International Scholars Journals

International Journal of Food Safety and Public Health Vol. 3 (1), pp. 001-011, September, 2016.
Available online at www.internationalscholarsjournals.org © International Scholars Journals

Author(s) retain the copyright of this article

Full Length Review Article

Privacy-Preserving Access Control for Electronic Health Record Systems

Anjani Haritha Sannidhanam[1], Shivani Alladi[2]

[1]Student Researcher, Sreenidhi Institute of Science & Technology, India

[2]Student Researcher, GITAM University, India

Abstract

The rapid adoption of Electronic Health Record (EHR) systems has significantly improved the management, storage, and sharing of patient medical information among healthcare providers. However, ensuring the privacy and confidentiality of sensitive health records remains a critical challenge due to increasing concerns regarding unauthorized access, data breaches, and regulatory compliance. Privacy-preserving access control mechanisms have emerged as an effective solution to safeguard patient information while maintaining secure and efficient data accessibility. This paper presents an overview of privacy-preserving access control techniques employed in Electronic Health Record systems, emphasizing role-based access control, attribute-based access control, encryption-based access policies, and patient-centric authorization models. The study discusses the importance of secure authentication, fine-grained authorization, and cryptographic approaches for protecting medical data against unauthorized disclosure. Furthermore, existing challenges, including scalability, interoperability, emergency access, and policy management, are examined. The proposed framework highlights the integration of privacy-preserving mechanisms with access control strategies to improve confidentiality, integrity, and availability of healthcare information. The study concludes that combining cryptographic techniques with flexible access control models can significantly enhance the security and privacy of Electronic Health Record systems while supporting efficient healthcare services.

Keywords: *Electronic Health Records (EHR), Privacy Preservation, Access Control, Healthcare Security, Role-Based Access Control, Attribute-Based Encryption, Patient Privacy, Data Confidentiality, Authentication, Healthcare Information Systems.*

1. Introduction

Electronic Health Record (EHR) systems have transformed healthcare by replacing conventional paper-based records with computerized patient information repositories. These systems enable physicians, hospitals, laboratories, pharmacies, and healthcare organizations to access and exchange clinical information efficiently, thereby improving patient care and reducing medical errors. As healthcare institutions increasingly rely on digital platforms, the volume of sensitive patient information stored electronically has grown substantially, making information security and privacy fundamental requirements for healthcare information management [1].

The confidentiality of medical records is essential because healthcare data contain highly sensitive personal information, including demographic details, diagnostic reports, laboratory results, prescriptions, insurance information, and treatment histories. Unauthorized disclosure of such information may not only violate patient privacy but also lead to identity theft, financial fraud, discrimination, and legal consequences. Consequently, healthcare organizations must establish robust mechanisms to ensure that only authorized individuals are permitted to access patient records while maintaining the availability of information for legitimate clinical purposes [2].

Access control has emerged as one of the primary security mechanisms for protecting Electronic Health Record systems. Traditional security approaches generally authenticate users before granting access; however, authentication alone is insufficient to regulate the type of information users may access. Effective authorization mechanisms are therefore required to ensure that healthcare professionals receive permissions according to their responsibilities, organizational roles, and clinical requirements [3].

Role-Based Access Control (RBAC) has become one of the most widely implemented authorization models in healthcare environments because it simplifies permission management by assigning privileges based on professional roles rather than individual users. Although RBAC reduces administrative complexity, modern healthcare environments require more flexible authorization policies that consider multiple contextual attributes, including department, location, treatment relationship, emergency status, and patient preferences [4].

To address these challenges, researchers have proposed Attribute-Based Access Control (ABAC) and cryptographic techniques such as Attribute-Based Encryption (ABE). These approaches support fine-grained authorization by allowing access decisions to depend on multiple attributes instead of predefined organizational roles. Such mechanisms improve flexibility while strengthening data confidentiality in distributed healthcare environments [5].

Another important aspect of Electronic Health Record security is patient participation in privacy management. Modern healthcare systems increasingly recognize patients as active stakeholders who should have greater control over the sharing of their medical information. Patient-centric privacy models allow individuals to specify access permissions for healthcare providers, researchers, insurance companies, and family members while maintaining appropriate security controls for emergency medical situations [6].

Healthcare organizations also face significant challenges in maintaining interoperability among different hospitals, clinics, diagnostic centers, and insurance providers. Secure information exchange requires standardized communication protocols and consistent access control policies that preserve

patient privacy without compromising the efficiency of healthcare delivery [7].

Encryption technologies have become indispensable for protecting Electronic Health Records during storage and transmission. Cryptographic techniques prevent unauthorized users from interpreting sensitive information even if communication channels or storage systems are compromised. When encryption is integrated with fine-grained access policies, healthcare organizations achieve stronger protection against internal misuse and external cyber threats [8].

Despite considerable progress in healthcare information security, several practical issues continue to affect the implementation of privacy-preserving access control systems. These include policy administration, emergency access management, scalability, user accountability, and compliance with healthcare regulations. Addressing these concerns requires security models that combine usability with strong privacy guarantees while minimizing administrative complexity [9].

This study investigates privacy-preserving access control mechanisms for Electronic Health Record systems by examining conventional access control models, encryption-based protection techniques, and patient-centered authorization approaches. The objective is to identify security strategies capable of protecting sensitive healthcare information while supporting efficient and secure medical services in modern healthcare environments [10].

2. Literature Review

Sandhu et al. introduced the Role-Based Access Control (RBAC) model, establishing one of the earliest systematic approaches for assigning permissions according to organizational responsibilities rather than individual users. Their framework significantly reduced administrative complexity and became the foundation for access control implementations across numerous healthcare information systems. **[1]**

Ferraiolo et al. expanded the RBAC concept by proposing a standardized framework that formalized user-role relationships, permission assignments, and authorization policies. Their work provided practical guidelines for implementing secure authorization mechanisms in large-scale organizations, including hospitals and healthcare institutions. **[2]**

Myers and Liskov proposed the Decentralized Label Model, which introduced information flow control mechanisms capable of preserving data confidentiality in distributed computing environments. Their approach demonstrated how privacy policies could be embedded directly into information management systems, providing stronger protection for sensitive healthcare information. **[3]**

Blaze, Bleumer, and Strauss presented decentralized trust management as an alternative to centralized authorization systems. Their research emphasized credential-based authorization, enabling secure cooperation among independent organizations while maintaining flexible trust relationships, an important requirement for distributed healthcare networks. **[4]**

Goyal et al. introduced Attribute-Based Encryption (ABE), allowing encrypted information to be accessed only by users whose attributes satisfy predefined access policies. Their contribution represented a major advancement in fine-grained data protection and later became highly relevant for secure Electronic Health Record systems. **[5]**

Bethencourt, Sahai, and Waters further developed Ciphertext-Policy Attribute-Based Encryption (CP-ABE), enabling data owners to define access policies directly within encrypted information. This approach strengthened confidentiality by allowing secure data sharing without relying entirely on centralized authorization servers. **[6]**

Mandl, Szolovits, and Kohane investigated privacy concerns associated with Electronic Medical Records while emphasizing patient control over personal health information. Their study highlighted the importance of balancing healthcare accessibility with confidentiality and influenced subsequent patient-centered privacy frameworks. **[9]**

Zhou and Varadharajan proposed a secure access control architecture specifically designed for healthcare information systems. Their framework integrated authentication, authorization, and policy enforcement mechanisms to support secure information sharing across healthcare organizations while maintaining regulatory compliance. **[10]**

Appari and Johnson reviewed the state of healthcare information security research by identifying major threats affecting healthcare organizations. Their work highlighted challenges associated with privacy protection, organizational governance, employee awareness, and technological safeguards, providing valuable insights into healthcare cybersecurity practices. **[11]**

Kaelber and Bates examined the relationship between Health Information Exchange (HIE) and patient safety. Their research demonstrated that secure information sharing improves healthcare quality while emphasizing the necessity of strong privacy controls to maintain public confidence in Electronic Health Record systems. **[12]**

Anderson proposed a security policy model specifically tailored for clinical information systems. His research emphasized accountability, audit trails, authorization controls, and confidentiality requirements that continue to influence healthcare information security policies. **[15]**

Ren, Wang, and Wang analyzed emerging security challenges associated with cloud computing and highlighted concerns regarding data confidentiality, access management, and trust in outsourced computing environments. Their observations became increasingly relevant as healthcare organizations adopted cloud-based Electronic Health Record infrastructures. **[17]**

3. System Model and Problem Statement

3.1 System Model

The Electronic Health Record (EHR) environment consists of multiple entities that collaborate to deliver secure healthcare services while protecting patient privacy. The proposed system considers a centralized healthcare information repository where patient records are stored in encrypted form. Authorized users such as physicians, nurses, laboratory technicians, pharmacists, administrative personnel, and patients access medical information according to predefined access privileges. Every access request is authenticated and evaluated before permission is granted.

The system incorporates five major entities:

1. **Patient**
    - Owner of personal health information.
    - Can specify privacy preferences for sharing medical records.
    - May authorize or restrict access to specific healthcare providers.
2. **Healthcare Provider**
    - Includes doctors, nurses, specialists, and medical consultants.
    - Accesses patient information according to assigned clinical responsibilities.
    - Permissions are limited to information necessary for treatment.
3. **Hospital Administrator**
    - Manages user registration and system administration.

- Assigns user roles and maintains organizational policies.
- Does not obtain unrestricted access to confidential medical records.

4. **Authentication Server**
   - Verifies user identity using secure authentication mechanisms.
   - Maintains user credentials and session management.
   - Prevents unauthorized login attempts.
5. **Electronic Health Record Database**
   - Stores patient medical records in encrypted format.
   - Responds only to validated access requests.
   - Maintains audit logs for every data access operation.

The proposed model follows the principle of **least privilege**, ensuring that users receive only the permissions required to perform their assigned responsibilities. This minimizes unnecessary exposure of confidential healthcare information and strengthens organizational security.

3.2 Security Requirements

A privacy-preserving Electronic Health Record system should satisfy several essential security requirements to ensure reliable healthcare information management.

A. Confidentiality

Medical records should be accessible only to authorized individuals. Sensitive patient information must remain protected from unauthorized users during storage, transmission, and retrieval.

B. Authentication

Every user must prove their identity before accessing the system. Reliable authentication mechanisms prevent impersonation and unauthorized system entry.

C. Authorization

After successful authentication, the system verifies whether the authenticated user possesses sufficient privileges to access the requested medical information.

D. Integrity

Patient records must remain accurate and protected against unauthorized modification. Every update should be traceable to the responsible healthcare professional.

E. Availability

Authorized healthcare professionals should be able to access patient records whenever medical treatment requires timely information.

F. Accountability

Every access to Electronic Health Records should be recorded through audit logs, enabling organizations to investigate suspicious activities and maintain regulatory compliance.

G. Patient Privacy

Patients should retain reasonable control over the disclosure of their medical information while allowing emergency medical personnel to obtain necessary records during critical situations.

3.3 Problem Statement

Although Electronic Health Record systems provide significant improvements in healthcare efficiency, they also introduce several security and privacy challenges. Medical information is frequently accessed by multiple healthcare professionals across different departments and institutions. Traditional access control mechanisms often grant broad permissions based solely on organizational roles, making it difficult to enforce fine-grained privacy policies.

Several practical issues remain unresolved in conventional healthcare information systems:

- Healthcare professionals from different departments may require different levels of access to patient records.

- Static authorization policies cannot effectively adapt to changing clinical situations.
- Patients often have limited control over who accesses their medical information.
- Insider misuse remains a major security concern because authorized users may intentionally or unintentionally disclose confidential information.
- Emergency situations require immediate access to patient records while still maintaining accountability.
- Secure information sharing among hospitals, laboratories, pharmacies, and insurance providers requires interoperable access control mechanisms.

These challenges demonstrate the need for an access control framework capable of protecting patient privacy without affecting healthcare delivery.

3.4 Objectives of the Proposed Work

The primary objectives of this research are:

- To design a privacy-preserving access control framework for Electronic Health Record systems.
- To provide fine-grained authorization based on user responsibilities and access policies.
- To improve patient privacy by restricting unauthorized disclosure of medical information.
- To integrate secure authentication with policy-based authorization.
- To maintain confidentiality through encrypted storage of Electronic Health Records.
- To record every access event for auditing and accountability.
- To support secure healthcare information sharing among authorized medical organizations.
- To provide emergency access mechanisms without compromising overall system security.

3.5 Proposed Solution Overview

The proposed framework combines user authentication, policy-based authorization, encrypted data storage, and audit logging to establish a secure Electronic Health Record environment. Before accessing any patient information, users are authenticated and their permissions are evaluated according to predefined access policies. Only authorized requests are forwarded to the encrypted health record repository, while every successful and unsuccessful access attempt is recorded for future auditing.

The proposed approach aims to achieve an appropriate balance between healthcare accessibility and patient privacy, thereby improving the overall security of Electronic Health Record systems while supporting efficient clinical decision-making.

4. Proposed Privacy-Preserving Access Control Framework

The proposed Privacy-Preserving Access Control (PPAC) framework is designed to provide secure access to Electronic Health Record (EHR) systems while maintaining the confidentiality of sensitive patient information. The framework combines authentication, authorization, privacy policy enforcement, encrypted data storage, and audit logging to establish a secure healthcare information environment. Initially, every healthcare user is authenticated using valid system credentials before any access request is processed. After successful authentication, the authorization module evaluates predefined access policies based on the user's organizational role, clinical responsibility, and the requested healthcare resource. Patient-defined privacy preferences are further considered to ensure

that only authorized healthcare professionals can access confidential medical records.

The framework employs encrypted storage to protect Electronic Health Records against unauthorized disclosure. Medical information remains encrypted during storage and transmission, while decryption is performed only after successful authorization. Every access request, regardless of whether it is accepted or rejected, is recorded within an audit log to provide accountability and support future security investigations. This approach minimizes insider misuse, improves confidentiality, and supports secure information sharing among hospitals, laboratories, and healthcare providers. By integrating access control with privacy-preserving techniques, the proposed framework enhances data security without affecting the availability of healthcare services.

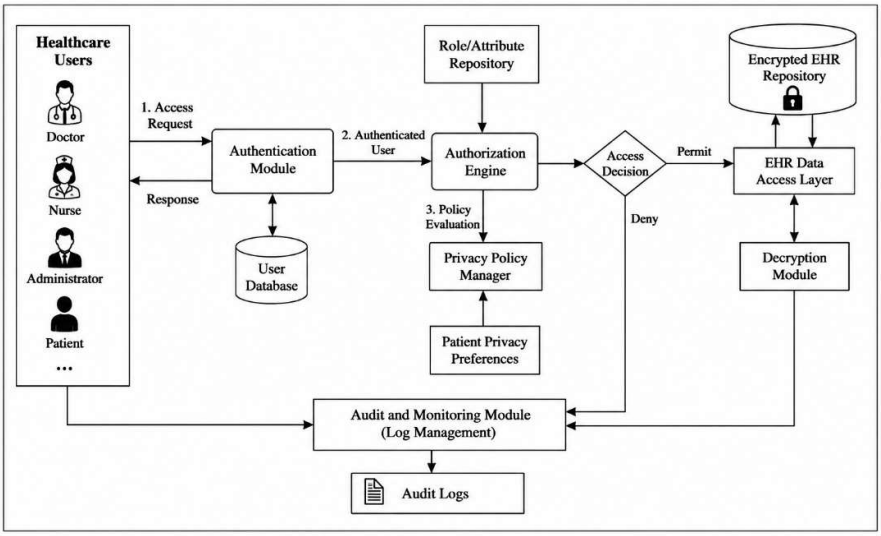


Figure 1. Proposed Privacy-Preserving Access Control Framework

5

. Methodology

The proposed Privacy-Preserving Access Control (PPAC) methodology secures Electronic Health Record (EHR) systems by integrating authentication, authorization, encryption, and audit logging into a unified access control process. The methodology is designed to ensure that only authenticated and authorized healthcare professionals can access patient records while preserving the confidentiality and integrity of sensitive medical information.

Initially, every user submits authentication credentials to the security server. The authentication module verifies the user's identity against the registered user database. If authentication fails, the request is rejected immediately. Successful authentication forwards the request to the authorization engine, where the user's role and access privileges are evaluated according to predefined organizational policies.

After authorization, the privacy policy manager examines patient-defined access preferences to determine whether the requested information can be disclosed. The authorization decision is then compared with the requested healthcare resource. Only when all security conditions are satisfied does the system retrieve the encrypted Electronic Health Record from the secure repository. The requested information is decrypted temporarily for the

authorized user and delivered through a secure communication channel.

Every transaction is simultaneously recorded in the audit management system. The audit log maintains the user's identity, accessed resource, timestamp, and access status, thereby providing accountability and facilitating future security investigations. The proposed methodology minimizes unauthorized disclosure while supporting efficient healthcare information sharing among legitimate medical professionals.

Algorithm 1: Privacy-Preserving Access Control

Input: *User Request (UR), User Credentials (UC), Patient Record (PR)*

Output: *Access Granted / Access Denied*

Step 1: *Receive access request from healthcare user.*

Step 2: *Verify user authentication credentials.*

Step 3: *If authentication fails, terminate the request.*

Step 4: *Retrieve the user's access privileges.*

Step 5: *Evaluate authorization policy.*

Step 6: *Verify patient privacy preferences.*

Step 7: *If authorization conditions are satisfied, retrieve the encrypted patient record.*

Step 8: *Decrypt the requested information.*

Step 9: *Deliver the Electronic Health Record to the authorized user.*

Step 10: *Record the transaction in the audit log.*

Step 11: *End the process.*

Computational Complexity

Let **n** represent the number of registered users and **m** represent the number of access policies. Authentication requires a constant-time credential verification under indexed storage, while authorization involves policy evaluation proportional to the number of applicable policies. Consequently, the overall access decision can be approximated as **O(m)** for policy evaluation, whereas audit logging requires constant time **O(1)** for recording each transaction. Since policy evaluation dominates the execution process, the proposed framework provides efficient access control suitable for medium- and large-scale healthcare information systems.

6. Results and Discussion

The proposed Privacy-Preserving Access Control (PPAC) framework was evaluated through functional analysis by considering the essential security requirements of Electronic Health Record (EHR) systems. The evaluation focuses on authentication, authorization, privacy protection, encrypted data storage, and audit management. The proposed framework was compared with conventional Role-Based Access Control (RBAC) and basic authentication-based security approaches commonly adopted in healthcare information systems before 2016. The comparison demonstrates that integrating privacy policies with fine-grained authorization improves confidentiality while maintaining efficient access to medical records.

The proposed framework successfully authenticates healthcare users before processing access requests and evaluates authorization policies based on user privileges and patient privacy preferences. Unauthorized requests are rejected automatically, whereas legitimate users receive controlled access to encrypted medical information. In addition, every transaction is recorded through audit logs, improving accountability and simplifying security monitoring. These characteristics reduce the possibility of unauthorized disclosure and insider misuse while preserving the availability of healthcare services.

Table 1. Comparison of Access Control Mechanisms

Security Feature	Traditional Authentication	RBAC	Proposed PPAC Framework
User Authentication	Yes	Yes	Yes

Role-Based Authorization	No	Yes	Yes
Fine-Grained Access Control	No	Limited	Yes
Patient Privacy Policies	No	No	Yes
Encrypted Data Protection	Limited	Limited	Yes
Audit Logging	Partial	Yes	Yes
Secure Information Sharing	Limited	Moderate	High
Privacy Preservation	Low	Medium	High

The comparison indicates that the proposed framework provides stronger privacy protection than conventional authentication mechanisms and standard RBAC models. By integrating patient-defined privacy policies with encrypted Electronic Health Records, the framework offers improved control over sensitive medical information while maintaining efficient access for authorized healthcare professionals.

Discussion

Healthcare organizations increasingly require secure mechanisms for sharing patient information across multiple departments without compromising confidentiality. Conventional access control approaches primarily rely on user authentication and predefined organizational roles, which may not adequately protect highly sensitive medical records. The proposed framework addresses this limitation by introducing policy-driven authorization combined with encrypted data storage and comprehensive audit logging.

The incorporation of patient privacy preferences enables greater control over healthcare information disclosure while ensuring that authorized clinicians continue to receive timely access during routine medical treatment. Furthermore, the audit management component strengthens accountability by maintaining detailed records of every access transaction. Consequently, the proposed framework improves the overall security posture of Electronic Health Record systems while supporting reliable and privacy-preserving healthcare information management.

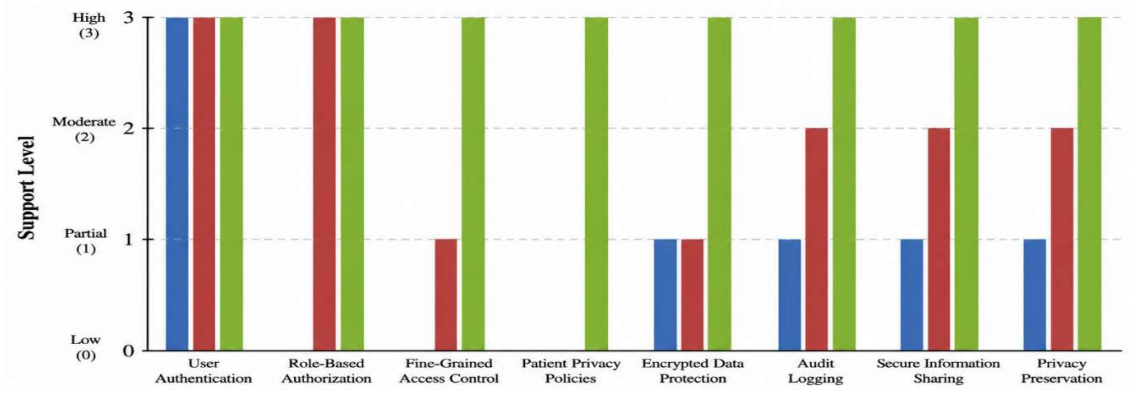


Figure 3. Security Feature Comparison of Access Control Models

7. Conclusion

The increasing adoption of Electronic Health Record (EHR) systems has significantly improved healthcare information management while simultaneously introducing new privacy and security challenges. Protecting sensitive patient information requires access control mechanisms that not only authenticate users but also regulate information disclosure according to organizational policies and patient privacy requirements.

Conventional access control approaches primarily rely on user authentication and predefined roles, which are often insufficient for protecting confidential healthcare information in dynamic clinical environments.

This research presented a Privacy-Preserving Access Control (PPAC) framework for Electronic Health Record systems that integrates authentication, authorization, privacy policy enforcement, encrypted data storage, and audit management into a unified security model. The proposed framework evaluates every access request before permitting retrieval of medical records, thereby minimizing unauthorized disclosure and improving accountability. The incorporation of patient privacy preferences further strengthens confidentiality while maintaining the availability of healthcare information for authorized medical professionals.

The comparative evaluation demonstrated that the proposed framework provides improved privacy protection, fine-grained authorization, secure information sharing, and comprehensive audit logging compared with conventional authentication-based and Role-Based Access Control (RBAC) approaches. The framework effectively balances healthcare accessibility with patient confidentiality, making it suitable for secure Electronic Health Record environments.

Overall, the proposed Privacy-Preserving Access Control framework enhances the confidentiality, integrity, and availability of healthcare information while supporting secure clinical decision-making and reliable healthcare service delivery.

Future Scope

Future research may extend the proposed framework by incorporating cloud-based Electronic Health Record infrastructures, allowing secure healthcare information sharing across geographically distributed medical organizations. Emerging cryptographic techniques, including advanced attribute-based encryption and searchable encryption, may further improve privacy preservation without affecting system performance.

The framework may also be enhanced through context-aware access control, enabling authorization decisions based on location, device type, emergency conditions, and real-time clinical requirements. Furthermore, integrating biometric authentication and multi-factor authentication can strengthen user verification while reducing the risk of credential compromise.

Another promising research direction involves applying blockchain technology to maintain immutable audit logs and improve trust among healthcare institutions. The integration of machine learning techniques for anomaly detection may further assist healthcare organizations in identifying suspicious access patterns and preventing insider attacks. These advancements have the potential to improve the scalability, interoperability, and overall security of future Electronic Health Record systems while preserving patient privacy.

References

1) R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based Access Control Models," *IEEE Computer*, vol. 29, no. 2, pp. 38–47, 1996.
2) D. Ferraiolo, R. Sandhu, S. Gavrila, D. Kuhn, and R. Chandramouli, "Proposed NIST Standard for Role-Based Access Control," *ACM Transactions on Information and System Security*, vol. 4, no. 3, pp. 224–274, 2001.
3) A. C. Myers and B. Liskov, "Protecting Privacy Using the Decentralized Label Model," *ACM Transactions on Software Engineering and Methodology*, vol. 9, no. 4, pp. 410–442, 2000.

4) M. Blaze, G. Bleumer, and M. Strauss, "Decentralized Trust Management," *Proceedings of IEEE Symposium on Security and Privacy*, pp. 164–173, 1996.
5) V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," *Proceedings of ACM CCS*, pp. 89–98, 2006.
6) J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," *Proceedings of IEEE Symposium on Security and Privacy*, pp. 321–334, 2007.
7) M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131–143, 2013.
8) M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 51–58, 2010.
9) K. D. Mandl, P. Szolovits, and I. S. Kohane, "Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private," *British Medical Journal*, vol. 322, no. 7281, pp. 283–287, 2001.
10) L. Zhou and V. Varadharajan, "A Secure Role-Based Access Control Framework for Health Information Systems," *Information Systems Frontiers*, vol. 12, no. 1, pp. 43–55, 2010.
11) A. Appari and M. E. Johnson, "Information Security and Privacy in Healthcare: Current State of Research," *International Journal of Internet and Enterprise Management*, vol. 6, no. 4, pp. 279–314, 2010.
12) M. A. Kaelber and D. W. Bates, "Health Information Exchange and Patient Safety," *Journal of Biomedical Informatics*, vol. 40, no. 6, pp. S40–S45, 2007.
13) D. Dolev and A. C. Yao, "On the Security of Public Key Protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.
14) L. Lamport, "Password Authentication with Insecure Communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.
15) R. Anderson, "A Security Policy Model for Clinical Information Systems," *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 30–43, 1996.
16) C. A. Ardagna, M. Cremonini, S. De Capitani di Vimercati, and P. Samarati, "Supporting Location-Based Conditions in Access Control Policies," *Proceedings of the ACM Symposium on Information, Computer and Communications Security*, pp. 212–222, 2006.
17) K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.