Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Distributed Approach for Securing Healthcare Data

Brahmanand Reddy Bhavanam

Info Way Solutions LLC, USA

ARTICLE INFO

Received: 05 Jan 2026

Revised: 12 Feb 2026

Accepted: 22 Feb 2026

ABSTRACT

Digitization of healthcare has provided opportunities for improving patient care but also has brought with it major security vulnerabilities that could compromise the confidentiality, availability, and integrity of protected health information. This article reviews the proposed distributed system constructs for providing health data security between heterogeneous systems, organizations, and multiple institutions. It categorizes and reviews three approaches to distributed healthcare security: (1) Advanced Encryption Algorithms, including symmetric, asymmetric and homomorphic algorithms for encrypting health information-at-rest and in-transit, and key management mechanisms for secure access to cryptographic material across multiple nodes that may not be trusted; (2) Distributed Storage Systems, including distributed-ledger technology (DLT), distributed file systems, and fragmentation approaches for immutable patient consent and audit trail logging, redundancy to tolerate physical node compromise, and avoiding total infrastructure data loss due to localized security attacks; and (3) Access Control Mechanisms, including multi-factor authentication, role-based access control, attribute-based access control, federated identity management for distributed healthcare organizations, and patient access control and monitoring for distributed threat detection. The distributed model is now more attractive in modern health systems. Perimeter security models do not adequately protect health data. The health data moves through networks connecting hospitals, outpatient clinics, clinical research organizations, insurance companies, and third-party organizations. The proposed framework satisfies regulations according to HIPAA, the General Data Protection Regulation (GDPR), and the Health Information Technology for Economic and Clinical Health (HITECH) Act. The system can be performance optimized to balance between cryptographic strength and system responsiveness. The combination of encryption, decentralized storage, and access control provides defense-in-depth protection against cyberattacks. Future developments, such as artificial intelligence-enabled threat detection, quantum-resistant cryptographic algorithms and models for patient data control will shape how to create secure healthcare systems in our growing digital health networks.

Keywords: Distributed Healthcare Security, Encryption Techniques, Blockchain Technology, Access Control Mechanisms, Data Privacy

Introduction

Digital technologies are revolutionizing the creation, storage, and sharing of medical information within the health ecosystem. These developments offer potentially unprecedented opportunities to

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

improve the quality of health care but also pose serious risks to the privacy and security of patients. Protected health information (PHI) is data such as clinical records, imaging and genomic data, and sensitive information about mental health, which, when disclosed, would cause a serious risk of harm to privacy, dignity, or safety [1]. The modern healthcare system has been designed to depend on the flow of information between disparate institutions, including hospitals, primary care offices, specialty clinics, pharmaceutical companies, health insurance companies, and research institutions. Each of these institutions becomes a potential point of cyber intrusion. These attacks are becoming more common, more advanced, and increasingly exploit legacy systems, unsecured network boundaries, and human vulnerabilities, such as credential theft and social engineering. Compliance frameworks impose a minimum level of protection for medical information due to the importance society places on privacy and the special role that the law gives it. The Health Insurance Portability and Accountability Act's (HIPAA) privacy and security rules provide standards for protecting protected health information under US federal law in terms of administrative, physical, and technical safeguards that business associates and covered entities must implement. The EU General Data Protection Regulation (GDPR) provides very high levels of protection for health data in terms of explicit consent for processing and rights to access, rectify, and erase personal data [2]. In the United States, the Health Information Technology for Economic and Clinical Health Act strengthens enforcement and breach notification rules regarding healthcare privacy. This article studies distributed security architectures that provide holistic protection of healthcare data across systems and organizational borders. If sensitive information is often in transit through multiple overlapping trust domains, are perimeter models sufficient to secure resources? The article talks about three connected research topics: using cryptographic security protocols to handle private data safely, decentralized DHT-based resource storage to avoid having a single point of failure, and distributed resource access control models to apply specific authorization rules. Known security principles and design objectives are security solutions, but actual ones must work across the full range of technical, organizational and operational domains.

2. Distributed Security Architecture for Healthcare Systems

2.1 Fundamental Principles of Distributed Healthcare Security

Distributed security architectures for healthcare systems are security models that use security controls spread out across different locations, rather than relying on a single, strong security system in one central building, because healthcare information is constantly shared across different organizations and technologies today. This architecture, which consists of nodes located in various places and domains, implements a security policy. Common protection architectures support security policies. Other approaches involve security zone separation for computer systems with different data sensitivity and the separation of data storage from processing prevents the exposure of protected data both while it is stored and during processing [3]. Threat modeling in the context of distributed healthcare systems also involves the consideration of attack vectors that exploit the complexity of multi-node systems. Vectors include unauthorized access or impersonation from stolen credentials, weak authentication or authorization systems, data leaks in networks or storage, man-in-the-middle attacks on data being transferred between nodes, and misuse of privileges by users who have too much access to compromise, delete, or change data. Building trust is challenging because it's tough to confirm who someone is and what they are allowed to do, especially when different organizations are involved and when access is based on a logical system instead of where the node is located. Zero-trust models consider all access attempts as potential attacks, irrespective of the origin of the request [4]. Trust boundaries may exist where there is a transition of trust between two different domains, such as from healthcare providers to patients, clinical systems to third-party analytics services, or internal networks to external collaboration systems. Data entering or exiting a trust boundary requires

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

authentication, authorization, and audit processes appropriate to the type and sensitivity of information being communicated between domains.

2.2 System Integration and Interoperability

In multi-platform interoperability, different systems can share a common security approach, like electronic health record systems that use various authentication application programming interfaces (APIs) and lab information systems with different processes, or imaging systems that handle large data files. These systems may have different architecture assumptions and domain models, and so next-generation health information networks may need to support machine-to-machine protocols between heterogeneous health technologies. Secure application programming interface protocols need to meet several requirements, including verifying who is requesting health information, allowing specific access based on clinical roles and patient consent, managing data flow to prevent service interruptions while still handling a lot of data, checking and cleaning input to stop harmful data from being added, and rejecting poorly formed requests. Though interoperability implies a standardization of data formats and communication mechanisms, the security permitted by a standard API may be constrained by the security features not supported by some implementations, including encryption, access control, and auditing. Health Level Seven and Fast Healthcare Interoperability Resources, which are common standards for sharing health information, outline how health data should be exchanged and need several security measures to prevent unauthorized access or changes when data is sent between different organizations and their legal areas.

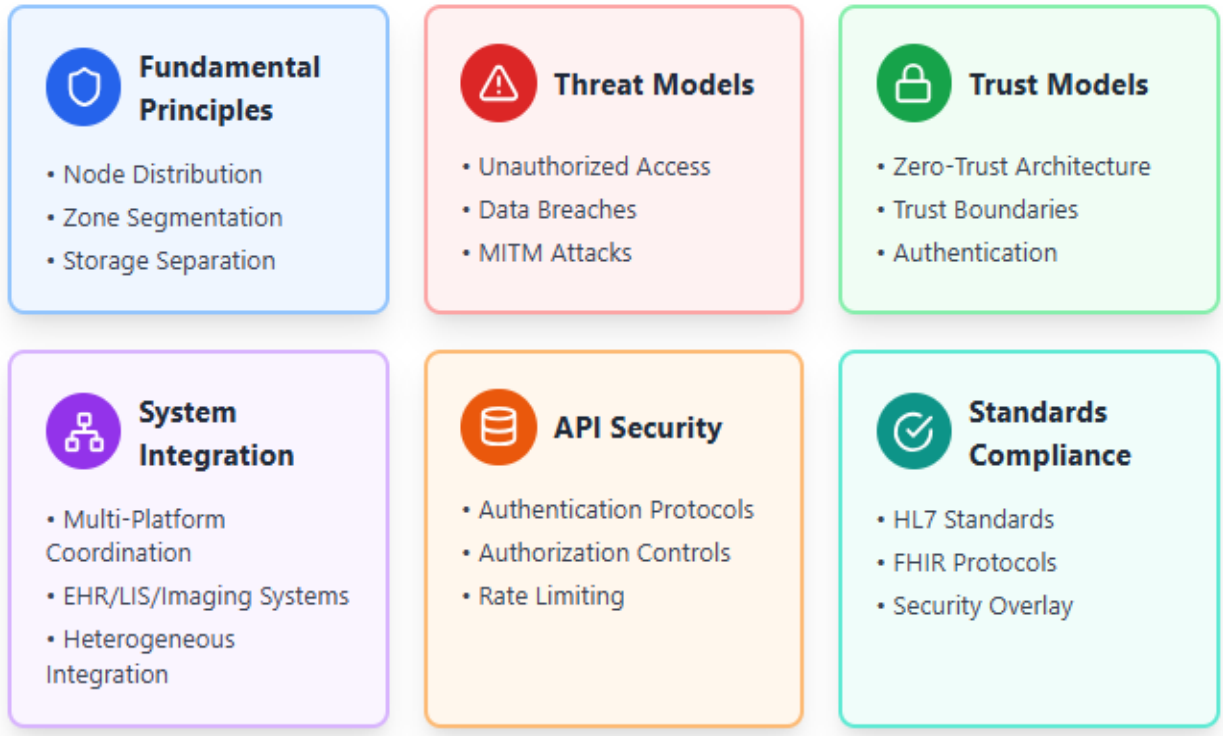

Fig. 1: Distributed Security Architecture for Healthcare Systems [3, 4]

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3. Distributed Encryption Techniques for Healthcare Data

3.1 Encryption Methodologies

End-to-end encryption (E2EE) in healthcare refers to techniques that encrypt communications and data for every stage of their lifecycle, typically through encryption at rest and encryption in transit. Encryption at rest is based on symmetric encryption algorithms that are computationally efficient for processing large healthcare data sets. Encryption in transit occurs when the data is encrypted by transport layer-controlled protocols to secure a channel for data exchange between communication parties. It is used to prevent data interception and eavesdropping. Because symmetric encryption algorithms are faster for this purpose, most bulk encryption is performed using symmetric encryption. Asymmetric encryption is also generally used for key establishment and digital signature purposes, at the cost of speed, so encryption protocols usually use hybrid architectures and first establish a session key using asymmetric encryption to be used with symmetric encryption. Homomorphic and functional encryption are types of cryptography that let healthcare organizations run calculations on encrypted health data without needing to decrypt it, which helps them analyze data, combine statistics, and make predictions about patient health while keeping the information secure. Key management presents significant operational challenges in distributed healthcare encryption, which include: distributed key generation to eliminate single points of compromise; secure key storage solutions that protect cryptographic material from unauthorized exposure while allowing access to authorized parties; key rotation frameworks that regularly rotate cryptographic keys to minimize the impact of a key leak; hardware security modules that are tamper-resistant and used for cryptographic operations and key protection; and key derivation functions that generate encryption keys from master secrets using computationally intensive algorithms to make brute-force attacks computationally infeasible.

3.2 Data Classification and Selective Encryption

Sensitivity-based encryption makes decisions about cryptographic protection by recognizing that not all healthcare data is equally sensitive. It provides strong protection for protected health information, keeps sensitive personal information safe from identity theft and unauthorized sharing, secures clinical notes to prevent changes to doctors' observations and unauthorized sharing of confidential information, and ensures that billing data remains accurate and private to prevent overcharging and fraud by providers. Sensitivity-based encryption allows organizations to accommodate differing data sensitivity levels and make efficient use of limited computing and communication resources. Field-level encryption allows for each field in a database record, or each element of a structured or unstructured document, to be encrypted separately and disclosed selectively under the control of access to decryption keys. In this way, the principles of data minimization and least privilege can be applied. Two main factors for optimizing the performance of distributed healthcare encryption are balancing cryptographic security and computational performance.

Component	Key Techniques	Primary Purpose
Encryption Methodologies	End-to-End, Homomorphic, Key Management	Protect data lifecycle & enable secure computation
Data Classification	Sensitivity-Based, Field-Level Encryption	Apply appropriate protection by data sensitivity
Performance Optimization	Algorithm Selection, Hardware Acceleration, Caching	Balance security strength with system efficiency

Table 1: Distributed Encryption Techniques for Healthcare Data [5, 6]

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

4. Decentralized Data Storage and Management

4.1 Distributed Storage Architectures

Also, the way blockchain and DLT work makes it possible to keep a clear record of all past access, changes, and transfers to a patient's record, which helps in checking how data was collected, changed, and shared to ensure it follows rules and policies. Consensus mechanisms in decentralized systems also avoid the single point of trust by distributing the responsibility for validating changes across many nodes in the network so that no one can unilaterally change a record without the knowledge of the rest of the network. Smart contract patient consent management is an application of smart contracts that stores and executes patient consent to allow access to their health data by a healthcare provider or researcher. A patient consent smart contract creates a cryptographically verifiable record of a patient's consent that is mutable but immutable in the sense that the full history can be preserved through blockchain. Another approach to building a decentralized healthcare data infrastructure uses distributed file systems with fragmentation and dispersion of files across multiple storage nodes, including replication of files in different geographical locations to have more copies of the data available in multiple locations. This would also provide fault tolerance to reconstruct the data from fragments upon node failure and geographic distribution to minimize latency and provide resilience against localized disasters [8]. Data fragmentation and sharding mean breaking healthcare records into smaller pieces and spreading them across different storage locations, so if one location is hacked, only part of the data is exposed and the full patient record remains safe. Combining cryptographic techniques on the fragments before distributing them provides defense-in-depth, as an attacker would have to compromise multiple nodes and break encryption to access useful data.

4.2 Data Integrity and Availability

In distributed storage systems, medical data on the nodes is replicated to allow continued access when it is corrupted by one or more hardware faults, a network partition, or malicious actors attempting to disrupt and compromise the data stored on the system. The replication factor balances the storage costs and the maximum number of faults it can withstand. The same encryption and access control policies are enforced on the synchronized replicas. Consistency models govern access to replicated shared data on distributed storage systems. Strong consistency models ensure that after an update operation is completed, all replicas share the same data set, erasing potential doubts among healthcare providers who need only the latest data, which is important to prevent harm to patients but incurs synchronization costs. Eventual consistency models permit temporary divergence among replicas while ensuring their eventual convergence. This feature is often used for less time-critical data, such as past records or administrative data. In a distributed environment, disaster recovery reduces the risk of catastrophic loss of an entire data center or region through geographic redundancy and automated replication practices that address legal and regulatory data retention, availability, and business continuity planning policies and requirements, often referred to as DR, backup, and replication.

Architecture Component	Core Mechanisms	Key Benefit
Blockchain & DLT	Immutable Audit Trails, Smart Contracts, Consensus	Tamper-evident tracking & consent management
Distributed File Systems	Fragmentation, Geographic Distribution, Sharding	Fault tolerance & breach resilience
Replication	Multi-Node Copies, Synchronized	High availability during failures

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Strategies	Protection	
Consistency Models	Strong Consistency, Eventual Consistency	Balance accuracy with performance

Table 2: Decentralized Data Storage and Management [7, 8]

5. Access Control Mechanisms and Secure Data Sharing

5.1 Authentication and Authorization Frameworks

Multi-factor authentication systems use different types of verification methods, like passwords (knowledge factors), hardware tokens or smartphone apps that create temporary passwords (possession factors), and biometric identifiers like retina scans or voice recognition (inherence factors). This combination greatly enhances security against unauthorized access, even if one method is compromised through credential theft or phishing attacks. Access control mechanisms such as role-based access control (RBAC) systems that assign system permissions to organizational roles that correspond with job functions and clinical responsibilities allow administrators to manage access to databases. This system allows for the prescription of medications or the modification of medical records based on a specific role rather than on individual user accounts. When combined with other factors like the user's department, their relationship to the patient, the sensitivity of the data, and the situation (such as where and when access is happening), RBAC-ABAC combinations offer a more detailed way to manage access, addressing the complex privacy needs in healthcare. Identity federation solves the problem of having to manage the population of user identities across highly distributed, independent healthcare delivery organizations by establishing trust links allowing users authenticated by their home institution to access partner systems without each partner having to maintain a separate set of credentials. Single sign-on mechanisms enable end users to authenticate once and gain access to multiple interrelated systems with reduced authentication friction during a session.

5.2 Secure Inter-Organizational Data Exchange

Consent management systems provide a patient-centered specification allowing patients to specify, selectively and in fine-grained detail, which portions of their medical record they are willing to share with specific healthcare provider organizations and researchers, and which portions they want to keep private from others. Machine-readable consents are checked automatically for compliance with permission and legal 'informed consent' requirements. Secure channels use cryptography to mutually authenticate and encrypt communications between computerized health care providers over untrusted networks. Transport layer security uses digital certificates to create a secure and verified connection, keeping data private with symmetric encryption and ensuring it hasn't been changed with message integrity checks. Virtual private networks encrypt the data that flows between different networks in an organization. Secure messaging systems encrypt clinical messages between healthcare providers that contain patient information using end-to-end encryption. An audit and monitoring system creates logs that maintain sufficient detail about provider access, including username and timestamp, data elements accessed, and purpose of access. Such logs allow for retrospective review of data access permissions and practices. Real-time monitoring systems can alert monitoring personnel to unusual access patterns that could indicate unauthorized access, either excessively high rates of access or access at unusual hours.

5.3 Third-Party Service Integration

Vendor risk management is the creation of systematic means by which an organization identifies the security posture of third-party healthcare applications prior to their use. Vendor risk assessment

Journal of Information Systems Engineering and Management
2026, 11(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

analyzes the security policies of healthcare application vendors, technical controls, compliance certifications, methods of data handling, and incident response in order to determine the applicability of organizational security requirements and acceptable risk boundaries. API gateway security acts as a central point that controls how third-party applications access healthcare data, ensuring that only authorized applications can get in by using standard methods to verify their identity, setting specific rules about which data they can see, limiting how much they can use the data, and keeping a record of all access for checking and spotting any unusual activity. Data minimization principles for use by healthcare organizations for data sharing with third-party services include the following: third-party services should be provided access to only the minimum data elements required by the third-party services for their intended use, with non-required patient information withheld by the healthcare organization. Anonymization or de-identification methods should be used in a way that still allows for effective analysis and operations while also putting in place technical measures to avoid accidentally sharing too much patient data.

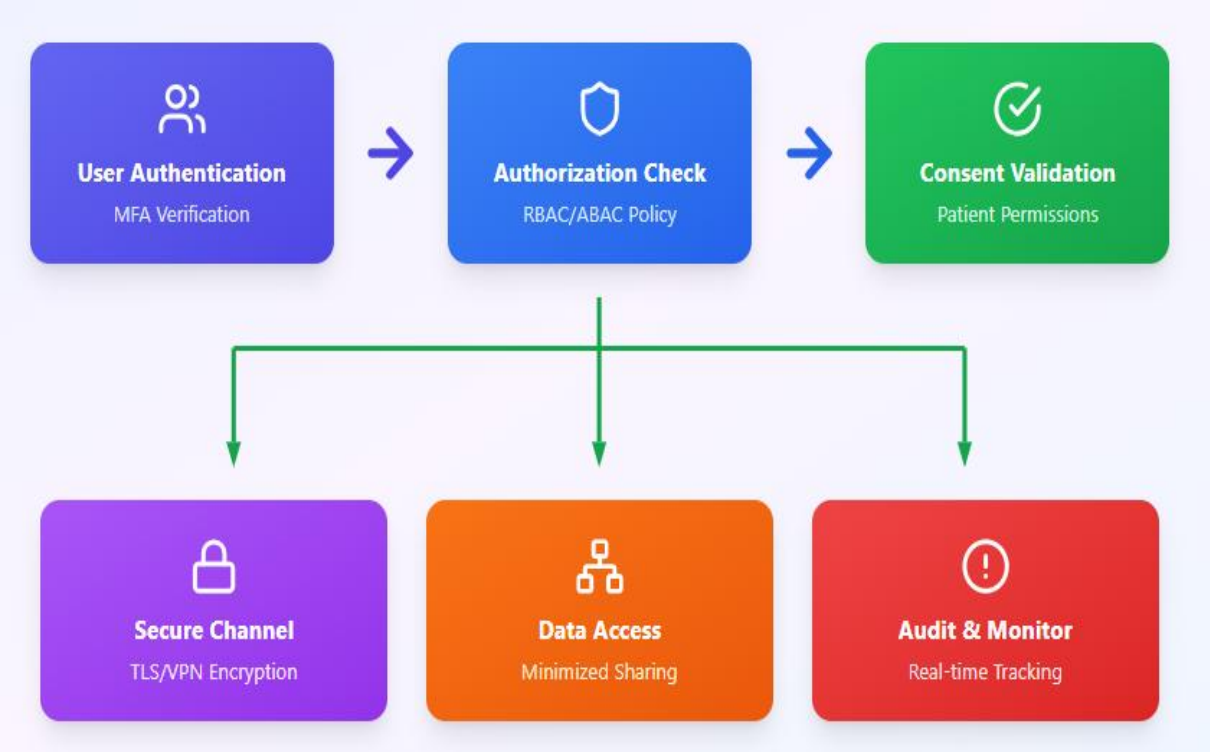

Fig. 2: Secure Data Access Flow [9, 10]

Conclusion

This dissertation secures and makes private distributed healthcare data available with consideration for increasing cyber threats, regulatory requirements, and the dynamic nature of medical data within heterogeneous, distributed, and cross-organizational environments. It looks at ways to keep medical data safe, accessible, and unaltered while managing who can access it, focusing on three main strategies: keeping data private by using encryption methods that allow calculations without revealing the data, using decentralized storage solutions like blockchain to avoid failures and ensure data is always available and consistent, and implementing detailed access controls with methods like multi-factor authentication and role-based access to manage permissions across different organizations. This chapter provides defense in depth, in that compromising any single security layer does not

compromise the system as a whole. The distributed architecture also helps prevent local attacks and infrastructure failures. The distributed security meets regulatory and legislative requirements, such as HIPAA, GDPR, and the HITECH Act, through audit logs, patient-centric consent, and cryptographic security. Distributed security also ensures good performance by using certain cryptographic algorithms, smart data placement to reduce access times, and consistency models that consider performance. Performance-aware consistency models deliver data that is either correct or out of date based on the performance profile of the underlying application feature. Rapid technology changes and the evolution of the threat landscape will drive future distributed healthcare security. They use artificial intelligence and machine learning to find threats by analyzing behavior and spotting unusual activities, quantum-resistant cryptographic algorithms to protect against future quantum computing threats to current encryption methods, better ways to manage patient data ownership with blockchain and self-sovereign identity, and ongoing improvements to distributed systems that ensure security while allowing easy access for important healthcare needs in a quickly digitalizing world.

References

[1] Clemens Scott Kruse et al., "Security Techniques for the Electronic Health Records," Journal of Medical Systems, 2017. Available: https://doi.org/10.1007/s10916-017-0778-4

[2] Karim Abouelmehdi et al., "Big healthcare data: preserving security and privacy," Journal of Big Data, 2018. Available: https://doi.org/10.1186/s40537-017-0110-7

[3] Shekha Chenthara et al., "Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing," IEEE Access, 2019. Available: https://doi.org/10.1109/ACCESS.2019.2919982

[4] Jigna J. Hathaliya and Sudeep Tanwar, "An exhaustive survey on security and privacy issues in Healthcare 4.0," Computer Communications Volume 153s, 2021. Available: https://www.sciencedirect.com/science/article/abs/pii/S0140366419311880

[5] Abbas Acar et al., "A Survey on Homomorphic Encryption Schemes: Theory and Implementation," ACM Computing Surveys (CSUR), Volume 51, Issue 4, 2018. Available: https://doi.org/10.1145/3214303

[6] Assad Abbas et al., "A cloud-based health insurance plan recommendation system: A user-centered approach," Future Generation Computer Systems Volumes 43–44, 2017. Available: https://www.sciencedirect.com/science/article/abs/pii/S0167739X14001587

[7] Asaph Azaria et al., "MedRec: Using Blockchain for Medical Data Access and Permission Management," IEEE International Conference on Open and Big Data, 2016. Available: https://doi.org/10.1109/OBD.2016.11

[8] Xia Qi et al., "BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments," MDPI Information, 2017. Available: https://doi.org/10.3390/info8020044

[9] José Luis Fernández-Alemán et al., "Security and privacy in electronic health records: A systematic literature review," Journal of Biomedical Informatics, June 2013. Available: https://doi.org/10.1016/j.jbi.2012.12.003

[10] Rui Zhang et al., "Security and Privacy on Blockchain," ACM Computing Surveys, September 2019. Available: https://doi.org/10.1145/3316481