 3. Platform dependency 4. High variation in cost due to implementation of additional application	Papers that focus on techniques to ensure the integrity and traceability of medical data over a network, frameworks/models/taxonomies that that support the improvement of user security over a network.	[21, 37, 40, 78, 105, 107, 113, 126, 135, 140, 143, 149, 150]
Cryptography			
1. Authorization 2. Consistency 3. Confidentiality 4. No Data Violation 5. Encryption is on the Data	1. Key size provides a lower bound on the security of the cryptosystem 2. Hash function can be tempered by two arbitrary inputs that having same hash value. 3. Information available from physical implementation of cryptosystem can be attacked	Papers that include cryptographic techniques and meth- ods such as: privacy- preserving medical record searching scheme for intelligent diagnosis, guarantee a tight data security, securely invoke and share past medical records to make diagnosis. Papers also cover the aspect of secure searching without leaking any other information on the two parties.	[23, 45, 45, 48, 72, 75, 86, 110, 113, 121, 136, 144, 153]

been proposed namely ***Mandatory Access Control*** **(MAC)**, RBAC [33], and ABAC [17, 117]. Modeling access control policies has been a topic of interest. XACML is a policy model based on the XML specification language [1, 134] which uses attributes to impose access control [67, 84].

EHR System with role-based access control (RBAC) [114]**:** This enables various types of users to possess different access privileges. Its hierarchical access structure grants access to authorized users and limits access rights to other users in the public domain. The policy transformation approach enables EHR data to be transferred from a private cloud to a public cloud with the corresponding transformation in the access control policy.

HIPAA three tier themes with respect to administrative, physical and technical safeguards [78]**:** These three safeguards encompass a vast array of security techniques that are implemented by healthcare organizations to further secure and protect the health information contained within EHRs. It focuses on compliance with security policies and procedures to prevent physical access to protected health information through hardware and software access by unauthorized users.

ESPAC: This implements granularity authorisation for data queries, based on ABE in eHealth [8, 152, 153].

Access control scheme: This is based on elliptic curve cryptography but there is no support to control the access granularity in the proposed authorisation process [1, 152].

GAA-FQ (Granular Access Authorisation supporting Flexible Queries): This comprises an access model and an access authorisation scheme. Unlike existing blockchain schemes, this access model can authorise different levels of granularity of authorisation, whilst maintaining compatibility with the underlying blockchain data structure. Furthermore, the authorisation, encryption, and decryption algorithms proposed in the GAA-FQ scheme dispense with the need to use a ***Public Key Infrastructure*** **(PKI)** and hence improve the computation performance needed to support more granular and distributed, yet authorized EMR data queries [152].

4.5.2 Blockchain Techniques. The blockchain, initially proposed in 2008 and utilized from 2009 [61], is foundational in establishing the Bitcoin network and facilitates third-party-free transactions. Its applications span across financial services, reputation management, and the ***Internet of Things*** **(IoT)**. In healthcare, blockchain is pivotal for secure data transmission, notably in EHR privacy [23, 28], biomedical [1, 31], and e-health data sharing [33]. Features like immutability, privacy, transparency, decentralization, and distributed ledgers enhance its appeal [34, 45, 61, 151].

Various scholars suggest blockchain for enhanced accuracy, security, and privacy preservation [91, 93, 99, 102]. However, challenges include cultural shifts, multiple access nodes, and centralized system implementation [60, 105, 118].

Comparative Analysis of Blockchain Solutions:

- *MedRec* and *MediBloc* both utilize blockchain for EHR management but differ in their approach. MedRec uses a combination of blockchain for metadata storage and ***Distributed Hash Table*** **(DHT)** with ***InterPlanetary File System*** **(IPFS)** for actual data, leveraging Ethereum's smart contracts for access control [1, 42, 108]. MediBloc, however, centralizes the patient as the data flow medium, emphasizing patient-centric data usage and healthcare data sovereignty [62, 73].
- ***Decentralized Medication Management System (DMMS)*** and *Medicalchain* demonstrate the use of blockchain for prescription management and patient access control, respectively. While DMMS focuses on encrypted prescription sharing [111], Medicalchain utilizes Hyperledger Fabric for patient-controlled data access [146].
- *Blockchain-Based Data Sharing Mechanism* [39] and *Blockchain based searchable encryption* [28] highlight blockchain's role in secure data sharing and accurate search results in research networks, emphasizing cryptographic algorithms and data integrity.
- *Estonia's healthcare system* and ***Healthcare Data Gateways (HDG)*** both integrate blockchain for data integrity and security. Estonia's system uses ***Keyless Signature Infrastructure*** **(KSI)** blockchain [41, 55], whereas HDG focuses on access granularity and attribute-specific data queries [139, 152].

The consensus algorithms used in these solutions vary. For instance, Ethereum-based systems like MedRec typically employ **Proof of Work (PoW)** or transitioning to **Proof of Stake (PoS)**, while Hyperledger Fabric used in Medicalchain and OmniPHR opts for more customizable consensus mechanisms.

Incorporating these comparative aspects provides a nuanced understanding of blockchain's versatility and adaptability in healthcare, particularly in enhancing EHR privacy and security.

Taxonomy of Blockchain systems:

- Public blockchain: Open for anyone to join, like Bitcoin [46] and Ethereum [68, 85].
- Private blockchain: Requires invitation or authorization, e.g., MultiChain [91] and GemOS [86].

— Consortium blockchain: Semi-private, used by authorized organizations, exemplified by Hyperledger Fabric [93] and Ethereum for consortium blockchains.

Blockchain, while promising, has limitations like slow processing, scalability issues, privacy challenges, and high energy consumption [133]. Understanding these nuances is crucial for advancing blockchain applications in healthcare, particularly for EHR privacy.

Blockchain based strategy A Survey of Blockchain-Based Strategies for Healthcare: A blockchain-based strategy can mitigate problems arising from issues threatening the privacy and integrity of patient information, due to blockchain's immutability, transparency and reliability [34].

MedRec [108]**:** This is a blockchain-based framework for storing EHRs which aims to tackle problems such as response time in data access, interoperability, and data quality. MedRec [42] is a blockchain-based decentralized record management system to handle EHRs. The meta-data is stored on blockchain and the real data is stored on ***Distributed Hash Table*** **(DHT)** by using ***Inter Planetary File System*** **(IPFS)**. A smart contract is used for access control and there is a transaction fee [18, 32].

MedShare: A MedShare-based solution involves a system consisting of four layers: (i) User layer: the data will be accessed through a graphical interface; (ii) Data query layer: a group of structures that process and respond to query requests in the system; (iii) Database infrastructure layer: a layer composed of the system databases, to which only a few specialist institutions have access; and (iv) Data structuring and provenance layer: responsible for processing within the system; in other words, it is the layer which contains the adopted blockchain network structure, consensus protocol, node authenticator, and smart contracts. It offers features like data provenance, auditing, and greater security for systems [145].

Medicalchain: This was built with the aid of a permissioned blockchain from the Hyperledger Fabric. The application enables patients to have access controls for all their information as well as being able to handle their healthcare data in a personalized way [146].

MediBchain: A novel blockchain-based EHR automation system for healthcare. It is a patient-centric healthcare data management system which uses blockchain as storage to maintain privacy. A decentralized feature of blockchain technology is that it eliminates vulnerabilities to protect data and maintain privacy and security [13, 89].

Decentralized Medication Management System (DMMS): A novel blockchain-based EHR automation system for healthcare. A physician examines the patient and writes a prescription. The prescription is encrypted with the patient's public key, and no one can access the patient's record without their private key. The patient can view their record and at the same time, the doctor can also view the patient's record with the approval of the patient [111].

Healthcare Data Gateway app: This is a blockchain-based security & privacy system for biomedical and healthcare. Information exchange systems enable patients to own, control or share data securely without infringing privacy, offering a new way to improve healthcare systems while maintaining patient data confidentiality [139].

Blockchain-Based Data Sharing Mechanism [39]**:** This provides a secure distributed research data-sharing network and a way to specify/control the parameters of sharing and providing full accountability of access to such data.

Blockchain based searchable encryption [28]**:** This guarantees that data user can receive accurate search results without additional verification. It enables cryptographic algorithms to be built to ensure data integrity, standardized auditing, and some formalized contracts for data access.

Decentralized and Hierarchical Data Sharing using Smart Contracts [149]**:** This scheme empowers patients by giving them control over their records, allowing them to selectively share

data with users that satisfy their privacy preferences. It gives patients access control over their records and eliminates the need for management services provided by record-generating parties.

Estonia health care system and Personal Care Record Platform (MyPCR): It is related to health data with its requirements, challenges and existing techniques for data security and privacy. It use *Keyless Signature Infrastructure* (KSI) blockchain to ensure data integrity and security in its system [41, 55].

Healthcare Data Gateways (HDG): Its access granularity is based upon blocks. It cannot support data queries to specific data attributes in blocks or restrict access authorisation to these attributes [139, 152].

Ancile, Privacy-preserving framework for access control and interoperability of EHR using blockchain technology [33]**:** A blockchain-based framework for secure, interoperable, and efficient access to medical records by patients, providers, and third parties, while preserving the privacy of patients' sensitive information. This framework, Ancile, utilizes smart contracts in an Ethereum-based blockchain for heightened access control and the obfuscation of data and employs advanced cryptographic techniques for further security.

Decentralized and Hierarchical Data Sharing using Smart Contracts [149]**:** This is a decentralized blockchain technology to mitigate security issues, privacy concerns and the inefficiencies of various centralized platforms such as financial systems. It is a secure, private and efficient electronic record sharing scheme that utilizes smart contracts deployed over a blockchain.

MediBloc [73]**:** This is an open-source healthcare data platform built on blockchain that can secure and integrate diffused data from numerous organizations. It can track a person's daily movements via smartphones, fit bands, smartwatches, and so forth [136] but it has performance, scalability and energy consumption issues. Medibloc also uses meta-data however the operations are different. In MediBloc, patients are the medium of data flow and exchange and utilize their health data as needed [62]. It integrates multiple hospital records into one safe decentralized ledger to establish a medical record data base in blockchain. MediBloc uses public blockchain that allows anyone to access transactions. It minimizes personal healthcare information leakage risks and maximizes the credibility of medical records. It also provides reliable, personalized and patient-centric health information. MediBloc ensures the privacy of health information and enhances data sovereignty in the medical ecosystem [66].

OmniPHR [116]**:** This uses the concept of blockchain (linking blocks) to store data which is broken into small pieces as blocks. The system improved interoperability, storage and scalability. The data which is stored on blockchain is encrypted with a key that is generated and stored by the body sensor node. This system can only be used for body sensor networks (wearable devices), however PHRs include health data from various resources.

MedVault [133]**:** This also stores health care data on blockchain and is a privacy preserving system. It is an attribute-based authentication system that enables EHR sharing in a patient-centric manner. But their study results showed that MedVault performed well supporting all EHR subject types but not with patient and physician subjects. This is mainly due to the fact that MedVault considers EHR accessibility on only all data sets, data elements and transactions. In addition, it ignores the non-exposure of patients data [87, 117].

Blockchain-Based Deep Learning as-a-Service (BinDaaS):This is an architectural framework for the secure transmission of EHRs [88, 119]. It integrates blockchain and deep-learning techniques for sharing EHR records among multiple healthcare users.

Table 6 presents a concise comparative analysis of key blockchain-based solutions in the Electronic Health Records (EHR) domain. It highlights various approaches adopted by these solutions, categorizing them based on their distinct blockchain technologies and consensus algorithms. This table is an essential tool for readers to grasp the diverse applications of blockchain in EHR,

Table 6. Comparative Analysis of Blockchain-Based Solutions for EHR

Solution	Blockchain Technology	Consensus Algorithm
MedRec [18, 32, 42, 108]	Ethereum	Proof of Stake (PoS)
MedShare [145]	Custom Blockchain	Not Specified
Medicalchain [146]	Hyperledger Fabric	Practical Byzantine Fault Tolerance (PBFT)
MediBchain [13, 89]	Custom Blockchain	Not Specified
Decentralized Medication Management System (DMMS) [111]	Custom Blockchain	Not Specified
Healthcare Data Gateway app [139]	Ethereum	Proof of Work (PoW)
Blockchain-Based Data Sharing Mechanism [39]	Custom Blockchain	Not Specified
Decentralized and Hierarchical Data Sharing using Smart Contracts [149]	Ethereum	Smart Contracts
Estonia healthcare system and MyPCR [41, 55]	KSI Blockchain	Not Specified
Healthcare Data Gateways (HDG) [139, 152]	Custom Blockchain	Not Specified
Ancile [33]	Ethereum-based	Smart Contracts
MediBloc [62, 66, 73, 136]	Public Blockchain	Not Specified
OmniPHR [116]	Custom Blockchain	Not Specified
MedVault [87, 117, 133]	Private Blockchain	Practical Byzantine Fault Tolerance (PBFT)
Blockchain-Based Deep Learning as-a-Service (BinDaaS) [88, 119]	Custom Blockchain	Not Specified

particularly in enhancing privacy and accessibility. By detailing each solution's technical foundation, the table aids in understanding the critical factors that contribute to the security, scalability, and effectiveness of these solutions in managing EHR privacy and accessibility concerns.

4.5.3 Cloud-based Techniques. Cloud-based platforms are useful for delivering electronic health services with ubiquitous network access, scalability, and cost saving. Transferring EHRs to the cloud poses major threats to privacy, data integrity, and confidentiality, and additional techniques are required to maintain data secrecy. Cloud-based utility services (such as storage) offer additional benefits to EHR systems, for example, they are more cost-effective, can be easier to manage (for example, access and retrieval), and support collaboration, with mobile technologies and devices to gather data [118].

Cloud-based EHR system Using Attribute-Based Cryptosystem and Blockchain [141, 143]**:** Wang and Song [142] proposed a cloud-based EHR system which uses ABE and IBE to encrypt data, ensuring fine-grained access control for encrypted data using an *Identity-Based Signature* (IBS) to implement digital signatures.

Attribute Based Encryption for Secure Access to Cloud Based EHR Systems [67]**:** Through this system every patient's visit is recorded as a separate node in the knowledge graph, ensuring strict data security, which makes it easier to query and speeds up data access procedures.

4.5.4 Cryptography Techniques. To prevent unauthorized users from accessing EHRs, a direct way is to encrypt EHRs before uploading them to cloud servers [3]. To protect data privacy and to mitigate threats, various encryption models have been proposed. ABE is one such interesting approach where the ciphertext, the secret key and the private key of the user are associated with the user's attributes [39, 43, 108]. Bethencourt et al. [22] developed a system called ***Ciphertext-Policy Attribute Based Encryption*** **(CPABE)** for implementing ABE using the attributes of the user to encrypt the document [39].

Cryptographic Role-Based Access Control Model: This ensures secure access to EHR resources by enforcing crypto- graphic access control with context and location awareness. A cryptographic role-based access control model for EHR systems uses location- and biometrics-based user authentication and a steganography-based technique to embed EHR data in electrocardiography host signals [118].

My Health My Data (MHMD): This technique is for data security and privacy sharing medical information and empowering their primary owner, the patient [94–96].

Ancile: Privacy-preserving framework: Using six separate contracts, Ancile improves the efficiency of the patient experience and reduces privacy threats. The patient is the only node

expressly given the location of their information. Ancile maintains the cryptographic hashes of stored records and query links, confirming the integrity of EHR databases.

Keyword searchable encryption and proxy re-encryption technology [133, 143]**:** It protects data security with a searchability guarantee that only authorized entities can access EHRs. [143] combines keyword searchable encryption and proxy re-encryption technology to ensure privacy preservation and secure data sharing for EHRs based on consortium blockchain technology and cloud storage. The secure cryptographic technique (proxy re-encryption) is applied to support efficient access control on secret data [133]. The re-encryption of cyphertext by the cloud ensures relatively good security to the data using the technique proposed by [143]. But the keyword searchable encryption method is not clearly described from the user's point of view. This technology can be adapted to make the data on the cloud more secure and it is capable of identifying and giving access to the right user [133, 143].

Privacy-preserving medical record searching scheme (PMRSS): This is a scheme for intelligent diagnosis in IoT healthcare which securely invokes and shares past medical records to assist a diagnosis. The input used for searching must be protected as well as the result. It securely searches the diagnosis report by only two rounds of interactions without leaking any other information of the two parties.

Personally Controlled Electronic Health Record (PCEHR) System**:** It uses ***Fully Homomorphic Encryption*** **(FHE)** to encrypt the patient's data. The decryption key is held by the patient therefore no other person can access the data without the patient's authorisation. [65] uses a verification technique such as cryptography to ensure only an authorized person can access corresponding records [29, 67].

5 SURVEY FINDINGS

After examining the selected literature and answering the survey questions, we identified a few major points:

5.1 Privacy, Confidentiality and Security: The Differences

The terms privacy, confidentiality and security are used interchangeably as they refer to related concepts. But there is a need to address the inconsistent usage of such terminologies as they actually have varied definitions. Data security governs access to data throughout the data life cycle. In contrast, data privacy sets this access based on privacy policies and laws that determine, for instance, who can view personal data, financial, medical or confidential information. The three paramount concepts of security are authentication, authorization and access control [15, 47, 87, 101]. Therefore, we can say that confidentiality protects secrets, security is broader than confidentiality and privacy determines authorization. Privacy is closely related to security and confidentiality but approaches data from a different perspective. Confidentiality controls and protects against the unauthorized use of information already in the hands of an institution, whereas privacy protects the rights of an individual to control the information that the institution collects, maintains and shares with others. One way to understand the relationship between privacy and confidentiality is that privacy requirements dictate the types of authorization granted to information, and confidentiality controls ensure that people and systems meet those privacy obligations (Table 7). Hence, when it comes to the management of EHR, first and foremost, it is important to understand the difference between its security, confidentiality, and privacy. It is at one's (or one's organization's) peril to substitute one for the other among security, confidentiality, and privacy, given their distinct roles in data protection. With a rich toolset available for EHR protection, it is crucial for data protection practitioners, IP attorneys, information security specialists, and privacy professionals to precisely understand the nuances of the health records in question. Ensuring the application of

Table 7. Difference between Privacy, Confidentiality and Security

Basis for Comparison	Privacy	Confidentiality	Security
Meaning	The state of being free from intrusion or interference.	A situation where someone is not expected to divulge information to any other person.	The state of being free from danger or threat.
What is it	Right to be let alone.	Agreement between the persons standing in fiduciary to maintain the secrecy of sensitive information and documents.	The process and practice of safeguarding data throughout its entire lifecycle.
Concept	Limits the access of the public.	Prevents information and documents from unauthorized access.	Protect data from unauthorized access, corruption, theft, damage or loss by putting in place specific controls, standard policies, and procedures.
Applies to	Individual.	Information.	Organization / System.
Obligatory	No, it is the personal choice of an individual.	Yes, when the information is professional and legal.	Yes, data is a valuable asset.
Disallowed	Everyone is disallowed from being involved the personal affairs of an individual.	Only unauthorized persons are disallowed from using the information.	Every harmful activity.

the proper protection paradigm acknowledging the unique aspects of security, confidentiality, and privacy is essential for effective data governance.

5.2 EHR Privacy Concerns

This review solely focused on the privacy aspect of EHR, that is, how the stored records of patients are kept private under various circumstances and what different techniques are mentioned by the researchers for ensuring the privacy of patients' EHRs. Technologies can host several risks; hence the privacy of information in these systems is of utmost importance. Regardless of the increased effectiveness and the growing eagerness to use EHRs, not much care is being given to the privacy issues that might arise. Mobility and the use of multiple mobile devices in collaborative healthcare increases the need for robust privacy preservation. Thus, large-scale EHR systems require secure access to privacy-sensitive data, data storage, and management [114]. One of the major security concerns is the issue of the increasing size of healthcare data but none of the reviewed articles highlighted this matter. As described in [152], HIPAA does not dictate the ways in which to create and implement the systems currently being used. This leads to many variations in the centralized systems used today and has prevented interoperability between medical institutions. A big downside to these models is that evidence is not inspected in a structured manner and the regulating procedures and guidelines also differ significantly throughout territories depending on local experience and the national implementation of privacy policies [47, 66, 137]. Table 8 lists the different technologies related to privacy, confidentiality and security. Privacy preservation needs to be reviewed in light of the changing privacy rules and legislation regarding sensitive personal data. Users should own and control their data without compromising security or limiting companies' and authorities' ability to provide personalized services. Researchers [152] are in favor of blockchain, smart contracts and their implementation by Ethereum to enforce verified negotiations of contracts between two participating parties over the blockchain. Like any other transaction processed over the blockchain, they are based upon cryptographic primitives that ensure their

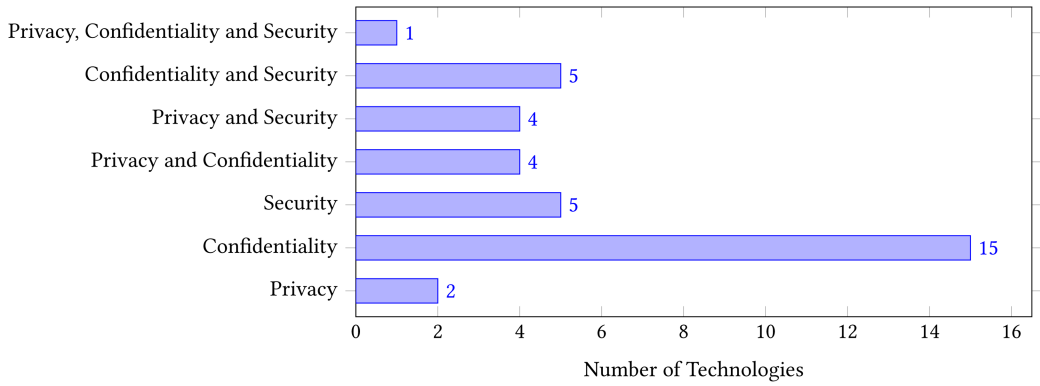

Fig. 4. Number of (reviewed) technologies covering the aspect(s), i.e., privacy, confidentiality, security.

integrity. Some researchers believe that both the cloud and blockchain can be used in combination to provide cost-efficient security solutions but organizations have realized that a one-size-fits-all approach may not work for cloud adoption in the case of public and private clouds.

Access control: Several studies proposed solutions for privacy-preserving data sharing based on ABE or CP-ABE in the cloud to encrypt data and to provide the hierarchical access structure for fine-grained data sharing. However, they did not provide policy dynamics. One of the challenges of data sharing is key management. Zhu et al. [155] identified the data security and access control issues associated with EHR sharing within the public domain owing to the heavy computation overhead in key distribution and data management, which occurs in applying fine-grained access control. They used ***Key-Policy ABE*** **(KP-ABE)**, ***Proxy Re-Encryption*** **(PRE)**, and lazy re-encryption to define and enforce access-control policies, but implementing secure and dynamic access rights is challenging [116].

Blockchain: The work in [2] proposed a blockchain-based framework for managing, maintaining, and sharing the electronic medical records of cancer patients. They adopted a permissioned blockchain technology to access, manage, and store encrypted patient data. Such proposed frameworks can be used to practically implement blockchain technology to access and manage the privacy and security of patient data and history in clinical practices. The Ancile framework discussed in [33] used smart contracts and permissioned blockchains but it is still in the early stages of development in the Ethereum community. Nonetheless, one cannot solely rely on Ancile as a remedy to the wider EHR security problem, but it can be adapted and incorporated into another technique to achieve optimum results. The work in [47, 112, 133] described various algorithms to efficiently share EHRs in blockchain-based electronic healthcare record systems for healthcare 4.0 applications with less communication time. The algorithms proposed in their article covers maximum number of collaborating parties which could be involved in EHRs. The security of the proposed system is evaluated by its performance through simulations and scenarios which is missing from other proposed approaches. But they only considered admin, patients, clinicians, and laboratory staff as participants in EHR system whereas other multiple participants, e.g., health organizations may be involved.

During the implementation of EHR, medical data sharing often faces critical limitations, such as a loss of control over data, data provenance, auditing, and secure data trailing on medical data. To address these limitations, MeDShare provides a safe and secure blockchain system for medical data exchange among untrusted parties. MeDShare can be used to share medical data and maintain EHRs among cloud service providers, hospitals, and healthcare research entities with

Table 8. Summary of Reviewed Technologies and the Aspects they Covered

Technique	Technology				Management Aspect		
	Access Control	Blockchain	Cloud-Based	Cryptography	Privacy	Confidentiality	Security
1. EHR system with role-based access control (RBAC)	✓		✓			✓	
2. HIPAA implements three safeguards: administrative, physical and technical	✓					✓	✓
3. ESPAC	✓	✓		✓		✓	✓
4. Access control scheme	✓	✓		✓		✓	
5. GAA-FQ (Granular Access Authorisation supporting Flexible Queries)	✓			✓		✓	
6. Ciphertext-policy attribute-based encryption (CP-ABE)	✓			✓		✓	
7. Blockchain based strategy		✓		✓	✓	✓	
8. MedRec	✓	✓		✓		✓	
9. MedShare		✓		✓			✓
10. Medicalchain	✓	✓			✓	✓	
11. MediBchain		✓			✓		✓
12. Decentralized Medication Management System (DMMS)		✓				✓	
13. Healthcare Data Gateway app		✓			✓	✓	✓
14. Blockchain-Based Data Sharing Mechanism		✓				✓	✓
15. Blockchain based searchable encryption	✓	✓		✓		✓	
16. Decentralized and Hierarchical Data Sharing	✓	✓				✓	
17. Estonia health care system and Personal Care Record Platform MyPCR	✓	✓			✓		✓
18. Healthcare Data Gateways (HDG)	✓	✓				✓	
19. Ancile: Privacy-preserving framework	✓	✓		✓		✓	✓
20. MediBloc		✓			✓	✓	

(Continued)

Table 8. Continued

Technique	Technology				Management Aspect		
	Access Control	Blockchain	Cloud-Based	Cryptography	Privacy	Confidentiality	Security
21. OmniPHR		✓		✓			✓
22. MedVault	✓	✓			✓		
23. Blockchain-Based Deep Learning as-a-Service (BinDaaS):		✓					✓
24. Cloud-based EHR system Using Attribute-Based Cryptosystem and Blockchain		✓	✓	✓		✓	
25. Cloud-based EHR system	✓		✓	✓			✓
26. Attribute Based Encryption for Secure Access to Cloud Based EHR Systems			✓				✓
27. Cryptographic Role-Based Access Control Model	✓		✓	✓		✓	
28. CureMD			✓				✓
29. Practice Fusion			✓			✓	
30. Athenahealth			✓			✓	
31. MyHealthMyData (MHMD)		✓		✓	✓		✓
32. Ancile: Privacy-preserving framework					✓		
33. Keyword searchable encryption and proxy re-encryption technology		✓	✓	✓		✓	✓
34. Privacy-preserving medical record searching scheme (PMRSS)				✓		✓	
35. Personally Controlled Electronic Health Record (PCEHR) System				✓		✓	

greater data provenance, personalized audit control, and minimal possible threats to data security and privacy [139].

Cloud-based: In cloud-based EHR, the dissemination of a patient's data is greatly beneficial but it must be undertaken in such a way that a patient's privacy is preserved. The model proposed in [112, 152] also follows a patient-centric approach for EHR management where the responsibility of authorizing data access is handled at the patients' end. This however creates significant overhead for the patient who has to authorize every access of their health record. This is not practical given

the multiple personnel involved in providing care and that at times, the patient may not be in a state to provide this authorization. Hence, there is a need to develop a proper authorization delegation mechanism for safe, secure and easy cloud-based EHR management. Despite the existing solutions, privacy issues are the major obstacles that are limiting the widespread adoption of public clouds across the globe. The main reason for this concern is that the information needs to be published to a broad and possibly anonymous set of receivers and it can be dangerous to outsource sensitive data the cloud so there is an increasing need to investigate data anonymization techniques applied to this domain.

Cryptography: The ciphertext data based on traditional encryption mechanisms make EHR sharing difficult to a large extent. Especially, it is very challenging for resource-limited IoT devices to perform burdensome computation tasks for fine-grained data sharing in mobile cloud computing. To fill this gap, ABE can be adopted to realize fine-grained access control on EHRs [16, 18, 29]. Along with our literature review, [82] also points out firewalls and cryptography as the most frequently discussed security techniques mentioned throughout the selected sample. A diverse set of techniques have been introduced to protect patients' privacy by applying various cryptographic and hybrid access control techniques [3, 46–48, 52, 53, 55, 58, 61, 65–67, 71, 76, 80–83, 87, 88, 91, 96, 109, 112]. However, most of these approaches have certain shortcomings making them less effective with respect to EHR privacy.

Standards' Compliance: The recent cloud-based blockchain approaches suggested by multiple researches [14, 16, 18, 37, 41, 47, 48, 76, 91, 105, 134, 136, 139, 143] focus on blockchain implementation along with some standards. But the paper contains conflicting descriptions about security standards. First, they favour GDPR subject to data rights and criticise HIPAA about medical records regulations and protecting only PHI but later they describe how some GDPR articles directly conflict with blockchain. So, it gives a confusing impression about whether or not to use GDPR with blockchain. Importantly, distributed methods for data integrity validation are not sufficient to solve all cybersecurity hazards. Despite having much potential to achieve data security for EHRs, the existing approaches require further strengthening by complying with the standards, e.g., HIPAA measures [47, 53, 120] to achieve data privacy, security and integrity while in a centralized setup.

For medical practices dealing with sensitive patient data, which are required to comply with the U.S. HIPAA rules, a private cloud may be appropriate. The research in [76] also mentions that numerous security standards have been developed, such as HIPAA, COBIT, and DISHA, which have been applied to protect patients' health information and can address privacy issues.

5.3 Discussion

When discussing EHRs, firstly, it is crucial to have a technical understanding of the actual definition and characteristics of PCS. Secondly, every technology has its merits and demerits, so depending on what is needed, the respective technology can then be adopted. No limitations have been found in the literature in relation to using a single technique to preserve the privacy of EHRs, but the advantages of combining two or more techniques can be attained to achieve the desired requirements. On the basis of this review, it can be clearly seen that no technique/solution can be considered as optimum for EHR privacy. All techniques utilize different technologies, i.e., cloud computing, Ethereum-based blockchain, cryptography and encryption techniques and/or access control techniques to ensure data privacy.

5.4 Limitations

Despite our best effort to survey as many relevant papers as possible, we present the limitations of this survey. A fundamental constraint that was identified during our survey process was a general lack of literature that discussed privacy preservation without confusing it with confidentiality and

security. As a result, there is a lack of primary articles that compare and contrast the privacy of EHR with confidentiality and security. Therefore, it was difficult to search for techniques and technologies which cover EHR privacy. We have also found it challenging to validate some studies simply based on their manuscripts. To the best of our knowledge, none of the existing studies tested their proposed method using either real samples or raw data of EHRs, which puts the external validity of these studies in question.

6 CONCLUSION AND FUTURE RESEARCH DIRECTIONS

This article has provided a comprehensive overview of EHRs and their privacy. Although EHRs are widely recognized and acknowledged for their importance, the survey revealed a lack of systematized knowledge on this topic with respect to their management. Existing surveys dealt with EHRs from more technical and technological perspectives using the three terms interchangeably, i.e., PCS and creates confusion. Instead, the survey presented in this article, through the analysis of the reviewed papers, clearly differentiates these three terminologies and gives answers to the research questions, namely (1) the currently available data sharing methods, (2) the role of privacy when sharing EHRs with different stakeholders, (3) the strengths and weaknesses of EHRs, (4) the difference between PCS, and (5) the different technologies available to preserve the privacy of EHRs. We believe that future research to safeguard EHRs should ensure all aspects of privacy, confidentiality, and security. These analyses supported the identification of future challenges that should drive research in the next few years to obtain a more systematic view of EHR management with the need to clarify concepts that specify EHR management, *that is,* PCS. This survey paves the way for a deeper understanding of the management of EHR beyond technical aspects, contributing to their management by first focusing on the requirements. An important aspect that this survey highlighted is that there is no clear definition on the terms privacy, confidentiality, and security for EHRs. This deserves special attention in establishing a common basis in the study of the differences and similarities of these three terms from the point of view of users and developers. It is worth noting that today, the use of technologies for data management with respect to privacy and security is different from the past, not only because of the growing number and variety of techniques, but also because various techniques can support each other and can be combined to maintain EHR data. Therefore, to preserve the privacy of EHRs, researchers and practitioners must consider the wise and appropriate use of terminologies (i.e., privacy, security and confidentiality) and technologies when developing and managing EHR systems, organizational processes, and everything that involves personal health data.

REFERENCES

[1] Ado Adamou Abba Ari, Olga Kengni Ngangmo, Chafiq Titouna, Ousmane Thiare, Alidou Mohamadou, and Abdelhak Mourad Gueroui. 2024. Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges. *Applied Computing and Informatics* 20, 1/2 (2024), 119–141.

[2] Aaron Adler, Michael J. Mayhew, Jeffrey Cleveland, Michael Atighetchi, and Rachel Greenstadt. 2013. Using machine learning for behavior-based access control: Scalable anomaly detection on TCP connections and HTTP requests. In *MILCOM 2013-2013 IEEE Military Communications Conference*. IEEE, 1880–1887.

[3] Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, and Yirong Xu. 2002. Hippocratic databases. In *VLDB'02: Proceedings of the 28th International Conference on Very Large Databases*. Elsevier, 143–154.

[4] Raag Agrawal and Sudhakaran Prabakaran. 2020. Big data in digital healthcare: Lessons learnt and recommendations for general practice. *Heredity* 124, 4 (2020), 525–534.

[5] M. Ahmed, E. Elaziz, and N. Mohamed. 2020. Nurse's knowledge, skills, and attitude toward electronic health records. *Journal of Nursing and Health Science* 9 (2020), 53–60.

[6] Tareq Ahram, Arman Sargolzaei, Saman Sargolzaei, Jeff Daniels, and Ben Amaba. 2017. Blockchain technology innovations. In *2017 IEEE Technology & Engineering Management Conference (TEMSCON)*. IEEE, 137–141.

[7] Jagmeet Singh Aidan, Harsh Kumar Verma, and Lalit Kumar Awasthi. 2017. Comprehensive survey on Petya ransomware attack. In *2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS)*. IEEE, 122–125.

[8] Sunday Adeola Ajagbe, A. O. Adesina, and J. B. Oladosu. 2019. Empirical evaluation of efficient asymmetric encryption algorithms for the protection of electronic medical records (EMR) on web application. *International Journal of Scientific and Engineering Research* 10, 5 (2019), 848–871.

[9] D. Akarca, P. Y. Xiu, D. Ebbitt, B. Mustafa, H. Al-Ramadhani, and A. Albeyatti. 2019. Blockchain secured electronic health records: Patient rights, privacy and cybersecurity. In *2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT)*. IEEE, 108–111.

[10] Mubeen Akhtar. 2024. Innovations in anesthesia delivery: Tailoring care to individual patient needs. *Cosmic Journal of Biology* 3, 1 (2024), 184–190.

[11] Bassim Al Bahrani, Itrat Medhi, and Itrat Mehdi. 2023. Copy-pasting in patients' electronic medical records (EMRs): Use judiciously and with caution. *Cureus* 15, 6 (2023).

[12] Abdullah Al Omar, Md Zakirul Alam Bhuiyan, Anirban Basu, Shinsaku Kiyomoto, and Mohammad Shahriar Rahman. 2019. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future Generation Computer Systems* 95 (2019), 511–521.

[13] Abdullah Al Omar, Mohammad Shahriar Rahman, Anirban Basu, and Shinsaku Kiyomoto. 2017. MediBchain: A blockchain based privacy preserving platform for healthcare data. In *Security, Privacy, and Anonymity in Computation, Communication, and Storage: SpaCCS 2017 International Workshops, Guangzhou, China, December 12-15, 2017, Proceedings 10*. Springer, 534–543.

[14] Hameed Hussain Almubarak, Mohamed Khairallah Khouja, and Ahmed Jedidi. 2022. Security and privacy recommendation of mobile app for Arabic speaking. *International Journal of Electrical & Computer Engineering (2088-8708)* 12, 5 (2022).

[15] Mahyar Amini and Negar Jahanbakhsh Javid. 2023. A multi-perspective framework established on diffusion of innovation (DOI) theory and technology, organization and environment (TOE) framework toward supply chain management system based on cloud computing technology for small and medium enterprises. *Organization and Environment (TOE) Framework Toward Supply Chain Management System Based on Cloud Computing Technology for Small and Medium Enterprises (January 2023). International Journal of Information Technology and Innovation Adoption* 11 (2023), 1217–1234.

[16] Muhammad Anshari. 2019. Redefining electronic health records (EHR) and electronic medical records (EMR) to promote patient empowerment. *IJID (International Journal on Informatics for Development)* 8, 1 (2019), 35–39.

[17] Guy Aridor, Yeon-Koo Che, and Tobias Salz. 2021. The effect of privacy regulation on the data industry: Empirical evidence from GDPR. In *Proceedings of the 22nd ACM Conference on Economics and Computation*. 93–94.

[18] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. 2016. MedRec: Using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)*. IEEE, 25–30.

[19] W. Bani Issa, I. Al Akour, A. Ibrahim, A. Almarzouqi, S. Abbas, F. Hisham, and J. Griffiths. 2020. Privacy, confidentiality, security and patient safety concerns about electronic health records. *International Nursing Review* 67, 2 (2020), 218–230.

[20] Jacqueline Lorene Bender, Alaina B. Cyr, Luk Arbuckle, and Lorraine E. Ferris. 2017. Ethics and privacy implications of using the internet and social media to recruit participants for health research: A privacy-by-design framework for online recruitment. *Journal of Medical Internet Research* 19, 4 (2017), e7029.

[21] Andrew R. Besmer, Jason Watson, and M. Shane Banks. 2020. Investigating user perceptions of mobile app privacy: An analysis of user-submitted app reviews. *International Journal of Information Security and Privacy (IJISP)* 14, 4 (2020), 74–91.

[22] John Bethencourt, Amit Sahai, and Brent Waters. 2007. Ciphertext-policy attribute-based encryption. In *2007 IEEE Symposium on Security and Privacy (SP'07)*. IEEE, 321–334.

[23] Lee A. Bygrave. 1990. The Privacy Act 1988 (Cth): A study in the protection of privacy and the protection of political power. *Federal Law Review* 19, 2 (1990), 128–153.

[24] Aisling R. Caffrey and Austin R. Horn. 2021. Considerations for protecting research participants. In *Pragmatic Randomized Clinical Trials*. Elsevier, 273–292.

[25] Roberto Cerchione, Piera Centobelli, Emanuela Riccio, Stefano Abbate, and Eugenio Oropallo. 2023. Blockchain's coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem. *Technovation* 120 (2023), 102480.

[26] Mike Chapple and David Seidl. 2021. *Cyberwarfare: Information Operations in a Connected World*. Jones & Bartlett Learning.

[27] Hsuan-Yu Chen, Zhen-Yu Wu, Tzer-Long Chen, Yao-Min Huang, and Chia-Hui Liu. 2021. Security privacy and policy for cryptographic based electronic medical information system. *Sensors* 21, 3 (2021), 713.

[28] Lanxiang Chen, Wai-Kong Lee, Chin-Chen Chang, Kim-Kwang Raymond Choo, and Nan Zhang. 2019. Blockchain based searchable encryption for electronic health record sharing. *Future Generation Computer Systems* 95 (2019), 420–429.

[29] Shekha Chenthara, Khandakar Ahmed, Hua Wang, Frank Whittaker, and Zhenxiang Chen. 2020. Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. *Plos One* 15, 12 (2020), e0243043.

[30] J. Randall Curtis, Seelwan Sathitratanacheewin, Helene Starks, Robert Y. Lee, Erin K. Kross, Lois Downey, James Sibley, William Lober, Elizabeth T. Loggers, James A. Fausto, et al. 2018. Using electronic health records for quality measurement and accountability in care of the seriously ill: Opportunities and challenges. *Journal of Palliative Medicine* 21, S2 (2018), S–52.

[31] Marek A. Cyran. 2018. Blockchain as a foundation for sharing healthcare data. *Blockchain in Healthcare Today* (2018).

[32] John D. Rummel, Margaret S. Race, and G. Horneck, the Princeton Workshop Participants. 2012. Ethical Considerations for Planetary Protection in Space Exploration: A Workshop. (2012).

[33] Gaby G. Dagher, Jordan Mohler, Matea Milojkovic, and Praneeth Babu Marella. 2018. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society* 39 (2018), 283–297.

[34] Erikson Júlio De Aguiar, Bruno S. Faiçal, Bhaskar Krishnamachari, and Jó Ueyama. 2020. A survey of blockchain-based strategies for healthcare. *ACM Computing Surveys (CSUR)* 53, 2 (2020), 1–27.

[35] Jacqueline A. De Leeuw, Hetty Woltjer, and Rudolf B. Kool. 2020. Identification of factors influencing the adoption of health information technology by nurses who are digitally lagging: In-depth interview study. *Journal of Medical Internet Research* 22, 8 (2020), e15630.

[36] B. D. Deebak and Fadi Al-Turjman. 2023. Secure-user sign-in authentication for IoT-based eHealth systems. *Complex & Intelligent Systems* 9, 3 (2023), 2629–2649.

[37] Nilüfer Demirsoy and Nurdan Kirimlioglu. 2016. Protection of privacy and confidentiality as a patient right: Physicians' and nurses' viewpoints. *Biomedical Research* 27, 4 (2016), 1437–1448.

[38] Michelle Finneran Dennedy, Jonathan Fox, and Thomas R. Finneran. 2014. Data and privacy governance concepts. In *The Privacy Engineer's Manifesto*. Springer, 51–72.

[39] Alevtina Dubovitskaya, Zhigang Xu, Samuel Ryu, Michael Schumacher, and Fusheng Wang. 2017. Secure and trustable electronic medical records sharing using blockchain. In *AMIA Annual Symposium Proceedings*, Vol. 2017. American Medical Informatics Association, 650.

[40] Sasidhar Duggineni. 2023. Impact of controls on data integrity and information systems. *Science and Technology* 13, 2 (2023), 29–35.

[41] e estonia. 2019. (2019). https://e-estonia.com/solutions/healthcare/ (Accessed 4 July 2019).

[42] Ariel Ekblaw, Asaph Azaria, John D. Halamka, and Andrew Lippman. 2016. A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data. In *Proceedings of IEEE Open & Big Data Conference*, Vol. 13. 13.

[43] Perihan Elif Ekmekci and Berna Arda. 2017. Interculturalism and informed consent: Respecting cultural differences without breaching human rights. *Cultura* 14, 2 (2017), 159–172.

[44] Guy Fagherazzi, Catherine Goetzinger, Mohammed Ally Rashid, Gloria A. Aguayo, and Laetitia Huiart. 2020. Digital health strategies to fight COVID-19 worldwide: Challenges, recommendations, and a call for papers. *Journal of Medical Internet Research* 22, 6 (2020), e19284.

[45] Mahdi Fahmideh, John Grundy, Aakash Ahmad, Jun Shen, Jun Yan, Davoud Mougouei, Peng Wang, Aditya Ghose, Anuradha Gunawardana, Uwe Aickelin, and others. 2022. Engineering blockchain based software systems: Foundations, survey, and future directions. *Comput. Surveys* (2022).

[46] Maryam Farhadi, Hisham Haddad, and Hossain Shahriar. 2018. Static analysis of HIPPA security requirements in electronic health record applications. In *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, Vol. 2. IEEE, 474–479.

[47] Orna Fennelly, Dearbhla Moroney, Michelle Doyle, Jessica Eustace-Cook, and Mary Hughes. 2024. Key interoperability factors for patient portals and electronic health records: A scoping review. *International Journal of Medical Informatics* (2024), 105335.

[48] José Luis Fernández-Alemán, Inmaculada Carrión Señor, Pedro Ángel Oliver Lozoya, and Ambrosio Toval. 2013. Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics* 46, 3 (2013), 541–562.

[49] Enrico M. Ferrazzi, Luigi Frigerio, Irene Cetin, Patrizia Vergani, Arsenio Spinillo, Federico Prefumo, Edda Pellegrini, and Gianluigi Gargantini. 2020. COVID-19 obstetrics task force, Lombardy, Italy: Executive management summary and short report of outcome. *International Journal of Gynecology & Obstetrics* 149, 3 (2020), 377–378.

[50] Craig Fink. 2012. Privacy and confidentiality in the virtual classroom: Instructor perceptions, knowledge, and strategies. MPA thesis, University of Victoria, June 26, 2012. Prepared for Distance Education Services, University of Victoria.
[51] Yong-Feng Ge, Elisa Bertino, Hua Wang, Jinli Cao, and Yanchun Zhang. 2023. Distributed cooperative coevolution of data publishing privacy and transparency. *ACM Transactions on Knowledge Discovery from Data* 18, 1 (2023), 1–23.
[52] Eugenijus Gefenas, J. Lekstutiene, V. Lukaseviciene, M. Hartlev, M. Mourby, and K. Ó Cathaoir. 2022. Controversies between regulations of research ethics and protection of personal data: Informed consent at a cross-road. *Medicine, Health Care and Philosophy* 25, 1 (2022), 23–30.
[53] Tasha Glenn and Scott Monteith. 2014. Privacy in the digital world: Medical and health data outside of HIPAA protections. *Current Psychiatry Reports* 16, 11 (2014), 1–11.
[54] Thore Graepel, Kristin Lauter, and Michael Naehrig. 2012. ML confidential: Machine learning on encrypted data. In *International Conference on Information Security and Cryptology*. Springer, 1–21.
[55] Guardtime. 2018.. https://guardtime.com/blog/world-s-first-blockchain-supported-personal-care-record-platform-launched-by-guardtime-and-partners (Accessed 4 July 2019).
[56] Jian Guo and Ron Steinfeld. 2024. *Advances in Cryptology–ASIACRYPT 2023: 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4–8, 2023, Proceedings, Part I*. Vol. 14438. Springer Nature.
[57] Amanda M. Gutierrez, Jacob D. Hofstetter, Emma L. Dishner, Elizabeth Chiao, Dilreet Rai, and Amy L. McGuire. 2020. A right to privacy and confidentiality: Ethical medical care for patients in United States immigration detention. *Journal of Law, Medicine & Ethics* 48, 1 (2020), 161–168.
[58] John D. Halamka, Andrew Lippman, and Ariel Ekblaw. 2017. The potential for blockchain to transform electronic health records. *Harvard Business Review* 3, 3 (2017), 2–5.
[59] Jalal Halwani and Doris Mouawad. 2021. Implementation of e-health innovative technologies in North Lebanon hospitals. *Eastern Mediterranean Health Journal* 27, 9 (2021), 892–898.
[60] Nancy D. Harada, Laural Traylor, Kathryn Wirtz Rugen, Judith L. Bowen, C. Scott Smith, Bradford Felker, Deborah Ludke, Ivy Tonnu-Mihara, Joshua L. Ruberg, Jayson Adler, and others. 2023. Interprofessional transformation of clinical education: The first six years of the Veterans Affairs Centers of Excellence in primary care education. *Journal of Interprofessional Care* 37, Sup1 (2023), S86–S94.
[61] Omar Hasan, Lionel Brunie, and Elisa Bertino. 2022. Privacy-preserving reputation systems based on blockchain and other cryptographic building blocks: A survey. *ACM Computing Surveys (CSUR)* 55, 2 (2022), 1–37.
[62] Bahar Houtan, Abdelhakim Senhaji Hafid, and Dimitrios Makrakis. 2020. A survey on blockchain-based self-sovereign patient identity in healthcare. *IEEE Access* 8 (2020), 90478–90494.
[63] Jingwei Huang, David M. Nicol, Rakesh Bobba, and Jun Ho Huh. 2012. A framework integrating attribute-based policies into role-based access control. In *Proceedings of the 17th ACM symposium on Access Control Models and Technologies*. 187–196.
[64] Rachel Hulkower, Matthew Penn, and Cason Schmit. 2020. Privacy and confidentiality of public health information. *Public Health Informatics and Information Systems* (2020), 147–166.
[65] Mohammad Shahid Husain, Muhamad Hariz Bin Muhamad Adnan, Mohammad Zunnun Khan, Saurabh Shukla, and Fahad U. Khan. 2021. *Pervasive Healthcare: A Compendium of Critical Factors for Success*. Springer.
[66] Hyowon Im, Ki-Hyung Kim, and Jai-Hoon Kim. 2020. Privacy and ledger size analysis for healthcare blockchain. In *2020 International Conference on Information Networking (ICOIN)*. IEEE, 825–829.
[67] Maithilee Joshi, Karuna Joshi, and Tim Finin. 2018. Attribute based encryption for secure access to cloud based EHR systems. In *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*. IEEE, 932–935.
[68] Tehsin Kanwal, Adeel Anjum, and Abid Khan. 2021. Privacy preservation in e-health cloud: Taxonomy, privacy requirements, feasibility analysis, and opportunities. *Cluster Computing* 24, 1 (2021), 293–317.
[69] Suchitra Kataria and Vinod Ravindran. 2020. Electronic health records: A critical appraisal of strengths and limitations. *Journal of the Royal College of Physicians of Edinburgh* 50, 3 (2020), 262–268.
[70] Gurleen Kaur and David D. Berg. 2024. The changing epidemiology of the cardiac intensive care unit. *Critical Care Clinics* 40, 1 (2024), 1–13.
[71] Grant Kelly, Bruce McKenzie, and others. 2002. Security, privacy, and confidentiality issues on the Internet. *Journal of Medical Internet Research* 4, 2 (2002), e861.
[72] Ismail Keshta and Ammar Odeh. 2021. Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal* 22, 2 (2021), 177–183.
[73] Ji Yeon Kim. 2018. A comparative study of block chain: Bitcoin· Namecoin· MediBloc. *Journal of Science and Technology Studies* 18, 3 (2018), 217–255.
[74] Barbara Kitchenham. 2004. Procedures for performing systematic reviews. *Keele, UK, Keele University* 33, 2004 (2004), 1–26.

[75] Johannes Knitza, Rachel Knevel, Karim Raza, Tor Bruce, Ekaterina Eimer, Isabel Gehring, Linda Mathsson-Alm, Maryam Poorafshar, Axel J. Hueber, Georg Schett, and others. 2020. Toward earlier diagnosis using combined eHealth tools in rheumatology: The joint pain assessment scoring tool (JPAST) project. *JMIR mHealth and uHealth* 8, 5 (2020), e17507.

[76] Sreelakshmi Krishnamoorthy, Amit Dua, and Shashank Gupta. 2023. Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: A survey, current challenges and future directions. *Journal of Ambient Intelligence and Humanized Computing* 14, 1 (2023), 361–407.

[77] Clemens Scott Kruse, Benjamin Frederick, Taylor Jacobson, and D. Kyle Monticone. 2017. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care* 25, 1 (2017), 1–10.

[78] Clemens Scott Kruse, Brenna Smith, Hannah Vanderlinden, and Alexandra Nealand. 2017. Security techniques for the electronic health records. *Journal of Medical Systems* 41, 8 (2017), 1–9.

[79] Nir Kshetri. 2017. Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy* 41, 10 (2017), 1027–1038.

[80] Adrienne C. Lahti, Dai Wang, Huiling Pei, Susan Baker, and Vaibhav A. Narayan. 2021. Clinical utility of wearable sensors and patient-reported surveys in patients with schizophrenia: Noninterventional, observational study. *JMIR Mental Health* 8, 8 (2021), e26234.

[81] Jinhyung Lee, Hyeyeong Kim, and Sung J. Choi. 2024. Do hospital data breaches affect health information technology investment? *Digital Health* 10 (2024), 20552076231224164.

[82] Gabriela Kato Lettieri, Aline Hung Tai, Aline Rodrigues Hütter, André Luiz Torres Raszl, Mariana Moura, and Raquel Barbosa Cintra. 2022. Medical confidentiality in the digital era: An analysis of physician-patient relations. *Revista Bioetica* 29 (2022), 814–824.

[83] Tian Li, Huaqun Wang, Debiao He, and Jia Yu. 2022. Blockchain-based privacy-preserving and rewarding private data sharing for IoT. *IEEE Internet of Things Journal* (2022).

[84] Qinyong Lin, Xiaorong Li, Ken Cai, Mohan Prakash, and D. Paulraj. 2024. Secure internet of medical things (IoMT) based on ECMQV-MAC authentication protocol and EKMC-SCP blockchain networking. *Information Sciences* 654 (2024), 119783.

[85] Yongsen Ma, Gang Zhou, and Shuangquan Wang. 2019. WiFi sensing with channel state information: A survey. *ACM Computing Surveys (CSUR)* 52, 3 (2019), 1–36.

[86] Imran Makhdoom, Mehran Abolhasan, Haider Abbas, and Wei Ni. 2019. Blockchain's adoption in IoT: The challenges, and a way forward. *Journal of Network and Computer Applications* 125 (2019), 251–279.

[87] Daisuke Mashima. 2012. *Safeguarding Health Data with Enhanced Accountability and Patient Awareness*. Georgia Institute of Technology.

[88] Isma Masood, Ali Daud, Yongli Wang, Ameen Banjar, and Riad Alharbey. 2024. A blockchain-based system for patient data privacy and security. *Multimedia Tools and Applications* (2024), 1–25.

[89] Isma Masood, Yongli Wang, Ali Daud, Naif Radi Aljohani, and Hassan Dawood. 2018. Towards smart healthcare: Patient data privacy and security in sensor-cloud infrastructure. *Wireless Communications and Mobile Computing* 2018 (2018).

[90] André Henrique Mayer, Cristiano André da Costa, and Rodrigo da Rosa Righi. 2020. Electronic health records in a Blockchain: A systematic review. *Health Informatics Journal* 26, 2 (2020), 1273–1288.

[91] Timothy McIntosh, A. S. M. Kayes, Yi-Ping Phoebe Chen, Alex Ng, and Paul Watters. 2021. Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions. *ACM Computing Surveys (CSUR)* 54, 9 (2021), 1–36.

[92] Lin-Chieh Meng, Shih-Tsung Huang, Ho-Min Chen, Ardeshir Z. Hashmi, Fei-Yuan Hsiao, and Liang-Kung Chen. 2023. Health care utilization and potentially preventable adverse outcomes of high-need, high-cost middle-aged and older adults: Needs for integrated care models with life-course approach. *Archives of Gerontology and Geriatrics* 109 (2023), 104956.

[93] R. C. Mesquita and I. de Edwards. 2020. Systematic literature review of my health record system. *Asia-Pac. J. Health Manag.* 15 (2020), 14–25.

[94] Data team M. H. M. 2019. (2019). http://www.myhealthmydata.eu/ (Accessed 1 July 2019).

[95] MHMD. 2017. Initial List of Main Requirements, Deliverable 1.1. (2017). http://www.myhealthmydata.eu/wp-content/themes/Parallax-One/deliverables/D1.1_InitialList-of-Main-Requirements.pdf

[96] MHMD. 2018. Shaping our Future, Newsletter 01. (2018). www.myhealthmydata.eu/wp-content/uploads/2017/10/MHMD_newsletter_01_DEF_WEB_pag_doppie_110718.pdf (Accessed 1 July 2019).

[97] Kaelan A.M. Moat, Mikayla Wicks, and Michael G. Wilson. 2016. Citizen Brief: Integrating data across sectors for public service improvement in ontario. Hamilton, Canada: McMaster Health Forum, 5 March 2016.

[98] Mohammad Mohammadi, Bagher Larijani, Seyed Hassan Emami Razavi, Akbar Fotouhi, Ahmad Ghaderi, Seyed Javad Madani, and Mohammad Naser Shafiee. 2018. Do patients know that physicians should be confidential? Study on patients' awareness of privacy and confidentiality. *Journal of Medical Ethics and History of Medicine* 11 (2018).

[99] Anastassia Negrouk, Denis Horgan, Alessandra Gorini, Ilaria Cutica, Lada Leyens, Sebastian Schee genannt Halfmann, and Gabriella Pravettoni. 2015. Clinical trials, data protection and patient empowerment in the era of the new EU regulations. *Public Health Genomics* 18, 6 (2015), 386–395.

[100] Raza Nowrozy and Khandakar Ahmed. 2023. Enhancing health information systems security: An ontology model approach. In *International Conference on Health Information Science*. Springer, 91–100.

[101] Raza Nowrozy, Khandakar Ahmed, Hua Wang, and Timothy Mcintosh. 2023. Towards a universal privacy model for electronic health record systems: An ontology and machine learning approach. In *Informatics*, Vol. 10. MDPI, 60.

[102] Phillip Olla, Joseph Tan, Lauren Elliott, and Mustafa Abumeeiz. 2022. Security and privacy issues. *Digital Health Care: Perspectives, Applications, and Cases* (2022), 105.

[103] Md. Mehedi Hassan Onik, Satyabrata Aich, Jinhong Yang, Chul-Soo Kim, and Hee-Cheol Kim. 2019. Blockchain in healthcare: Challenges and solutions. In *Big Data Analytics for Intelligent Healthcare Management*. Elsevier, 197–226.

[104] J. Marc Overhage and David McCallie Jr. 2020. Physician time spent using the electronic health record during outpatient encounters: A descriptive study. *Annals of Internal Medicine* 172, 3 (2020), 169–174.

[105] Sandeep Kumar Panda, Ajay Kumar Jena, Santosh Kumar Swain, and Suresh Chandra Satapathy. 2021. *Blockchain Technology: Applications and Challenges*. Springer.

[106] Dharmaraj R. Patil and Tareek M. Pattewar. 2022. Majority voting and feature selection based network intrusion detection system. *EAI Endorsed Transactions on Scalable Information Systems* 9, 6 (2022), e6–e6.

[107] David Peloquin, Michael DiMaio, Barbara Bierer, and Mark Barnes. 2020. Disruptive and avoidable: GDPR challenges to secondary research uses of data. *European Journal of Human Genetics* 28, 6 (2020), 697–705.

[108] Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Brent Waters. 2006. Secure attribute-based systems. In *Proceedings of the 13th ACM Conference on Computer and Communications Security*. 99–112.

[109] Argyro Pountoukidou, Maria Potamiti-Komi, Vrisiis Sarri, Michail Papapanou, Eleni Routsi, Anna Maria Tsiatsiani, Nikolaos Vlahos, and Charalampos Siristatidis. 2021. Management and prevention of COVID-19 in pregnancy and pandemic obstetric care: A review of current practices. In *Healthcare*, Vol. 9. MDPI, 467.

[110] Sarah Qahtan, Khaironi Yatim, Hazura Zulzalil, Mohd Hafeez Osman, A. A. Zaidan, and H. A. Alsattar. 2023. Review of healthcare industry 4.0 application-based blockchain in terms of security and privacy development attributes: Comprehensive taxonomy, open issues and challenges and recommended solution. *Journal of Network and Computer Applications* 209 (2023), 103529.

[111] Bipin Kumar Rai. 2023. PcBEHR: Patient-controlled blockchain enabled electronic health records for healthcare 4.0. *Health Services and Outcomes Research Methodology* 23, 1 (2023), 80–102.

[112] Swamynathan Ramakrishnan, S. Jijitha, and T. Amudha. 2024. Roadmap of AI and IoMT in smart healthcare: Current applications and future perspectives. *Internet of Medical Things in Smart Healthcare* (2024), 137–161.

[113] Protection Regulation. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council. *Regulation (EU)* 679 (2016), 2016.

[114] Fatemeh Rezaeibagha, Yi Mu, Willy Susilo, and Khin Than Win. 2016. Multi-authority security framework for scalable EHR systems. *International Journal of Medical Engineering and Informatics* 8, 4 (2016), 390–408.

[115] Fatemeh Rezaeibagha, Khin Than Win, and Willy Susilo. 2015. A systematic literature review on security and privacy of electronic health record systems: Technical perspectives. *Health Information Management Journal* 44, 3 (2015), 23–38.

[116] Alex Roehrs, Cristiano André da Costa, Rodrigo da Rosa Righi, Sandro José Rigo, and Matheus Henrique Wichman. 2018. Toward a model for personal health record interoperability. *IEEE Journal of Biomedical and Health Informatics* 23, 2 (2018), 867–873.

[117] Naiyana Sahavechaphan, U. Suriya, Nattapon Harnsamut, Jessada Phengsuwan, Kamron Aroonrua, and others. 2012. An efficient technique for aspect-based EHR access policy administration on ABAC. In *2011 Ninth International Conference on ICT and Knowledge Engineering*. IEEE, 27–33.

[118] K. Selvakumar and S. Lokesh. 2024. A cryptographic method to have a secure communication of health care digital data into the cloud. *Automatika* 65, 1 (2024), 373–386.

[119] Muhammad Shafay, Raja Wasim Ahmad, Khaled Salah, Ibrar Yaqoob, Raja Jayaraman, and Mohammed Omar. 2023. Blockchain for deep learning: Review and open challenges. *Cluster Computing* 26, 1 (2023), 197–221.

[120] Leila Shahmoradi, Alireza Darrudi, Goli Arji, and Ahmadreza Farzaneh Nejad. 2017. Electronic health record implementation: A SWOT analysis. *Acta Medica Iranica* (2017), 642–649.

[121] Xinghua Shi and Xintao Wu. 2017. An overview of human genetic privacy. *Annals of the New York Academy of Sciences* 1387, 1 (2017), 61–72.

[122] Alexis Shore, Anisha Reddy, and Carrie Klein. 2022. A student-centered privacy model for responsible technology use. *Higher Education Implications for Teaching and Learning During COVID-19* (2022), 81.

[123] Asad Ali Siyal, Aisha Zahid Junejo, Muhammad Zawish, Kainat Ahmed, Aiman Khalil, and Georgia Soursou. 2019. Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. *Cryptography* 3, 1 (2019), 3.

[124] Daniel J. Solove and Woodrow Hartzog. 2022. Unifying privacy and data security. In *Breached! Why Data Security Law Fails and How to Improve It*. New York: Oxford University Press.
[125] Julio Souza, Diana Pimenta, Ismael Caballero, and Alberto Freitas. 2020. Measuring data credibility and medical coding: A case study using a nationwide Portuguese inpatient database. *Software Quality Journal* 28, 3 (2020), 1043–1061.
[126] Mesala M. Sravani and S. Ananiah Durai. 2021. Attacks on cryptosystems implemented via VLSI: A review. *Journal of Information Security and Applications* 60 (2021), 102861.
[127] Vivek Subbiah. 2023. The next generation of evidence-based medicine. *Nature Medicine* 29, 1 (2023), 49–58.
[128] Chang Sun, Lianne Ippel, Johan Van Soest, Birgit Wouters, Alexander Malic, Onaopepo Adekunle, Bob van den Berg, Ole Mussmann, Annemarie Koster, Carla van der Kallen, and others. 2019. A privacy-preserving infrastructure for analyzing personal health data in a vertically partitioned scenario. *MedInfo* 264 (2019), 373–377.
[129] Joshua D. Symons, Hutan Ashrafian, Rachel Dunscombe, and Ara Darzi. 2019. From EHR to PHR: Let's get the record straight. *BMJ Open* 9, 9 (2019), e029582.
[130] Sudeep Tanwar, Karan Parekh, and Richard Evans. 2020. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications* 50 (2020), 102407.
[131] Gurvirender P. S. Tejay and Zareef A. Mohammed. 2023. Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. *Information & Management* 60, 3 (2023), 103751.
[132] Joan M. Teno, Rebecca Anhang Price, and Lena K. Makaroun. 2017. Challenges of measuring quality of community-based programs for seriously ill individuals and their families. *Health Aff. (Millwood)* 36, 7 (2017), 1227–1233. https://doi.org/10.1377/hlthaff.2017.0161
[133] Thein Than Thwin and Sangsuree Vasupongayya. 2018. Blockchain based secret-data sharing model for personal health record system. In *2018 5th International Conference on Advanced Informatics: Concept Theory and Applications (ICAICTA)*. IEEE, 196–201.
[134] Zhouyu Tian, Lening Qiu, and Litao Wang. 2024. Drivers and influencers of blockchain and cloud-based business sustainability accounting in China: Enhancing practices and promoting adoption. *Plos One* 19, 1 (2024), e0295802.
[135] Mueen Uddin. 2021. Blockchain medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry. *International Journal of Pharmaceutics* 597 (2021), 120235.
[136] Shubhangi V. Urkude, Himanshu Sharma, Seethamsetty Uday Kumar, and Vijaykumar R. Urkude. 2021. Anatomy of blockchain implementation in healthcare. In *Blockchain Technology: Applications and Challenges*. Springer, 51–76.
[137] N. Venkateswaran and S. Prabaharan Prabaharan. 2022. An efficient neuro deep learning intrusion detection system for mobile adhoc networks. *EAI Endorsed Transactions on Scalable Information Systems* 9, 6 (2022), e7–e7.
[138] Garima Verma. 2024. Blockchain-based privacy preservation framework for healthcare data in cloud environment. *Journal of Experimental & Theoretical Artificial Intelligence* 36, 1 (2024), 147–160.
[139] Edgar R. Dulce Villarreal, Jose García-Alonso, Enrique Moguel, and Julio Ariel Hurtado Alegría. 2023. Blockchain for healthcare management systems: A survey on interoperability and security. *IEEE Access* 11 (2023), 5629–5652.
[140] Pasupathy Vimalachandran, Yanchun Zhang, Jinli Cao, Lili Sun, and Jianming Yong. 2018. Preserving data privacy and security in Australian my health record system: A quality health care implication. In *International Conference on Web Information Systems Engineering*. Springer, 111–120.
[141] Louisa Walsh, Sophie Hill, Meredith Allan, Susan Balandin, Andrew Georgiou, Isabel Higgins, Ben Kraal, Shaun McCarthy, and Bronwyn Hemsley. 2018. A content analysis of the consumer-facing online information about My Health Record: Implications for increasing knowledge and awareness to facilitate uptake and use. *Health Information Management Journal* 47, 3 (2018), 106–115.
[142] Hao Wang and Yujiao Song. 2018. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. *Journal of Medical Systems* 42, 8 (2018), 1–9.
[143] Yong Wang, Aiqing Zhang, Peiyun Zhang, and Huaqun Wang. 2019. Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain. *IEEE Access* 7 (2019), 136704–136719.
[144] Vinden Wylde, Nisha Rawindaran, John Lawrence, Rushil Balasubramanian, Edmond Prakash, Ambikesh Jayal, Imtiaz Khan, Chaminda Hewage, and Jon Platts. 2022. Cybersecurity, data privacy and blockchain: A review. *SN Computer Science* 3, 2 (2022), 1–12.
[145] Qi Xia, Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang Du, and Mohsen Guizani. 2017. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access* 5 (2017), 14757–14767.
[146] Ashok Kumar Yadav, Karan Singh, Ali H. Amin, Laila Almutairi, Theyab R. Alsenani, and Ali Ahmadian. 2023. A comparative study on consensus mechanism with security threats and future scopes: Blockchain. *Computer Communications* 201 (2023), 102–115.
[147] Xu Yang, Xuechao Yang, Junwei Luo, Xun Yi, Ibrahim Kahlil, Shangqi Lai, Wei Wu, and Albert Y. Zomaya. 2023. Towards sustainable trust: A practical SGX aided anonymous reputation system. *IEEE Transactions on Sustainable Computing* (2023).

[148] Jiao Yin, MingJian Tang, Jinli Cao, Mingshan You, Hua Wang, and Mamoun Alazab. 2022. Knowledge-driven cybersecurity intelligence: Software vulnerability coexploitation behavior discovery. *IEEE Transactions on Industrial Informatics* 19, 4 (2022), 5593–5601.

[149] Ehab Zaghloul, Tongtong Li, and Jian Ren. 2019. Security and privacy of electronic health records: Decentralized and hierarchical data sharing using smart contracts. In *2019 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 375–379.

[150] Li Zhang, Jianbo Xu, Pandi Vijayakumar, Pradip Kumar Sharma, and Uttam Ghosh. 2022. Homomorphic encryption-based privacy-preserving federated learning in IoT-enabled healthcare system. *IEEE Transactions on Network Science and Engineering* (2022).

[151] Rui Zhang, Rui Xue, and Ling Liu. 2019. Security and privacy on blockchain. *ACM Computing Surveys (CSUR)* 52, 3 (2019), 1–34.

[152] Xiaoshuai Zhang and Stefan Poslad. 2018. Blockchain support for flexible queries with granular access control to electronic medical records (EMR). In *2018 IEEE International Conference on Communications (ICC)*. IEEE, 1–6.

[153] Jun Zhao, Kai Zhang, Junqing Gong, and Haifeng Qian. 2024. Lavida: Large-universe, verifiable and dynamic fine-grained access control for e-health cloud. *IEEE Transactions on Information Forensics and Security* (2024).

[154] Yifeng Zheng, Menglun Zhou, Songlei Wang, Hejiao Huang, Xiaohua Jia, Xun Yi, and Cong Wang. 2023. SecDR: Enabling secure, efficient, and accurate data recovery for mobile crowdsensing. *IEEE Transactions on Dependable and Secure Computing* (2023).

[155] Fei Zhu, Xun Yi, Alsharif Abuadbba, Ibrahim Khalil, Xinyi Huang, and Feihong Xu. 2023. A security-enhanced certificateless conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems* (2023).

Received 28 March 2023; revised 18 January 2024; accepted 7 March 2024