SmartMed: Uma Ferramenta de Controle de Acesso a Dados de Saúde baseado em Contratos Inteligentes

Yago de R. dos Santos[1], Lucio Henrik A. Reis[1], Guilherme N. N. Barbosa[1], Nicollas R. de Oliveira[1], Ana Carolina R. Mendes[1], Rafael Valle[2], Dianne S. V. Medeiros[1], Diogo M. F. Mattos[1]

[1] LabGen/MídiaCom – TET/IC/PPGEET/UFF
Universidade Federal Fluminense (UFF)
Niterói, RJ – Brasil

[2]Rede Nacional de Ensino e Pesquisa (RNP)
Rio de Janeiro, RJ – Brasil

Abstract. *This paper proposes SmartMed, a tool that aims to control access to distributed medical data through smart contracts running on a private blockchain. SmartMed promotes access to various digital health systems and their interoperability. It enables secure and agile access to information stored in non-standard and heterogeneous data silos, ensuring compliance with regulations and data privacy laws. Smart contracts ensure the tool conforms to security requirements as sensitive data access transactions are executed and recorded in a blockchain immutable way, providing a complete audit trail for sensitive data access. The demonstration at SBSeg focuses on traceability in electronic medical record systems by integrating them with SmartMed via the OAuth2.0 protocol for authentication and access control.*

Resumo. *Este artigo propõe o SmartMed, uma ferramenta que visa controlar o acesso a dados médicos distribuídos por meio de contratos inteligentes executados em uma cadeia de blocos privada. A SmartMed facilita o acesso a vários sistemas digitais de saúde e sua interoperabilidade, permitindo acesso seguro e ágil às informações armazenadas em silos de dados não padronizados e heterogêneos, garantindo a conformidade com os regulamentos e leis de privacidade dos dados. Os contratos inteligentes garantem à ferramenta a adequação a requisitos de segurança, pois as transações de acesso a dados confidenciais são executadas e registradas de forma imutável, fornecendo uma trilha de auditoria completa para acesso a dados confidenciais. A demonstração na SBSeg tem como foco a rastreabilidade em sistemas de prontuário eletrônico através da integração com a SmartMed pelo protocolo OAuth2.0 para autenticação e controle de acesso.*

1. Introdução

A crescente digitalização de dados, especialmente de dados pessoais, possibilita que esses dados sejam compartilhados de forma facilitada [Oliveira et al., 2023]. Há di-

Este trabalho foi realizado com recursos do CNPq, CAPES, FAPERJ e RNP e Prefeitura de Niterói/FEC/UFF (Edital PDPA 2020).

versas iniciativas governamentais que promovem a digitalização desses dados[1]. No entanto, a digitalização dos dados torna o seu compartilhamento praticamente impossível de ser rastreável, em muitos casos, afetando a privacidade das pessoas. É fundamental que informações pessoais sensíveis, como dados de saúde, tenham elevado nível de privacidade. Dados gerais e estatísticos, por outro lado, requerem proteção moderada, pois são usados principalmente para pesquisas e análises estatísticas que não afetam diretamente a privacidade das pessoas [Ali et al., 2023]. Nesse sentido, legislações relativas a dados pessoais vêm sendo implementadas em diversos países. No Brasil, por exemplo, vigora a Lei Geral de Proteção de Dados (LGPD) desde 2018. A LGPD é fortemente baseada no Regulamento Geral de Proteção de Dados (*General Data Protection Regulation* – GDPR) em vigor na União Europeia. A finalidade da GDPR é estabelecer diretrizes para o tratamento de dados pessoais de todos na União Europeia, seja por pessoas, empresas ou organizações [Haque et al., 2021]. Considerando apenas os dados de saúde, para o cumprimento da lei é essencial realizar previamente o processo de identificação desses dados. O processamento de dados sensíveis, como os dados de saúde, estão sujeitos à regras específicas. Exige-se consentimento por parte do titular ou seu responsável legal para tratamento desses dados. Nos Estados Unidos, há uma legislação específica para tratamento de dados de saúde, diferentemente da LGPD e da GDPR que são leis para tratamento de dados gerais. Nos Estados Unidos, a Lei de Portabilidade e Responsabiliade de Seguro Saúde (*Health Insurance Portability and Accountability Act* – HIPPA), criada em 1996, estabelece padrões de privacidade e segurança apenas para as informações médicas.

Os dados de saúde podem ser armazenados digitalmente em Registros Médicos Eletrônicos (*Electronic Medical Records* – EMRs). Contudo, esses dados normalmente estão distribuídos em silos de dados distintos, tornando a informação digitalizada particionada. Dessa forma, entidades distintas possuem apenas uma fração da informação de um paciente. O particionamento dificulta o tratamento e a garantia de privacidade desses dados, uma vez que se torna praticamente impossível detectar possíveis violações. Além do problema da privacidade, o particionamento também pode implicar duplicação e perda de dados.

Considerando o complexo cenário da privacidade dos dados em saúde e as exigências cada vez mais severas das legislações de proteção de dados, torna-se indispensável o uso de tecnologias computacionais para o controle de acesso distribuído aos dados. Ademais, as tecnologias da informação e comunicação são aplicadas para promover a prevenção, o diagnóstico, o tratamento e a reabilitação de doenças de forma abrangente, originando o paradigma de *e-health* [Dang et al., 2018]. De forma complementar, a tecnologia de cadeia de blocos (*blockchain*) é utilizada para promover segurança adicional aos sistemas digitais de saúde, permitindo a conformidade com a legislação. A conformidade é possível graças a características intrínsecas da tecnologia, que garantem ao sistema as propriedades de imutabilidade, não-repúdio, integridade e capacidade de auditoria. Assim, um dos principais desafios dos sistemas médicos com dados distribuídos é garantir que o acesso aos dados seja visualizado somente pelos profissionais e pacientes autorizados. Para tanto, é necessário um sistema de controle de acesso distribuído, confiável e verificável.

[1]Disponível em `https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2022/11/brasil-e-reconhecido-como-segundo-lider-em-governo-digital-no-mundo`.

Este artigo propõe a ferramenta SmartMed, cujo objetivo é realizar o controle de acesso a dados médicos distribuídos através de atributos armazenados em um sistema central de gestão de identidade [de Oliveira et al., 2022]. Os contratos inteligentes são registrados em uma cadeia de blocos privada implementada utilizando a plataforma *Ethereum*. A ferramenta facilita o acesso a múltiplos sistemas de saúde digitais e a interoperabilidade entre eles, permitindo o acesso seguro e ágil a informações armazenadas em silos de dados não padronizados e heterogêneos, provendo ainda segurança e suporte na adequação dos sistemas de saúde à LGPD, GDPR e HIPPA.

O restante do artigo está organizado da seguinte forma. A Seção 2 discute os trabalhos relacionados. A arquitetura e o funcionamento da ferramenta são apresentados na Seção 3. A Seção 4 descreve a demonstração da ferramenta. Finalmente, a Seção 5 conclui o artigo.

2. Trabalhos Relacionados

Trabalhos anteriores propõem mecanismos baseados em cadeia de blocos para registros médicos eletrônicos. Liang *et al.* propõem um sistema baseado em cadeia de blocos para aplicativos médicos em dispositivos móveis que permite aos usuários controlar seus próprios dados de saúde e compartilhá-los com profissionais especializados [Liang et al., 2017]. A cadeia de blocos é utilizada pelos autores para garantir a integridade dos dados, fornecer acesso aos dados e realizar auditoria no acesso aos dados. O compartilhamento dos dados é feito de forma colaborativa, utilizando uma árvore de Merkle para garantir a eficiência e escalabilidade. Entretanto, a proposta não visa a interoperabilidade, requisito fundamental para sistemas de saúde.

Jiang *et al.* propõem a plataforma BlocHIE, baseada em cadeia de blocos, para troca de informações de saúde [Jiang et al., 2018]. A arquitetura consiste em duas cadeias de blocos separadas, identificadas como EMR-Chain e PHD-Chain. A primeira, tem o objetivo de armazenar EMRs, enquanto a segunda armazena registros pessoais de saúde. Os autores utilizam uma estratégia de armazenamento fora da cadeia de blocos (*off-chain*), de forma que os dados são armazenados em servidores que não participam da cadeia de blocos, mas a verificação da integridade dos dados é realizada por transações na cadeia de blocos, garantindo a privacidade e autenticidade. Entretanto, isso aumenta a complexidade do sistema de controle de acesso e, consequentemente, afeta o seu desempenho.

Fan *et al.* propõem um sistema baseado em cadeia de blocos para compartilhar registros médicos eletrônicos entre usuários autorizados [Fan et al., 2018]. A proposta implementa o gerenciamento e o compartilhamento de EMRs, além de um mecanismo de acesso. Contudo, possui alto custo de processamento. Zhang *et al.* propõem o FHIR-Chain, uma arquitetura baseada em cadeia de blocos projetada para encapsular o padrão HL7 *Fast Healthcare Interoperability Resources* (FHIR) para dados clínicos compartilhados [Zhang et al., 2018]. Os autores propõem realizar o controle de acesso aos dados por meio de um contrato inteligente executado na rede pública *Ethereum*, a fim de garantir maior disponibilidade. Contudo, por utilizar a rede pública, está sujeito ao custo monetário para execução do contrato.

O SmartMed propõe um sistema de controle de acesso amparado por contratos inteligentes que executam na cadeia de blocos, com foco na garantia da autenticidade e não refutabilidade dos eventos de acessos a dados médicos. Para isso, a proposta usa

o *Keycloak* como sistema gerenciador de identidade e acesso aos sistemas de saúde. O módulo SmartMed faz a captura dos eventos do *Keycloak* e os registra na sua cadeia de blocos privada. Além disso, o SmartMed integra o *Keycloak* à cadeia de blocos por meio de contratos inteligentes baseados na plataforma *Ethereum*.

3. A Ferramenta SmartMed

A arquitetura da ferramenta SmartMed, apresentada na Figura 1, é composta por três módulos: *Edge Datacenter*, *Blockchain* e Visualização. A ferramenta é implementada utilizando a plataforma *Ethereum* [2], por ter uma simples implementação e possibilitar a implantação de uma rede privada, completamente desvinculada da rede pública, inclusive com parâmetros próprios de inicialização. O ***Edge Datacenter*** atua como *middleware*, responsável pela integração das aplicações de registros médicos eletrônicos com os contratos inteligentes. Para isso, é necessário que as aplicações de registros médicos eletrônicos, representadas na figura pelo componente Aplicações EHR (*Electronic Health Records*), comuniquem-se através do protocolo OAuth 2.0 [3] com o *Keycloak* [4]. O *Keycloak* é um *software* de código aberto que fornece gerenciamento de identidade e acesso para diversos tipos de aplicações. A função do *Keycloak* na ferramenta SmartMed é prover acesso através da integração com um Nó Leve da *Ethereum* (*LightNode*), responsável pela execução de contratos inteligentes no módulo *Blockchain*.

O módulo ***Blockchain*** é responsável pelo armazenamento distribuído de contratos inteligentes utilizados para autorizar o acesso aos dados armazenados nas Aplicações EHR. Isso garante segurança do ponto de vista de disponibilidade, uma vez que não há uma entidade central, responsável por essa autorização. A cadeia de blocos fornece segurança do ponto de vista de integridade, pois não é possível apagar os registros das transações já realizadas, garantindo uma auditoria total de todos os acessos já realizados. A rede privada *Ethereum* tem como objetivo suportar a execução dos contratos inteligentes e utiliza o algoritmo de consenso Prova de Autoridade (*Proof-of-Authority* – PoA). Esse algoritmo requer que os nós validadores confirmem suas identidades antes de ingressar na rede [Manolache et al., 2022]. O PoA é mais tolerante a riscos do que outros mecanismos de consenso, como a Prova de Trabalho (*Proof-of-Work* – PoW), uma vez que é necessário uma quantidade de nós maliciosos superior a 50% do total de nós na rede para comprometer o mecanismo.

Por fim, o módulo de **Visualização** tem o objetivo de apresentar graficamente, em tempo real, as métricas de desempenho dos nós na rede *Ethereum*, como informações sobre transações, capacidade operacional dos nós, blocos na cadeia de blocos, dentre outras. Para isso, os nós enviam as informações relacionadas à rede para o InfluxDB [5], um banco de dados de série temporal. Os dados armazenados no banco de dados são consumidos pelo Grafana[6], *software* que fornece a visualização gráfica dos dados temporais na forma de painel de visualização (*dashboard*). Tanto o InfluxDB quanto o Grafana são implementados utilizando containers Docker[7].

[2]Disponível em `https://ethereum.org/`.
[3]Disponível em `https://oauth.net/2/`.
[4]Disponível em `https://www.keycloak.org/`.
[5]Disponível em `https://www.influxdata.com/influxdb/`.
[6]Disponível em `https://www.grafana.com`.
[7]Disponível em `https://www.docker.com/`.

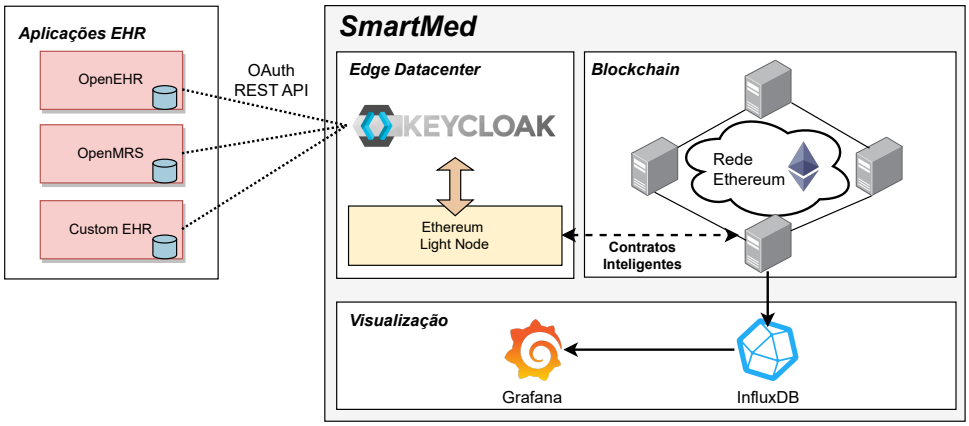

Figura 1. Arquitetura da plataforma SmartMed. O módulo *Edge Datacenter* age como um *middleware* que recebe chamadas de autenticação e controle de acesso na interface OAuth2.0 e as executa na cadeia de blocos *Ethereum* através de um *Light Node*. O módulo de Visualização expõe métricas de desempenho dos nós em tempo real.

A ferramenta SmartMed utiliza o modelo de Controle de Acesso baseado em Atributo (*Attribute-Based Access Control* – ABAC), executando-o no *Keycloak*. Para conceder acesso aos dados para o usuário, esse modelo utiliza políticas que são representadas por combinações lógicas de atributos. Os atributos podem estar relacionados ao usuário, como nome e cargo, aos recursos, como data de criação de um recurso, e ao ambiente, como informações geográficas do recurso a ser acessado. Quando um usuário emite uma solicitação de acesso, a política é aplicada, explorando valores dos atributos para retornar uma resposta. As respostas contêm a decisão sobre o pedido. Assim, o ABAC requer uma associação prévia entre usuários e os atributos pré-definidos e os usuários devem estar cadastrados em um sistema central de gestão de identidade, como Protocolo Leve de Acesso a Diretórios (*Lightweight Directory Access Protocol* – LDAP) ou Diretório Ativo (*Active Directory* – AD).

O padrão XACML (*XML Access Control Markup Language*) é uma linguagem responsável por definir os componentes para implementação do ABAC: *Policy Administration Point* (PAP), *Policy Enforcement Point* (PEP), *Policy Decision Point* (PDP), *Policy Information Point* (PIP). Todas as políticas, solicitações e respostas do ABAC são expressas nessa linguagem. A Figura 2 mostra a interação entre os diversos componentes do ABAC. Inicialmente, o PAP armazena e gerencia um conjunto de políticas que são associadas a identificadores de destino. Desse modo, antes de uma solicitação de acesso a qualquer informação por parte do usuário, (1) o PAP deve possuir as políticas previamente configuradas, a fim de disponibilizá-las ao componente de decisão, o PDP. Em seguida, a requisição de acesso é feita para o PEP (2). Nessa etapa, a requisição pode conter valores de atributos. Desse modo, o PEP é responsável por receber as requisições de acesso, interrompendo o fluxo de execução até a tomada de decisão por parte do PDP. Em seguida, o PEP envia as solicitações para o PDP através de uma requisição XACML padrão (3). O PDP é o componente responsável por recuperar os atributos e informações contextuais através de requisições feitas ao PIP (4), armazenando essas informações. Em contrapartida, o PIP devolve as informações ao PDP através de um novo fluxo (5). O PDP atua mais uma vez, recuperando as políticas armazenadas no PAP (6) de acordo com a finalidade da requisição. O PAP retorna as políticas ao PDP através de um novo fluxo (7)

e o PDP avalia a política vigente, retornando o contexto de resposta XACML padrão para o PEP (8). Desse modo, o PDP é o componente que recupera os atributos e informações contextuais do PIP, avaliando as políticas previamente definidas e responsável pela tomada de decisão sobre o acesso requisitado. Por último o PEP executa a decisão do PDP (9).

Devido à complexidade da operação dos sistemas de EMR, o controle de acesso pode não ser adequadamente configurado, resultando em maior permissividade do que a necessária [de Oliveira et al., 2023]. A implementação do modelo ABAC nos sistemas de EMR permite alcançar maior granularidade no controle de acesso às informações. Contudo, essa implementação é desafiadora devido à dificuldade de modelagem para compartilhamento de dados entre organizações, por exemplo durante cuidados intensivos. Por essa razão, o controle de acesso baseado em ABAC nesses sistemas normalmente não consideram o cenário de cuidados intensivos [de Oliveira et al., 2023]. A ferramenta SmartMed permite a implementação completa do modelo ABAC, para qualquer cenário de cuidados médicos, com ou sem compartilhamento de informação entre entidades distintas.

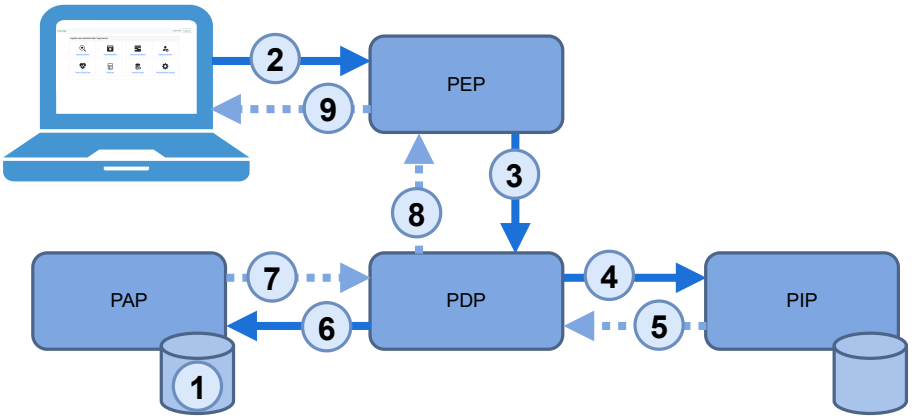

Figura 2. Interação entre os componentes do padrão XACML. As políticas devem ser previamente armazenadas no PAP para que o PDP possa requisitá-las a fim de decidir sobre a requisição de acesso realizada por um usuário. Para tomar essa decisão, o PDP recupera informações de contexto e valores de atributo no PIP. O PEP recebe requisições de acesso, propaga-as para o PDP e bloqueia o fluxo de execução enquanto o PDP não toma uma decisão. Após a decisão tomada pelo PDP, o PEP executa o resultado, liberando ou negando o acesso.

4. Demonstração do SmartMed

O funcionamento da ferramenta SmartMed será demonstrado por meio do acompanhamento da inserção de um registro de acesso na cadeia de blocos. A demonstração evidencia a aplicabilidade da solução, apresentando as funcionalidades essenciais para a garantia da autenticidade e não refutabilidade das operações sobre registros médicos. O registro de acesso será gerado ao simular a interação de um usuário com uma aplicação médica em um computador durante o Salão de Ferramentas no SBSeg. O computador possui uma aplicação de exemplo que representa um sistema de registro médico eletrônico integrado com a ferramenta, sendo também um nó da cadeia de blocos, juntamente com uma instância do *Keycloak*.

A interação do usuário com a aplicação de exemplo irá disparar um evento do *Keycloak* representando um registro de acesso. Esse evento será capturado pelo módulo Edge Datacenter do SmartMed e enviado para a rede de cadeia de blocos por meio da execução de uma transação do contrato inteligente. A execução do contrato inteligente resulta no registro do evento na cadeia de blocos em forma de *log*. A Figura 3 mostra o esquema da apresentação do funcionamento da ferramenta. Todo o processo será apresentado pelo acompanhamento dos *logs* dos serviços envolvidos na interação entre o sistema médico, o *Keycloak* e o nó da cadeia de blocos. Além disso, a demonstração também contará com a visualização do estado geral da rede da cadeia de blocos, apresentado em tempo real pelo painel de visualização do Grafana.

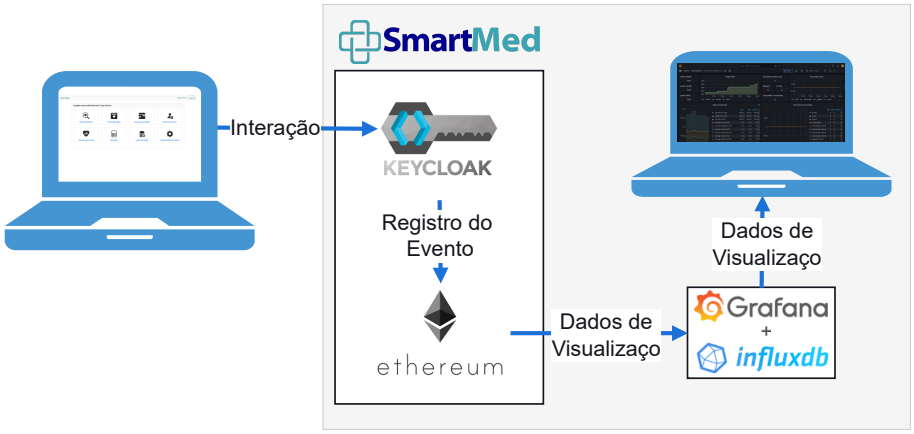

Figura 3. Esquema da apresentação do funcionamento da ferramenta SmartMed. O computador de apresentação irá executar a aplicação médica integrada na ferramenta. Os eventos do *Keycloak* serão captados pelo módulo SmartMed e registrados na cadeia. Por fim, no painel do Grafana apresentado em um outro computador, será visualizado o estado da rede em tempo real para a verificar as transações na cadeia de blocos.

5. Conclusão

Dados médicos estão frequentemente distribuídos em diversos silos de dados, representados por hospitais e clínicas que atendem um paciente ao longo de sua vida. O controle de acesso aos dados de um paciente é bastante dificultado pela natureza distribuída dos seus dados. A principal abordagem para evitar o acesso distribuído aos dados é a centralização dos registros médicos em uma única plataforma. Contudo, essa solução apresenta entraves socio-culturais relativos à gestão dos dados locais, além de entraves técnicos devido à existência de diversos padrões de representação de dados em saúde, além de sistemas que armazenam dados não padronizados. Dessa forma, este artigo propôs a ferramenta SmartMed, um mecanismo de controle de acesso a dados de saúde utilizando contratos inteligentes em uma cadeia de blocos (*Blockchain*) privada. A ferramenta garante requisitos de segurança, uma vez que as transações de acesso a dados sensíveis é executada em contratos inteligentes e o registro das ações permanece imutável, garantindo assim completa auditoria no acesso a dados sensíveis. A demonstração no SBSeg foca na rastreabilidade das ações executadas em sistemas de registros médicos eletrônicos com suporte ao protocolo OAuth2.0 para a realização de autenticação e controle de acesso. A ferramenta e a documentação para sua instalação e utilização estão disponíveis na página do GT-SmartMed[8], projeto desenvolvido com apoio da Rede Nacional

[8]Disponível em `https://www.labgen.lid.uff.br/smartmed/`.

de Ensino e Pesquisa (RNP). Como trabalhos futuros, pretende-se aprimorar a ferramenta incluindo os atributos contextuais nos contratos inteligentes.

Referências

Ali, M., Naeem, F., Tariq, M. e Kaddoum, G. (2023). Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey. *IEEE Journal of Biomedical and Health Informatics*, 27(2):778–789.

Dang, L., Dong, M., Ota, K., Wu, J., Li, J. e Li, G. (2018). Resource-efficient secure data sharing for information centric e-health system using fog computing. Em *2018 IEEE International Conference on Communications (ICC)*, p. 1–6. IEEE.

de Oliveira, M. T., Reis, L. H. A., Verginadis, Y., Mattos, D. M. F. e Olabarriaga, S. D. (2022). Smartaccess: Attribute-based access control system for medical records based on smart contracts. *IEEE Access*, 10:117836–117854.

de Oliveira, M. T., Verginadis, Y., Reis, L. H., Psarra, E., Patiniotakis, I. e Olabarriaga, S. D. (2023). AC-ABAC: Attribute-based access control for electronic medical records during acute care. *Expert Systems with Applications*, 213:119271.

Fan, K., Wang, S., Ren, Y., Li, H. e Yang, Y. (2018). MedBlock: Efficient and secure medical data sharing via blockchain. *Journal of medical systems*, 42:1–11.

Haque, A. B., Islam, A. K. M. N., Hyrynsalmi, S., Naqvi, B. e Smolander, K. (2021). Gdpr compliant blockchains–a systematic literature review. *IEEE Access*, 9:50593–50606.

Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M. e He, J. (2018). Blochie: a blockchain-based platform for healthcare information exchange. Em *2018 ieee international conference on smart computing (smartcomp)*, p. 49–56. IEEE.

Liang, X., Zhao, J., Shetty, S., Liu, J. e Li, D. (2017). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. Em *2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC)*, p. 1–5. IEEE.

Manolache, M. A., Manolache, S. e Tapus, N. (2022). Decision making using the blockchain proof of authority consensus. *Procedia Computer Science*, 199:580–588. The 8th International Conference on Information Technology and Quantitative Management (ITQM 2020 & 2021): Developing Global Digital Economy after COVID-19.

Oliveira, N., Rezende, Y., Barbosa, G., Mendes, A. C. R., Oliveira, M., Valle, R. e Medeiros, D. (2023). Padrões e soluções para armazenamento, compartilhamento e estruturação de dados em saúde digital: Privacidade, integração e desafios. Em *Minicursos do XXIII Simpósio Brasileiro de Computação Aplicada à Saúde*, p. 134–186, Porto Alegre.

Zhang, P., White, J., Schmidt, D. C., Lenz, G. e Rosenbloom, S. T. (2018). FHIRChain: applying blockchain to securely and scalably share clinical data. *Computational and structural biotechnology journal*, 16:267–278.