Journal of Computer Science

Research Paper

Safeguarding Electronic Health Records: A Review of Privacy and Security in EHR Workflows

Gayathri Hegde M., P. Deepa Shenoy, Venugopal K. R.

Department of Computer Science & Engineering, University Visvesvaraya College of Engineering, Bengaluru, India

Article history
Received:
Revised:
Accepted:

*Corresponding Author:
Gayathri Hegde M,
Department of Computer Science & Engineering, University Visvesvaraya College of Engineering, India
Email: gaya3kamath@gmail.com

Abstract: Electronic Health Records (EHRs) have revolutionized the healthcare industry by improving the accessibility to patient data, optimizing workflows and refining clinical decision making. The increasing use of digital records raises serious privacy and security concerns, particularly about healthcare data storage and management, access and retrieval, and sharing and interoperability. This survey paper comprehensively reviews existing privacy-preserving and security-enhancing approaches across the key stages of the EHR workflow. This review explored several cryptographic methods, access control models, blockchain-based designs, and interoperability standards that aim to protect patient data while ensuring the seamless exchange of EHR data. Furthermore, we examine the limitations of the current approaches, encompassing scaling issues, computation overhead, and regulatory compliance challenges. Finally, the paper pinpoints the recent accomplishments and emerging trends to identify potential future directions for improving privacy and security in EHR systems, encompassing AI-driven threat detection, Zero-Trust architectures and decentralized identity management. This review is a significant resource for researchers, regulatory bodies and healthcare professionals aiming to create more secure and privacy oriented EHR solutions.

Keywords: Access Control Methods, Blockchain, Cloud-based Storage, Electronic Health Records, Interoperability Standards, InterPlanetary File System, Multi-Factor Authentication, Privacy, Security

Introduction

Due to the digitization of EHR, the healthcare industry has evolved tremendously over generations from Healthcare 1.0 to Healthcare 5.0, with notably significant developments in recent decades. Each stage of this evolution builds on the preceding one to provide a more personalized, efficient, and technologically unified healthcare system. Fig. 1 shows the evolution and characteristics of the technology from Healthcare 1.0 to 5.0. This timeline exemplifies the rapid technological advancements transforming modern healthcare from manual and industrialized systems to digital, intelligent and highly personalized healthcare solutions.

Traditional paper-based healthcare records in Healthcare 1.0 are cumbersome to share. Therefore, a new method collects and stores health-related data electronically during the transition from paper-based to digital health records in Healthcare 2.0. The EHRs, which were created solely to be applied within healthcare facilities dedicated to storing and retrieving patients' information, failed in terms of interoperability. This hindered the sharing of data across institutions. Healthcare 3.0 overcame the interoperability issue with standards Health Level (HL7) and Fast Health Interoperability Resources (FHIR), which enabled data sharing across institutions. The real-time integration of EHR with IOT devices, wearables, and telemedicine platforms is evidenced in Healthcare 4.0, which helps with continuous monitoring and predictive care. Cloud-based storage, remote access and scalability enhanced collaboration. In Healthcare 5.0, EHRs are highly personalized, leveraging technologies like Artificial

Intelligence (AI), Machine Learning (ML), Blockchain, Federated Learning and Big Data for Precision Medicine. Table 1 lists the different features of EHRs that have evolved during Healthcare 1.0 to Healthcare 5.0.

Benefits of Implementing EHR

EHRs bring a number of advantages to current healthcare as they enhance accuracy, efficiency and patient outcomes. They provide instant access to patients' medical histories, enhancing early disease detection and diagnosis and ensuring decision-making based on medical history and allergies. EHRs support ongoing shared care by providing reminders for immunizations and visits, minimizing waiting times, eliminating duplicate testing, and saving patient costs. In addition, de-identified EHR information can be provided to public health research to identify and control epidemic diseases. EHRs bolster the responsibility of healthcare professionals by limiting errors and rationalizing the workflow. Besides, EHRs advance health insurance makes policy design, risk assessment and fastening claim payments easier. This results in an effective and dependable healthcare system.

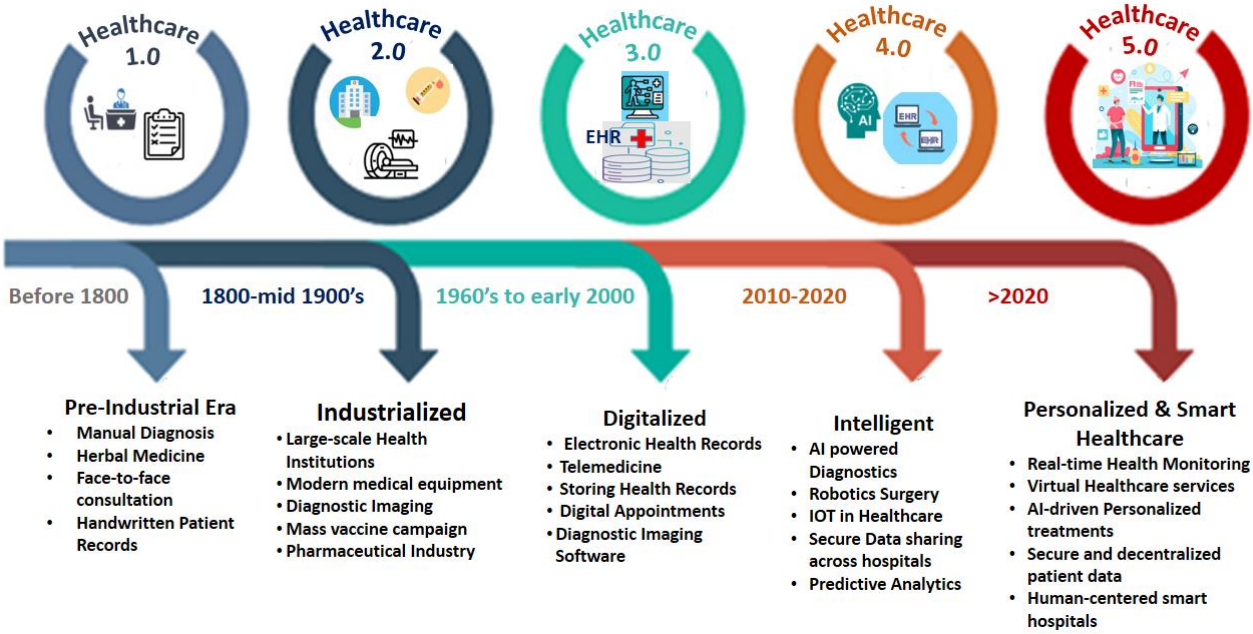

Fig. 1. Evolution of Healthcare 1.0 to Healthcare 5.0

Table 1. EHR Features From Healthcare 1.0 To Healthcare 5.0

Features	Healthcare 1.0	Healthcare 2.0	Healthcare 3.0	Healthcare 4.0	Healthcare 5.0
Data Format	Paper-based	Basic digital records	Interoperable digital data	Connected and real-time	AI and Big Data-driven
Access	Manual retrieval	Internal hospital systems	Limited cross-institution	Cloud-based, real-time	Decentralized patient-centric
Functionality	Storage only	Storage and retrieval	Evidence-based analytics	Predictive care	Precision Medicine
Technology	Manual Records	Early EHR systems	Interoperable EHRs	Cloud-based EHRs, IoT	AI, Blockchain-based EHRs, Federated Learning
Challenges/ Limitations	• Inefficiency in accessing and sharing patient information. • Risk of errors due to illegible handwriting or lost documents • Limited continuity	• Siloed data prevented. • Seamless integration across healthcare providers. • No advanced analytics or real-time decision making.	• Fragmented implementation led to disparities in adoption. • Privacy and security risks emerged due to growing reliance on digital systems.	• Increased risk of cyber security attacks. • Dependence on internet connectivity and technology infrastructure. • High-cost implementation and maintenance of EHRs	• Security and privacy. • Regulatory challenges in implementing advanced systems across jurisdictions.

Adoption of EHR Scenario

EHR adoption is increasing at an unprecedented rate in developed countries such as New Zealand, Australia, the US, and the UK. Strong policies, interoperability standards, and financial incentives contribute to the high adoption rates.

Conversely, developing countries face challenges in adopting EHR due to infrastructure deficiency, high implementation costs, and resistance to change. In India, Ayushman Bharat Digital Mission (ABDM) aims to develop digital health infrastructure by initially providing digital health IDs that can be connected to health records.

Ethical issues in EHRs

The high adoption rates of EHRs are due to their benefits to healthcare providers and patients, but they also pose ethical issues in EHRs. The author (Jamshed et al., 2015) gave a general overview of hazards due to EHR adoption; hence, protecting individual health is a real challenge. The major obstacle to the adoption of EHR is privacy and security.

As healthcare centers increasingly rely on digitization and cloud-based EHRs, they are exposed to increasing risks (Mehrtak et al., 2021) related to data availability, confidentiality, integrity and protection against network threats such as unauthorized access and data leaks. The authors (Mehraeen et al., 2016) highlighted that technical, physical and administrative safeguards in healthcare centers are unevenly implemented. The administrative safeguards, typically being the weakest, increase the risk of information compromise.

Thus, safeguarding EHRs presents an excellent challenge for authorities, public health officials and healthcare providers. Few security measures adopted by healthcare practitioners are categorized into three safeguard themes (Kruse et al., 2017): physical, technical and administrative. Privacy safeguards the rights of patients by monitoring data accessibility. On the other hand, confidentiality is maintained through Role-Based Access Controls (RBAC) and authorization protocols. There are also significant dangers associated with security breaches. Unauthorized exposure of data undermines the trust of the patients. Therefore, implementing strong security measures such as firewalls, risk assessment, encryption, and regular audits will help eliminate these threats.

EHR implementation also faces challenges, such as high costs, clinician resistance, and workflow interruptions, which entail careful planning and collaboration. In addition, data inaccuracies caused by copy-pasting, narrow input fields, loss or destruction of data during data transfer, and medical identity theft may jeopardize patient safety and result in billing errors.

To get the best performance out of EHR systems while keeping patient data secure and maintaining integrity, these challenges must be tackled with standardized processes, user-friendly interfaces, and solid data protection measures.

Motivation

With the release of Healthcare 3.0, data breaches and cyber-attacks emerged as significant threats to healthcare data. Healthcare data ranks as one of the most sensitive classes of patient personal/health information and is often besieged by cybercriminals due to its high value in the black market. The consequences of data breaches are identity theft, insurance scams, and misuse of sensitive health information, potentially resulting in psychological, financial and social damage to the victims.

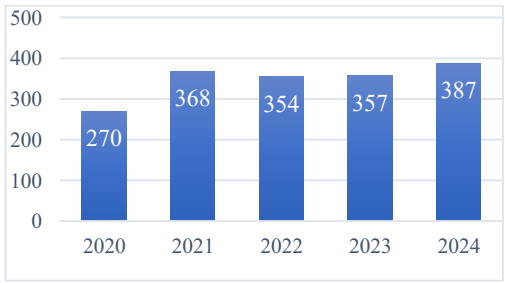

Fig. 2. Healthcare Data Breaches (2020-2024)

According to the Health Insurance Portability and Accountability Act (HIPAA)("Healthcare Data Breaches," n.d.), Figures 2 and 3 depict the number of records breached and the cause for healthcare data breaches yearly between 2020 and 2024. Each record contains millions of healthcare data. In 2024, nearly 45,555,982 healthcare data were breached, and confirmation was received during the year's first half. The primary cause for data breaches is hacking/IT incidents and illegal access, underlining the need for stronger security and access control methods to protect sensitive healthcare data.

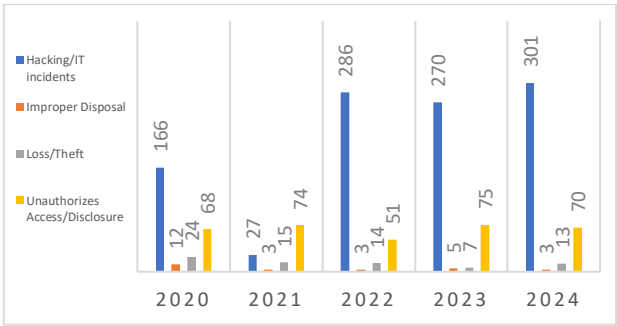

Fig. 3. Causes for Healthcare Data Breaches

Contributions

The main contribution of this survey is to provide an in-depth study of the different security and privacy techniques used in various phases of the EHR workflow.

- To enlighten on EHR data and its structure.
- To analyze the different phases in EHR workflow.
- To review the existing EHR data storage techniques, challenges and future trends.
- To identify the security methods used during data access and retrieval, challenges, and future directions.
- To investigate the data sharing techniques, available interoperability standards, challenges and future trends.

Review Methodology

This review was conducted following a structured literature survey approach. Relevant articles were identified from electronic databases including ACM Digital Library, IEEE Xplore, PubMed, SpringerLink, Elsevier ScienceDirect, and Google Scholar. Search terms included combinations of *"Electronic Health Records"*, *"EHR security"*, *"privacy"*, "EHR Storages", *"blockchain in healthcare"*, *"Role-Based access control"*, *"attribute-based access control"* and "*Interoperability"*.

The search covered publications from **2015** to **2024**. Only peer-reviewed journal articles, conference papers, and review articles written in English were included. Studies focusing on security and privacy issues, proposed algorithms, access control mechanisms, and blockchain-based solutions for EHRs were considered.

Duplicates were removed, and papers were screened by title, abstract, and full text to determine relevance. A total of **110** papers were selected for detailed review. For each study, we extracted and summarized the key concepts, proposed methods/algorithms, and limitations, which were then synthesized to identify current challenges and research gaps.

Literature Review

Table 2 presents the survey papers on security and privacy in EHR, emphasizing the objectives and phases of the EHR workflow.

Singh et al. (2024) conducted an extensive literature analysis on privacy-preserving methodologies for EHRs, encompassing blockchain, federated learning, and cryptographic techniques. The survey addressed data storage and sharing strategies and their role in regulating access and secure data transmission.

A comprehensive technical analysis of privacy-preserving EHR solutions utilizing various methods, including cryptography, blockchain, and cloud-based frameworks, to protect patient data is discussed (Nowrozy et al., 2024).

Hathaliya & Tanwar (2020) investigated cloud, IoT, and blockchain technologies to secure and preserve privacy in Healthcare 4.0. It emphasized mainly the storage and sharing of healthcare data.

Shi et al. (2020) examined the benefits of decentralized security frameworks in thwarting unauthorized data breaches. The survey lacks details about hybrid security solutions incorporating technologies like AI-driven access control and multi-layer encryption.

The blend of blockchain and ML to enhance EHR security is analyzed in Zukaib et al. (2023). It emphasized federated learning, encryption techniques, and blockchain to safeguard privacy.

The effect of trust and privacy on healthcare data sharing in EHR systems is examined in Cherif et al. (2021). It focused on patient perspectives on protocols and data availability.

Privacy-preserving methods like anonymization and differential privacy are discussed within the healthcare data (Chong, 2021). The study examined the ways to mitigate re-identification issues in EHR data while preserving privacy. Real-time privacy risks such as homomorphic encryption need to be addressed.

Al-Slais (2020) evaluated privacy-preserving approaches and their adherence to the General Data Protection Regulation (GDPR) and Privacy by Design principles. The study offered a robust basis for privacy frameworks. The study focused only on generic IT systems instead of EHR-specific security models.

The proposed survey emphasized three phases of EHR workflow: Data storage and management, Data access and retrieval, and Data Sharing and Interoperability.

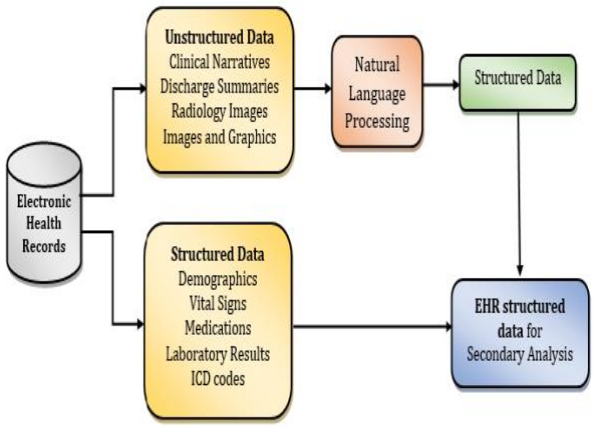

Fig. 4. Structure of HER

Table 1: Survey Papers on Security and Privacy

Authors	Objective	EHR Data Storage techniques	Data Access & Retrieval Methods	Secure Data Sharing and Interoperability
(Singh et al., 2024)	EHR management focuses on privacy, security, and healthcare quality, leveraging deep learning, federated algorithms, blockchain, and cloud-based solutions.	✓	✗	✓
(Nowrozy et al., 2024)	EHR privacy preservation uses access control, blockchain, cloud-based, and encryption, with a fusion proposed for greater security.	✗	✓	✓
(Hathaliya & Tanwar, 2020)	Examines Healthcare 4.0 security and privacy methods, including blockchain-based solutions, and discusses obstacles and future research.	✓	✗	✓
(Shi et al., 2020)	Provides secure EHR through blockchain technology	✓	✓	✗
(Zukaib et al., 2023)	Review of blockchain and ML for EHR security, including encryption and federated learning.	✓	✗	✓
(Cherif et al., 2021)	Examine how trust and patient privacy affect EHR data sharing.	✗	✓	✓
(Chong, 2021)	Review of privacy-enhancing methods for healthcare informatics with an emphasis on anonymization and differential privacy.	✗	✗	✓
(Al-Slais, 2020)	Review of privacy engineering approaches to evaluate GDPR and Privacy by Design compliance.	✗	✓	✗
Proposed Survey	**Reviews security and privacy techniques in EHR workflow phases**	✓	✓	✓

Overview of EHRs

Definition and Structure of EHR

EHR is a digital version of an individual's consolidated medical data in structured and unstructured form to provide a unified platform for healthcare delivery. The structured data includes patient characteristics, demographics, laboratory results, vital signs, fluid output, medications, diagnosis codes and physiological measurements. The unstructured data include clinical narratives, progress notes, surgery characteristics, and discharge

summaries, which can be used to profile patients. These data are the primary source of healthcare intelligence, but analyzing the unstructured data by Tayefi et al. (2021) is complex and time-consuming. Advanced statistical algorithms in Natural Language Processing, Machine Learning, and Deep Learning analyze unstructured data.

EHR Workflow

EHR workflow is the backbone of modern healthcare, which acts as a centralized digital repository for patient healthcare data, with its actual value residing in the ease with which healthcare providers can access, update, and employ this information in patient care. It seamlessly blends patient data across administrative, clinical, and Figure 5 shows the workflow of EHR with five phases. The phases of EHR workflow are:

A. Data Entry and Documentation

The initial phase is patient registration, which includes creating and entering patient data. Data can be recorded manually and automatically, and patient input can be provided through interfacing with medical devices and other health information systems (Kruse et al., 2017). Manual entry is necessary but time-consuming and error-prone, which can be tiresome for healthcare providers if not optimized (Bhatt et al., 2021). Automatic data integration from medical devices eliminates manual workload and reduces data entry errors from 20% to 0%, as mentioned in Bauer et al. (2020). Patients can also provide inputs to EHR from healthcare portals or wearables, which is advantageous and encourages patient participation and care plan adherence(F. A. Khan & Hajiarbabi, 2024). According to the study, Cheng et al. (2023), robust validation methods like mandatory fields and related auto-completion are essential to ensure accurate data. This automated method results in accurate data between 84%-94% compared to manual entries. This phase provides the basic administrative, clinical, and research data.

B. Data Storage and Management

The patient information entered in the previous phase is stored securely and effectively in the databases, which can be easily accessed for clinical and administrative purposes within the EHR system. Contemporary storage solutions are cloud, on-premise, or hybrid storage. Cloud storage offers scalability and affordability but requires robust encryption to minimize the risk of data breaches (Srinivas et al., 2023). On-premise storage enhances data control at a higher maintenance cost. The data is ordered efficiently, ensuring unified storage and retrieval of structured and unstructured data (Vamsi & Reddy, 2020). Advanced encryption techniques, such as attribute-based and homomorphic encryption methods, are used to store the data securely. It also ensures privacy by allowing only authorized individuals to access patient data (Wei et al., 2019). Adherence to legal frameworks such as HIPAA and GDPR protects patient data, and blockchain technology ensures transparency and compliance with these standards (Ettaloui et al., 2023). Archiving data for historical records is very important for keeping things safe and easy to find over time. It helps with research and meets necessary regulations (J. Wang et al., 2023). Also, using optimization algorithms can reduce computational and storage overhead (Dr. T. et al., 2019). These processes make managing EHRs secure, efficient and compliant, eventually leading to better patient care and smoother operations.

Table 2. Storage Techniques

Storage Method	Location	Advantages	Limitations
On-premise	Data stored on internal servers within healthcare organizations	• Complete control • Local compliance	• High costs • Limited Scalability
Cloud	Data is hosted in third-party cloud providers	• Scalable • Cost-effective • Accessible	• Privacy risks • Dependency on providers
Hybrid	Blends on-premise and cloud storage	• Balance Control • Scalable	• Complex to manage dual environments
Blockchain+cloud	Combines blockchain's security features with cloud storage's scalability	• Immutability • Scalability • Enhanced security	• High computational overhead • Vulnerable to transmission attacks
Blockchain+IPFS	Integrates blockchain for immutability and security with IPDS for decentralized faster data retrieval and sharing	• Decentralized • Faster Data retrieval • Tamper-proof storage • Enhanced traceability	• High computational overhead, • Resource-intensive integration • High Latency • Limited Scalability

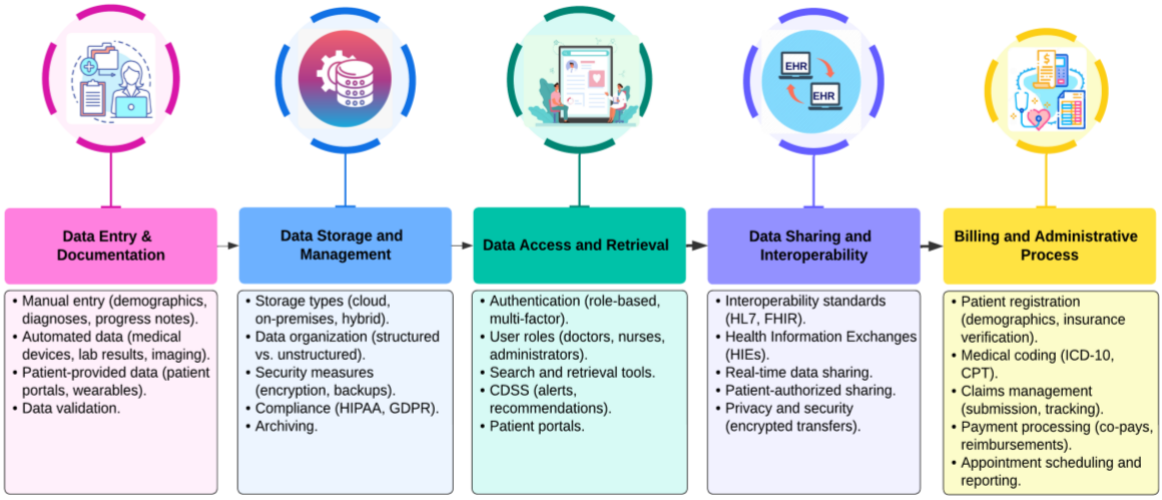

Fig. 5. EHR Workflow

C. Data Access and Retrieval

To secure and preserve privacy in the EHR workflow, efficient methods like Multi-Factor Authentication(MFA) and RBAC grant access to EHRs only to authorized healthcare providers, nurses, administrators and patients based on their roles (Mamta Dhaka et al., 2024). Search and retrieval tools enhance data access by allowing users to quickly find relevant information, thereby minimizing the time spent examining enormous records (Zarezadeh et al., 2020). Clinical Decision Support System (CDSS) optimizes this process by utilizing recovered data to deliver real-time alerts, therapeutic suggestions, and diagnostic support, improving clinical decision making and patient outcomes (Mebrahtu et al., 2021). Patient portals authorize individuals by providing access to their health information, facilitating appointment scheduling, examining the test results and enabling secure communication with healthcare practitioners. These systems are instrumental in enhancing patient participation, health literacy and compliance with healthcare protocols (Simola et al., 2023). Data access and retrieval methods guarantee that EHR systems maintain a balance of accessibility, usability, and security.

D. Data Sharing and Interoperability

The primary function of EHR is to exchange healthcare information with stakeholders, including healthcare professionals, laboratories, pharmacists, and insurance firms, to support coordinated and integrated patient care. To solve the differences in EHR systems (Hidayat & Hermanto, 2020), interoperability standards such as HL7 and FHIR support standardized data architecture and exchange through RESTful APIs. Health Information Exchange(HIE) facilitates the sharing of patient information between institutions despite issues such as technology incompatibility and confidentiality (Mukhiya & Lamo, 2021). Combining FHIR and blockchain facilitates real-time data sharing, improving collaborative clinical decision-making and reducing response time in critical care scenarios (Dubovitskaya, Novotny, et al., 2020). Patient-authorized sharing and access controls to their EHRs, ensure transparency while abiding compliance with HIPAA's privacy requirements. The sophisticated security measures such as encrypted data transfer and blockchain technology address privacy concerns, enabling scalability and interoperability in a secure manner (McMurry et al., 2024). This stage ensures that the EHR systems enable coordinated care, regulatory compliance and enhanced patient outcomes.

E. Billing and Administrative Details

This phase confirms refining how we handle finances, making everything run more smoothly and accurately. Patient registration is all about gathering people's demographic information, verifying their insurance coverage and eligibility and streamlining the details for claims (Kasih & Achadi, 2023). Standardized billing codes like ICD-10 and CPT help reduce mistakes and boost compliance (Kilanko, 2023). Computerized claims management systems make submission and tracking a breeze, which means faster payments (Wilkinson, 2024). Payment processing focuses on integrating reimbursements and co-pays when scheduling appointments (J.A et al., 2019). This phase ensures maximizing efficiency and helps maintain financial stability in healthcare settings.

EHR workflow boosts coordination between healthcare providers by maximizing data entry, protecting data storage, enabling instant access and effortless exchange and refining administrative processes while respecting privacy and security policies.

Table 3. Existing Research Work on EHR Data Storage and Management

Authors/Year	Objective	Storage Method Used	Advantages	Limitations
(Riadi et al., 2022)	To design a blockchain-IPFS system to store and exchange COVID-19 EHR securely.	Blockchain + IPFS for distributed storage	• Highly secure • Data availability	• Computational overhead • Bandwidth challenges
(Nguyen et al., 2019)	To propose a mobile cloud EHR for secure data sharing	Blockchain + IPFS on mobile cloud platforms	• Lightweight access control • Low latency • Enhanced data privacy	• Scalability challenges for larger healthcare systems
(Reegu et al., 2023)	To design an interoperable framework for secure EHR storage and sharing	Blockchain with compliance to HL7 and HIPAA	• Enhanced security • Patient control • Interoperable	• Focused on conceptual framework without practical implementation
(Rajkomar et al., 2018)	To demonstrate scalable and accurate predictive models	Structured FHIR-based storage	• High accuracy in predictive models • Support multi-center data harmonization	• Requires high computational power • Complex data integration techniques
(Shen et al., 2023)	To introduce a certificateless PDP scheme for cloud-based EHRs	Distributed cloud storage with PDP	• Enhanced data integrity • Security with multicopy redundancy	• Increased complexity in managing distributed systems
(S et al., 2024)	To develop a secure EHR storage system	Solana Blockchain +IPFS	• Improved scalability • Highly secure • Efficient storage of EHR data	• Limited implementation scope
(Lakshmanan et al., 2024)	To design a novel approach to storing EHR data	Blockchain+ Advanced cryptographic techniques	• Enhanced Security • Data integrity • Preserves privacy • Scalable	• High Computational overhead • Complex implementation
(H. Zhang et al., 2018)	To secure EHR cloud storage	Cloud + Secret sharing with verifiable reconstruction outsourcing	• Enhanced privacy and security • Data integrity verification	• Increased computational overhead • Dependency on multiple cloud servers • Large-scale adoptions in real-world settings
(Srinivas et al., 2023)	To propose a secure framework for sharable EHR storage	Encrypted cloud storage	• Secure and efficient EHR sharing with robust encryption	• Vulnerable to cloud-based attacks
(Zheng et al., 2018)	To propose a storage model	Blockchain+IPFS	• Decentralized secure storage • Improved scalability	• Limited real-world implementation • Performance validation
(Shah et al., 2020)	To design a decentralized storage solution	Blockchain+ decentralized cloud storage	• Improved data availability • Transparency • Cost-effective	• High computational and storage overhead
(S. Wang et al., 2019)	To develop a secure cloud storage framework with access control mechanisms	Blockchain-based access control framework	• Improved security • Decentralized control • Robust access control policies	• Highly complex in implementing access control at scale.

With the development of EHR workflow technology, it is necessary to recognize that such a continuous flow of EHR presents significant issues regarding security and privacy. With sensitive data in EHR, these are critical issues apparent at every level of EHR management.

This survey explicitly targets security and privacy measures adopted at crucial phases of the EHR life cycle, particularly Data Storage and Management, Data Access and Retrieval, and Data Sharing and Interoperability, which play a major role in ensuring the integrity, confidentiality, and availability of patient data.

Data Storage and Management - Existing Techniques, Challenges and Future Trends

This phase is important in supporting the integrity of the data, ensuring efficient accessibility, and securely storing the patient's medical records.

The principle goals of EHR storage management are to safeguard sensitive information against unauthorized access, comply with laws such as HIPAA and GDPR, and ensure that backup data are available for recovery in case of an outage.

Table 3 lists the storage techniques, storage location, advantages and limitations.

Secure Storage Techniques:

Secure EHR storage is a major problem since they hold private health information that could be compromised by illegal access to data, likely at risk of data breaches, privacy infringements, and unauthorized access. Various cutting-edge technologies, like encryption, blockchain, cloud computing, etc., are utilized to strengthen the safety of EHR storage. The existing fundamental approaches to securely storing EHR are as follows:

In the research, Riadi et al. (2022) integrated blockchain and IPFS to securely store and manage COVID-19-related EHR data. It guarantees data security, availability, and integrity inside a decentralized network. However, the framework encountered difficulties related to computational overhead and bandwidth demands.

The study by Nguyen et al. (2019) introduced a mobile-cloud EHR platform backed by blockchain and IPFS, facilitating secure data interchange with minimal latency. Blockchain technology provides transaction immutability and transparency alongside IPFS for decentralized file storage. This combination guarantees safe storage and access to sensitive healthcare data without dependence on centralized systems. The framework was confined to mobile health applications.

Reegu et al. (2023) proposed an EHR system based on blockchain to address important concerns about privacy, security, and interoperability in the healthcare industry. The framework is highly relevant to modern healthcare systems because it conforms to international standards like HIPAA and interoperability protocols like HL and FHIR.

Rajkomar et al. (2018) exhibited scalable prediction models for EHR data through FHIR-based storage. The method attained high precision in clinical forecasts but necessitated substantial computational power and complex integration.

A cloud-based EHR introduces a certificateless Provable Data Possession (PDP) approach for secure storage (Shen et al. 2023). This technology enhances data security and redundancy but presents issues related to system complexity in distributed contexts.

An innovative EHR management method by S et al. (2024) blends Solana blockchain technology and IPFS, ensuring the data is securely stored and accessible only to authorized users.

The decentralized data storage eases risks like a single point of failure and data manipulation, building a tamperproof and trustworthy environment for EHRs.

Lakshmanan et al. (2024) presented a novel approach to storing EHR data effectively leveraging blockchain technology and advanced cryptographic techniques. It incorporates two methods, Data Sanitization and Polynomial Interpolation-based cryptography (DSPIC), which encrypt the privacy of the EHR. The optimal key is generated using the Modernized Position-based Coot and Penguins Search Optimization Algorithm (MP-CPeSOA) and uses a digital signature to ensure the high security of EHR. This approach is validated through experiments conducted on different EHR management schemes, demonstrating its superiority in safeguarding the security and privacy of EHR.

Using Shamir's secret sharing method, security and privacy challenges when storing EHR data on the cloud are addressed (H. Zhang et al., 2018). This approach divides an EHR into multiple segments by healthcare center. These segments are then distributed across various cloud servers. When the EHR needs to be retrieved, the healthcare center collects segments from a subset of these servers to reconstruct the complete EHR. It identifies the reconstruction burden on healthcare centers or patients, introducing a practical scheme that outsources this reconstruction process to a cloud computing service provider. The reconstructed EHRs are verified to ensure the integrity and correctness of the data.

Table 4. Access Control Techniques

Techniques	Description	Security Features	Advantages	Limitations
RBAC	Regulates access according to user roles (Physician, nurse, administrator)	Fine-grained role-based policies	• Easy to manage • Ensures compliance with least privilege access	• Limited flexibility in dynamic environments
MFA	Blends two or more authentication methods	Enhances identity verification and access security	• Provides strong authentication • Reduces unauthorized access	• Can cause usability challenges for stakeholders
ABAC	Uses attributes like location, time and user actions to access permissions dynamically	Context-aware policies for access restriction	• Highly flexible • Adaptive to dynamic healthcare environments	• It is computationally complex to implement and manage
BBAC	Uses blockchain technology to record and verify access events securely and immutably	Tamper-proof records and decentralized access policies	• Enhances transparency and security in access logs	• High computational costs • Limited scalability

Srinivas et al. (2023) proposed a framework integrating encrypted cloud storage with access controls to securely store shareable EHRs. This framework provided strong protection yet was still vulnerable to cloud-based threats.

An IPFS-based blockchain storage paradigm by Zheng et al. (2018), improved data storage efficiency and scalability. Although the concept guarantees decentralized storage, further evaluation is required to see how well it performs in real-world scenarios and under heavy workloads.

Shah et al. (2020) presented a decentralized cloud storage framework utilizing blockchain technology, emphasizing transparency and accessibility. This approach encounters difficulties with resource overhead in extensive applications.

In S. Wang et al. (2019), a secure cloud storage architecture leveraging blockchain technology, including improved access control, was devised. Decentralized control guarantees strong security, but the complexity of establishing precise access regulations constrains scalability in extensive networks.

Challenges in EHR Data Storage and Management

Scalability and Storage Capacity. The exponential growth of patient information, high-resolution medical imaging, and real-time monitoring data has created unprecedented demands for EHR storage infrastructure. Conventional cloud and blockchain solutions struggle to scale effectively while maintaining performance and cost-efficiency.

Security and Privacy. EHRs contain highly sensitive patient information, making them prime targets for cyberattacks, including ransomware, data breaches, and unauthorized access. While blockchain-based systems offer enhanced security through immutability, they face significant computational overhead. Conversely, cloud-based storage solutions remain vulnerable to sophisticated security breaches despite advanced encryption protocols.

High Resource and Computational Costs. Blockchain-based storage platforms (e.g., Ethereum, Hyperledger Fabric, Solana) provide robust security but require substantial computational resources, resulting in latency issues and elevated costs for real-time data access. IPFS-based approaches mitigate redundancy but demand high bandwidth, potentially compromising system performance in resource-constrained environments.

Interoperability and Integration. The healthcare ecosystem lacks standardization, with various EHR systems employing disparate data formats including HL7, FHIR, and DICOM. This heterogeneity creates significant barriers to seamless data exchange across hospitals, clinics, and healthcare networks, resulting in fragmented and siloed healthcare delivery systems.

Regulatory Compliance. Healthcare data storage must comply with stringent regulations such as HIPAA (United States), GDPR (European Union), and HITECH Act requirements. These frameworks mandate comprehensive data access controls, detailed audit trails, and robust encryption mechanisms, substantially complicating storage solution implementation. Cross-border healthcare systems face additional complexities regarding data sovereignty and international data sharing requirements.

Table 5. Existing Techniques in Role-Based Access Control

Author	Objective	Methodology	Advantages	Disadvantages
(Zhou et al., 2016)	An anonymous RBAC model to preserve patient privacy and allow secure access	Anonymous RBAC with role-based policies and semantic security	• Ensures data privacy • Supports anonymous access • Low computational costs	• Limited to privacy concerns • Does not address emergency scenarios
(W. Liu et al., 2015)	To design auditing and revocation capabilities for RBAC in EHR systems	RBAC integrated with forward revocation and auditing mechanism	• Prevents unauthorized future access • Supports auditing and fine-grained control	• Overhead in revocation and auditing processes
(Tiwari & Kumar, 2015)	To develop an on-demand RBAC algorithm for secure access classification of EHRs	Role-specific classification of data using data isolation	• Supports dynamic policy application • Robust against unauthorized role access	• Does not focus on real-time updates or external attacks
(De Carvalho Junior & Bandiera-Paiva, 2020)	To strengthen RBAC by incorporating GDPR complaint explicit patient consent	Integration of RBAC with patient-centric permission	• Aligns with GDPR • Allows encryption and patient-controlled access	• Reduce efficiency due to manual patient involvement
(Guo et al., 2019)	To design a hybrid blockchain edge RBAC architecture for secure access control	Blockchain-based logs with edge computing policy enforcement	• Tamper-proof logs • Decentralized control • Real-time processing	• High latency in blockchain processing • Computationally expensive
(Rose Ann & Susan, 2017)	To design a TRBAC model for fine-grained control of PHRs	Dynamic task-role assignment coupled with role-based restrictions	• Greater flexibility and granularity for PHRs	• Implementation complexity • Not extensively validated in large systems
(Butt et al., 2023)	To optimize RBAC by introducing a trust-based mechanism for user behavior in cloud EHR systems	Trust-based access control integrated with SQL-based modules	• Reduces risks from malicious users • Scalable for large cloud systems	• Limited to cloud-based systems • Required periodic trust recalibration
(Tsegaye & Flowerday, 2020)	To combine RBAC, ABAC and Clark Wilson models for secure EHR systems	Dynamic authorization using hybrid RBAC and ABAC	• Comprehensive security • Supports emergency overrides	• High computational requirements • Lacks scalability testing
(De Carvalho & Bandiera-Paiva, 2017)	To evaluate RBAC against ISO privacy standards using the Colored Petri Nets model	Simulated role-based data segregation policies	• Validates compliance with ISO standards • Identifies policy conflicts	• Only focuses on ISO compliance without broader adaptability
(Mamta Dhaka et al., 2024)	To develop an RBAC for standardized EHR systems, including universal IDs	Creates a framework for interoperability using standardized coding and role-based permissions	• Supports interoperability through standardization • Secure login mechanisms	• Requires high upfront infrastructure
(Riad et al., 2019)	To design SEAC for IoT-based EHRs	Combines RBAC with IoT-specific dynamic attributes for fine-grained access control	• Fine-grained access • Compatible with dynamic IOT setups	• High energy and resource demands for IOT integration
(Gope & Amin, 2016)	To design an RBAC model for emergency data access in EHRs	A multi-level hierarchy combining RBAC and	• Maintains security even during emergencies	• Implementation complexity in

		mandatory access control policies for emergency		multi-institutional environments
(Zarezadeh et al., 2020)	To develop a cloud-based RBAC model	CP-ABE for secure and scalable RBAC	• Supports multi-level data flow • Guarantees the user access control • Anonymity of the user or data owner during data retrieval • Resistant to collusion between unauthorized retrievers to access the data. • Secure and efficient for Cloud-based EHRs	• Policy updates and scalability are challenging

Data Integrity and Redundancy. Ensuring long-term accuracy, accessibility, and integrity of EHRs remains a critical challenge, particularly in decentralized storage architectures. Many blockchain-based systems lack efficient real-time update mechanisms, potentially resulting in outdated or inconsistent patient records that compromise clinical decision-making.

Future Directions in EHR Data Storage and Management

Hybrid Cloud-Blockchain Architectures. Emerging solutions integrate cloud infrastructure for scalability with blockchain technology for enhanced security and immutability, creating balanced storage paradigms that leverage the strengths of both approaches while mitigating their individual limitations.

AI-Driven Data Management. Machine learning and artificial intelligence technologies are revolutionizing storage efficiency through automated data classification, intelligent compression, and predictive security threat detection. AI-powered anomaly detection systems and automated encryption protocols will significantly enhance data security postures while reducing administrative overhead.

Standardized and Interoperable EHR Frameworks. Next-generation storage solutions will comprehensively integrate established healthcare standards including HL7, FHIR, DICOM, and SNOMED CT to facilitate seamless data exchange across healthcare providers. Federated learning approaches enable collaborative AI model training on decentralized EHR datasets without compromising patient privacy or requiring centralized data aggregation.

Zero-Trust Security Architectures. Implementation of Zero-Trust security models ensures continuous authentication and authorization of all access requests, effectively mitigating insider threats and unauthorized access. Integration of multi-factor authentication (MFA) with AI-driven behavioral analytics provides adaptive, context-aware access control mechanisms.

Quantum-Resistant Cryptography. As quantum computing capabilities advance, healthcare organizations must transition to Post-Quantum Cryptography (PQC) algorithms to protect stored EHRs against emerging quantum-based cryptographic attacks that could compromise current encryption standards.

Edge Computing for Real-Time Processing. Edge computing architectures enable data storage and processing at the point of care (e.g., IoT medical devices, wearable sensors, hospital networks), substantially reducing latency and enhancing real-time clinical decision-making capabilities. IoT-enabled medical devices can securely store patient vital signs on edge nodes before synchronizing with centralized EHR systems, ensuring data availability even during network disruptions.

Self-Sovereign Identity and Patient-Centric EHRs. Decentralized Identity (DID) solutions and Self-Sovereign Identity (SSI) frameworks empower patients to control their healthcare data, enabling selective disclosure and patient-mediated information exchange. This paradigm shift toward patient-centric data governance enhances privacy while facilitating authorized data sharing across healthcare providers.

Future research must prioritize the development of secure, interoperable, and patient-centric EHR storage solutions that enhance healthcare delivery efficiency while ensuring robust data protection. The convergence of emerging technologies, including hybrid cloud-blockchain architectures, AI-driven management systems, quantum-resistant cryptography, and edge computing, presents promising pathways toward addressing current limitations and establishing resilient, scalable healthcare information infrastructures.

Table 6. Existing Techniques in MFA

Authors	Objectives	Methodology	Advantages	Limitations
(ALSaleem & Alshoshan, 2021)	To develop an MFA system integrating graphical passwords and user-chosen images	• The user selects three images in the registration phase. • Verification occurs during login following the sequential order.	• Prevents key-logging and screen capture attacks • Economical	• Utilizes user memory • For enterprise systems, it might not scale effectively
(Ometov et al., 2018)	• To develop a system using Shamir's Secret Sharing	• Reversed language polynomial for user authentication, even with missing factors	• Allows flexible authentication without sharing sensitive biometric data	• Requires further validation for large-scale deployments
(Simha.R et al., 2025)	• To design an MFA system blending graphical passwords, CNN-based facial recognition and QR codes.	• Two-layer graphical password with CNN for facial recognition and QR code verification	• Success rate of 93% with robust protection	• Limited Scalability • High Computational requirements
(S. H. Khan et al., 2015)	• To develop a biometric-based two-factor authentication framework	• Integrates handwritten signature biometrics with password-derived secure keys	• Safeguards the integrity of biometric templates	• Depends on biometric dataset quality for robust results.
(Gandhi & Patil, 2023)	• To explore three-factor authentication in EHR systems	• TAM-based analysis of user behavior	• Improves security and privacy • Promotes the implementation of robust authentication in healthcare systems	• Demands more verification via trial implementations in EHR settings
(Hamed & Yassin, 2023)	• To develop MFA for EHR systems using cryptographic techniques	• Integrated Chameleon digital signatures and asymmetric encryption	• High resistance to malicious attacks • Comprehensive security	• High reliance on system administrators • Single-point failure risks
(Voege & Ouda, 2022)	• To design a framework using AI and chatbots for dynamic MFA challenges	• Big data and ML-enabled authentication to generate adaptive challenges	• Customizable and dynamic • Reduces predictability in security breaches	• Requires validation for EHR-specific contexts
(Fakroon et al., 2021)	• To introduce a secure telehealth system using MFA and PUFs	• Biometric-based authentication via PUFs for mutual authentication and key exchange	• Safeguards multiple types of attack • Formal security proofs validated effectively	• Focused on IoT edge devices
(Sharaf & Shilbayeh, 2019)	• To propose an MFA-based G-cloud framework for secure government healthcare services in Saudi Arabia	• Integrated multi-authority CP-ABE and hierarchical structure with MFA for secure access	• Ensures secure data sharing via cloud-based EHR systems	• Necessitates infrastructure enhancement for extensive implementation.
(Albarki et al., 2019)	• To develop a three-factor authentication protocol for secure EHR exchange over insecure channels	• Used biometrics, smart devices, and passwords with AVISPA validation tools	• Robust security • Reduced communication overhead	• Heavy resources for multi-user environments
(Alghamdi et al., 2022)	• To propose an MFA scheme for secure IOT-enabled smart emergency medical transporters	• Combined PUF-based mutual authentication for ambulance systems	• Strong resistance to cyber-attacks during patient transport	• Limited application of the scheme to emergency medical transport systems

(Suleski & Ahmed, 2023)	• To design Adaptive MFA for IOHT environments	• Developed a theoretical data taxonomy for AMFA systems in IOHT	• Customized for IOHT data architecture • Adaptive to user and device behaviours	• Lacks practical implementation and validation
(Kaul et al., 2020)	• To develop a biometric-based lightweight authentication system for personalized EHR services	• Integrated biometric verification with local and global identifier handling for privacy	• Provides emergency access recovery while preserving privacy	• Concentrated on lightweight systems • Untested on large-scale platforms
(Hathaliya et al., 2019)	• To present a biometric-based scheme for secure EHR access in Healthcare 4.0.	• Utilized iris and fingerprint biometrics validates via the AVISPA tool	• Enhanced computational efficiency	• Restrictions on expanding biometric infrastructure in distributed settings
(Velásquez et al., 2018)	• To create a framework for selecting optimal MFA techniques for software systems.	• A theoretical framework to compare and install MFA systems based on the situation.	• Helps system designers choose proper MFA methods for healthcare applications	• Theoretical focus with limited real-world testing.

Data Access and Retrieval

In order to protect patient privacy and comply with regulations such as HIPAA and GDPR, it is imperative to secure and control access to EHRs. Identity theft, data breaches, and regulatory infractions can arise from unauthorized access to EHRs. Various access control strategies are employed in data access and retrieval operations within healthcare systems to alleviate these dangers, like Role-based Access Control (RBAC), Multi-Factor Authentication (MFA), Attribute-Based Access Control (ABAC) and Blockchain-Based Access Control (BBAC). These methods enhance security and maintain system effectiveness by ensuring that only authorized personnel can access and modify sensitive patient data. Through these methods, patients, clinicians, and administrators, and patients can get the information they need for engagement, decision making and operational procedures.

Table 5 illustrates how EHR systems leverage access control mechanisms to balance security, usability and compliance.

Role-based Access Control (RBAC)

One of the most common access control paradigms in EHR systems is RBAC, in which permissions are granted based on roles defined in the healthcare industry. Certain access privileges are granted to approve users, who inherit these permissions by their assigned responsibilities, rather than being granted authorization to individual users. For example, a physician may see a patient's diagnosis or medical history, whereas a receptionist can solely view demographic information for scheduling appointments.

RBAC is implemented in EHR systems to protect sensitive patient data by granting access only to authorized users. It simplifies access control in complex environments, such as hospitals with multiple roles, and ensures compliance with regulations like HIPAA, GDPR, and ISO standards. Its scalability makes it a standard in healthcare IT infrastructure.

A few existing techniques using RBAC are:

An RBAC architecture by Zhou et al. (2016) preserves patient privacy while facilitating secure access to EHRs. The methodology entailed integrating RBAC with semantic security and role-based regulations, providing data privacy and anonymous access while maintaining minimal computational costs. It needs to address access to EHRs during emergency situations.

W. Liu et al. (2015) proposed a paradigm incorporating auditing and forward revocation procedures into RBAC-EHR systems. The forward revocation feature prevents unwanted future access, and the auditing tool facilitates accountability and precise control of the EHR. However, these methods come with additional costs for auditing and revocation processes.

The RBAC model by Tiwari & Kumar (2015), provides on-demand secure access to required data for specific roles. It used the technique of data segregation and role-specific rules to protect against unauthorized access to data. The model lacks usability as it does not prioritize real-time updates and external threats. De Carvalho Junior & Bandiera-Paiva (2020) enhanced RBAC by integrating GDPR-complaint, patient-centric permission to boost privacy laws in EHR systems. This methodology allowed patients to encrypt and regulate access to their records following GDPR, enhancing patient autonomy and confidentiality. Patients' manual

involvement reduces operational efficiency.

A hybrid blockchain edge RBAC architecture was presented to enhance access control security in EHR systems (Guo et al., 2019). Blockchain facilitated immutable logging, but edge computing permitted decentralized policy enforcement and instantaneous processing. The paradigm caused significant delays in blockchain processing and required enormous computational resources.

Rose Ann & Susan (2017) created a Task RBAC(TRBAC) paradigm for the precise regulation of Personal Health Records (PHRs). The methodology entailed allocating dynamic tasks and role limitations to enhance flexibility. The solution also encountered implementation challenges and lacked validation in extensive environments.

Trust-based mechanisms for user behavior in cloud-based EHR systems are implemented to optimize RBAC (Butt et al., 2023). The model employed trust-based scoring with SQL modules to identify malicious users and improve scalability for extensive systems. It required regular recalibration of trust scores and was limited to cloud environments.

Tsegaye & Flowerday (2020) combined the RBAC, ABAC and Clark-Wilson models to provide dynamic authorizations for secure EHR systems. The strategy offered complete security through hybrid authorizations and supported emergency overrides. The method demands significant processing, and restricted scalability assessments.

To measure adherence to ISO privacy standards, RBAC systems are evaluated with Colored PetriNets (De Carvalho & Bandiera-Paiva, 2017). This method emulates role-based policies to detect conflicts and verify compliance with ISO standards. It exhibited insufficient adaptability for non-ISO-compliant systems.

In Mamta Dhaka et al. (2024), a standardized EHR system framework was implemented using universal identifiers and uniform role-based access rights. This method enabled interoperability and secure login procedures but required substantial initial investment in infrastructure.

The Sensitive and Energetic IoT Access Control(SEAC) model proposed by Riad et al. (2019) combined RBAC with IoT-specific dynamic attributes to enhance fine-grained access control. The technology was especially appropriate for dynamic IOT configurations, but difficulties were encountered regarding energy and resource requirements during integration.

Gope & Amin (2016) proposes a “break the glass” RBAC model for emergency data access in EHR systems. The model integrates a multi-level hierarchy with mandatory access control policies to ensure that the right individual accesses the correct information during emergencies.

To enhance scalability and access security, Zarezadeh et al. (2020) create a cloud-based RBAC architecture utilizing Ciphertext Policy Attribute-Based Encryption (CP-ABE). The system guaranteed user access control and anonymity during data retrieval. The scalability and policy revisions posed challenges.

Table 6 summarizes the research on RBAC techniques for EHR systems, focusing on their contributions, advantages and limitations.

Challenges in RBAC in EHR systems

Lack of Granularity and Flexibility: RBAC allocates privileges according to specified roles, but practical implementation requires dynamic access control. Additionally, even though the doctors might need a patient’s medical history for consultation, they should not have permanent access to it.

Role Proliferation and Management Complexity: Large healthcare organizations need many personnel to provide a range of access needs. It can get tiresome to manage permissions, exceptions, and role hierarchies. The burden on the administration increases due to assigning roles and access privileges to different personnel, such as cardiologists, radiologists, pediatricians, etc.

Absence of Contextual Awareness: RBAC does not consider contextual elements like location, time, emergency situations, or medical devices. Access rights to in-house doctors and doctors operating remotely should have different privileges and access controls.

Security flaws: The static roles cannot adapt to threats such as unauthorized role escalation and credential theft that occur in real time. It is also necessary to keep an eye on the insider threat problem,

Challenges in Emergency Access Management: In an emergency, healthcare providers may require prompt access to the patient's EHR in the emergency ward. RBAC needs to address this issue by providing an automatic, real-time override mechanism for these situations.

Regulatory compliance and audibility issues: RBAC must regularly audit and revise access policies to comply with HIPAA, GDPR, and HITECH laws. Managing

EHR access, including user identity, time, and purpose, is crucial, but RBAC alone cannot provide complete audit trails.

Future trends in RBAC in EHR systems:

Design Context-Aware RBAC: Incorporating contextual factors (location, time, urgency and patient consent) into access control policies. A surgeon may possess complete access to patient records within the operating room but not from an external device or an untrusted network.

AI-driven Adaptive RBAC: To employ AI and ML to automate role allocations, identify anomalous behaviour, and adapt permission in real-time.

Integration of RBAC with ABAC: A hybrid methodology that integrates RBAC with ABAC will provide more nuanced access by considering user roles and dynamic attributes. For example, A cardiologist (role) can access only cardiology-specific EHR data (Attribute-based) rather than unrestricted access to all medical records.

Role management utilizing Blockchain Technology: Blockchain can establish immutable role assignments and access logs, enhancing auditability and security. Smart contracts can provide automatic role-based access policies, guaranteeing adherence to regulations such as HIPAA.

Zero Trust Security Framework for RBAC: Zero-trust models do not rely on user roles for trust; they continuously authenticate access requests using real-time identity verification, behavioral analysis, and risk assessment.

Self-Sovereign Identity (SSI) for RBAC: Patients will exert enhanced control over their EHR data, determining access to their records instead of depending on centralized RBAC policies.

RBAC is essential for access control in EHR systems, but its inflexibility, scalability limitations and lack of contextual awareness are present in modern healthcare. Adapting to future trends will enable secure, efficient access to sensitive patient data, balancing security and usability in the digital healthcare revolution.

Multi-Factor Authentication (MFA)

MFA enhances security by requiring users to provide their identity through multiple authentication mechanisms rather than only using passwords. These usually include passwords, security questions, One-Time Passwords, biometric verification, etc. They prevent unauthorized access even when passwords are stolen.

Recent research has analyzed several MFA approaches tailored to the particular requirements of healthcare, using advanced cryptographic techniques, biometrics, and adaptive processes. This section analyzes several approaches, focusing on their methods, benefits, and challenges.

A graphical password MFA system is presented by ALSaleem & Alshoshan (2021) in which users select a series of images at registration, which is confirmed during login. This method mitigates risks related to key logging and screen-capture threats while remaining economically viable. In larger systems, reliance on user memory presents usability challenges.

Ometov et al. (2018) conducted a comprehensive survey on the development of MFA and introduced Shamir's Secret Sharing (SSS) system for authentication. The approach used polynomial functions to recover authentication information without particular elements, providing flexibility and secure user authentication.

A new MFA system by Simha.R et al. (2025) combined graphical passwords face recognition based on CNN, and QR codes for secure authentication. The system achieved high success rates in preventing unauthorized access and offered high levels of protection. The limitation of this method is scalability because of the computational cost in resource-constrained systems.

S. H. Khan et al. (2015) developed a two-factor authentication system based on biometric handwritten signatures and secure key derivation functions. The system ensured that biometric templates would be protected even during password compromise. The effectiveness of the system relied on the quality of biometric information.

A three-factor authentication of EHR systems by Gandhi & Patil (2023) highlights the perceived utility and confidence linked to enhanced authentication techniques. The three factors considered are biometrics, OTP, and behavioural aspects. The system needs to address further empirical validation within healthcare settings.

An MFA framework is designed by Hamed & Yassin (2023) utilizing cryptographic methods such as chameleon digital signatures and symmetric encryption. The system exhibited resilience against many attack vectors, yet single-point failures in administrative components persisted as a concern.

A dynamic MFA framework employing AI-driven adaptive challenges is presented in Voege & Ouda (2022). The platform utilizes big data analytics to tailor security challenges according to user habits, diminishing

predictability in security breaches. The validation within the healthcare systems was limited.

A combined Physically Unclonable Functions (PUFs) with MFA for telehealth systems is designed to facilitate mutual authentication and key exchange (Fakroon et al., 2021). The system demonstrated robust resistance to replay and impersonation assaults. The emphasis on IoT contexts limits its generalizability.

A cloud-based MFA architecture for governmental healthcare services in Saudi Arabia is proposed by Sharaf & Shilbayeh (2019). CP-ABEs integration with MFA facilitated secure data transfer, although significant infrastructure enhancements were required for extensive implementation.

Albarki et al. (2019) introduced a three-factor authentication scheme incorporating biometrics, smart devices and passwords, which was confirmed using Automated Validation of Internet Security-sensitive Protocols and Applications (AVISPA) techniques. The framework's resilience to unauthorized access was hindered by its resource-intensive characteristics, which restricted its scalability for multi-user systems.

A PUF-based MFA architecture is proposed by Alghamdi et al., 2022 to secure IoT-enabled emergency medical systems. It is resilient to cyberattacks during patient transport but restricted to emergencies.

An Adaptive MFA(AMFA) system is designed by Suleski & Ahmed (2023) specifically for Internet of Health Things (IoHT) contexts. It presents a theoretical data taxonomy for personalization but is deficient in practical application and verification.

Kaul et al. (2020) have created a lightweight biometric-based MFA system for individualized EHR services. The methodology includes emergency access recovery protocols that safeguard privacy while remaining unexamined on extensive platforms.

A biometric-based MFA strategy by Hathaliya et al. (2019) was tested using AVISPA tools for Healthcare 4.0 systems. It enhanced computing efficiency but encountered difficulties scaling biometric infrastructure across decentralized contexts.

A theoretical framework by Velásquez et al. (2018) was offered to identify effective MFA strategies and improve system designers' ability to customize authentication methods for particular use cases. However, it must still address its practical application in actual EHR systems.

Table 7 summarizes the existing MFA techniques, including author name, objective, methodology, advantages and limitations.

Challenges in MFA Techniques

Scalability: MFA methods must achieve effective scalability in a vast healthcare network comprising numerous users, devices, and access points. Biometric and Cryptographic methods tend to be resource-intensive and hence unsuitable for massive deployments.

Usability and Accessibility: The complicated authentication protocols can restrict the usability of such systems for health professionals particularly in emergency situations where rapid entry to patient records is essential.

Computational and Energy Expenses: AI or blockchain-based MFA solutions are computationally expensive and energy intensive, and hence, they are not viable for low-resource environments.

Integration with Legacy Systems: Most health organizations possess legacy systems incompatible with contemporary MFA methods. This discourages the implementation of safe access controls.

Privacy issues: Biometric technologies are prone to raise privacy concerns, since mishandling of sensitive data may lead to serious violations of trust.

IoT and Remote Access risks: IoT devices in healthcare present supplementary vulnerabilities. Securing authentication in IoT-enabled systems such as emergency medical transport systems is challenging.

Future Trends in MFA Techniques

AI-driven Adaptive Authentication: MFA will incorporate ML and behavioral analysis to provide real-time risk assessment and adaptive authentication levels. Adaptive MFA is expected to become widespread as it can change security requirements based on user behavior.

Integration of Decentralized Systems: Blockchain-based systems that handle authentication logs and credential verification are becoming increasingly popular. Integrating blockchain with cryptographic MFA techniques could increase security and transparency, especially in decentralized healthcare settings.

Federated Identity Management: MFA systems will progressively depend on federated identity management frameworks to ensure smooth and safe authentication across institutions, enhancing interoperability across healthcare networks.

Table 7. Existing Techniques on ABAC

Authors	Objective	Methodology	Advantages	Limitations
(Xu et al., 2018)	To propose a FABAC dynamic context necessitating exceptional access	Employed fuzzy evaluation for policy alignment and credit adjustment auditing	• Enhances access flexibility while reducing hazards	• Concentrated on business time optimization • Excludes healthcare specific contexts
(Psarra et al., 2022)	To develop a context-aware ABAC system for emergency access to EHRs utilizing predictive metrics	LSTM neural networks to forecast patient status Fuzzy context handlers for decision making	• Resilient emergency access regulation • Patient focused protocols	• Significant computational burden resulting from LSTM and fuzzy systems.
(Das et al., 2017)	To introduce a heuristic approach for policy adaptation in ABAC for inter-organizational collaboration	Enhanced strategies for mining and adapting ABAC policies to facilitate collaboration	• Accelerates the transition to ABAC for companies	• Lacks scalability testing for large healthcare settings
(Zhu et al., 2021)	To develop an ABAC attribute extraction method for unstructured text via hybrid neural networks	RoBERTa-BiLSTM-CRF for attribute extraction in heterogeneous data settings	• Enhances semantic precision in attribute identification	• Significant resource requirements resulting from DL methods
(Abu Jabal et al., 2020)	To propose Polisma, a framework for deriving ABAC policies from previous data logs	Data mining and ML to develop and enhance ABAC policy	• Facilitates the automation of ABAC policy formulation, reducing manual labor	• Demands superior data logs for efficient policy formulation
(Ma et al., 2019)	To implement ABAC-SC for secure cross-organizational EHR sharing	Ethereum smart contracts to augment reliability and mitigate security concerns	• Offers immutable access logs and scalability	• Constrained by latency • Lack of storage on blockchain networks
(H. Wang & Song, 2018)	To propose a secure cloud-based EHR system utilizing an ABE and blockchain	Integrated ABAC and blockchain to securely encrypt and monitor medical data	• Facilitates precise access regulation with robust integrity assurance	• Computationally expensive for large scale systems
(Alohaly et al., 2022)	To integrate ABAC with the deception method to identify insider risks within EHR systems	Implemented ABAC policies and honey-based deception strategies to monitor malevolent insider threats	• Augments protection against internal threats	• Restricted validation in dynamic healthcare settings
(Abou et al., 2019)	To automate the creation of ABAC rules from event logs	Integrate process mining and data mining methods for extracting ABAC rules	• Streamlines ABAC implementation through the automation of rule generation	• Depends on precise and exhaustive event records
(Khamaiseh et al., 2018)	Model-driven testing of mandatory ABAC system	A testing model to incorporate functional models and obligation limitations for ABAC policies	• Recognizes and alleviates deficiencies in policy execution	• Limited evaluation for healthcare settings
(Ait El Hadj et al., 2017)	To generate ABAC rule	Utilizing KNN for clustering of ABAC rules to achieve dimensionality reduction	• Streamlines intricate ABAC policies • Minimizes rule redundancy	• Emphasized general ABAC systems, excluding healthcare settings
(Abou et al., 2019)	To design ABAC for EHRs utilizing Hyperledger Fabric	Use blockchain-based ABAC regulations through Hyperledger Fabric	• Augments security • Enhances transparency and compliance	• Limited validation in large-scale systems
(Cappelletti et al., 2019)	To assess symbolic and non-symbolic ML for ABAC policy mining	Used PCA and t-SNE for data analysis Evaluated ML algorithms for ABAC policy inference	• Emphasizes the efficacy of ML in the formulation of dynamic ABAC policy	• Significant reliant on data quality for accurate rule formulation

(Karimi & Joshi, 2018)	To develop unsupervised learning-based ABAC policy mining from access logs	Employed clustering methods to discern trends in access records and formulate ABAC rules	• Facilitates the automation of ABAC rule generation, reducing manual effort	• Limited scalability in distributed systems
(Paul & Sural, 2021)	To enhance ABAC assessment for emergency access to medical information	Adopted C-ND tree indexing for efficient high dimensional policy searches	• Effectively manages relaxed access for emergencies	• Computational Challenges in High dimensional Policy Contexts
(Perez-Haro & Diaz-Perez, 2024)	To design ABAC policy extraction	Uses Biclique analysis and synthetic data creation Constructed access logs as affiliation networks Derived graph-based ABAC rules	• Encompasses a greater array of resources with diminished regulations, preventing rule proliferation	• Demands expertise in graph theory for execution
(Z. Liu et al., 2020)	To propose CP-ABE for ABAC in EHRs	Incorporated encryption with ABAC features to enhance security and efficiency.	• Facilitates meticulous regulation of encrypted data	• Complex setup process • High computational overhead

Multi-Biometric Authentication: Integrating various biometric modalities (e.g., facial recognition, ear scans, iris scans, and fingerprints) enhances accuracy and mitigates spoofing concerns.

Lightweight and Economical Solutions: More focus will be placed on developing lightweight MFA systems in resource constrained environments, for example, rural health centers

IoT-specific MFA: The wide-scale use of IoT in healthcare calls for utilizing MFA systems specifically developed for IoT devices and remote access points to ensure a secure connection.

Regulatory Compliance and Standardization: Future MFA systems must conform to emerging rules such as HIPAA, GDPR, and HITRUST. Standardized frameworks for applying MFA in healthcare will diminish variability and improve interoperability.

Attribute-Based Access Control (ABAC)

ABAC is a robust access control mechanism that grants privileges according to attributes associated with individuals, assets and environmental contexts. It supports EHR systems in maintaining context awareness, safety and complaint access to personal healthcare information. ABAC policies can evaluate user roles, location, access time, and other dynamic characteristics to grant or restrict access. This ensures that healthcare personnel can only view information they are authorized to access.

A Fuzzy-extended ABAC (F-ABAC) method by Xu et al. (2018) is introduced to overcome the shortcomings of conventional ABAC systems in managing exceptional authorization requests. The system employed fuzzy assessment methods to gauge policy alignment and implemented supplementary credit mechanisms for risk reduction. It improves adaptability and functionality while preserving policy governance in fluctuating contexts.

A context-aware, predictive ABAC system by Psarra et al. (2022) is created for emergency EHR access. It uses LSTM neural networks to forecast patient parameters and incorporates fuzzy context handlers to assess critical circumstances. This effective technique improves emergency decision-making while protecting sensitive patient information.

A heuristic method for modifying ABAC policies is presented by Das et al. (2017) in inter-organizational healthcare cooperation. The research enhanced policy mining and adaption methods to reduce redundancy and policy disputes. However, scalability issues need to be addressed.

An advanced ABAC attribute mining system by Zhu et al. (2021) is presented for unstructured data environments with hybrid DL methodologies, specifically ROBERTA BiLSTM-CRF. The solution enhances the semantic precision of attribute extraction, facilitating superior decision-making in heterogeneous EHR systems.

The Polisma framework was proposed to synthesize ABAC policies from previous access histories (Abu Jabal et al. 2020). ML and data mining can automatically generate ABAC policies by reducing manual effort. It is centered on log-based learning, pointing to the relevance of previous knowledge in policy decisions.

Table 8. Blockchain Platforms

Blockchain Platform	Consensus Mechanism	Scalability	Privacy and security features	Smart Contract support	Suitability for EHR access control	Limitations
Ethereum	Proof of Stake (POS)	Moderate (Gas fees can be high)	Public Ledger Encryption Permissioned Access	Yes Solidity	Suitable for decentralized identity management Audit trails	• High transaction fees • Slower processing
Hyperledger Fabric	Byzantine Fault Tolerance (BFT)	High (Permissioned Network)	Strong Privacy controls Supports Permissioned Access	Yes (chaincode-based smart contract)	Ideal for secure, private EHR access control with compliance and regulations	• Requires trusted participants to set complexity
Solana	Proof of History + POS	High (speedy transactions)	Public ledger Cryptographic security	Yes (Rust, C-based smart contract)	Real-time EHR access tracking, secure and efficient health data transactions	• Less adoption in healthcare • Potential centralization risks
Corda	Notary-based consensus	High (Permissioned Network)	Private transactions between participants have strong encryption	Yes (CorDapps smart contract)	Inter-hospital EHR sharing Financial transaction	• Limited scalability
IPFS	No consensus	High (Decentralized storage)	Encrypted, content-addressed storage Immutable records	No (Used with blockchain for security)	EHR document storage	• Requires integration with blockchain for access control
EOS	Delegated Proof of Stake	High (fast block production	Smart contract-based access	Yes (Web Assembly smart contract)	Suitable for high-speed large-scale healthcare organizations	• More centralized
Algorand	Pure Proof of Stake	High	Privacy enhanced transactions Permissioned access	Yes (TEAL-based smart contract)	Real-time secure transactions in EHR systems	• Limited adoption in healthcare

ABAC-SC, an attribute-based access control system implemented on blockchain (Ma et al., 2019), was proposed to securely share electronic health records (EHRs) among organizations. The scheme employs Ethereum smart contracts to provide immutable access logs, thereby increasing flexibility and trust in organizational data exchange.

A secure cloud-based ABAC system for EHRs was proposed by Wang and Song (2018) through the integration of attribute-based encryption (ABE) with blockchain technology. The system provides fine-grained access control and immutable logging, fulfilling essential data integrity and transparency requirements in cloud-based EHR environments.

An integrated ABAC model with honey-based deception strategies was introduced by Alohaly et al. (2022) to enhance protection against insider attacks in EHR systems. The combination of cyber-deception techniques and ABAC policies enables real-time detection of malicious behavior, offering an innovative approach to mitigating insider threats.

Abou et al. (2019) automated the development of ABAC rules by applying process-mining techniques. Their approach streamlined ABAC implementation in healthcare environments by extracting policies from event logs, thereby reducing the need for manual configuration.

A model-based testing framework for ABAC policies with obligation constraints was presented by Khamaiseh et al. (2018). The framework improves ABAC policy implementation by identifying faults and execution issues; however, it does not specifically address healthcare applications.

Ait El Hadj et al. (2017) aimed to reduce the complexity of ABAC rules by applying similarity-based computation methods. The use of k-nearest neighbors (KNN) clustering to group ABAC policies facilitated redundancy removal and improved system efficiency.

S. A. B. et al. (2023) investigated the use of the Hyperledger Fabric blockchain platform to implement ABAC in EHR systems. Their approach enhanced security, transparency, and compliance with HIPAA requirements, although scalability in large-scale healthcare environments was not thoroughly evaluated.

Cappelletti et al. (2019) evaluated machine learning techniques for extracting ABAC policies by employing dimensionality-reduction methods such as principal component analysis (PCA) and t-distributed stochastic neighbor embedding (t-SNE). The proposed automated policy-inference approach streamlined policy formulation but was highly dependent on the quality of the training data.

Karimi and Joshi (2018) proposed an unsupervised clustering algorithm to extract ABAC policies from access records. By analyzing behavioral patterns, the approach automated ABAC rule generation and reduced administrative effort; however, scalability in distributed healthcare systems remained a limitation.

The C-ND Tree indexing method (Paul & Sural, 2021) is introduced to enhance ABAC policy evaluation for healthcare emergencies. This system effectively manages high-dimensional policies and facilitates rapid access in urgent situations. However, it encountered difficulties in complicated environments.

Paul and Sural (2021) introduced the C-ND tree indexing method to improve ABAC policy evaluation in healthcare emergency scenarios. The method efficiently manages high-dimensional policies and supports rapid access during critical situations, although it encounters challenges in complex environments.

Perez-Haro and Diaz-Perez (2024) applied biclique analysis to extract ABAC policies from access records modeled as affiliation networks. Their approach reduced rule redundancy and covered a large number of resources with fewer policies, thereby improving scalability in dynamic environments.

Liu et al. (2020) proposed integrating ciphertext-policy attribute-based encryption (CP-ABE) with ABAC for EHR systems to provide strict control over encrypted data and enhance privacy and security. However, the approach requires substantial computational resources and specialized expertise for deployment.

Challenges in ABAC Techniques

High computational complexity: Techniques like F-ABAC and DL-based attribute mining are computationally intensive, limiting their scalability in real-time healthcare applications.

Rule explosion and redundancy: Governing large policy sets leads to redundancy and wastage, which can be observed in manual and unsupervised learning.

Scalability in Distributed Systems: Alternatives based on blockchain face latency and storage constraints, making them less suitable for widespread EHR applications.

Lack of interoperability standards: Inter-organizational ABAC systems need standardized frameworks for effective policy enforcement.

Dependence on Data Integrity: ML and process mining techniques heavily depend on proper, high-quality data logs, which may not be readily available.

Intricacy during Emergencies: Context-sensitive systems often face difficulties balancing the speed of decision making with security during emergencies.

New Trends in ABAC Techniques

Incorporation of Next-Generation AI Models: Next-generation ML and AI models will be critical in policy automation and enhancing context-aware decision making, adaptability, and scalability.

Blockchain for assurance and clarity: Using efficient blockchain-based ABAC systems is expected to offer immutable logging and decentralized governance.

Lightweight, efficient models: The emphasis will transition to lightweight ABAC solutions tailored for resource-limited contexts, such as IoT-enabled healthcare systems.

Standardization for interoperability: Developing universal frameworks guarantees seamless enforcement of ABAC policies across various healthcare institutions.

Dynamic and Real-time policies: Adaptive ABAC system utilizing behavioral analytics and real-time contextual data will improve security and usability in crises.

Advanced Privacy Mechanisms: Privacy-preserving ABAC approaches incorporating encryption will be crucial for adhering to legislation such as HIPAA and GDPR.

The current ABAC data access and retrieval mechanisms in EHR systems demonstrate the potential for fine-grained, context-aware, and dynamic access control. ABAC leverages attributes related to users, resources, and environmental factors to address complex situations, such as emergency data access, inter-organizational data sharing and insider threat mitigation. Integrating newer technologies like blockchain, ML, and fuzzy logic has greatly enhanced ABAC's potential to handle dynamic access requirements. Despite its advantages, ABAC implementations have considerable obstacles in scalability, computational efficiency, and practical adoption within healthcare settings.

Blockchain-Based Access Control (BBAC)

Before discussing BBAC, it is important to know the most popular blockchain platforms that enable secure decentralized access in EHR systems. Blockchain technology provides an immutable, tamper-evident, transparent platform for controlling access to healthcare information. However, most platforms offer different capabilities, security models, and scalable solutions.

Table 9 summarizes the comparison of the most commonly used blockchain platforms for access control in EHR systems, focusing on key features such as consensus mechanisms, scalability, privacy, and suitability for healthcare applications.

Numerous blockchain platforms provide secure access control. Criteria including scalability, transaction velocity, interoperability, and consensus protocols determine the selection of a blockchain platform.

The subsequent phase involves examining the application of these technologies to manage, authenticate, and regulate user access to sensitive healthcare data via BBAC Control mechanisms.

Existing methods for BBAC are:

Guo et al. (2019) proposed a hybrid edge-computing blockchain framework for secure EHR access control. Hyperledger Composer was employed to implement identity management and immutable logging, thereby enhancing data traceability and security in healthcare systems. By offloading computational tasks to edge nodes, the hybrid architecture reduced latency and proved suitable for mid-scale healthcare networks; however, its scalability for large-scale health networks remains unaddressed.

Nguyen et al. (2019) developed a blockchain-based secure EHR sharing system for mobile cloud platforms. The study utilized the Ethereum blockchain for access policy management and the InterPlanetary File System (IPFS) for decentralized data storage, improving data privacy and reducing latency in mobile environments. Nevertheless, efficiency and scalability limitations were observed when handling large datasets.

Chen et al. (2024) introduced a multidimensional access-control framework for elderly care within EHR systems using Ethereum. The framework integrates ciphertext-policy attribute-based encryption (CP-ABE) with token-based authorization to support flexible access policies and secure data exchange. Despite its strong privacy guarantees, the framework incurs significant computational and temporal overhead due to the complexity of multidimensional controls.

Yakubu et al. (2024) presented a patient-centered blockchain framework for managing infectious-disease test records. Implemented on Hyperledger Fabric, the system enables granular access control while ensuring patient privacy and regulatory compliance. Although the framework demonstrates robust security and reduced latency, its applicability to large-scale healthcare infrastructures requires further validation.

Boumezbeur and Zarour (2022) examined a privacy-preserving EHR sharing system based on Ethereum. The approach employs cryptographic primitives to ensure secure data transfer and encryption across varying file sizes. However, increased computational complexity when managing large datasets was identified as a limitation.

Sonkamble et al. (2023) proposed a blockchain–IPFS architecture for patient-centric EHR management using Hyperledger Fabric. Smart contracts enforce access policies, while IPFS supports decentralized data storage. The integration of SPAKE encryption enhances security; however, the system lacks validation in real-world healthcare environments.

Gupta et al. (2022) introduced a blockchain-based EHR system that combines role-based access control (RBAC) with IPFS for secure data storage. The framework supports efficient data retrieval and sharing while maintaining data integrity, although ambiguity regarding the underlying blockchain platform limits reproducibility.

Walid et al. (2023) investigated semantically robust differential access control for secure cloud-based EHR systems. By integrating Ethereum with semantic attributes and differential access policies, the approach enables privacy-preserving and fine-grained access control. Nonetheless, the computational overhead associated with semantic processing was identified as a key challenge.

Table 9: Existing Techniques on BBAC

Authors/ Blockchain Platform	Objective	Methodology	Advantages	Limitations
(Guo et al., 2019)/ Hyperledger Composer	To establish a hybrid blockchain edge framework for secure EHR access control	Blockchain controller for access regulations utilizing off-chain storage on edge nodes	• Offers secure logging • Instantaneous performance monitoring	• Limited to small-scale healthcare setup
(Nguyen et al., 2019)/ Ethereum	To ensure the secure sharing of EHRs in mobile cloud environments	Smart contract integrating blockchain and IPFS	• Lightweight access control • Data privacy	• High dependency on mobile cloud network reliability
(Chen et al., 2024)/ Ethereum	To develop flexible and fine-grained access control for elderly healthcare services	CP-ABE with blockchain	• Supports privacy-preserving access for elderly patients	• Computationally expensive encryption schemes
(Yakubu et al., 2024)/ Hyperledger Fabric	To develop a granular access control for infectious disease-related test records	Blockchain framework with smart contracts for patient consent and access	• Highly scalable • Privacy preservation	• Limited focus on integration with existing healthcare IT systems
(Boumezbeur & Zarour, 2022) / Ethereum	To design a privacy-preserving framework for EHR sharing using blockchain	Smart contract with cryptographic algorithms	• Secure against tampering and unauthorized access	• High computation cost for encryption and decryption process
(Sonkamble et al., 2023) / Hyperledger Fabric	To securely retrieve EHR data	Smart contract with SPAKE encryption	• Improves patient-centric access and encryption	• Computational overhead for SPAKE encryption
(Gupta et al., 2022)/ Not Mentioned	To develop blockchain with RBAC for EHR systems	Integrated blockchain and IPFS for data storage and retrieval	• Simplifies EHR storage and retrieval process	• Requires optimization for high throughput environments
(Walid et al., 2023)/ Ethereum	To develop semantically rich differential access control for secure cloud EHR	Integrated blockchain with semantic attributes and differential policies for fine-grained access control	• Ensures privacy-preserving access and efficient retrieval	• Requires high computational resources for semantic matching and blockchain processes
(Alahmadi et al., 2021)	To build a web service-based health record retrieval system	Centralized access control framework for secure EHR retrieval using REST APIs	• Simplifies retrieval processes for end users	• Does not utilize decentralized or immutable blockchain protocols.

(Chinnasamy & Deepalakshmi, 2022)	TO design HCAC for EHR retrieval in the cloud	Combined symmetric and asymmetric cryptography with blockchain for secure retrieval	• Enhances security using hybrid cryptography	• Computationally complex
(Walid et al., 2020)/ Ethereum	To design a cloud-based encrypted EHR system with semantically rich access	Blockchain for policy enforcement Searchable encryption for efficient EHR retrieval	• Ensures privacy and transparency • Search over encrypted records	• High resource utilization for searchable encryption • Policy enforcement on large datasets.

Alahmadi et al. (2021) introduced a web service–oriented EHR retrieval system based on a centralized architecture. The system employed RESTful APIs to streamline data retrieval operations for healthcare providers. While effective for small-scale deployments, the absence of blockchain integration limits its suitability for decentralized healthcare environments.

Chinnasamy and Deepalakshmi (2022) presented a hybrid cryptographic access control (HCAC) approach for secure EHR retrieval in cloud-based settings. The framework integrates symmetric and asymmetric encryption techniques to enhance data security. However, the increased computational complexity associated with hybrid cryptographic operations was identified as a key limitation.

Walid et al. (2020) proposed a cloud-based encrypted EHR system featuring semantically rich access control mechanisms. The system utilizes Ethereum for policy enforcement and searchable encryption to enable secure and efficient data retrieval. Despite its strong privacy guarantees, the framework requires substantial computational resources, which may hinder scalability.

Table 10 summarizes the existing works in BBAC mechanisms for data access and retrieval in EHR systems.

Challenges in Blockchain-Based Access Control

Scalability: Blockchain networks, particularly public blockchains like Ethereum, encounter difficulties processing extensive healthcare datasets due to elevated transaction costs and restricted throughput. Managing increasing data volumes in healthcare presents a challenge for systems integrating IPFS and blockchain.

High computational and Energy costs: Cryptographic systems like CP-ABE, zero-knowledge proofs, and smart contracts impose considerable computational burden. Resource-intensive blockchain platforms may be impractical for resource-limited situations.

Latency concerns: Blockchain transactions like mining and consensus validation result in necessary delays in medical situations where immediate availability is typically demanded.

Legacy System Integration: Most health organizations use non-compatible systems for blockchain platforms, making adoption non-viable. *Regulatory and Privacy issues:* It can be difficult to maintain decentralization while complying with HIPAA, GDPR, and HITRUST. Safeguarding sensitive information during metadata storage on blockchain necessitates sophisticated privacy-preserving techniques.

User Adoption and Usability: The complexity of blockchain technologies may impede their adoption by healthcare practitioners and patients.

Future trends in Blockchain-based Access Control

Hybrid Models: Implementing hybrid blockchain architectures that integrate public and private blockchains (e.g., Ethereum with Hyperledger Fabric) will enhance scalability, cost efficiency, and security. Integration with off-chain storage systems like IPFS or distributed cloud solutions would significantly improve performance.

AI-Driven Blockchain Systems: Blockchain will be integrated with ML models to create dynamic and predictive access control policies based on user behavior and context.

Interoperability Standards: New standards and frameworks will enable easy integration of blockchain technology with current healthcare infrastructure and other organizations.

Lightweight Cryptography: The study will optimize cryptographic operations in order to decrease computing costs at the expense of security, specifically for IoT and edge devices in the healthcare sector.

Privacy-Preserving Approaches: Homomorphic encryption, differential privacy, and zero-knowledge

proofs will protect privacy and meet regulatory requirements.

Decentralized Identity Management: Blockchain-based identity management will enable patients to manage their information using SSIs, where they can securely grant or withdraw access.

Tokenization for Access to Data: Blockchain tokens will represent access rights and encourage the safe sharing of healthcare information.

Collaborative Regulation: Blockchain developers will collaborate with the government and regulatory bodies to create compliance-based blockchain structures specifically tailored for healthcare networks.

BBAC is a novel model of healthcare data management with greater security, transparency and interoperability. Breaking scalability, privacy and usability barriers will be pivotal to broad adoption. Innovation in hybrid models, light weight cryptography and privacy-preserving protocols positions blockchain to revolutionize EHR systems, making patient-centered, secure and efficient healthcare delivery possible.

Table 10. Types Of Interoperability, Description, Technology Used, Advantages and Challenges

Types of interoperability	Description	Technology used	Advantages	Challenges
Semantic	Guarantees that the significance of shared data is maintained and uniformly comprehended by various systems	Terminologies like SNOMED CT, LOINC standards like FHIR	• Assists accurate clinical decision making	• It entails complete standardization across institutions
Syntactic	Concentrates on the format and structure of shared data, guaranteeing that systems can interpret and process the transmitted information	Message format: HL7, FHIR Data scheme: XML, JSON	• Enables data processing and exchange between systems	• Lacks semantic context
Decentralized	Data sharing does not rely on a central authority and uses blockchain technology.	Blockchain, smart contracts, IPFS	• Improves security, privacy and auditability	• Resource intensive • Computationally expensive
Real-time	Facilitates immediate data sharing and processing to provide prompt reactions in clinical environments	High speed networks Middleware solutions Edge computing	• Facilitates crucial applications like emergency care and remote monitoring	• High bandwidth • Invest in significant infrastructure
Centralized	It depends on the central authority or repository to standardize and manage data sharing across systems.	HIE, centralized databases	• Eases standardization and governance	• Single Point of Failure • Centralized security breaches
System-level	Focuses on the technical integration of heterogeneous systems to facilitate seamless data transfer and interaction among platforms, applications and devices	Protocol Translators Middleware APIs	• Enables communication between heterogeneous systems and applications	• Resource intensive • Complex integration process
Structured Data	Focuses on sharing structured data	Structured formats: XML, JSON Standards: FHIR, HL7, DICOM	• Permits automated data processing and retrieval	• Does not handle unstructured or semi-structured data.

Data Sharing and Interoperability

They enable seamless and coordinated care between healthcare organizations. Interoperability enables effective exchange and understanding of patient data regardless of the technology used by various providers. This enables improved clinical decision-making, eliminates redundant tests, and encourages holistic patient care.

EHR interoperability can be categorized into various core types, each focusing on specific data sharing and integration aspects. EHR systems can build a robust framework for unhampered, secure and meaningful data exchange, supporting improved patient care and operational efficiency among healthcare organizations.

Table XI below depicts the types of interoperability, the technology used, and the advantages and challenges.

Essential facilitators of interoperability comprise standards such as HL7, FHIR and DICOM with frameworks like HIEs that define data sharing protocols. Recent innovations, including blockchain integration have augmented data exchange security and trustworthiness by offering immutable records and decentralized access. Apart from its significance, attaining genuine interoperability encounters obstacles like technology diversity, privacy issues, and regulatory limitations.

Existing methods in Data sharing and Interoperability are:

Sonkamble et al. (2021) investigated blockchain-based interoperability for EHR systems using the Ethereum platform in combination with off-chain storage solutions. The proposed approach enabled secure data sharing across heterogeneous healthcare systems while ensuring semantic interoperability. Although privacy was enhanced through cross-chain data exchange, the high computational costs associated with Ethereum transactions remained a significant challenge.

Reegu et al. (2023) introduced a blockchain-based framework that incorporates Fast Healthcare Interoperability Resources (FHIR) standards to enable secure and interoperable EHR sharing. The system ensures compliance with HIPAA regulations and supports both semantic and syntactic interoperability across healthcare platforms. However, high implementation and deployment costs were identified as major barriers to adoption.

Jabbar et al. (2020) proposed BiiMEd, a blockchain-based platform designed to improve EHR interoperability and data integrity. The framework employs dynamic verification mechanisms to support decentralized data sharing, providing tamper-resistant audit trails and secure inter-provider communication. Nevertheless, the resource-intensive nature of blockchain technologies raises scalability concerns for large-scale deployment.

Najjar et al. (2022) presented an FHIR-based interoperability framework that integrates artificial intelligence techniques to standardize unstructured EHR data. The system effectively processes heterogeneous data formats while maintaining compliance with interoperability standards. Despite its effectiveness, the high computational requirements of AI-driven data mapping limit scalability and real-time applicability.

Dagliati et al. (2021) demonstrated an interoperability framework for EHR sharing aimed at supporting healthcare systems during the COVID-19 pandemic. The solution enabled real-time data exchange across institutions, thereby enhancing analytics and collaborative research for public health emergency management.

Margheri et al. (2020) designed a blockchain-enabled platform to manage shared EHR data provenance. By adhering to FHIR and HL7 standards, the platform achieved semantic and syntactic interoperability while providing transparent and immutable audit trails. However, real-time provenance tracking introduced additional system overhead.

Zhang et al. (2018) proposed FHIRChain, a blockchain-based system that integrates FHIR standards to support secure and scalable healthcare data sharing. The framework ensures semantic and syntactic interoperability while enabling decentralized, tamper-resistant data exchange.

Anand and Sadhna (2023) examined the integration of blockchain-based decentralized access control with FHIR standards to enhance semantic interoperability and support clinical research. Although the approach addresses critical challenges related to data security and sharing, the lack of empirical validation limits its practical applicability.

George and Chacko (2022) introduced a patient-centric EHR framework that integrates the Quorum blockchain with FHIR standards. The system facilitates secure and authorized data exchange while supporting semantic interoperability. Despite emphasizing patient autonomy and confidentiality, comprehensive validation across diverse healthcare ecosystems remains necessary.

Warren et al. (2019) analyzed inter-hospital data exchange practices in England using standardized EHR systems to improve care continuity and patient outcomes. The study identified regional disparities in EHR adoption as a major obstacle to scalable interoperability across institutions.

Dubovitskaya et al. (2020) proposed a patient-centered blockchain framework based on Hyperledger Fabric for secure EHR sharing in oncology. By integrating FHIR standards, the framework supports semantic interoperability and patient-controlled data access. However, scalability across multi-institutional healthcare networks has not yet been fully validated.

Quintero et al. (2024) presented a blockchain-integrated EHR sharing system that leverages FHIR standards to enhance semantic interoperability. The framework enables secure and decentralized data exchange while ensuring regulatory compliance. Nonetheless, the substantial computational overhead associated with blockchain integration remains a key limitation.

Table 11 summarizes the existing techniques in data sharing and interoperability.

The current methods for data sharing and interoperability in EHR systems exhibit considerable progress in tackling the issues of secure and efficient data interchange among healthcare organizations. Crucial technologies such as blockchain, FHIR standards, HIEs and middleware solutions have facilitated semantic and syntactic interoperability. Although these strategies have enhanced care coordination and regulatory compliance, issues like scalability, processing overhead, and the absence of worldwide standardization remain to be addressed.

Challenges in Data Sharing and Interoperability

Computational Overhead: Methods like AI, ML, DL and blockchain need substantial processing resources, complicating real-time interoperability, especially for resource-limited organizations.

Table 11. Existing Techniques on Data Sharing and Interoperability

Authors	Objective	Technique	Interoperability capabilities	Advantages	Limitations
(Sonkamble et al., 2023)	To facilitate privacy-preserving interoperable EHR sharing	Blockchain and off-chain storage solutions	• Enhances semantic interoperability • Enables cross-chain data exchange	• Improves privacy and access control	• High computational costs for Ethereum transactions
(Reegu et al., 2023)	To design an interoperable framework for EHR sharing	Blockchain + FHIR	• Integrates FHIR standards for semantic and syntactic interoperability. • Facilitate data exchange among various systems. • Blockchain guarantees decentralized, tamper-proof sharing.	• Ensures security • Standardized data sharing	• High deployment • Costs for large-scale systems
(Jabbar et al., 2020)	To develop a framework for interoperability and integrity	Blockchain + BiiMED	• Offers decentralized interoperability • Guarantees data consistency across providers • Enable dynamic data verification	• Immutable audit trails • Improved cross-institutional sharing	• Resource intensive for large-scale systems • High computational requirements.

(Najjar et al., 2022)	To utilize AI to standardize unstructured EHR data for seamless sharing across systems.	FHIR with AI	• FHIR for syntactic interoperability • Uses AI for mapping unstructured data to standardized formats	• Support heterogeneous systems. • Improves interoperability using AI-based data standardization	• Significant computational resource requirements for real-time AI driven data preprocessing
(Dagliati et al., 2021)	To develop a collaborative framework for EHR sharing	Collaborative data infrastructures	• Assists in real-time interoperability between institutions, enabling shared research and analytics	• Facilitates real-time data sharing for coordinated care and research purposes	• Limited verification in non-pandemic or general healthcare applications
(Margheri et al., 2020)	To ensure transparency and manage the provenance of shared EHR data	Blockchain-based provenance	• Uses FHIR and HL7 standards to aid semantic and syntactic interoperability for provenance tracking and data integrity	• Improves traceability and auditability. • Ensure tamper proof EHR data.	• Increased overhead resulting from real-time provenance monitoring and supplementary metadata administration.
(P. Zhang et al., 2018)	To combine blockchain and FHIR for scalable and secure clinical data sharing	FHIR chain	• Facilitates semantic and syntactic interoperability with FHIR standards and blockchain technology for data exchange	• Decentralized scalable, secure clinical data sharing	• High energy consumption for blockchain implementation
(Anand & Sadhna, 2023)	To investigate the combination of blockchain and FHIR for clinical research and interoperability	Blockchain + FHIR	• Blends semantic interoperability with blockchain decentralized access control for secure EHR sharing	• Enhances data standardization and research efficiency	• Integration at an early stage • Limited real-time implementation in healthcare systems
(George & Chacko, 2022)	To build a patient-centric interoperable	Quorum blockchain+FHIR	• Permissioned blockchain facilitates secure HER sharing • FHIR provides	• Assists patient-centric control and privacy. • Supports secure structured EHR sharing	• Lacks validation in multi-institutional networks
(Warren et al., 2019)	To develop data sharing between hospitals	Inter-hospital data sharing	• Establishes uniformity in structured data interoperability among institutions to provide continuity of care	• Improves continuity of care via superior data sharing methods	• The regional misalignment of EHR systems constrains scalability across all institutions

(Dubovitskaya, Baig, et al., 2020)	To design a patient-centric blockchain for secure EHR sharing	Blockchain	• Implements FHIR standards for interoperability between hospitals	• Decentralized patient-centric access control • Data integrity	• Limited scalability for multi-institutional networks
(Quintero et al., 2024)	To enhance data sharing using blockchain and semantic standards	Blockchain +FHIR	• Semantic interoperability • Secure decentralized data sharing	• Increases semantic knowledge sharing across healthcare	• High computational overhead for blockchain implementation

Technical Heterogeneity: Interoperability is hindered by different data formats and system architectures between institutions. Non–uniform adoption standards like FHIR and HL7 lead to fragmentation in healthcare systems.

Implementation cost: Developing sophisticated technology for middleware solutions is expensive for small healthcare facilities, limiting its extensive implementation.

Regulatory and policy barriers: Compliance with different national and international regulations prevents data exchange owing to the varied requirements across jurisdictions. Establishing agreements among healthcare institutions on a shared infrastructure continues to be problematic.

Future Trends in Data Sharing and Interoperability

Hybrid Systems: Blending public and private blockchains with cloud storage will give a cost-effective and scalable system for secure decentralized data sharing.

AI-based Interoperability: Advances in AI and ML technologies will automate data standardization and mapping, making sharing heterogeneous and unstructured data between platforms more seamless.

Adoption of International standards: International interoperability standards like FHIR, HL7 and DICOM would enable standardized data exchange and semantic understanding between systems.

Lightweight Cryptographic Methods: Efficient cryptographic methods, including homomorphic encryption and differential privacy, will minimize computational complexity while guaranteeing secure data transmission.

Real-time Interoperability: Edge computing and middleware technologies will facilitate faster and more efficient data sharing, facilitating real-time care coordination and decision support.

Blockchain Interoperability: Cross-chain solutions will become interoperable with all blockchain systems, increasing information flow among healthcare organizations with different systems.

Regulatory collaboration: Governments and healthcare organizations will collaborate to establish regulatory standards and incentives for deploying interoperable systems.

Conclusion

Healthcare data breaches, unauthorized access, and cyber-attacks pose significant risks; therefore, privacy and security are crucial in successfully implementing EHRs. As EHRs hold vast sensitive patient data, robust security controls must be applied to protect data confidentiality, integrity, and availability, thus maintaining patient confidence and regulatory compliance.

The study reviewed current approaches in various stages of EHR workflows, including encryption, blockchain, cloud security, RBAC, ABAC, BBAC, MFA, and interoperability standards like FHIR and HL7. These approaches improve data protection and present challenges like scalability, interoperability limitations, cyber security threats, and regulatory limitations.

Future research in EHR workflow security needs to address scaling concerns, enhance interoperability frameworks, and develop AI-based access control systems that adaptively change security depending on user behavior. Quantum-resistant cryptography, blockchain identity management and Federated Learning are new trends with the potential to boost EHR security and privacy. Zero-trust architectures will reduce insider threats by continuously verifying access requests.

Healthcare organizations must develop multi-layered security policies, carry out regular security audits, and implement privacy-preserving interoperability

frameworks to retain patient confidence and compliance with regulatory requirements. Based on upcoming technology trends, the healthcare industry can build a secure, scalable, and privacy-oriented EHR ecosystem in the future.

Acknowledgement

The authors gratefully acknowledge the University Visvesvaraya College of Engineering (UVCE), Bangalore University, Bangalore, Karnataka, India for providing the necessary resources, access to relevant materials and data sources, and the infrastructure that supported the successful completion of this work.

Funding Information

The authors have not received any financial support or funding.

Author Contributions

All authors contributed to the conceptualization, analysis, and preparation of the manuscript and approved the final version for publication.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and there are no ethical issues involved.

References

Abou, R., Amani, and A., Nour, and G., & Walid. (2019). *Extracting Attribute-Based Access Control Rules from Business Process Event Logs*.

Abu Jabal, A., Bertino, E., Lobo, J., Law, M., Russo, A., Calo, S., & Verma, D. (2020). Polisma—A Framework for Learning Attribute-Based Access Control Policies. In L. Chen, N. Li, K. Liang, & S. Schneider (Eds.), *Computer Security – ESORICS 2020* (Vol. 12308, pp. 523–544). Springer International Publishing. https://doi.org/10.1007/978-3-030-58951-6_26

Ait El Hadj, M., Benkaouz, Y., Freisleben, B., & Erradi, M. (2017). ABAC Rule Reduction via Similarity Computation. In A. El Abbadi & B. Garbinato (Eds.), *Networked Systems* (Vol. 10299, pp. 86–100). Springer International Publishing. https://doi.org/10.1007/978-3-319-59647-1_7

Alahmadi, R., Almimony, S., Bahakeem, R., & Alnahdi, A. (2021). Health Records Retrieval System: A Web-Service Approach. *2021 5th International Conference on Medical and Health Informatics*, 145–149. https://doi.org/10.1145/3472813.3473181

Albarki, I., Rasslan, M., Bahaa-Eldin, A. M., & Sobh, M. (2019). Robust Hybrid-Security Protocol for HealthCare Systems. *Procedia Computer Science*, *160*, 843–848. https://doi.org/10.1016/j.procs.2019.11.001

Alghamdi, T., Gebali, F., & Salem, F. (2022). Multifactor Authentication for Smart Emergency Medical Response Transporters. *International Journal of Telemedicine and Applications*, *2022*, 1–17. https://doi.org/10.1155/2022/5394942

Alohaly, M., Balogun, O., & Takabi, D. (2022). Integrating Cyber Deception Into Attribute-Based Access Control (ABAC) for Insider Threat Detection. *IEEE Access*, *10*, 108965–108978. https://doi.org/10.1109/ACCESS.2022.3213645

ALSaleem, B. O., & Alshoshan, A. I. (2021). Multi-Factor Authentication to Systems Login. *2021 National Computing Colleges Conference (NCCC)*, 1–4. https://doi.org/10.1109/NCCC49330.2021.9428806

Al-Slais, Y. (2020). Privacy Engineering Methodologies: A survey. *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)*, 1–6. https://doi.org/10.1109/3ICT51146.2020.9311949

Anand, G., & Sadhna, D. (2023). Electronic health record interoperability using FHIR and blockchain: A bibliometric analysis and future perspective. *Perspectives in Clinical Research*, *14*(4), 161–166. https://doi.org/10.4103/picr.picr_272_22

Bauer, J. C., John, E., Wood, C. L., Plass, D., & Richardson, D. (2020). Data Entry Automation Improves Cost, Quality, Performance, and Job Satisfaction in a Hospital Nursing Unit. *JONA: The Journal of Nursing Administration*, *50*(1), 34–39. https://doi.org/10.1097/NNA.0000000000000836

Bhatt, V., Li, J., & Maharjan, B. (2021). DocPal: A Voice-based EHR Assistant for Health Practitioners. *2020 IEEE International Conference on E-Health Networking, Application & Services (HEALTHCOM)*, 1–6. https://doi.org/10.1109/HEALTHCOM49281.2021.9399013

Boumezbeur, I., & Zarour, K. (2022). Privacy Preservation and Access Control for Sharing Electronic Health Records Using Blockchain Technology. *Acta Informatica Pragensia*, *11*(1), 105–122. https://doi.org/10.18267/j.aip.176

Butt, A. U. R., Mahmood, T., Saba, T., Bahaj, S. A. O., Alamri, F. S., Iqbal, M. W., & Khan, A. R. (2023). An Optimized Role-Based Access Control Using Trust Mechanism in E-Health Cloud Environment. *IEEE Access*, *11*, 138813–138826. https://doi.org/10.1109/ACCESS.2023.3335984

Cappelletti, L., Valtolina, S., Valentini, G., Mesiti, M., & Bertino, E. (2019). On the Quality of Classification Models for Inferring ABAC Policies from Access Logs. *2019 IEEE International Conference on Big Data (Big Data)*, 4000–4007. https://doi.org/10.1109/BigData47090.2019.9005959

Chen, D., Zhang, L., Liao, Z., Dai, H.-N., Zhang, N., Shen, X., & Pang, M. (2024). Flexible and Fine-Grained Access Control for EHR in Blockchain-Assisted E-Healthcare Systems. *IEEE Internet of Things Journal*, *11*(6), 10992–11007. https://doi.org/10.1109/JIOT.2023.3328382

Cheng, A. C., Banasiewicz, M. K., Johnson, J. D., Sulieman, L., Kennedy, N., Delacqua, F., Lewis, A. A., Joly, M. M., Bistran-Hall, A. J., Collins, S., Self, W. H., Shotwell, M. S., Lindsell, C. J., & Harris, P. A. (2023). Evaluating automated electronic case report form data entry from electronic health records. *Journal of Clinical and Translational Science*, *7*(1), e29. https://doi.org/10.1017/cts.2022.514

Cherif, E., Bezaz, N., & Mzoughi, M. (2021). Do personal health concerns and trust in healthcare providers mitigate privacy concerns? Effects on patients' intention to share personal health data on electronic health records. *Social Science & Medicine*, *283*, 114146. https://doi.org/10.1016/j.socscimed.2021.114146

Chinnasamy, P., & Deepalakshmi, P. (2022). HCAC-EHR: Hybrid cryptographic access control for secure EHR retrieval in healthcare cloud. *Journal of Ambient Intelligence and Humanized Computing*, *13*(2), 1001–1019. https://doi.org/10.1007/s12652-021-02942-2

Chong, K. M. (2021). Privacy-preserving healthcare informatics: A review. *ITM Web of Conferences*, *36*, 04005. https://doi.org/10.1051/itmconf/20213604005

Dagliati, A., Malovini, A., Tibollo, V., & Bellazzi, R. (2021). Health informatics and EHR to support clinical research in the COVID-19 pandemic: An overview. *Briefings in Bioinformatics*, *22*(2), 812–822. https://doi.org/10.1093/bib/bbaa418

Das, S., Sural, S., Vaidya, J., & Atluri, V. (2017). Policy Adaptation in Attribute-Based Access Control for Inter-Organizational Collaboration. *2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC)*, 136–145. https://doi.org/10.1109/CIC.2017.00028

De Carvalho Junior, M. A., & Bandiera-Paiva, P. (2020). Strengthen Electronic Health Records System (EHR-S) Access-Control to Cope with GDPR Explicit Consent. *Journal of Medical Systems*, *44*(10), 172. https://doi.org/10.1007/s10916-020-01631-5

De Carvalho, M. A., & Bandiera-Paiva, P. (2017). Evaluating ISO 14441 privacy requirements on role based access control (RBAC) restrict mode via Colored Petri Nets (CPN) modeling. *2017 International Carnahan Conference on Security Technology (ICCST)*, 1–8. https://doi.org/10.1109/CCST.2017.8167833

Dr. T., P., S., P., E., P., & J., P. (2019). Data Sharing with Sensitive Information Hiding for Secure Cloud Storage. *International Journal of Engineering Research and Technology*, *7*.

Dubovitskaya, A., Baig, F., Xu, Z., Shukla, R., Zambani, P. S., Swaminathan, A., Jahangir, M. M., Chowdhry, K., Lachhani, R., Idnani, N., Schumacher, M., Aberer, K., Stoller, S. D., Ryu, S., & Wang, F. (2020). ACTION-EHR: Patient-Centric Blockchain-Based Electronic Health Record Data Management for Cancer Care. *Journal of Medical Internet Research*, *22*(8), e13598. https://doi.org/10.2196/13598

Dubovitskaya, A., Novotny, P., Xu, Z., & Wang, F. (2020). Applications of Blockchain Technology for Data-Sharing in Oncology: Results from a Systematic Literature Review. *Oncology*, *98*(6), 403–411. https://doi.org/10.1159/000504325

Ettaloui, N., Arezki, S., & Gadi, T. (2023). An Overview of Blockchain-Based Electronic Health Records and Compliance with GDPR and HIPAA. *Data and Metadata*, *2*, 166. https://doi.org/10.56294/dm2023166

Fakroon, M., Gebali, F., & Mamun, M. (2021). Multifactor authentication scheme using physically unclonable functions. *Internet of Things*, *13*, 100343. https://doi.org/10.1016/j.iot.2020.100343

Gandhi, N., & Patil, K. (2023). Understanding the Users' Intention to Use the Three-Factor Authentication for Preserving the Privacy of Patient Data. *Journal of Applied Security Research*, *18*(3), 597–626. https://doi.org/10.1080/19361610.2022.2060025

George, M., & Chacko, A. M. (2022). A Patient-Centric Interoperable, Quorum-based Healthcare System for Sharing Clinical Data. *2022 International Conference for Advancement in Technology (ICONAT)*, 1–6. https://doi.org/10.1109/ICONAT53423.2022.9725924

Gope, P., & Amin, R. (2016). A Novel Reference Security Model with the Situation Based Access Policy for Accessing EPHR Data. *Journal of Medical Systems*, *40*(11), 242. https://doi.org/10.1007/s10916-016-0620-4

Guo, H., Li, W., Nejad, M., & Shen, C.-C. (2019). *Access Control for Electronic Health Records with Hybrid Blockchain-Edge Architecture* (Version 1). arXiv. https://doi.org/10.48550/ARXIV.1906.01188

Gupta, A., Rodrigues, R., Tripathi, A., Coutinho, R., & Gomes, J. (2022). Blockchain for EHR: An off-chain based approach. *2022 IEEE Region 10 Symposium (TENSYMP)*, 1–6. https://doi.org/10.1109/TENSYMP54529.2022.9864405

Hamed, N., & Yassin, A. (2023). A Privacy-Preserving Scheme for Managing Secure Data in Healthcare System. *Iraqi Journal for Electrical and Electronic Engineering*, *19*(2), 70–82. https://doi.org/10.37917/ijeee.19.2.9

Hathaliya, J. J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. *Computer Communications*, *153*, 311–335. https://doi.org/10.1016/j.comcom.2020.02.018

Hathaliya, J. J., Tanwar, S., Tyagi, S., & Kumar, N. (2019). Securing electronics healthcare records in Healthcare 4.0: A biometric-based approach. *Computers & Electrical Engineering*, *76*, 398–410. https://doi.org/10.1016/j.compeleceng.2019.04.017

Healthcare Data Breaches. (n.d.). *HIPAA Journal*. Retrieved December 3, 2024, from https://www.hipaajournal.com/healthcare-data-breach-statistics/

Hidayat, I. F., & Hermanto, B. R. (2020). A Preliminary Implementation of HL7 FHIR to Achieve Interoperability in Indonesia's Local EHR. *2020 27th International Conference on Telecommunications (ICT)*, 1–5. https://doi.org/10.1109/ICT49546.2020.9239534

J.A, L., B, A., Y, K., & Aditya Varma, A. S. R. V. (2019). Patient Management System. *International Journal of Computer Trends and Technology*, *67*(3), 75–77. https://doi.org/10.14445/22312803/IJCTT-V67I3P115

Jabbar, R., Fetais, N., Krichen, M., & Barkaoui, K. (2020). Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, 310–317. https://doi.org/10.1109/ICIoT48696.2020.9089570

Jamshed, N., Ozair, F., Sharma, A., & Aggarwal, P. (2015). Ethical issues in electronic health records: A general overview. *Perspectives in Clinical Research*, *6*(2), 73. https://doi.org/10.4103/2229-3485.153997

Karimi, L., & Joshi, J. (2018). An Unsupervised Learning Based Approach for Mining Attribute Based Access Control Policies. *2018 IEEE International Conference on Big Data (Big Data)*, 1427–1436. https://doi.org/10.1109/BigData.2018.8622037

Kasih, J., & Achadi, A. (2023). Feasibility Study of Implementation of Electronic Administration Systems in Hospitals. *International Journal of Social Health*, *2*(6), 385–390. https://doi.org/10.58860/ijsh.v2i6.55

Kaul, S. D., Murty, V. K., & Hatzinakos, D. (2020). Secure and Privacy preserving Biometric based User Authentication with Data Access Control System in the Healthcare Environment. *2020 International Conference on Cyberworlds (CW)*, 249–256. https://doi.org/10.1109/CW49994.2020.00047

Khamaiseh, S., Chapman, P., & Xu, D. (2018). Model-Based Testing of Obligatory ABAC Systems. *2018 IEEE International Conference on Software Quality, Reliability and Security (QRS)*, 405–413. https://doi.org/10.1109/QRS.2018.00054

Khan, F. A., & Hajiarbabi, M. (2024). BERT-Driven Automation in Electronic Health Record Management System. *SoutheastCon 2024*, 398–404. https://doi.org/10.1109/SoutheastCon52093.2024.10500252

Khan, S. H., Ali Akbar, M., Shahzad, F., Farooq, M., & Khan, Z. (2015). Secure biometric template generation for multi-factor authentication. *Pattern Recognition*, *48*(2), 458–472. https://doi.org/10.1016/j.patcog.2014.08.024

Kilanko, V. (2023). The Transformative Potential of Artificial Intelligence in Medical Billing: A Global Perspective. *International Journal Of Scientific Advances*, *4*(3). https://doi.org/10.51542/ijscia.v4i3.8

Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security Techniques for the Electronic Health Records. *Journal of Medical Systems*, *41*(8), 127. https://doi.org/10.1007/s10916-017-0778-4

Lakshmanan, M., Anandha Mala, G. S., & Anandkumar, K. M. (2024). Highly secured EHR management system based on blockchain technology with digitally signed authentication using data sanitization and polynomial interpolation. *Biomedical Signal Processing and Control*, *87*, 105412. https://doi.org/10.1016/j.bspc.2023.105412

Liu, W., Liu, X., Liu, J., Wu, Q., Zhang, J., & Li, Y. (2015). Auditing and Revocation Enabled Role-Based Access Control over Outsourced Private EHRs. *2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems*, 336–341. https://doi.org/10.1109/HPCC-CSS-ICESS.2015.10

Liu, Z., Wang, F., Chen, K., & Tang, F. (2020). A New User Revocable Ciphertext-Policy Attribute-Based Encryption with Ciphertext Update. *Security and Communication Networks*, *2020*, 1–11. https://doi.org/10.1155/2020/8856592

Ma, Z., Zhao, M., Liu, X., Shen, C., & Ma, J. (2019). Cross-Organizational Access Control for EHRs: Trustworthy, Flexible, Transparent. *2019 IEEE Global Communications Conference (GLOBECOM)*, 1–6. https://doi.org/10.1109/GLOBECOM38437.2019.9013842

Mamta Dhaka, Sharma, D. P., & Sharma, P. (2024). Standardized Electronic Health Record and its Controlled Access. *International Journal of Next-Generation Computing*. https://doi.org/10.47164/ijngc.v15i2.1644

Margheri, A., Masi, M., Miladi, A., Sassone, V., & Rosenzweig, J. (2020). Decentralised provenance for healthcare data. *International Journal of Medical Informatics*, *141*, 104197. https://doi.org/10.1016/j.ijmedinf.2020.104197

McMurry, A. J., Gottlieb, D. I., Miller, T. A., Jones, J. R., Atreja, A., Crago, J., Desai, P. M., Dixon, B. E., Garber, M., Ignatov, V., Kirchner, L. A., Payne, P. R. O., Saldanha, A. J., Shankar, P. R. V., Solad, Y. V., Sprouse, E. A., Terry, M., Wilcox, A. B., & Mandl, K. D. (2024). Cumulus: A federated electronic health record-based learning system powered by Fast Healthcare Interoperability Resources and artificial intelligence. *Journal of the American Medical Informatics Association*, *31*(8), 1638–1647. https://doi.org/10.1093/jamia/ocae130

Mebrahtu, T. F., Skyrme, S., Randell, R., Keenan, A.-M., Bloor, K., Yang, H., Andre, D., Ledward, A., King, H., & Thompson, C. (2021). Effects of computerised clinical decision support systems (CDSS) on nursing and allied health professional performance and patient outcomes: A systematic review of experimental and observational studies. *BMJ Open*, *11*(12), e053886. https://doi.org/10.1136/bmjopen-2021-053886

Mehraeen, E., Ayatollahi, H., & Ahmadi, M. (2016). Health Information Security in Hospitals: The Application of Security Safeguards. *Acta Informatica Medica*, *24*(1), 47. https://doi.org/10.5455/aim.2016.24.47-50

Mehrtak, M., Seyed Alinaghi, S., MohsseniPour, M., Noori, T., Karimi, A., Shamsabadi, A., Heydari, M., Barzegary, A., Mirzapour, P., Soleymanzadeh, M., (2021). Security challenges and solutions using healthcare cloud computing. *Journal of Medicine and Life*, *14*(4), 448–461. https://doi.org/10.25122/jml-2021-0100

Mukhiya, S. K., & Lamo, Y. (2021). An HL7 FHIR and GraphQL approach for interoperability between heterogeneous Electronic Health Record systems. *Health Informatics Journal*, *27*(3), 14604582211043920. https://doi.org/10.1177/14604582211043920

Najjar, A., Amro, B., & Macedo, M. (2022). islEHR, a model for electronic health records interoperability. *Bio-Algorithms and Med-Systems*, *18*(1), 39–54. https://doi.org/10.1515/bams-2021-0117

Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems. *IEEE Access*, *7*, 66792–66806. https://doi.org/10.1109/ACCESS.2019.2917555

Nowrozy, R., Ahmed, K., Kayes, A. S. M., Wang, H., & McIntosh, T. R. (2024). Privacy Preservation of Electronic Health Records in the Modern Era: A Systematic Survey. *ACM Computing Surveys*, *56*(8), 1–37. https://doi.org/10.1145/3653297

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, *2*(1), 1. https://doi.org/10.3390/cryptography2010001

Paul, P., & Sural, S. (2021). Towards Efficient Evaluation of ABAC Policies using High-Dimensional Indexing Techniques. *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, 243–251. https://doi.org/10.1109/TPSISA52974.2021.00027

Perez-Haro, A., & Diaz-Perez, A. (2024). ABAC Policy Mining through Affiliation Networks and Biclique Analysis. *Information*, *15*(1), 45. https://doi.org/10.3390/info15010045

Psarra, E., Apostolou, D., Verginadis, Y., Patiniotakis, I., & Mentzas, G. (2022). Context-Based, Predictive Access Control to Electronic Health Records. *Electronics*, *11*(19), 3040. https://doi.org/10.3390/electronics11193040

Quintero, V., Chevel, C., & Sanmartin-Mendoza, P. (2024). Analysis on the Interoperability of health information systems. *2024 IEEE Technology and Engineering Management Society (TEMSCON LATAM)*, 1–6. https://doi.org/10.1109/TEMSCONLATAM61834.2024.10717770

Rajkomar, A., Oren, E., Chen, K., Dai, A. M., Hajaj, N., Hardt, M., Liu, P. J., Liu, X., Marcus, J., Sun, M., Sundberg, P., Yee, H., Zhang, K., Zhang, Y., Flores, G., Duggan, G. E., Irvine, J., Le, Q., Litsch, K., … Dean, J. (2018). Scalable and accurate deep learning with electronic health records. *Npj Digital Medicine*, *1*(1), 18. https://doi.org/10.1038/s41746-018-0029-1

Reegu, F. A., Abas, H., Gulzar, Y., Xin, Q., Alwan, A. A., Jabbari, A., Sonkamble, R. G., & Dziyauddin, R. A. (2023). Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System. *Sustainability*, *15*(8), 6337. https://doi.org/10.3390/su15086337

Riad, K., Hamza, R., & Yan, H. (2019). Sensitive and Energetic IoT Access Control for Managing Cloud Electronic Health Records. *IEEE Access*, *7*, 86384–86393. https://doi.org/10.1109/ACCESS.2019.2926354

Riadi, I., Ahmad, T., Sarno, R., Purwono, P., & Ma'arif, A. (2022). Developing Data Integrity in an Electronic Health Record System using Blockchain and InterPlanetary File System (Case Study: COVID-19 Data). *Emerging Science Journal*, *4*, 190–206. https://doi.org/10.28991/esj-2021-SP1-013

Rose Ann, Z., & Susan, F. (2017). A Design for Task-Role Based Access Control for Personal Health Record Systems. *International Journal of Health Informatics*, *38*(2`), 150–162.

S A B, A. R., J, J., N, K. K., S, H., & R, S. K. (2023). ABAC Scheme on Electronic Health Records Using Hyperledger Fabric. *International Research Journal on Advanced Science Hub*, *5*(Issue 05S), 489–495. https://doi.org/10.47392/irjash.2023.S065

S, T., S, A., Managavi, C., R, M., & Harikant, C. N. (2024). Secure EHR Storage System using Solana Blockchain and IPFS. *2024 3rd International Conference for Innovation in Technology (INOCON)*, 1–6. https://doi.org/10.1109/INOCON60754.2024.10511572

Shah, M., Shaikh, M., Mishra, V., & Tuscano, G. (2020). Decentralized Cloud Storage Using Blockchain. *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*, 384–389. https://doi.org/10.1109/ICOEI48184.2020.9143004

Sharaf, S., & Shilbayeh, N. F. (2019). A Secure G-Cloud-Based Framework for Government Healthcare Services. *IEEE Access*, *7*, 37876–37882. https://doi.org/10.1109/ACCESS.2019.2906131

Shen, J., Zeng, P., Choo, K.-K. R., & Li, C. (2023). A Certificateless Provable Data Possession Scheme for Cloud-Based EHRs. *IEEE Transactions on Information Forensics and Security*, *18*, 1156–1168. https://doi.org/10.1109/TIFS.2023.3236451

Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K.-K. R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & Security*, *97*, 101966. https://doi.org/10.1016/j.cose.2020.101966

Simha.R, K., H K, R., Prabhu, A., & Joshi, P. (2025). Beyond passwords: A multi-factor authentication approach for robust digital security. *Internet Technology Letters*, *8*(2), e555. https://doi.org/10.1002/itl2.555

Simola, S., Hörhammer, I., Xu, Y., Bärkås, A., Fagerlund, A. J., Hagström, J., Holmroos, M., Hägglund, M., Johansen, M. A., Kane, B., Kharko, A., Scandurra, I., & Kujala, S. (2023). Patients' Experiences of a National Patient Portal and Its Usability: Cross-Sectional Survey Study. *Journal of Medical Internet Research*, *25*, e45974. https://doi.org/10.2196/45974

Singh, Y., Jaiswal, S., & Kumar, V. (2024). A Comprehensive Literature Review on Privacy, Security, and Data Management in Healthcare. *2024 2nd International Conference on Disruptive Technologies (ICDT)*, 220–224. https://doi.org/10.1109/ICDT61202.2024.10489013

Sonkamble, R. G., Bongale, A. M., Phansalkar, S., Sharma, A., & Rajput, S. (2023). Secure Data Transmission of Electronic Health Records Using Blockchain Technology. *Electronics*, *12*(4), 1015. https://doi.org/10.3390/electronics12041015

Sonkamble, R. G., Phansalkar, S. P., Potdar, V. M., & Bongale, A. M. (2021). Survey of Interoperability in Electronic Health Records Management and Proposed Blockchain Based Framework: MyBlockEHR. *IEEE Access*, *9*, 158367–158401. https://doi.org/10.1109/ACCESS.2021.3129284

Srinivas, D. B., M, D. K., P, R. H., & H, L. (2023). Securing Sharable Electronic Health Records on Cloud Storage. *2023 7th International Conference on Computing Methodologies and Communication (ICCMC)*, 1054–1059. https://doi.org/10.1109/ICCMC56507.2023.10083743

Suleski, T., & Ahmed, M. (2023). A Data Taxonomy for Adaptive Multifactor Authentication in the Internet of Health Care Things. *Journal of Medical Internet Research*, *25*, e44114. https://doi.org/10.2196/44114

Tayefi, M., Ngo, P., Chomutare, T., Dalianis, H., Salvi, E., Budrionis, A., & Godtliebsen, F. (2021). Challenges and opportunities beyond structured data in analysis of electronic health records. *WIREs Computational Statistics*, *13*(6), e1549. https://doi.org/10.1002/wics.1549

Tiwari, B., & Kumar, A. (2015). Role-based access control through on-demand classification of electronic health record. *International Journal of Electronic Healthcare*, *8*(1), 9. https://doi.org/10.1504/IJEH.2015.071637

Tsegaye, T., & Flowerday, S. (2020). A Clark-Wilson and ANSI role-based access control model. *Information & Computer Security*, *28*(3), 373–395. https://doi.org/10.1108/ICS-08-2019-0100

Vamsi, D., & Reddy, P. (2020). Electronic Health Record Security in Cloud: Medical Data Protection Using Homomorphic Encryption Schemes. In C. Chakraborty (Ed.), *Advances in Healthcare Information Systems and Administration* (pp. 22–47). IGI Global. https://doi.org/10.4018/978-1-7998-0261-7.ch002

Velásquez, I., Caro, A., & Rodríguez, A. (2018). Authentication schemes and methods: A systematic literature review. *Information and Software Technology*, *94*, 30–37. https://doi.org/10.1016/j.infsof.2017.09.012

Voege, P., & Ouda, A. (2022). An Innovative Multi-Factor Authentication Approach. *2022 International Symposium on Networks, Computers and Communications (ISNCC)*, 1–6. https://doi.org/10.1109/ISNCC55209.2022.9851710

Walid, R., Joshi, K. P., & Geol Choi, S. (2023). Semantically Rich Differential Access to Secure Cloud EHR. *2023 IEEE 9th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, 1–9. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS58521.2023.00012

Walid, R., Joshi, K. P., Geol Choi, S., & Kim, D. (2020). Cloud-based Encrypted EHR System with Semantically Rich Access Control and Searchable Encryption. *2020 IEEE International Conference on Big Data (Big Data)*, 4075–4082. https://doi.org/10.1109/BigData50022.2020.9378002

Wang, H., & Song, Y. (2018). Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain. *Journal of Medical Systems*, *42*(8), 152. https://doi.org/10.1007/s10916-018-0994-6

Wang, J., Yin, X., Ning, J., Xu, S., Xu, G., & Huang, X. (2023). Secure Updatable Storage Access Control System for EHRs in the Cloud. *IEEE Transactions on Services Computing*, *16*(4), 2939–2953. https://doi.org/10.1109/TSC.2022.3232230

Wang, S., Wang, X., & Zhang, Y. (2019). A Secure Cloud Storage Framework With Access Control Based on Blockchain. *IEEE Access*, *7*, 112713–112725. https://doi.org/10.1109/ACCESS.2019.2929205

Warren, L. R., Clarke, J., Arora, S., & Darzi, A. (2019). Improving data sharing between acute hospitals in England: An overview of health record system distribution and retrospective observational analysis of inter-hospital transitions of care. *BMJ Open*, *9*(12), e031637. https://doi.org/10.1136/bmjopen-2019-031637

Wei, J., Chen, X., Huang, X., Hu, X., & Susilo, W. (2019). RS-HABE: Revocable-storage and Hierarchical Attribute-based Access Scheme for Secure Sharing of e-Health Records in Public Cloud. *IEEE Transactions on Dependable and Secure Computing*, 1–1. https://doi.org/10.1109/TDSC.2019.2947920

Wilkinson, T. M. (2024). Medical Records in Field Operations: A No-Code Approach. *Disaster Medicine and Public Health Preparedness*, *18*, e158. https://doi.org/10.1017/dmp.2024.248

Xu, Y., Gao, W., Zeng, Q., Wang, G., Ren, J., & Zhang, Y. (2018). A Feasible Fuzzy-Extended Attribute-Based Access Control Technique. *Security and Communication Networks*, *2018*, 1–11. https://doi.org/10.1155/2018/6476315

Yakubu, B. M., Ali, S. M., Khan, M. I., & Bhattarakosol, P. (2024). PatCen: A blockchain-based patient-centric mechanism for the granular access control of infectious disease-related test records. *PLOS ONE*, *19*(9), e0310407. https://doi.org/10.1371/journal.pone.0310407

Zarezadeh, M., Ashouri-Talouki, M., & Siavashi, M. (2020). Attribute-based Access Control for Cloud-based Electronic Health Record (EHR) Systems. *The ISC International Journal of Information Security*, *12*(2). https://doi.org/10.22042/isecure.2020.174338.458

Zhang, H., Yu, J., Tian, C., Zhao, P., Xu, G., & Lin, J. (2018). Cloud Storage for Electronic Health Records Based on Secret Sharing With Verifiable Reconstruction Outsourcing. *IEEE Access*, *6*, 40713–40722. https://doi.org/10.1109/ACCESS.2018.2857205

Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. *Computational and Structural Biotechnology Journal*, *16*, 267–278. https://doi.org/10.1016/j.csbj.2018.07.004

Zheng, Q., Li, Y., Chen, P., & Dong, X. (2018). An Innovative IPFS-Based Storage Model for Blockchain. *2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI)*, 704–708. https://doi.org/10.1109/WI.2018.000-8

Zhou, X., Liu, J., Liu, W., & Wu, Q. (2016). Anonymous Role-Based Access Control on E-Health Records. *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, 559–570. https://doi.org/10.1145/2897845.2897871

Zhu, Z., Ren, Z., & Du, X. (2021). Unstructured Text ABAC Attribute Mining Technology Based On Deep Learning. *2021 3rd International Academic Exchange Conference on Science and Technology Innovation (IAECST)*, 34–39. https://doi.org/10.1109/IAECST54258.2021.9695911

Zukaib, U., Cui, X., Hassan, M., Harris, S., Hadi, H. J., & Zheng, C. (2023). Blockchain and Machine Learning in EHR Security: A Systematic Review. *IEEE Access*, *11*, 130230–130256. https://doi.org/10.1109/ACCESS.2023.3333229