Modelos de control de acceso más utilizados en la seguridad de datos médicos

Access control models most used in medical data security

Brian Campos-Montero
Universidad Nacional de Trujillo, Perú
bcampos@unitru.edu.pe
https://orcid.org/0000-0003-4198-9161
Cesar Rodríguez-Sandoval
Universidad Nacional de Trujillo., Perú
crodriguezs@unitru.edu.pe
https://orcid.org/0000-0002-3471-3557
Alberto Mendoza de los Santos
Universidad Nacional de Trujillo, Perú
amendozad@unitru.edu.pe
https://orcid.org/0000-0002-0469-915X

Recepción: 15 Enero 2023
Aprobación: 17 Mayo 2023

Acceso abierto diamante

Resumen

El acceso no autorizado a datos sensibles de pacientes es un problema que atenta contra ellos mismos y la seguridad de las organizaciones dedicadas al servicio de salud, para lo cual es fundamental implementar controles de acceso (CA), los cuales deben impedir el acceso y uso malintencionado de los datos, por ese motivo se hizo una investigación basada en revisión sistemática, utilizando como metodología a Prisma; además, se utilizó SCOPUS como base de datos incluyendo 82 artículos, que sirvieron para encontrar los modelos de control de acceso más utilizados; por consiguiente, se identificó 5 modelos que fueron los más utilizados (ABE, ABAC, RBAC, BBAC y MAC), representando un total del 52% de todos los estudios revisados, mientras que un 29% pertenecía a los que se implementaron una única vez y el 19% restante a las que surgieron por la solución de problemas identificados dentro de los 5 modelos de uso frecuente.

Palabras clave: Control de acceso, esquema, modelo, seguridad, datos médicos.

Abstract

Unauthorized access to sensitive patient data is a problem that threatens themselves and the security of organizations dedicated to the health service, for which it is essential to implement access controls (CA), which must prevent access and use malicious data, for this reason an investigation was carried out based on a systematic review, using Prisma as a methodology; In addition, SCOPUS was used as a database including 82 articles, which served to find the most used access control models; therefore, 5 models were identified that were the most used (ABE, ABAC, RBAC, BBAC and MAC), representing a total of 52% of all the studies reviewed, while 29% belonged to those that were implemented only once and the remaining 19% to those that arose from solving problems identified within the 5 frequently used models.

Keywords: Access control, scheme, model, security, medical data.

Introducción

En el sector de salud los datos médicos o los datos de pacientes son generados en grandes cantidades y son utilizados por diferentes actores de un sistema, por lo cual aquellos datos deben ser confidenciales y no deben ser compartidos a través de una red pública; sin embargo, el intercambio de datos de pacientes es necesario debido a que los médicos al encontrarse en diferentes ubicaciones físicas necesitan tomar decisiones con ayuda de la opinión de otros expertos, sin embargo, la privacidad de los datos es la principal preocupación, por lo cual dicho intercambio debe tener lugar en un proceso seguro y autenticado [1]. Por lo tanto, la seguridad de datos médicos debe enfocarse principalmente en proporcionar un equilibrio entre los riesgos de confidencialidad, integridad y disponibilidad [2]. Seguidamente, cabe mencionar primero que la confidencialidad se asegura de que ningún usuario no autorizado acceda a datos o recursos, segundo que la integridad se asegura de que los datos o recursos estén en su forma original y no sean modificados de forma intencional o accidental y por último la disponibilidad de recursos se asegura de que los datos o recursos estén accesibles y listos para su uso [3]. Para ello, es necesaria la implementación de controles de acceso (CA), ya que logran evitar el acceso ilegal a la información [2].

Un control de acceso está conformado por las fases de identificación, autorización y autenticación. En la fase de identificación, el usuario puede usar credenciales y autenticarse, después de proporcionar las credenciales correctas, el usuario queda autorizado para acceder solo a los recursos otorgados por un administrador a través de permisos o reglas de control de acceso; en conclusión, un control de acceso busca preservar la seguridad de los datos médicos, controlando el acceso a través de permisos a datos y recursos confidenciales. Además, cuando nos referimos a controles de acceso surge el concepto de modelos de control de acceso los cuales son representaciones formales de políticas de seguridad y mediante los cuales dichas políticas son implementadas y diseñadas de acuerdo a los escenarios y necesidades de la industria. [3]

Aquellos modelos también están relacionados con los privilegios que tiene una entidad al manejar objetos de datos particulares. Estos están basados en modelos de CA de identidad de usuario, como el control de acceso basado en roles (RBAC), control de acceso obligatorio (MAC) y control de acceso discrecional (DAC). Además de estos enfoques estáticos, se ha desarrollado el paradigma de control de acceso basado en atributos (ABAC), que es de naturaleza dinámica y flexible [4].

A los modelos de CA también se les conoce bajo la denominación de esquemas de control de acceso, de los cuales se han presentado muchos que adoptan el cifrado basado en atributos (ABE) para el CA detallado. Los usuarios con atributos que cumplan con la política de acceso pueden desencriptar los datos de registros médicos. Los esquemas de control de acceso basados en roles (RBAC) también permiten un CA detallado. Definen una política basada en roles para una organización jerárquica con cifrado de transmisión basado en identidad (HIBBE). Si bien las propuestas anteriores logran la confidencialidad de los datos médicos, la preservación de la privacidad de los pacientes sigue siendo un problema sin resolver. Sin embargo, al existir una falta de consideración con respecto a la privacidad de la identidad de los propietarios de registros médicos electrónicos, se pueden utilizar técnicas de anonimización para garantizar la privacidad de la identidad de los usuarios. Existen algunos esquemas ABE anónimos que abordan no solo la privacidad de los datos sino también la privacidad de la identidad; por ende, aquellos esquemas proporcionan un análisis de confidencialidad, anonimato y flexibilidad [76].

Metodología

Se llevó a cabo una revisión sistemática sobre toda la literatura científica encontrada, con el fin de rescatar la información más importante respecto al tema sobre modelos de control de acceso, con base en la adaptación de la metodología denominada PRISMA. La pregunta planteada para la investigación que fue desarrollada bajo el

proceso metodológico elegido fue: ¿Cuáles son los modelos de control de acceso más utilizados en la seguridad de datos médicos entre los años 2017 y 2022?

Fundamentación de la metodología

Las revisiones sistemáticas se basan en resúmenes presentados de forma clara y bien estructurada acerca de un tema de investigación específico, orientada a dar respuesta a una interrogante planteada a partir de un problema o tema de investigación. Además representan el más alto grado de evidencia debido a que están respaldadas por una variedad de fuentes de información con contenido verídico y confiable.

Proceso de recolección de información

Para la presente investigación se utilizó como base de datos a SCOPUS. El rango de años de búsqueda permitido incluyó publicaciones de los últimos cinco años, desde el 2017 hasta el 2022. Para el proceso de búsqueda de información, se partió de la pregunta de investigación planteada y se emplearon los siguientes términos: “Access control”, “Medical data”, “Medical record”, “Security”. Para lograr mayor efectividad en los resultados de la búsqueda, se realizaron muchas combinaciones entre los términos establecidos; además, se hizo uso de los operadores booleanos tal como se aprecia a continuación:

SCOPUS

(TITLE (“access control”) AND (TITLE-ABS-KEY (“medical data”) OR TITLE-ABS-KEY (“medical record”) OR TITLE-ABS-KEY (health))) AND PUBYEAR > 2016 AND (LIMIT-TO (OA , “all”)) AND (LIMIT-TO (PUBSTAGE , “final”)) AND (LIMIT-TO (DOCTYPE , “ar”)) AND (LIMIT-TO (LANGUAGE , “English”) OR LIMIT-TO (LANGUAGE , “Portuguese”) OR LIMIT-TO (LANGUAGE , “Spanish”))

Criterios de exclusión e inclusión

Figura 1
Diagrama de flujo de criterios de exclusión e inclusión de artículos

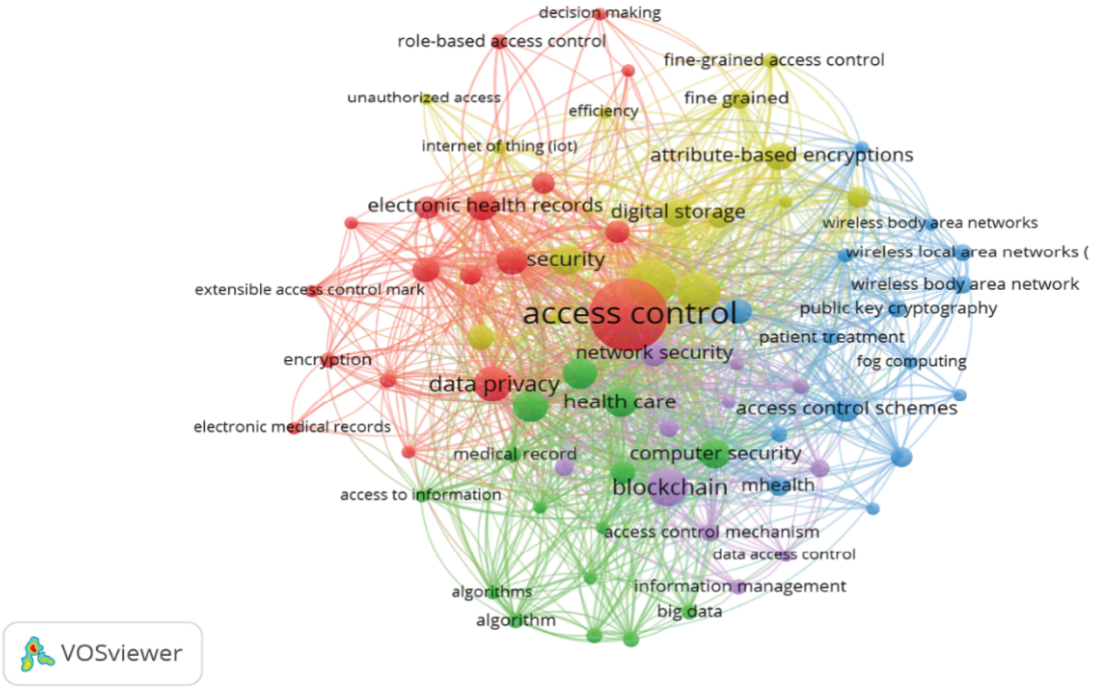

Figura 2
Red bibliométrica de palabras clave

Resultados

La red bibliométrica incluye las palabras claves más frecuentes encontrados en los artículos incluidos en la investigación. La red de palabras claves se originó de un total de 82 artículos de revisión, encontrados en la base de datos “Scopus”.

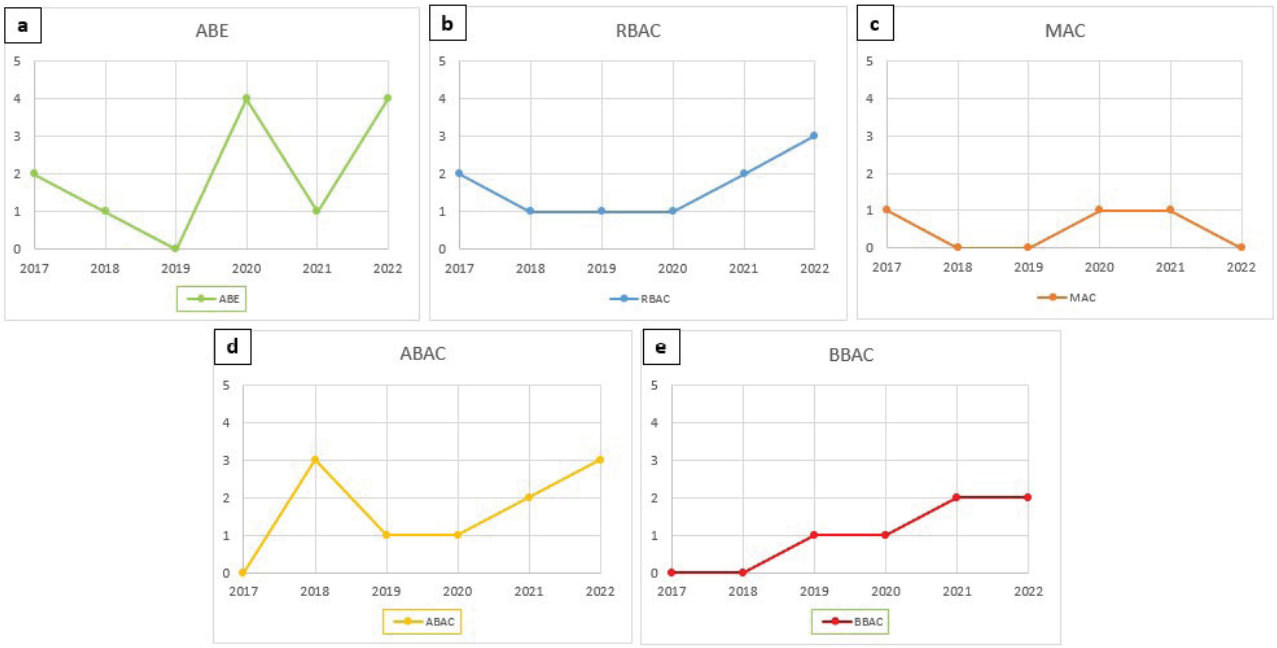

Figura 3

Tendencia de los modelos de control de acceso tradicionales a Cifrado basado en atributos b Control de acceso basado en roles c Control de acceso al medio d Control de acceso basado en atributos y e Control de acceso basado en blockcha

Cuadro 1
Problemas encontrados en los modelos de control de acceso tradicionales

Modelos de control de acceso	Problemas detallados en los estudios	N° referencia
Cifrado basado en atributos (ABE)	•Problema de escalabilidad una vez que aumenta el tamaño de los datos.	[33], [49]
	•Ausencia de mecanismo efectivo para llevar a cabo la revocación del derecho de acceso después de una emergencia.	[33], [41]
	•Requiere muchos recursos de almacenamiento.	[39]
	•Costos computacionales elevados en dispositivos móviles.	[39]
	•Filtraciones de la privacidad del propietario del PHR.	[44, 49]
	•Dificultad para identificar al usuario malicioso que intencionalmente reveló su clave privada (parcial o modificada).	[49]
	•No puede llevar el control del acceso a los flujos de datos de forma independiente.	[57]
	•Las políticas de acceso están en formato de texto no cifrado y revelan información confidencial relacionada con la salud en los registros de salud codificados.	[71]
	•De forma general admite una serie de atributos pequeños, obteniendo una limitante indeseable en los despliegues prácticos debido a que el tamaño de sus parámetros públicos crece linealmente con el tamaño de la serie.	[71]
	•La custodia, la exposición y el abuso de las claves privadas aún dificultan su aplicación práctica en el sistema PHR.	[73]
	•Sobrecarga computacional y demora en la función de cifrado	[78]
Control de acceso basado en atributos (ABAC)	•Carece de una semántica de relación detallada para el acceso a EHR con un mecanismo eficiente de preservación de la privacidad.	[56]
	•Dificulta el tratamiento de primeros auxilios cuando la vida del paciente está en peligro porque el personal de primeros auxilios en el sitio no está autorizado a obtener los datos médicos históricos del paciente.	[58]
Control de acceso basado en roles (RBAC)	•Requiere un gran número de reglas.	[59]
	•Proceso costoso para definir roles.	[59]

Cuadro 2.
Modelos de control de acceso mejorados derivados de la solución de los problemas presentes en los modelos mencionados en el cuadro 1.

N°	Modelos de control de acceso mejoradas	Modelos tradicionales		
		Cifrado basado en atributos (ABE)	Control de acceso basado en atributos (ABAC)	Control de acceso basado en roles (RBAC)
1	Control de acceso a datos para equipos de cuidados agudos (AC-AC)	✓		
2	Cifrado de búsqueda basado en atributos basado en contrato inteligente (SC-ABSE)	✓		
3	Búsqueda segura de múltiples palabras clave y control de acceso (SMKS-AC)	✓		
4	Cifrado basado en atributos de política de texto cifrado(CP-ABE) eficiente con capacidad de revocación de atributos (AC-FEH)	✓		
5	Cifrado basado en atributos de políticas de texto cifrado (CP-ABE) de ocultamiento de políticas ligero para el s-health orientada a IoT	✓		
6	Control de acceso rastreable y de ocultación de políticas detallado para Sistemas móviles de salud (HTAC)	✓		
7	Control de acceso basado en la semántica de relaciones con conciencia de privacidad (PRSX-AC)	✓		
8	ShareHealth control de acceso criptográficamente reforzado	✓		
9	Control de accesos de deduplicación		✓	
10	Control de acceso de múltiples capas (MLAC)		✓	✓
11	Control de acceso de grano fino.	✓		
12	Control de acceso a prueba de roturas		✓	
13	CP-ABE con políticas de acceso parcialmente ocultas (PASH)	✓		
14	Control de acceso basado en atributos de política de texto cifrado coordinado con responsabilidad de usuario (CCP-ABAC-UA)	✓		
15	Cifrado basado en atributos de política de texto cifrado CP-ABE basado en grupos modificado (G-CP-ABE)	✓		

Cuadro 3.
Modelos de control de acceso recientes implementados una sola vez.

N°	Modelos recientes utilizados solo una vez	N° referencia	Año
1	Marco de privacidad FAIR	[11]	2022
2	Control de acceso basado en token distribuido (DTAC)	[13]	2022
3	Control de acceso seguro y establecimiento de claves para un sistema de salud inteligente sostenible a largo plazo (ACM-SH)	[15]	2022
4	Control de acceso basado en reconocimiento facial	[16]	2022
5	Control de acceso de conclusión de clave (uso de múltiples claves generadas)	[18]	2022
6	Control de acceso dinámico	[19]	2022
7	Control de acceso y función física no clonable (PUF)	[22]	2022
8	Marco de control de acceso e intercambio de EHR	[23]	2022
9	Control de acceso adaptable al riesgo basado en la entropía	[24]	2022
10	Control de acceso de cifrado de signos heterogéneo	[28]	2022
11	Control de acceso de distribución de contenidos eficiente y segura (ES_CD)	[29]	2021
12	Distribución de contenidos eficiente y segura (ES_CD)	[31]	2021
13	Protocolo de límite de distancia (ACIMD)	[42]	2021
14	Niveles de acceso	[48]	2020
15	SoTRAACE (Control de acceso adaptable al riesgo sociotécnico)	[53]	2020
16	Marco de monitoreo remoto seguro y eficiente (SRM)	[55]	2019
17	Control de acceso sensible y enérgico (SE-AC)	[60]	2019
18	Control de acceso de autorización distribuída	[61]	2019
19	Control de Acceso de Emergencia (EACMS)	[62]	2019
20	Control de acceso ligero para dispositivos portátiles	[64]	2019
21	Control de acceso a sensores basado en aprendizaje por refuerzo	[65]	2019
22	Control de acceso que aplica un Analizador de similitud jerárquica (HSA)	[76]	2017
23	Control de acceso GeoXACML	[79]	2017

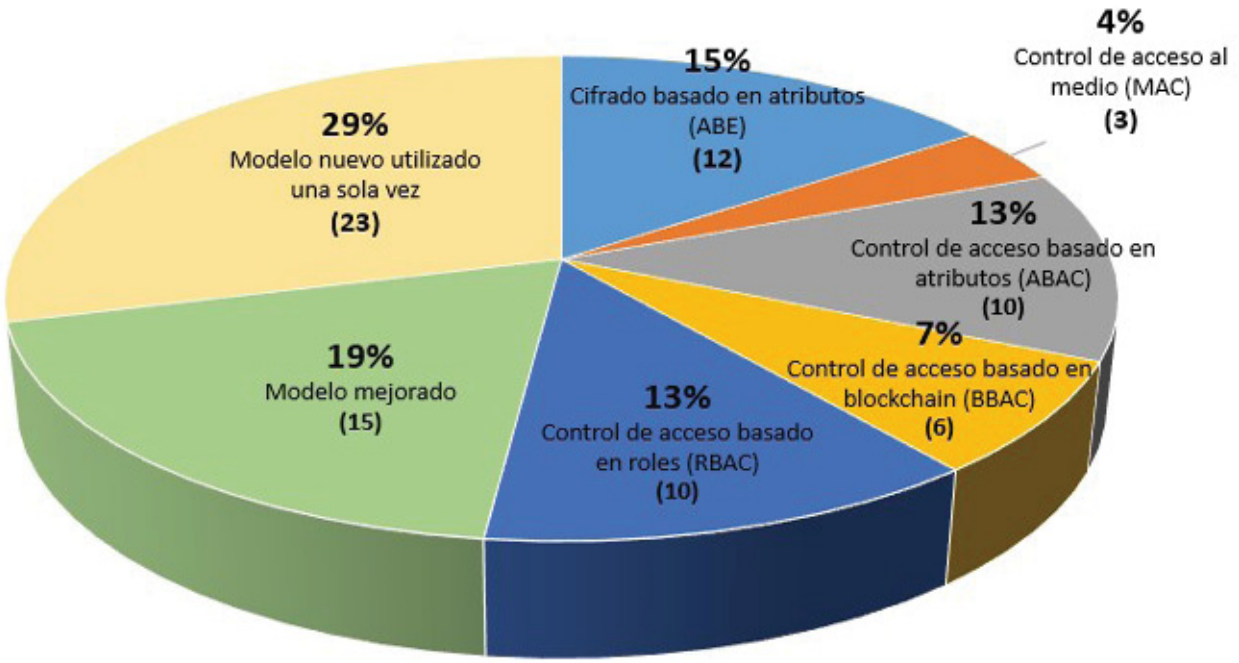

Figura 4.
Modelos de control de acceso encontrados.

Los modelos tradicionales en conjunto representan un 52% de todos los estudios encontrados, mientras que los modelos derivados de mejoras un 19% y los nuevos modelos un 29%.

Discusión

Luego de mostrar los resultados, continuamos discutiendo dicha información, se encontró 5 modelos de control de acceso tradicionales, estas son: el modelo de control de acceso basado en atributos (ABAC), basado en roles (RBAC), basado en blockchain (BBAC) y el cifrado basado en atributos (ABE), sin embargo la más utilizada es la última mencionada encontrada en 12 artículos, también se pudo obtener las tendencias de cada modelo de control de acceso entre los años 2017 y 2022 que se visualiza en la figura 3, interpretando que los modelos más antiguos son las de ABE y RBAC que vienen siendo implementados mucho antes del año 2017 mientras que las más actuales como ABAC y BBAC surgieron a partir del 2018, por último podemos observar que actualmente el modelo ABE es implementada en mayor cantidad para la seguridad de datos médicos mientras que BBAC es la menos utilizada.

Dentro de los artículos revisados también se pudo identificar problemas en los modelos tradicionales, mostrando e implementando las soluciones y realizando la comparación para destacar la superioridad frente a los modelos de referencia, dichos problemas los podemos observar en el cuadro 1, dando como resultado que el modelo con mayor cantidad de problemas es la de ABE, sin embargo eso no le impide seguir siendo la más implementada hasta el momento según los resultados que se muestra en la figura 4 obteniendo el mayor porcentaje con un valor de 15%, sin embargo dicho modelo presenta una cantidad de 12 versiones como resultado de mejoras tal como se muestra en el cuadro 2.

También se encontró otra serie de nuevos modelos que se encontraron una única vez, en el cuadro 3 se menciona a cada una de ellas, obteniendo un total de 23 modelos con una tendencia ascendente, siendo el año 2022 el periodo con más modelos nuevos implementados.

Conclusiones

Para realizar la presente investigación se tomó como punto de inicio el problema sobre el acceso no autorizado a los datos sensibles que se registra en las organizaciones dedicadas al servicio de salud, lo cual dio pie al desarrollo sobre el tema de los modelos de control de acceso que se vienen utilizando en ese tipo de organizaciones.

Partiendo de toda la información hallada, pudimos conocer los modelos tradicionales de mayor uso siendo un total de 5 las cuales son: ABE, ABAC, RBAC, BBAC y MAC; además, se identificó 15 modelos que surgieron de mejorar los tradicionales y por último se identificó 23 modelos nuevos que se implementaron una sola vez; por lo tanto, se obtuvo un total de 42 variaciones de modelos de control de acceso.

También se logró identificar los problemas que padecen algunos de los esquema tradicionales de control de acceso, por lo cual el esquema de ABE resultó ser el menos efectivo por los diversos inconvenientes presentes, sin embargo, los resultados mostraron que fue el más utilizado, además no se encontró un único esquema que abarque la solución completa de todos esos problemas, por lo cual es necesario recurrir a una combinación que cubra al menos gran parte de los problemas presentes.

La investigación realizada puede contribuir al conocimiento de las organizaciones sobre qué modelos o esquemas existentes se pueden implementar, para preservar la seguridad de los datos médicos o investigar más a fondo sobre alguno de su interés.

Recomendaciones

Para próximas investigaciones, se recomienda realizar un minucioso proceso de identificación de modelos y enfocarse en las características más notables así como las limitaciones que presentan, aportará mucha valor conocer qué tan efectivas pueden ser para futuras implementaciones.

Referencias

[1] S. K. Rana et al., «Blockchain Technology and Artificial Intelligence Based Decentralized Access Control Model to Enable Secure Interoperability for Healthcare», Sustainability, vol. 14, n.o 15, Art. n.o 15, ene. 2022, doi: 10.3390/su14159471.

[2] K. Srivastava y N. Shekokar, «Design of machine learning and rule based access control system with respect to adaptability and genuineness of the requester», EAI Endorsed Trans. Pervasive Health Technol., vol. 6, n.o 24, pp. 1-12, 2020, doi: 10.4108/eai.24-9-2020.166359.

[3] A. K. Malik et al., «From conventional to state-of-the-art iot access control models», Electron. Switz., vol. 9, n.o 10, pp. 1-34, 2020, doi: 10.3390/electronics9101693.

[4] E. Psarra, D. Apostolou, Y. Verginadis, I. Patiniotakis, y G. Mentzas, «Context-Based, Predictive Access Control to Electronic Health Records», Electronics, vol. 11, n.o 19, Art. n.o 19, ene. 2022, doi: 10.3390/electronics11193040.

[5] X. Zhou, J. Liu, Q. Wu, y Z. Zhang, «Privacy Preservation for Outsourced Medical Data with Flexible Access Control», IEEE Access, vol. 6, pp. 14827-14841, 2018, doi: 10.1109/ACCESS.2018.2810243.

[6] A. Bouani, Y. B. Maissa, R. Saadane, A. Hammouch, y A. Tamtaoui, «A Comprehensive Survey of Medium Access Control Protocols for Wireless Body Area Networks», Wirel. Commun. Mob. Comput., vol. 2021, 2021, doi: 10.1155/2021/5561580.

[7] Y. Zia, F. Bashir, y K. N. Qureshi, «Dynamic superframe adaptation using group-based media access control for handling traffic heterogeneity in wireless body area networks», Int. J. Distrib. Sens. Netw., vol. 16, n.o 8, 2020, doi: 10.1177/1550147720949140.

[8] S. K. Memon, N. I. Sarkar, y A. Al-Anbuky, «Multiple preemptive EDCA for emergency medium access control in distributed WLANs», Wirel. Netw., vol. 23, n.o 5, pp. 1523-1534, 2017, doi: 10.1007/s11276-016-1236-9.

[9] G. Kang y Y.-G. Kim, «Secure Collaborative Platform for Health Care Research in an Open Environment: Perspective on Accountability in Access Control», J. Med. Internet Res., vol. 24, n.o 10, p. e37978, oct. 2022, doi: 10.2196/37978.

[10] S. Salonikias, M. Khair, T. Mastoras, y I. Mavridis, «Blockchain-Based Access Control in a Globalized Healthcare Provisioning Ecosystem», Electronics, vol. 11, n.o 17, Art. n.o 17, ene. 2022, doi: 10.3390/electronics11172652.

[11] P. H. P. Jati et al., «Data Access, Control, and Privacy Protection in the VODAN-Africa Architecture», Data Intell., pp. 1-29, ago. 2022, doi: 10.1162/dint_a_00180.

[12] M. Fareed y A. A. Yassin, «Privacy-preserving multi-factor authentication and role-based access control scheme for the E-healthcare system», Bull. Electr. Eng. Inform., vol. 11, n.o 4, Art. n.o 4, ago. 2022, doi: 10.11591/eei.v11i4.3658.

[13] J. R. Amalraj y R. Lourdusamy, «A Novel Distributed Token-Based Access Control Algorithm Using A Secret Sharing Scheme for Secure Data Access Control», Int. J. Comput. Netw. Appl., vol. 9, n.o 4, p. 374, ago. 2022, doi: 10.22247/ijcna/2022/214501.

[14] L. Zhang et al., «BDSS: Blockchain-based Data Sharing Scheme With Fine-grained Access Control And Permission Revocation In Medical Environment», KSII Trans. Internet Inf. Syst. TIIS, vol. 16, n.o 5, pp. 1634-1652, 2022, doi: 10.3837/tiis.2022.05.012.

[15] S. Thapliyal et al., «ACM-SH: An Efficient Access Control and Key Establishment Mechanism for Sustainable Smart Healthcare», Sustainability, vol. 14, n.o 8, Art. n.o 8, ene. 2022, doi: 10.3390/su14084661.

[16] Q. Wang, L. Hou, J.-C. Hong, X. Yang, y M. Zhang, «Impact of Face-Recognition-Based Access Control System on College Students' Sense of School Identity and Belonging During COVID-19 Pandemic», Front. Psychol., vol. 13, 2022, Accedido: 8 de noviembre de 2022. [En línea]. Disponible en: https://www.frontiersin.org/articles/10.3389/fpsyg.2022.808189

[17] H. Saidi, N. Labraoui, A. A. A. Ari, L. A. Maglaras, y J. H. M. Emati, «DSMAC: Privacy-Aware Decentralized Self-Management of Data Access Control Based on Blockchain for Health Data», IEEE Access, vol. 10, pp. 101011-101028, 2022, doi: 10.1109/ACCESS.2022.3207803.

[18] K. Zala et al., «On the Design of Secured and Reliable Dynamic Access Control Scheme of Patient E-Healthcare Records in Cloud Environment», Comput. Intell. Neurosci., vol. 2022, p. e3804553, ago. 2022, doi: 10.1155/2022/3804553.

[19] T.-W. Chiang et al., «Novel Lagrange interpolation polynomials for dynamic access control in a healthcare cloud system», Math. Biosci. Eng., vol. 19, n.o 9, Art. n.o mbe-19-09-427, 2022, doi: 10.3934/mbe.2022427.

[20] K. Thilagam et al., «Secure IoT Healthcare Architecture with Deep Learning-Based Access Control System», J. Nanomater., vol. 2022, p. e2638613, may 2022, doi: 10.1155/2022/2638613.

[21] X. Li, «A Blockchain-Based Verifiable User Data Access Control Policy for Secured Cloud Data Storage», Comput. Intell. Neurosci., vol. 2022, p. e2254411, abr. 2022, doi: 10.1155/2022/2254411.

[22] S. Shi, M. Luo, Y. Wen, L. Wang, y D. He, «A Blockchain-Based User Authentication Scheme with Access Control for Telehealth Systems», Secur. Commun. Netw., vol. 2022, p. e6735003, mar. 2022, doi: 10.1155/2022/6735003.

[23] I. Boumezbeur y K. Zarour, «Privacy Preservation and Access Control for Sharing Electronic Health Records Using Blockchain Technology», Acta Inform. Pragensia, vol. 11, n.o 1, pp. 105-122, mar. 2022, doi: 10.18267/j.aip.176.

[24] R. Jiang, S. Han, M. Shi, T. Gao, y X. Zhao, «Healthcare Big Data Privacy Protection Model Based on Risk-Adaptive Access Control», Secur. Commun. Netw., vol. 2022, p. e3086516, mar. 2022, doi: 10.1155/2022/3086516.

[25] S. Xu, Y. Li, R. H. Deng, Y. Zhang, X. Luo, y X. Liu, «Lightweight and Expressive Fine-Grained Access Control for Healthcare Internet-of-Things», IEEE Trans. Cloud Comput., vol. 10, n.o 1, pp. 474-490, ene. 2022, doi: 10.1109/TCC.2019.2936481.

[26] K. C. y Dr. R. S., «Top-Down Approach in Access Control with Timing Enabled Key Distribution for Hierarchical Systems in Electronic Health Records», Indian J. Comput. Sci. Eng., vol. 13, n.o 1, pp. 34-39, feb. 2022, doi: 10.21817/indjcse/2022/v13i1/221301033.

[27] S. Khan et al., «An Efficient and Secure Revocation-Enabled Attribute-Based Access Control for eHealth in Smart Society», Sensors, vol. 22, n.o 1, 2022, doi: 10.3390/s22010336.

[28] I. Ullah, H. Zahid, F. Algarni, y M. A. Khan, «An access control scheme using heterogeneous signcryption for IoT environments», Comput. Mater. Contin., vol. 70, n.o 3, pp. 4307-4321, 2022, doi: 10.32604/cmc.2022.017380.

[29] Z. Szabó y V. Bilicki, «Evaluation of EHR Access Control in a Heterogenous Test Environment», Acta Cybern., vol. 25, n.o 2, pp. 485-516, 2021, doi: 10.14232/ACTACYB.290283.

[30] A. Iftekhar, X. Cui, Q. Tao, y C. Zheng, «Hyperledger fabric access control system for internet of things layer in blockchain-based applications», Entropy, vol. 23, n.o 8, 2021, doi: 10.3390/e23081054.

[31] H. H. Hlaing, Y. Funamoto, y M. Mambo, «Secure content distribution with access control enforcement in named data networking», Sensors, vol. 21, n.o 13, 2021, doi: 10.3390/s21134477.

[32] F. Khan, S. Khan, S. Tahir, J. Ahmad, H. Tahir, y S. A. Shah, «Granular data access control with a patient-centric policy update for healthcare», Sensors, vol. 21, n.o 10, 2021, doi: 10.3390/s21103556.

[33] M. T. de Oliveira, H.-V. Dang, L. H. A. Reis, H. A. Marquering, y S. D. Olabarriaga, «AC-AC: Dynamic revocable access control for acute care teams to access medical records», Smart Health, vol. 20, 2021, doi: 10.1016/j.smhl.2021.100190.

[34] H. M. Hussien, S. M. Yasin, N. I. Udzir, y M. I. H. Ninggal, «Blockchain-based access control scheme for secure shared personal health records over decentralised storage», Sensors, vol. 21, n.o 7, 2021, doi: 10.3390/s21072462.

[35] P. Meier, J. H. Beinke, C. Fitte, J. Schulte to Brinke, y F. Teuteberg, «Generating design knowledge for blockchain-based access control to personal health records», Inf. Syst. E-Bus. Manag., vol. 19, n.o 1, pp. 13-41, 2021, doi: 10.1007/s10257-020-00476-2.

[36] M. Antonio de Carvalho Junior y P. Bandiera-Paiva, «Implications of loosened Role-based Access Control session control implementation for the enforcement of Dynamic Mutually Exclusive Roles properties on Health Information Systems», Inform. Med. Unlocked, vol. 27, 2021, doi: 10.1016/j.imu.2021.100780.

[37] F. Chen et al., «Data Access Control Based on Blockchain in Medical Cyber Physical Systems», Secur. Commun. Netw., vol. 2021, 2021, doi: 10.1155/2021/3395537.

[38] S.-C. Haw, O. Tahir Yinka, T. T. V. Yap, y S. Subramaniam, «Improving the data access control using blockchain for healthcare domain», F1000Research, vol. 10, 2021, doi: 10.12688/f1000research.72890.2.

[39] Y. Ding, H. Xu, Y. Wang, F. Yuan, y H. Liang, «Secure Multi-Keyword Search and Access Control over Electronic Health Records in Wireless Body Area Networks», Secur. Commun. Netw., vol. 2021, 2021, doi: 10.1155/2021/9520941.

[40] Y. Chen, L. Meng, H. Zhou, y G. Xue, «A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection», Wirel. Commun. Mob. Comput., vol. 2021, 2021, doi: 10.1155/2021/6685762.

[41] J. Zhao, P. Zeng, y K.-K. R. Choo, «An Efficient Access Control Scheme with Outsourcing and Attribute Revocation for Fog-Enabled E-Health», IEEE Access, vol. 9, pp. 13789-13799, 2021, doi: 10.1109/ACCESS.2021.3052247.

[42] C. Camara, P. Peris-Lopez, J. M. De Fuentes, y S. Marchal, «Access Control for Implantable Medical Devices», IEEE Trans. Emerg. Top. Comput., vol. 9, n.o 3, pp. 1126-1138, 2021, doi: 10.1109/TETC.2020.2982461.

[43] J. Sun, L. Ren, S. Wang, y X. Yao, «A blockchain-based framework for electronic medical records sharing with fine-grained access control», PLoS ONE, vol. 15, n.o 10 October, 2020, doi: 10.1371/journal.pone.0239946.

[44] J. Sun, H. Xiong, X. Liu, Y. Zhang, X. Nie, y R. H. Deng, «Lightweight and Privacy-Aware Fine-Grained Access Control for IoT-Oriented Smart Health», IEEE Internet Things J., vol. 7, n.o 7, pp. 6566-6575, 2020, doi: 10.1109/JIOT.2020.2974257.

[45] T. T. Thwin y S. Vasupongayya, «Performance analysis of blockchain-based access control model for personal health record system with architectural modelling and simulation», Int. J. Networked Distrib. Comput., vol. 8, n.o 3, pp. 139-151, 2020, doi: 10.2991/ijndc.k.200515.002.

[46] M. Ali, M.-R. Sadeghi, y X. Liu, «Lightweight fine-grained access control for wireless body area networks», Sens. Switz., vol. 20, n.o 4, 2020, doi: 10.3390/s20041088.

[47] S. R. Vulapula y S. Malladi, «Attribute-Based Encryption for Fine-Grained Access Control on Secure Hybrid Clouds», Int. J. Adv. Comput. Sci. Appl., vol. 11, n.o 10, pp. 380-387, 2020, doi: 10.14569/IJACSA.2020.0111047.

[48] M. Guclu, C. Bakir, y V. Hakkoymaz, «A New Scalable and Expandable Access Control Model for Distributed Database Systems in Data Security», Sci. Program., vol. 2020, 2020, doi: 10.1155/2020/8875069.

[49] Q. Li, Y. Zhang, T. Zhang, H. Huang, Y. He, y J. Xiong, «HTAC: Fine-Grained Policy-Hiding and Traceable Access Control in mHealth», IEEE Access, vol. 8, pp. 123430-123439, 2020, doi: 10.1109/ACCESS.2020.3004897.

[50] L. O. Nweke, P. Yeng, S. D. Wolthusen, y B. Yang, «Understanding attribute-based access control for modelling and analysing healthcare professionals' security practices», Int. J. Adv. Comput. Sci. Appl., n.o 2, pp. 683-690, 2020, doi: 10.14569/ijacsa.2020.0110286.

[51] X. Zhou, J. Liu, Z. Zhang, y Q. Wu, «Secure Outsourced Medical Data against Unexpected Leakage with Flexible Access Control in a Cloud Storage System», Secur. Commun. Netw., vol. 2020, 2020, doi: 10.1155/2020/8347213.

[52] K. Edemacu, B. Jang, y J. W. Kim, «Efficient and Expressive Access Control with Revocation for Privacy of PHR Based on OBDD Access Structure», IEEE Access, vol. 8, pp. 18546-18557, 2020, doi: 10.1109/ACCESS.2020.2968078.

[53] P. Moura, P. Fazendeiro, P. R. M. Inácio, P. Vieira-Marques, y A. Ferreira, «Assessing Access Control Risk for mHealth: A Delphi Study to Categorize Security of Health Data and Provide Risk Assessment for Mobile Apps», J. Healthc. Eng., vol. 2020, 2020, doi: 10.1155/2020/5601068.

[54] Y. Zhang et al., «Research on electronic medical record access control based on blockchain», Int. J. Distrib. Sens. Netw., vol. 15, n.o 11, 2019, doi: 10.1177/1550147719889330.

[55] Y. Chen, W. Sun, N. Zhang, Q. Zheng, W. Lou, y Y. T. Hou, «Towards Efficient Fine-Grained Access Control and Trustworthy Data Processing for Remote Monitoring Services in IoT», IEEE Trans. Inf. Forensics Secur., vol. 14, n.o 7, pp. 1830-1842, 2019, doi: 10.1109/TIFS.2018.2885287.

[56] T. Kanwal et al., «Privacy-aware relationship semantics–based XACML access control model for electronic health records in hybrid cloud», Int. J. Distrib. Sens. Netw., vol. 15, n.o 6, 2019, doi: 10.1177/1550147719846050.

[57] E. Greene, P. Proctor, y D. Kotz, «Secure sharing of mHealth data streams through cryptographically-enforced access control», Smart Health, vol. 12, pp. 49-65, 2019, doi: 10.1016/j.smhl.2018.01.003.

[58] Y. Yang, X. Zheng, W. Guo, X. Liu, y V. Chang, «Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system», Inf. Sci., vol. 479, pp. 567-592, 2019, doi: 10.1016/j.ins.2018.02.005.

[59] S. Chenthara, K. Ahmed, y F. Whittaker, «Privacy-Preserving Data Sharing Using Multi-Layer Access Control Model in Electronic Health Environment», EAI Endorsed Trans. Scalable Inf. Syst., vol. 6, n.o 22, pp. 1-12, 2019, doi: 10.4108/eai.13-7-2018.159356.

[60] K. Riad, R. Hamza, y H. Yan, «Sensitive and Energetic IoT Access Control for Managing Cloud Electronic Health Records», IEEE Access, vol. 7, pp. 86384-86393, 2019, doi: 10.1109/ACCESS.2019.2926354.

[61] Q. Wang, H. Wang, Y. Wang, y R. Guo, «A Distributed Access Control with Outsourced Computation in Fog Computing», Secur. Commun. Netw., vol. 2019, 2019, doi: 10.1155/2019/6782753.

[62] A. R. Rajput, Q. Li, M. Taleby Ahvanooey, y I. Masood, «EACMS: Emergency Access Control Management System for Personal Health Record Based on Blockchain», IEEE Access, vol. 7, pp. 84304-84317, 2019, doi: 10.1109/ACCESS.2019.2917976.

[63] T. T. Thwin y S. Vasupongayya, «Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems», Secur. Commun. Netw., vol. 2019, 2019, doi: 10.1155/2019/8315614.

[64] F. P. Diez, D. S. Touceda, J. M. S. Cámara, y S. Zeadally, «Lightweight Access Control System for Wearable Devices», IT Prof., vol. 21, n.o 1, pp. 50-58, 2019, doi: 10.1109/MITP.2018.2876985.

[65] G. Chen, Y. Zhan, G. Sheng, L. Xiao, y Y. Wang, «Reinforcement Learning-Based Sensor Access Control for WBANs», IEEE Access, vol. 7, pp. 8483-8494, 2019, doi: 10.1109/ACCESS.2018.2889879.

[66] A. Margheri, M. Masi, R. Pugliese, y F. Tiezzi, «A Rigorous Framework for Specification, Analysis and Enforcement of Access Control Policies», IEEE Trans. Softw. Eng., vol. 45, n.o 1, pp. 2-33, 2019, doi: 10.1109/TSE.2017.2765640.

[67] Y. Zhang, R. H. Deng, G. Han, y D. Zheng, «Secure smart health with privacy-aware aggregate authentication and access control in Internet of Things», J. Netw. Comput. Appl., vol. 123, pp. 89-100, 2018, doi: 10.1016/j.jnca.2018.09.005.

[68] J. Sun, X. Wang, S. Wang, y L. Ren, «A searchable personal health records framework with fine-grained access control in cloud-fog computing», PLoS ONE, vol. 13, n.o 11, 2018, doi: 10.1371/journal.pone.0207543.

[69] Y. Ming y T. Zhang, «Efficient privacy-preserving access control scheme in electronic health records system», Sens. Switz., vol. 18, n.o 10, 2018, doi: 10.3390/s18103520.

[70] Y. Yang, X. Liu, y R. H. Deng, «Lightweight break-glass access control system for healthcare internet-of-things», IEEE Trans. Ind. Inform., vol. 14, n.o 8, pp. 3610-3617, 2018, doi: 10.1109/TII.2017.2751640.

[71] Y. Zhang, D. Zheng, y R. H. Deng, «Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control», IEEE Internet Things J., vol. 5, n.o 3, pp. 2130-2145, 2018, doi: 10.1109/JIOT.2018.2825289.

[72] U. Salama, L. Yao, y H.-Y. Paik, «An internet of things based multi-level privacy-preserving access control for smart living», Informatics, vol. 5, n.o 2, 2018, doi: 10.3390/informatics5020023.

[73] G. Lin, L. You, B. Hu, H. Hong, y Z. Sun, «A coordinated ciphertext policy attribute-based PHR access control with user accountability», KSII Trans. Internet Inf. Syst., vol. 12, n.o 4, pp. 1832-1853, 2018, doi: 10.3837/tiis.2018.04.024.

[74] A. Small y D. Wainwright, «Privacy and security of electronic patient records – Tailoring multimethodology to explore the socio-political problems associated with Role Based Access Control systems», Eur. J. Oper. Res., vol. 265, n.o 1, pp. 344-360, 2018, doi: 10.1016/j.ejor.2017.07.041.

[75] K. Seol, Y.-G. Kim, E. Lee, Y.-D. Seo, y 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, doi: 10.1109/ACCESS.2018.2800288.

[76] S. Bhartiya, D. Mehrotra, y A. Girdhar, «Proposing hierarchy-similarity based access control framework: A multilevel Electronic Health Record data sharing approach for interoperable environment», J. King Saud Univ. - Comput. Inf. Sci., vol. 29, n.o 4, pp. 505-519, 2017, doi: 10.1016/j.jksuci.2015.08.005.

[77] M. Abomhara, H. Yang, G. M. Køien, y M. B. Lazreg, «Work-Based Access Control Model for Cooperative Healthcare Environments: Formal Specification and Verification», J. Healthc. Inform. Res., vol. 1, n.o 1, pp. 19-51, 2017, doi: 10.1007/s41666-017-0004-7.

[78] S. M. Bhaskaran y R. Sridhar, «Hybrid solution for privacy-preserving access control for healthcare data», Adv. Electr. Comput. Eng., vol. 17, n.o 2, pp. 31-38, 2017, doi: 10.4316/AECE.2017.02005.

[79] S. Arunkumar, B. Soyluoglu, M. Sensoy, M. Srivatsa, y M. Rajarajan, «Location attestation and access control for mobile devices using GeoXACML», J. Netw. Comput. Appl., vol. 80, pp. 181-188, 2017, doi: 10.1016/j.jnca.2016.11.028.

[80] P. G. Shynu y K. J. Singh, «An enhanced ABE based secure access control scheme for E-health clouds», Int. J. Intell. Eng. Syst., vol. 10, n.o 5, pp. 29-37, 2017, doi: 10.22266/ijies2017.1031.04.

[81] S. Chatterjee et al., «On the Design of Fine Grained Access Control with User Authentication Scheme for Telecare Medicine Information Systems», IEEE Access, vol. 5, pp. 7012-7030, 2017, doi: 10.1109/ACCESS.2017.2694044.

[82] Z. Qin, J. Sun, D. Chen, y H. Xiong, «Flexible and Lightweight Access Control for Online Healthcare Social Networks in the Context of the Internet of Things», Mob. Inf. Syst., vol. 2017, 2017, doi: 10.1155/2017/7514867.

Brian Campos-Montero, Cesar Rodríguez-Sandoval, Alberto Mendoza de los Santos

Modelos de control de acceso más utilizados en la seguridad de datos médicos

Access control models most used in medical data security

Tecnología en marcha
vol. 37, núm. 1, p. 114 - 127, 2024
Instituto Tecnológico de Costa Rica, Costa Rica
revistatm@itcr.ac.cr

/ ISSN-E: 2215-3241