Privacy-Preserving Access Control Model for E-medical Systems

Abstract—**With the high speed development of information technology, the healthcare system increasingly relies on cloud servers for data storage and complex computation, patient data privacy issues stem from healthcare systems' vulnerability to breaches, despite data encryption emphasis, insufficient focus on preventing unauthorized access risks compromises patient information confidentiality. Consequently, the need to protect privacy within the healthcare system has gained significant attentions. However, existing research primarily concentrates on data encryption processes, but there is comparatively less attention given to addressing potential privacy leaks concerning data visitors. In this paper, we propose a privacy-preserving access control model for healthcare cloud data visitors. Our model combines the RBAC (Role-Based Access Control) model with the PSI (Private Set Intersection) technique to ensure the privacy and security of data visitors. The performance analysis of our proposed solution demonstrates its relative efficiency and practicality when applied to E-medical systems.**

Index Terms—**E-medical; PSI; Privacy-preserving; Access control**

I. Introduction

With the advent of the digital age, cloud computing has gained widespread popularity across various industries due to its robust computing capabilities, ample storage capacity, and efficient resource allocation operations [1]. It has found extensive applications in fields such as healthcare, scientific research, and commerce. With the rapid development of medical information, electronic medical records (EMR) and electronic health records (EHR), as important carriers of medical information systems, are playing an increasingly important role in medical information systems. EMRs enable patients to stay updated on their own medical conditions, aiding in their recovery process; For doctors, it can save consultation time while effectively accumulating reliable medical data, bringing great convenience to both doctors and patients. While the medical cloud, as a distinct application domain within cloud computing, has significantly enhanced the convenience and accuracy of public healthcare services, it also presents challenges related to the handling of highly sensitive patient information (e.g., personal details, contact information, specific medical conditions). The potential risks include data breaches, theft, and the subsequent consequences of privacy invasion, such as harassing phone calls or denial of insurance compensation. Such incidents pose threats to the personal and property security of individuals, inflicting irreparable losses to medical organizations and patients.

A. Privacy in E-medical

Access control has become a critical technology for ensuring information security in the field of electronic healthcare. It plays a significant role in securely safeguarding electronic health records (EHR) data, thereby protecting sensitive information. By governing and restricting the authorized actions of individuals with access rights (such as doctors, patients, nurses, etc.) on specific entities (such as electronic medical records, EHR, etc.), access control effectively prevents unauthorized access to these entities and unauthorized activities by legitimate users. As a result, it ensures that electronic medical resources are utilized in a controlled and legal manner. Therefore, it is crucial to design appropriate encryption and access control mechanisms that meet the specific requirements of protecting the privacy of medical data [2].

An **access control policy** establishes rules for authorized resource or information access, vital for data protection in sectors like healthcare and finance. It includes authentication, authorization, and enforcement mechanisms, deploying techniques like RBAC, MAC, DAC, and ABAC to preserve data integrity, confidentiality, and availability, thwarting unauthorized breaches. The existing research on access control in healthcare cloud primarily focuses on data encryption and the authorization access process, but less focusing on the protection of visitors' personal data. Among various access control techniques, the role-based access control (RBAC) model has gained popularity as it enables the logical separation of users and permissions by introducing roles. **In this paper**, we present a privacy-preserving access control model based on the RBAC model for data visitors (such as doctors, healthcare organizations, patients, etc.) in the medical cloud environment. The proposed model effectively addresses the issue of private data leakage for data visitors and caters to the personalized privacy requirements of different visitors. Firstly, our model ensures that the medical cloud is only aware of the visitor's role information that aligns with the access policy, without any knowledge of additional roles the visitor may possess. This guarantees the confidentiality of visitor information. Secondly,

This work was supported by the National Natural Science Foundation of China under Grant No. 62072105.

Corresponding author: lxiangchen@fjnu.edu.cn

in scenarios where the visitor's role significantly deviates from the access control policy, the medical cloud remains unaware of the visitor's role, thereby providing complete privacy protection. Moreover, our model demonstrates adaptability in emergency situations, further enhancing its convenience and usability.

B. Contribution

The contribution of this paper lies in addressing the privacy protection issues in medical information systems, particularly focusing on the data security concerns within medical clouds. The contributions of our work are as follows:

(1) Recognizing the importance of privacy protection for access requesters (such as patients, doctors, and medical institutions), we address a research gap where existing studies primarily focus on data encryption and access control.

(2) We propose a privacy-preserving access control model for e-medical systems by combining role-based access control with the PSI protocol. Our model aims to ensure that users obtain appropriate access rights while minimizing the exposure of private information to access requesters on medical cloud servers. This approach effectively addresses the issue of privacy data leakage for access requesters.

(3) Our presented model is secure again malicious adversaries, and it demonstrates relative efficiency and practicality when applied to e-medical systems.

C. Overview of the Paper

The subsequent sections of this paper are organized as follows: Section 2 discusses the related work. Section 3 presents fundamental concepts and definitions. Section 4 introduces the medical information system model. Lastly, Section 5 presents the protocol for the medical system.

II. Related work

In this section, we discuss recent studies related to privacy protection in cloud-based EHR systems. In 2018, the work [4] by Seol *et al.* presented a cloud-based EHR model that incorporates attribute-based access control using an extensible access control markup language. The model ensures secure exchange of medical documents through XML encryption and XML digital signature techniques. Pandey *et al.* [5] proposed a secret sharing scheme based on the Chinese remainder theorem to segment medical images into multiple shared images. This approach addresses the issue of legal ownership of information and allows the recovery of medical information by the authorized entity. Liu *et al.* [6] introduced an efficient framework for retrieving traditional Chinese medicine medical records from a medical cloud. The framework enables accurate retrieval of target cases from electronic medical records and offers template-based medical report visualization. Liu *et al.* [8] proposed a fine-grained EHR access control scheme based on the standard model. The scheme addresses privacy security and resource constraints in data transmission within EHR systems, enhancing privacy and security while optimizing computational resources. Zhang *et al.* applied cryptographic access control techniques to enhance privacy in integrated health records systems in work [9], and their policy-hiding technique encrypts access policies alongside patient data, offering flexible sharing while protecting privacy and addressing governance and accountability challenges. In 2019, a work [7] by Yang *et al.* presented a dual access control mechanism adaptable to normal and emergency situations in healthcare systems. The mechanism grants access to healthcare professionals under normal conditions and employs a password-based broken-glass access mechanism in emergencies, ensuring secure and controlled access to medical data. In 2020, the study [3] by Prince *et al.* introduced a revolutionary access control model that prioritizes healthcare data privacy, confidentiality, and availability. The model utilizes a privacy level approach to meet user requirements and ensure proper data access. However, these works paid less attentions on the privacy disclose problem of data visitor. In 2022, *Yang et al.* introduced privacy-preserving record linkage techniques for large attribute domains using property-preserving encryption and PSI, and their protocol enabled secure matching by converting attributes into private set insertion representations. However, these techniques require substantial computational resources due to heavy computation. Building on these related works, our study aims to address privacy concerns in record linkage by leveraging private set insertion (PSI) and RBAC, this forms the main motivation for our research.

III. Preliminaries

In this section, we present the fundamental concepts and definitions that will be employed in the following sections.

A. Notations

The notations used in this paper is illustrated in TABLE I.

TABLE I: Notations

Variable	Description	Variable	Description
DU	Data user	MC	Medical cloud
MI	Medical institutions	CA	Central authority
S	Sender in PSI	R	Receiver in PSI
i	U/S set index	j	MC/R set index
X	Receiver's set	Y	Sender's set
x_i	An element of X	y_j	An element of Y
SP	System par.	1^{λ}	len. λ sec. par.
PKG	Private key generator	O	Output $X \cap Y$
H_1, H_2	Hash function	g, h	Generators
exp	Exponentiation	pair	Bilinear pairing

B. Role-Based Access Control

Access control is a crucial technology for safeguarding the security of information systems. Its primary objective is to regulate the access authorization of subjects, such as users, programs, and systems, to specific resources, including files, data, and processes. The access control model ensures that authorized users can appropriately access system resources within the confines of their legal authorization, while unauthorized users are prohibited from accessing such resources. RBAC is an efficient and widely used access control model in complex environments. It consists of four interconnected concepts: subject, object, role, and permission. Roles, rather than users, are assigned permissions, enabling a separation between users and permissions. Subjects can have multiple roles, and roles can be assigned to different subjects. Similarly, permissions can be associated with multiple objects, and objects can be accessed with different permissions. The relationship between subjects and objects is established through roles and permissions. Users obtain roles upon entering the system, and access control is enforced by policies that link users to roles and the corresponding permissions. Unlike traditional methods, RBAC offers a flexible and scalable approach to authorization management. See Fig. 1 for an illustration of the relationships between users, roles, objects, and permissions in the RBAC model.

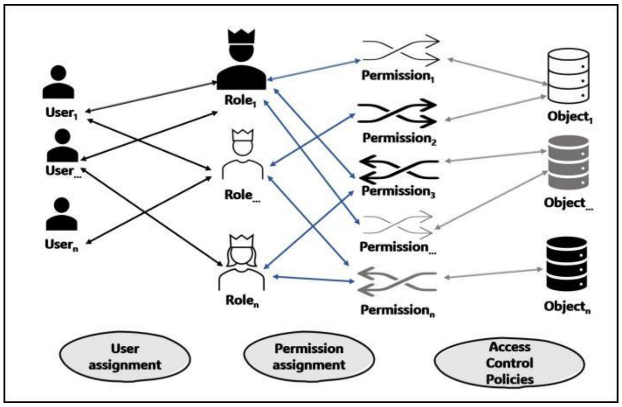


Fig. 1: RBAC model

C. Private Set Intersection (PSI)

Private set intersection techniques are a vital component of secure multiparty computing. The 2-party PSI protocols enable two parties, each holding private sets X and Y , to collaboratively compute the intersection $X \cap Y$ without revealing any additional information about their respective sets. In essence, generalized secure computing protocols have the potential to address various privacy computing problems. As hospitals share medical information and there is a growing need for medical experts to conduct joint research while preserving data privacy, medical institutions are increasingly investing in privacy computing technologies.

D. Hardness Assumption

Computational Diffie-Hellman (CDH) : Let $\mathbb{G}_q$ is a group of order q, g is a generator of $\mathbb{G}_q$. $a, b \in \mathbb{Z}_p^*$. The CDH problem is a given tuple (g^a, g^b, g^c), compute g^{ab}. In general, the assumption of CDH is that there is no probability polynomial time algorithm that can solve the CDH problem with an undeniable advantage.

IV. System Model

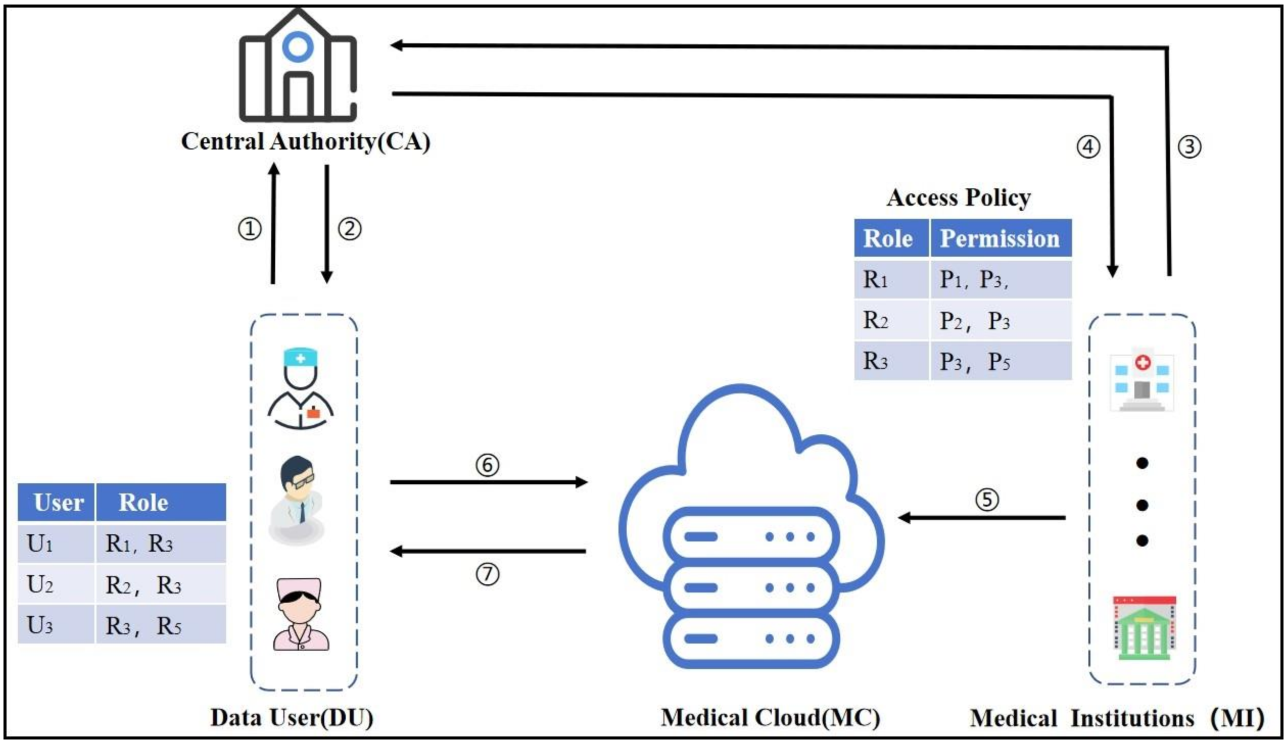
A. System Model

Our system model is illustrated in Fig. 2. There are four primary entities as below:

- **Data User (DU)**: Users, including doctors, patients, or family members of patients, can request access to the medical system. Prior to applying for access, each user is required to verify their identity (using ID, password, fingerprint, etc.) with the central authority. Once the role request is successfully authenticated by the central authority, a set of roles is sent to the user.
- **Medical Cloud (MC)**: Medical Cloud refers to the public cloud server of the medical system, which can provide storage of health records, electronic medical records, and computing resources for different medical institutions, respond to user data access queries, verify the legitimacy of DU, match user roles and access policies, and if the match is successful, visitors will obtain access permissions. However, MC is also an honest and curious entity that can honestly execute protocols, also be curious about the data stored in the public cloud.
- **Medical Institutions (MI)**: MI encompass health clinics, hospitals, medical research institutes, and similar establishments that possess patient information and medical experimental data for healthcare purposes. As the custodians of medical and health records, MI maintains ownership and control over the data. It is the responsibility of MI to upload access policies certified by CA and encrypted data to the MC.
- **Central Authority (CA)**: CA is fully trusted and serves as the system manager in the system, mainly responsible for generating system parameters, user authentication, and managing roles. CA plays a central role in the access control process, acting as an intermediary between users and cloud servers. Its responsibilities include authenticating users and their assigned roles and ensuring that access requests comply with predefined access policies. The role of the authentication center is to establish a link between the authority of the operation object and the subject, achieving a separation between the subject and the authority. This separation can fine-grained access control effectively.

Our work aims to enable authorized users to gain legal access while minimizing the exposure of user information to the public cloud. To achieve this security objective, the protection of user's private information is ensured by restricting the provider's access to requester's information, allowing only the disclosure of roles that match the permissions during the resource access request process. Notably, the user's role information remains fully protected in cases where the user's privilege operation access request fails to align with the access control policy. The detailed explanation of the system subprocess depicted in Fig. 3 is provided below.

① DU initiates an application to CA for authentication of their own ID credentials (password, fingerprint, facial



Role	Permission
R_1	P_1, P_3,
R_2	P_2, P_3
R_3	P_3, P_5

User	Role
U_1	R_1, R_3
U_2	R_2, R_3
U_3	R_3, R_5

Fig. 2: System Model

recognition, etc.) in order to obtain tickets for accessing resources.

② CA authenticates DU based on its ID, and if DU fails system authentication, it is forced to exit; If pass, the system will relevant business logic implementation, etc., and assign the corresponding set of role to DU.

③ MI sends a policy and identity authentication response to CA.

④ CA distributes the set of authenticated roles to the MI based on the security policy request submitted by the MI.

⑤ MI uploads data such as CA-authenticated access policies to the MC.

⑥ DU sends access requests to the MC.

⑦ MC responds to the access request from user. The two parties interact to execute the PSI protocol to confirm whether the role applying for access privileges is in compliance with the access policy, and if so, returns a response that allows access, otherwise, returns a response that denies access.

V. The Proposed Scheme

Our scheme addresses the issue of privacy protection for data visitors in healthcare systems. It introduces an access control scheme that combines the RBAC model and PSI techniques to achieve privacy-preserving access control. For simplify description, the set of authentication roles held by the healthcare data visitor is denoted as $X = \{x_1, \cdot\cdot\cdot, x_n\}$, while the set of authentication roles on the medical cloud is denoted as $Y = \{y_1, \cdot\cdot\cdot, y_k\}$. In the system model, the healthcare data visitor aims to prevent the disclosure of any private information beyond the intersection of roles to the healthcare cloud, while still maintaining legal authorization for data access. Under the assumption that the participants do not collude with the untrustworthy cloud, The primary result of our work is outlined as follows:

A. System setup

Given the security parameter λ as input, the key generation center (PKG) generates the system parameter. The detailed procedures are described as follows.

- Step 1: PKG generates a G_q, which is the subgroup of Z_p^* with prime order q, and g is generator of G_q, $p = 2q + 1$ is prime.
- Step 2: Choose two full-domain hash functions H_1, H_2 where $H_1 : \{0, 1\}^* \to G_q$, $H_2 : G_q \to \{0, 1\}^l$.

B. Identity authentication

CA is responsible for handling authorization services, which involve role-permission assignment and management. In order to gain access to the medical cloud, users are required to apply for identity authorization from the central authority. The detailed procedures are described as follows.

- Step 1: DU submits their ID and other identification documents to CA for the purpose of applying for identity authentication.
- Step 2: DU is authenticated based on their ID, and if DU fails the system verification, They were rejected. If DU passes the authentication, the CA will assess and analyze DU based on system configurations, relevant business

logic, and other factors, and allocate the corresponding authorized role set X to the user.

C. Policy authentication response

The step-by-step process followed by MI when sending authorization requests for access policy to CA is as follows:

- Step 1: MI formulates access control policies for all roles based on the system configuration and submits them to the central authority to apply for CA.
- Step 2: CA responds to MI's request and verifies medical institutions's authorization request. If the validation is successful, return the authorized role set Y , otherwise return a null value.

D. Access and acquisition of resources

This stage primarily consists of two main parts: the authentication of access requests and the matching of access policies. These objectives can be accomplished by executing the PSI protocol.

- Step 1: DU sends access requests to the MD, and the MD verifies the validity of the request. If the request passes the verification process, the system proceeds to execute the PSI protocol between the DU and the MD. However, if the request fails to pass the verification, the system rejects the request and terminates the access attempt.
- Step 2: The system executes the PSI protocol (as depicted in Fig. 3) to perform the necessary computations and obtain the intersection of roles. If the user's role matches the role associated with the access control policy, the system allows the user's role to execute the corresponding permissions, thereby enabling access. However, if there is no match or the output of the PSI protocol is empty, access is denied as DU does not meet the requirements of the access policy.

E. Privacy protection algorithm in the medical cloud

In this section, our focusing is on the algorithm for privacy protection and access control schemes within the medical cloud environment. Taking inspiration from the work by Chu *et al.* [10], we propose a practical PSI protocol based on the k-out-of-n miraculous oblivious transfer (OT) protocol. The detailed algorithm is presented in Fig. 3.

VI. Analysis and Evaluation

A. Correctness Analysis

In this subsection, we provide a correctness analysis of our proposed protocol. Based on the proposed PSI protocol, we hold K_j where

$$K_j = \frac{D_i}{B^\beta} = \frac{D_i}{B^\beta} = \frac{(A_j)^\alpha}{(g^\alpha)^\beta}$$

and we run the intersecting algorithm $\mathsf{Match}(H_1(y_j), H_1(x_i))$ as below:

$$\begin{aligned} &\mathsf{Match}(H_1(y_j),\ H_1(x_i)) \\ &= C_i \oplus H_2(K_j) \\ &= \ H_2(H_1(x_i))^\alpha) \ \oplus \ H_2((H_1(y_j))^\alpha) \end{aligned}$$

Initialization:

1. Assuming λ is a security parameter, PKG generates a G_q, which is the subgroup of Z_p^* with prime order q, and g is generator of G_q, $p = 2q + 1$ is prime.
2. H_1, H_2 are two full-domain hash functions. H_1 : $\{0, 1\}^* \to G_q$, $H_2 : G_q \to \{0, 1\}^l$.
3. The system parameter SP = (g, H_1, H_2, G_q).

Input:

1. DU (sender) in PSI protocol, owns a private set $X = \{x_1, \cdots, x_n\}$ in our PSI protocol.
2. MC (receiver) role in PSI protocol, owns a private set $Y = \{y_1, \cdots, y_k\}$ in our PSI protocol.

Protocol:

1. MC : picks a random $\beta \in Z_p^*$ as the secret key, compute $A_j = H_1(y_j) \cdot g^\beta$, where $j \in [1, k]$.
2. MC → DU : MC sends $\{A_1, A_2, \cdots, A_k\}$ to DU.
3. DU picks a random $\alpha \in Z_p^*$ as the secret key, $B = g^\alpha$, $D_j = (A_j)^\alpha$, $C_i = H_2(H_1(x_i)^\alpha)$, where $i \in [1, n]$.
4. DU → MC : DU sends B, $\{C_1, \cdots, C_n\}$, $\{D_1, \cdots, D_k\}$ to MC.
5. MC computes the outputs through running matching algorithm as: $\forall j$, computes $K_j = \frac{D_i}{B^\beta}$, and $\mathsf{Match}(H_1(y_j),\ H_1(x_i))$.

Output: Output $X \cap Y$ for MC, No output for U.

Fig. 3: Our Model based on PSI for E-medical Systems

In the matching algorithm, the condition for $\mathsf{Match}(H_1(y_j),\ H_1(x_i)) = 0$ is that $H_1(y_j) = H_1(x_i)$. Otherwise, $\mathsf{Match}(H_1(y_j),\ H_1(x_i))$ outputs as a random value.

B. Performance Evaluation

In this subsection, we present a performance evaluation of our approach, considering factors such as communication overhead and computational complexity. The details are outlined below:

1) *Communication Overhead:*

- From MC to DU , MC needs to send k elements under G to the DU, and it is liner complexity with $|Y|$.
- From DU to MC, it needs to send $k + n + 1$ elements (one element under G, $K + n$ elements under H_2 which is l bits length).
- The total communication cost amounts to $2k + n + 1$ elements, indicating a linear overall communication complexity.

2) *Computational Complexity:*

- MC requires k times modulo exponentiation, H_1 and modulo multiplication which under G, However, achieving this goal comes at the expense of increased computation, primarily performed on MC side. While this process can be costly, it is a necessary step to strike the desired balance between communication and computation efficiency in medical could systems.

TABLE II: Scheme Comparison

Scheme	Communication	Computation	Key Tech	Policy Hidden
[9]	$(3k+4)\|G\| + 2n(\|G_T\|$	$(6k+2n+3)$ **exp** $+ (2n+4)$ **pair**	CP-ABE	No
[11]	$(2k+34)\|G\| + n^2/2 + 3\lambda\ \|G_T\|$	$(\lambda \cdot k + kn)$ **exp** $+ (2n^2)$ **pair**	PSI	Yes
Ours	$(k+n+1)\|G\|$	$(3n+k+1)$ **exp** $+ 0$ **pair**	PSI	Yes

- DU in protocol needs to compute $3n + 1$ modulo exponentiation, n times H_1 and H_2 under G.
- The total computational cost consists of $3n+k+1$ modulo exponentiation operations, as well as $n + k$ computations of H_1 and n computations of H_2 within G, indicating a linear overall computational complexity.

3) Efficiency Comparison: In this subsection, we present a comparison of the communication and computation costs, as illustrated in the detailed results in Table II. Through comparison, our solution exhibits lower communicationoverhead compared to the other two approaches.

VII. Conclusion

In this paper, we introduce a privacy-preserving access control model designed specifically for visitors accessing healthcare cloud services. The model addresses privacy concerns related to data access by leveraging the RBAC model. Our proposed approach effectively tackles the problem of role leakage among healthcare cloud visitors through the integration of the PSI protocol. Notably, the model guarantees comprehensive privacy protection for visitors in cases where their roles do not align with the access control requirements of the healthcare cloud.

References

[1] C. Stergiou and K. E. Psannis, "Recent advances delivered by mobile cloud computing and internet of things for big data applications: a survey," *International Journal of Network Management*, vol. 27, no. 3, p. e1930, 2017.

[2] C. S. Kruse, B. Smith, H. Vanderlinden, and A. Nealand, "Security techniques for the electronic health records," *Journal of medical systems*, vol. 41, pp. 1–9, 2017.

[3] P. B. Prince and S. J. Lovesum, "Privacy enforced access control model for secured data handling in cloud-based pervasive health care system," *SN Computer Science*, vol. 1, no. 5, p. 239, 2020.

[4] K. Seol, Y.-G. Kim, E. Lee, Y.-D. Seo, and D.-K. Baik, "Privacy-preserving attribute-based access control model for xml-based electronic health record system," *IEEE Access*, vol. 6, pp. 9114–9128, 2018.

[5] A. K. Pandey, P. Singh, N. Agarwal, and B. Raman, "Secmed: A secure approach for proving rightful ownership of medical images in encrypted domain over cloud," in *2018 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)*, pp. 390–395, IEEE, 2018.

[6] L. Liu, L. Liu, X. Fu, Q. Huang, X. Zhang, and Y. Zhang, "A cloud-based framework for large-scale traditional chinese medical record retrieval," *Journal of biomedical informatics*, vol. 77, pp. 21–33, 2018.

[7] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving smart iot-based healthcare big data storage and self-adaptive access control system," *Information Sciences*, vol. 479, pp. 567–592, 2019.

[8] Y. Liu, Y. Zhang, J. Ling, and Z. Liu, "Secure and fine-grained access control on e-healthcare records in mobile cloud computing," *Future Generation Computer Systems*, vol. 78, pp. 1020–1026, 2018.

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

[10] C.-K. Chu and W.-G. Tzeng, "Efficient k-out-of-n oblivious transfer schemes with adaptive and non-adaptive queries," in *Public Key Cryptography-PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23-26, 2005. Proceedings 8*, pp. 172–183, Springer, 2005.

[11] L. Yang, C. Li, Y. Cheng, S. Yu, and J. Ma, "Achieving privacy-preserving sensitive attributes for large universe based on private set intersection," *Information Sciences*, vol. 582, pp. 529–546, 2022.