UNIVERSIDADE DE BRASÍLIA – UNB
Faculdade de Tecnologia
Departamento de Engenharia Elétrica
Programa de Pós-Graduação Profissional em Engenharia Elétrica (PPEE)

IMPLEMENTAÇÃO DE *BLOCKCHAIN* PRIVADA PARA REGISTRO E GERENCIAMENTO DE *LOGS* EM SISTEMAS DE CONTROLE DE ACESSO

Implementation of Private Blockchain for Log Recording and Management in Access Control Systems

Raimundo Leite de Oliveira Neto

Curso de Pós-Graduação Lato Sensu em Privacidade e Segurança da Informação

Professor Orientador
Prof. Dr. William Ferreira Giozza

Brasília - DF

RESUMO

Os Sistemas de Controle de Acesso por Reconhecimento Facial, utilizando dispositivos biométricos para autenticação de usuários, constituem componentes essenciais da infraestrutura de segurança organizacional. Esses sistemas geram *logs* de eventos e registros de auditoria, elementos fundamentais para investigações forenses e conformidade regulatória. A centralização tradicional desses registros em bancos de dados convencionais apresenta vulnerabilidades críticas, permitindo que agentes maliciosos alterem ou suprimam dados históricos. Este trabalho propõe uma arquitetura híbrida implementada na plataforma Gestor de Acesso, utilizando tecnologia *blockchain* como camada de notarização descentralizada complementar ao repositório operacional. A solução proposta permite assegurar integridade, imutabilidade e auditabilidade irrefutável de todos os eventos administrativos, incluindo verificação de autenticidade de *backups* do sistema. Através de uma rede de nós independentes e mecanismo de consenso baseado em Prova de Trabalho adaptado, o sistema proposto estabelece um registro cronológico à prova de adulteração, aumentando significativamente a confiabilidade dos dados de auditoria sem comprometer a performance operacional.

Palavras-chave: *Blockchain* Privada. Controle de Acesso Biométrico. Segurança da Informação. Imutabilidade de Logs. Prova de Trabalho.

ABSTRACT

Physical Access Control Systems (PACS) based on facial recognition constitute essential components of organizational security infrastructure, utilizing advanced biometric devices for user authentication while generating event logs fundamental for forensic investigations and regulatory compliance. Traditional centralization of these records in conventional databases presents critical vulnerabilities, allowing malicious agents or privileged administrators to alter historical data. This work proposes a hybrid architecture implemented in the Access Manager platform, utilizing blockchain technology as a decentralized notarization layer complementary to the operational database. The proposed solution allows to ensure immutability, integrity, and irrefutable auditability of all administrative actions, including backup authenticity verification. Through a network of independent nodes and an adapted Proof of Work consensus mechanism, the proposed system establishes a tamper-proof chronological record, significantly increasing audit data reliability without compromising operational performance.

Keywords: *Private Blockchain. Biometric Access Control. Information Security. Log Immutability. Proof of Work.*

1. INTRODUÇÃO

A segurança da informação constitui fundamento essencial para preservação da integridade operacional em ambientes industriais, corporativos e de infraestrutura crítica. Neste contexto, os sistemas de controle biométrico emergem como uma primeira linha de defesa perante vulnerabilidades de segurança crescentes, utilizando dispositivos baseados em câmeras de alta resolução e algoritmos de inteligência artificial para autenticação através de características faciais únicas (SHARMA; DWIVEDI, 2024).

Os dispositivos modernos capturam imagens em tempo real, extraem características distintivas através de algoritmos de aprendizagem profunda (*deep learning*) e comparam com modelos previamente cadastrados. Cada tentativa de autenticação gera registros detalhados, incluindo identificação do usuário, registro de data/hora preciso, qualidade da captura, *score* de similaridade, *status* da verificação, localização do dispositivo e metadados sobre condições ambientais, constituindo dados fundamentais para investigações forenses e conformidade regulatória (RAJUROY; JOHN, 2025).

A arquitetura tradicional de armazenamento de dados baseia-se em bancos de dados relacionais centralizados, otimizados para velocidade, mas apresentando vulnerabilidades críticas devido à mutabilidade inerente dos dados (PUNIA *et al*., 2024)

Pesquisas recentes demonstram crescimento nas investigações sobre sistemas biométricos baseados em *Blockchain*, uma tecnologia DLT (*Distributed Ledger Technology*) projetada para prover segurança em sistemas de informação distribuídos (DAI *et al*., 2024; SHARMA; DWIVEDI, 2024). Entretanto observa-se que poucos desses trabalhos abordam especificamente a imutabilidade de *logs* em ambientes com requisitos de tempo real, como controle de acesso físico.

A integração da tecnologia *Blockchain* com sistemas de reconhecimento facial apresenta dois desafios críticos identificados na literatura (GHAFOURIAN *et al*., 2025). O primeiro refere-se à latência e volume: usuários esperam resposta de autenticação quase instantânea, e ambientes de alto tráfego podem gerar milhares de tentativas por hora, tornando uma *Blockchain* pública inviável devido aos longos tempos de bloco. O segundo consiste na integridade temporal: para uma auditoria forense eficaz, *logs*

precisam manter ordem cronológica garantida e imutável, pois a adulteração pode reordenar eventos e comprometer a cadeia de custódia digital (RAJUROY; JOHN, 2025).

Este trabalho propõe uma implementação prática de solução híbrida que aplica princípios *Blockchain* no sistema Gestor de Acesso, unindo eficiência operacional de repositórios tradicionais com segurança inviolável de *Blockchain* privada customizada, resolvendo os problemas específicos de mutabilidade em sistemas biométricos e contribuindo para o avanço da segurança de dados de auditoria. Além disso, a longevidade da solução proposta baseia-se na robustez dos algoritmos criptográficos empregados, especialmente frente a potenciais avanços da computação quântica, o que constitui desafio adicional a ser considerado.

A estrutura deste trabalho está organizada da seguinte forma. A seção 2 apresenta a fundamentação teórica e a revisão de trabalhos correlatos. Em seguida, o desenho da arquitetura híbrida proposta e o modelo de ameaças são detalhados na seção 3. A implementação prática da solução é descrita na seção 4. A seção 5 é dedicada à avaliação de desempenho do sistema, cobrindo tanto a resiliência de segurança quanto as métricas de performance. Por fim, a seção 6 apresenta as conclusões do trabalho, com um resumo das contribuições e apontamentos para pesquisas futuras.

2. FUNDAMENTAÇÃO TEÓRICA E TRABALHOS CORRELATOS

2.1 Sistemas de Reconhecimento Facial

Os sistemas de reconhecimento facial atuais utilizam algoritmos de visão computacional e inteligência artificial para identificação através de características biológicas. Os dispositivos de reconhecimento facial modernos incorporam câmeras de alta resolução, processadores dedicados e algoritmos de aprendizado profundo para capturar, processar e comparar características em tempo real. (SHARMA; DWIVEDI, 2024).

Os *logs* gerados contêm informações críticas específicas desta modalidade, incluindo identificação única do usuário, registro de data/hora da tentativa, *score* de

similaridade calculado pelo algoritmo, resultado da comparação (compatível/não compatível), identificação do dispositivo, localização física, qualidade da imagem capturada, condições de iluminação ambiente e dados sobre detecção de vivacidade para prevenir ataques com fotografias. Esses registros são essenciais para auditoria, investigações forenses e conformidade regulatória (SHARMA; DWIVEDI, 2024).

Os sistemas de gerenciamento e armazenamento de dados tradicionais apresentam pontos únicos de falha, tornando-os inadequados para as demandas atuais de alta segurança (PUNIA *et al*., 2024). Em sistemas biométricos, essa vulnerabilidade é amplificada pela sensibilidade dos dados e pela necessidade de manter registros íntegros de todas as tentativas, incluindo falsos positivos que podem indicar tentativas de burla.

Dentre as vulnerabilidades críticas em arquiteturas centralizadas, além da existência de pontos únicos de falha no servidor de processamento, acrescentam-se, dependência de terceiros confiáveis para algoritmos, possibilidade de alteração maliciosa que pode comprometer investigações, e riscos específicos relacionados a ataques de *spoofing* e manipulação de nível de confiança (*score*) em registros históricos (MA *et al*., 2024).

2.2 Cadeia de Custódia

A validade e integridade de evidências digitais são essenciais para investigações forenses. Todas as novas evidências e *logs* de acesso devem ser registrados em um documento chamado 'cadeia de custódia', que rastreia o manuseio dos dados (RAJUROY; JOHN, 2025). Em uma investigação digital tradicional, partes confiáveis, como administradores de sistema, têm acesso permitido à evidência e seguem um processo rigoroso.

A parte mais vulnerável desta cadeia reside precisamente na junção entre o privilégio humano e a mutabilidade da tecnologia de armazenamento (RAJUROY; JOHN, 2025). O repositório central de *logs*, geralmente um banco de dados relacional ou arquivos de texto, constitui um ponto único de falha. Um administrador com acesso privilegiado possui a capacidade técnica de alterar ou suprimir registros, utilizando comandos SQL padrão como *UPDATE* ou *DELETE*. Se essa manipulação for feita de

forma habilidosa, apagando também os *logs* de auditoria do próprio banco de dados, a adulteração pode se tornar indetectável, quebrando irreparavelmente a cadeia de custódia (PUNIA *et al*., 2024). Esta vulnerabilidade fundamental, onde o guardião da evidência também é seu potencial adulterador, é o problema central que a implementação de uma camada de notarização imutável, como a *Blockchain*, se propõe a resolver.

2.3 *Blockchain*

Blockchain constitui uma estrutura de dados distribuída que mantém uma lista continuamente crescente de registros (blocos) ligados através de *hashes* criptográficos. Cada bloco contém *hash* do bloco anterior, registro de data/hora (*timestamp*) e dados da transação, formando uma cadeia imutável (NAKAMOTO, 2008).

A integridade de *logs* em sistemas biométricos baseados em *Blockchain*, pode ser feita segundo diversas abordagens, das quais ressalta-se as apresentadas a seguir.

2.3.1. *Blockchain* Pública

A *Blockchain* pública oferece máxima descentralização e resistência a ataques, mas apresenta latência incompatível com requisitos de tempo real, custos elevados de transação e exposição de metadados em rede pública, violando requisitos de privacidade de dados biométricos (KARADUMAN; GÜLHAS, 2025).

2.3.2. *Blockchain* Privada

Neste trabalho, a tecnologia de *Blockchain* privada com mecanismo de consenso Prova de Trabalho (PoW) foi selecionada por combinar imutabilidade distribuída com controle sobre a rede, latência ajustável e operação em ambiente isolado, características essenciais para sistemas que exigem rastreabilidade e integridade de dados (KARADUMAN; GÜLHAS, 2025). Embora alternativas como Prova de Autoridade (*PoA*) ofereçam maior eficiência energética, a natureza crítica dos dados biométricos exige validação baseada em prova criptográfica objetiva (NAKAMOTO, 2008; ZHAO, X. *et al*., 2024).

A vulnerabilidade fundamental do mecanismo de consenso *PoA* em ambientes de segurança crítica reside na facilidade de comprometimento dos nós validadores: em uma rede com três nós, um adversário precisaria comprometer fisicamente apenas dois para controlar o consenso através de acesso físico, coerção ou infiltração de credenciais (ZHAO, W. *et al*., 2025). O mecanismo de consenso *PoW*, em contraste, estabelece uma barreira econômica e temporal significativa, exigindo recursos computacionais substanciais para reescrever o histórico mesmo após comprometimento físico dos nós, criando uma janela temporal para detecção e mitigação (NAKAMOTO, 2008).

Para a cadeia de custódia forense, evidências baseadas em *PoW* podem ser verificadas matematicamente por auditores independentes através da análise criptográfica dos *hashes*, enquanto evidências baseadas em *PoA* dependem da confiança na integridade das autoridades validadoras (ZHAO, W. *et al*., 2025). A escolha pelo *PoW* baseou-se na simplicidade de implementação e robustez comprovada do mecanismo (NAKAMOTO, 2008). Em ambiente *air-gapped* com número restrito de nós, o risco de ataques de 51% é mitigado pelo controle administrativo sobre a rede (ZHAO, W. *et al*., 2025).

O sistema apresenta limitações inerentes: dependência da integridade inicial dos *templates* biométricos, necessidade de sincronização entre nós geograficamente distribuídos, consumo computacional do processo de mineração, e notarização apenas de metadados por questões de privacidade e conformidade regulatória (KARADUMAN; GÜLHAS, 2025). Em termos de viabilidade, o custo computacional da *PoW* de baixa dificuldade é modesto, permitindo execução em máquinas de baixo custo ou servidores com recursos ociosos. O Retorno sobre o Investimento (ROI) é medido pela mitigação de riscos: prevenir a adulteração de uma única evidência em investigações de fraude, espionagem ou incidentes de segurança pode superar em ordens de magnitude o custo de manutenção da rede (KARADUMAN; GÜLHAS, 2025).

2.4 Modelo de Ameaças (*Threat Model*)

A arquitetura de segurança proposta foi projetada para mitigar ameaças específicas, predominantemente de origem interna. O modelo de ameaças considerado

elenca como principal vetor de ameaça (adversário) o administrador de sistema interno malicioso ou comprometido. Esse adversário possui privilégios elevados, incluindo acesso direto ao servidor do "Gestor de Acesso" e ao banco de dados operacional (*SQLite*).

Além disso, o adversário possui diversas capacidades, dentre as quais, elenca-se: a) manipulação de banco de dados, uma vez que pode executar comandos SQL arbitrários para alterar, suprimir (*DELETE*) ou reordenar (*UPDATE* de *timestamps*) registros de *logs*; b) acesso físico a um dos nós da *Blockchain*, com a capacidade de desligá-lo ou tentar corromper sua cópia local da cadeia; c) adulteração de *backups*, notadamente a modificação de arquivos de *backup* antes de um processo de restauração para inserir dados falsos.

O adversário possui, ainda, o objetivo de ocultar atividades fraudulentas, apagar evidências de incidentes de segurança, ou quebrar a cadeia de custódia.

Dessa forma, a arquitetura proposta como solução mitiga essas ameaças através de notarização assíncrona de todos os eventos em uma cadeia imutável, estabelece consenso distribuído entre múltiplos nós, impedindo que a adulteração de um único nó invalide a rede e, por fim, garante a verificação de integridade de *backups* via *hash* notarizado.

3. ARQUITETURA DO SISTEMA

A plataforma base proposta é o Gestor de Acesso, desenvolvida pelo próprio autor, que é um sistema desenvolvido em *Python* com interface *Qt* (*PySide6*) e um servidor *web Flask*, projetado para integração com dispositivos biométricos de reconhecimento facial e gerenciamento de *logs* de autenticação em tempo real.

3.1 Arquitetura Operacional Base

Antes de abordar a implementação da camada *Blockchain*, é fundamental compreender a arquitetura operacional padrão do sistema. O Gestor de Acesso opera em um modelo cliente-servidor robusto, estruturado em componentes interconectados

que gerenciam a comunicação entre administradores, software central e dispositivos biométricos distribuídos.

O sistema funciona através de dois ciclos principais e contínuos que convergem para o repositório central de dados: Ciclo de Monitoramento de Eventos (Fluxo Reativo) e Ciclo de Gerenciamento Administrativo (Fluxo Proativo).

3.1.1 Ciclo de Monitoramento de Eventos (Fluxo Reativo)

O processo inicia quando um usuário se apresenta a um dispositivo biométrico. O equipamento captura características faciais, processa através de algoritmos internos e gera resultado de autenticação (acesso concedido/negado). Esse resultado, acompanhado de metadados estruturados (registro de data/hora, score de similaridade, ID do dispositivo), é formatado e transmitido via requisição *HTTP* para *endpoint* específico no Servidor Central. A Lógica Central executa persistência imediata no Banco de Dados Operacional (*SQLite*), otimizada para velocidade, garantindo disponibilidade instantânea na interface de monitoramento em tempo real.

3.1.2 Ciclo de Gerenciamento Administrativo (Fluxo Proativo)

Iniciado por operadores através das Interfaces de Usuário (*Desktop GUI* ou plataforma Web remota), esse ciclo processa ações administrativas como cadastro de usuários, remoção de dispositivos ou acionamento remoto de portas. O servidor desempenha função dupla: gera *logs* de auditoria detalhados das ações administrativas e, quando necessário, utiliza o Módulo de Comunicação (*API Client*) para traduzir comandos internos nos protocolos específicos dos dispositivos físicos.

3.2 Arquitetura Híbrida

A solução proposta adota um modelo híbrido, evitando substituição completa do repositório operacional. O sistema opera em duas camadas distintas que se integram ao fluxo operacional existente: Aplicação-Operação e Notarização-Integridade.

3.2.1 Aplicação e Operação

Compreende o Gestor de Acesso integrado com dispositivos biométricos e banco *SQLite*, mantendo os ciclos operacionais descritos anteriormente. Esta camada preserva o processamento de autenticações em tempo real, gerenciamento de modelos de usuários, execução de algoritmos de comparação e operações de alta frequência sem modificações na performance crítica.

3.2.2 Notarização e Integridade

Constitui a rede de nós *Blockchain* privada que se integra de forma transparente aos fluxos existentes. Durante o Ciclo de Monitoramento de Eventos, após a persistência no *SQLite*, os metadados do *log* são simultaneamente formatados como transação *JSON* (Notação de Objetos do J*avaScript*) e transmitidos para a rede *Blockchain*. No Ciclo de Gerenciamento Administrativo, todas as ações administrativas são igualmente notarizadas, criando registro imutável paralelo ao banco operacional.

Esta arquitetura garante imutabilidade dos *logs* sem impactar a performance crítica da verificação em tempo real, operando de forma assíncrona após a conclusão das operações principais.

O sistema foi projetado com resiliência em mente. Se a transmissão de um *log* para a rede *Blockchain* falhar (por exemplo, devido a uma desconexão de rede), o *log* ainda existe no banco de dados *SQLite*. Um processo de reconciliação periódico, ou acionado manualmente, pode ser executado para comparar os *logs* do *SQLite* com as transações da *Blockchain* e transmitir quaisquer registros que falharam em ser notarizados anteriormente.

3.3 Ambiente de Rede Isolada (*Air-Gapped*)

O sistema proposto opera em rede completamente segmentada e isolada da Internet, característica fundamental para ambientes de infraestrutura crítica e alta segurança. Essa arquitetura *air-gapped* elimina vetores de ataque externos e garante que tanto os dados biométricos quanto os registros *Blockchain* permaneçam em

ambiente controlado. Esta implantação de nós em uma infraestrutura de servidores controlada está alinhada com as melhores práticas para garantir a integridade e a segurança da rede blockchain (ZHAO, W. *et al*., 2025).

A rede isolada compreende dispositivos biométricos, servidores do Gestor de Acesso e nós *Blockchain* interconectados via infraestrutura de rede local dedicada. Esta segmentação física impede vazamento de dados, ataques remotos e comprometimento via internet, sendo especialmente relevante para organizações que processam informações classificadas ou operam infraestrutura crítica. A figura 1 ilustra os componentes e o fluxograma da arquitetura híbrida proposta.

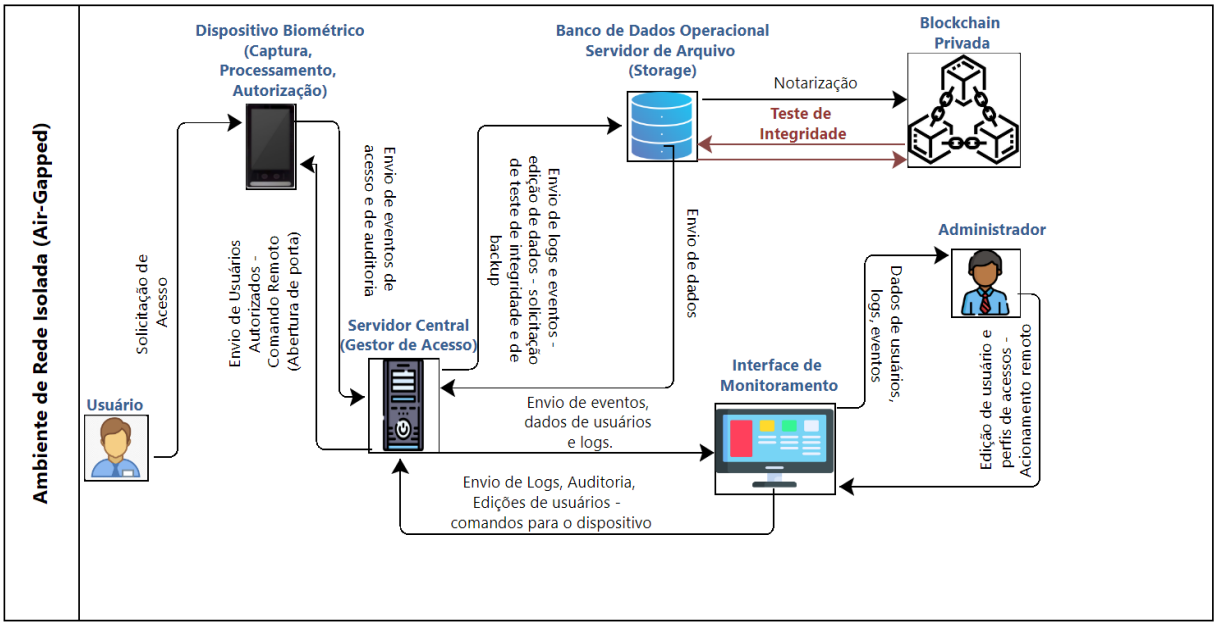

Figura 1: Fluxograma da Arquitetura Híbrida

4. IMPLEMENTAÇÂO DA PROPOSTA

A arquitetura híbrida descrita na Seção 3 foi implementada de forma prática na plataforma Gestor de Acesso. Esta seção detalha o funcionamento de cada camada, seguindo o fluxo de dados ilustrado na Figura 1 e apresentando evidências visuais da operação do sistema.

4.1. Aplicação e Operação

Esta fase inicial corresponde ao fluxo de trabalho convencional do sistema, responsável pela captura do evento de acesso e seu registro primário para fins operacionais imediatos.

O ponto de origem de todos os dados de acesso, conforme ilustrado no início do fluxo da figura 1, é o dispositivo de reconhecimento facial. Para a implementação deste trabalho, foi utilizado o terminal Intelbras XPE 3200 Face. Quando um usuário solicita acesso, o dispositivo captura e analisa a imagem, decidindo pela autorização ou negação e, em seguida, envia os metadados do evento via requisição HTTP para o Servidor Central.

É fundamental reconhecer que dispositivos baseados primariamente em análise de imagem 2D apresentam vulnerabilidades inerentes a ataques de apresentação *spoofing* (XING *et al*., 2025; MA *et al*., 2024), como o uso de fotografias ou vídeos. Esta suscetibilidade reforça um princípio central deste trabalho: se a camada de autenticação física pode ser comprometida, a integridade do registro desse evento torna-se a próxima e mais crucial linha de defesa. A possibilidade de um acesso fraudulento ser bem-sucedido torna imperativo que o *log* gerado seja absolutamente imutável, justificando a necessidade do processo de notarização.

Após o recebimento da requisição do dispositivo, o módulo de servidor *web* do Gestor de Acesso a encaminha para o módulo de persistência de dados, que executa a escrita imediata do *log* no Banco de Dados Operacional (*SQLite*). O resultado desta operação é exibido em tempo real na Interface de Monitoramento, fornecendo um retorno visual instantâneo sobre a atividade na rede, como demonstrado na figura 2. Esta fase síncrona é otimizada para velocidade, garantindo que a operação de acesso não sofra atrasos perceptíveis.

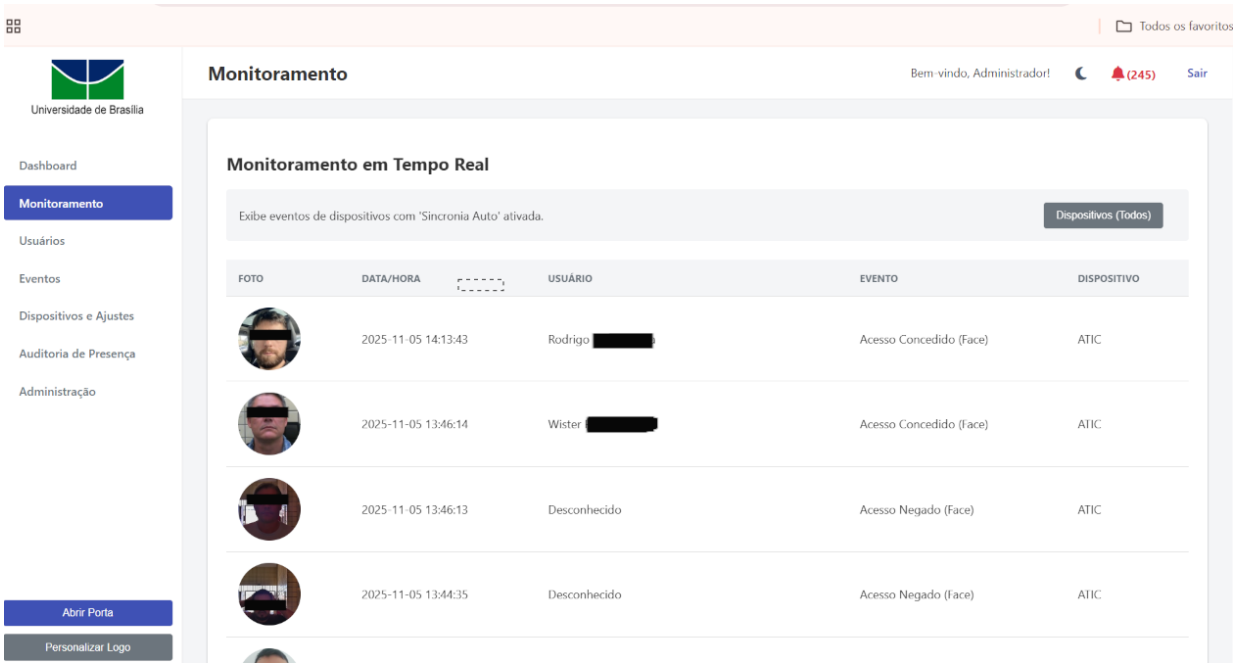

Figura 2: Interface de Monitoramento

Adicionalmente, as ações proativas realizadas pelo Administrador através da interface, como a edição de usuários ou o acionamento remoto de portas, também são processadas pelo Servidor Central e geram *logs* de auditoria detalhados. Tanto os *logs* de acesso (fluxo reativo) quanto os de auditoria (fluxo proativo) servem como gatilho para a camada de notarização descrita a seguir.

4.2 Notarização e Imutabilidade via *Blockchain*

Esta fase opera de forma assíncrona e constitui-se no núcleo central da contribuição deste trabalho. Sua função é receber os registros da fase operacional e selá-los de forma permanente e inviolável na *Blockchain* Privada. Imediatamente após um *log* ser salvo no *SQLite*, o Servidor Central prepara a transação para a *Blockchain*. Conforme a lógica implementada, o pacote de dados do *log* é processado para garantir privacidade e performance: a imagem facial é removida, e um *hash* SHA-256 da imagem é calculado para servir como prova criptográfica. O objeto *JSON* resultante, contendo apenas metadados e o *hash*, é então transmitido para todos os nós registrados na rede.

Cada nó da rede, ao receber uma nova transação, a adiciona à sua lista de transações pendentes e inicia automaticamente o processo de mineração. O nó

executa a Prova de Trabalho (*PoW*) até encontrar um *nonce* que satisfaça a dificuldade da rede. O primeiro nó a encontrar a solução forja um novo bloco e o transmite para os outros. O resultado é um registro permanente e verificável, como pode ser inspecionado diretamente na cadeia conforme ilustrado na figura 3.

Figura 3: Cadeia de Blocos

A natureza distribuída da rede é gerenciada administrativamente através da interface do Gestor de Acesso. Conforme mostrado na Figura 4, o Administrador pode registrar o endereço de rede de múltiplas máquinas, que passarão a atuar como nós validadores.

Figura 4: Interface de Adição de Nós na Blockchain

A robustez da rede é garantida por um mecanismo de consenso automático implementado em cada nó. Periodicamente (a cada 60 segundos) e antes de cada tentativa de mineração, cada nó executa seu algoritmo de resolução de conflitos. Ele consulta os outros nós da rede, compara o comprimento das cadeias e, se encontrar

uma cadeia válida mais longa que a sua, substitui sua própria versão. Esse processo resolve automaticamente bifurcações (*forks*) e garante que todos os participantes convirjam para uma única versão da verdade, assegurando a integridade da rede mesmo em cenários de falha ou dessincronização temporária de um nó.

4.3 Integridade de *Backups* com *Blockchain*

Além da notarização de eventos individuais em tempo real, a arquitetura proposta estende o uso da *Blockchain* para verificar a integridade de arquivos de *Backup*. Esse mecanismo estabelece uma cadeia de custódia digital para o estado completo do sistema, com o objetivo de detectar tentativas de adulteração de registros em massa antes de um processo de restauração.

O fluxo de criação de um *Backup* seguro é iniciado pelo administrador através da interface do Gestor de Acesso. O Servidor Central gera um arquivo estruturado contendo dados críticos como o histórico de logs, os modelos biométricos dos usuários e as configurações dos dispositivos. Antes de salvar este arquivo, o sistema calcula uma assinatura criptográfica única (*hash* SHA-256) para todo o seu conteúdo. Este *hash*, juntamente com metadados que identificam o *Backup*, é formatado como uma transação e transmitido para a rede *Blockchain*. A transação é então minerada e incluída em um novo bloco, o que sela permanentemente a assinatura do *backup* na cadeia, criando um registro inviolável de seu estado original.

O principal benefício desta notarização é aplicado durante o processo de restauração, que segue um protocolo de "verificar antes de confiar". Ao selecionar um arquivo de *Backup*, o Servidor Central primeiro calcula o *hash* SHA-256 do arquivo em tempo real. Em seguida, ele consulta a cadeia de blocos para recuperar o *hash* original que foi notarizado no momento da criação daquele *Backup*, em uma interação representada pela seta "Teste de Integridade" na figura 1.

A etapa final é a comparação criptográfica entre os dois *hashes*, o original da *Blockchain* e o do *Backup*. Se forem idênticos, o sistema confirma a autenticidade do arquivo e procede com a restauração. Contudo, se houver qualquer divergência, isso serve como prova irrefutável de que o arquivo foi adulterado. Neste caso, o sistema aborta imediatamente o processo de restauração e gera um alerta de

segurança, protegendo o ambiente operacional da injeção de dados corrompidos e mitigando a ameaça de "*Backup* Adulterado" detalhada na Tabela 1.

5. AVALIAÇÃO DE DESEMPENHO E ANÁLISE DE RESULTADOS

A eficácia da arquitetura proposta foi validada através de simulações que demonstram sua resiliência contra vetores de ataque e quantificam sua performance operacional. Para isso, dois experimentos principais foram realizados: o primeiro para validar a resiliência do ciclo de vida do *log* contra adulterações, e o segundo para analisar a segurança e a performance em um ambiente isolado.

5.1 EXPERIMENTO: Ciclo de Vida de *Log* Crítico

Este experimento simula o fluxo completo de um registro de acesso, desde sua criação legítima até uma tentativa de supressão maliciosa, para avaliar a robustez da solução contra adulterações.

Em uma operação normal, quando um usuário é autenticado com sucesso, a aplicação registra simultaneamente os dados detalhados no *SQLite* para consulta imediata. Paralelamente, uma transação *JSON* estruturada, contendo os metadados operacionais (ID pseudoanonimizado, resultado, *timestamp*, etc.), é transmitida para a rede *Blockchain*. Um nó da rede minera um novo bloco contendo esta transação, selando permanentemente o registro. Conforme a decisão arquitetural para conformidade com a LGPD (BRASIL, 2018), a imagem facial ou o *template* biométrico nunca são armazenados na cadeia, preservando a privacidade dos dados sensíveis.

Neste cenário, simula-se um evento onde um administrador interno mal-intencionado executa um comando *DELETE* no banco de dados *SQLite* para suprimir um registro comprometedor. Para consultas operacionais, o rastro do evento desaparece.

Contudo, ao executar a função de sistema "Restaurar *Logs* Faltantes da Rede *Blockchain*", o Gestor de Acesso consulta a cadeia de blocos, que serve como fonte imutável da verdade. O sistema identifica, por comparação, que o *log* está ausente no banco de dados operacional e procede à sua reinserção automática, com todos os

metadados originais preservados. A tentativa de ocultação é, portanto, não apenas revertida, mas também documentada como um novo evento de auditoria.

A tabela 1 resume a eficácia da arquitetura proposta na mitigação de diferentes vetores de ataque em comparação com sistemas tradicionais.

Vetor de Ataque	Vulnerabilidade Tradicional	Mitigação com a Arquitetura Proposta
Supressão de *Log*	Um *DELETE* no *SQL* remove o registro permanentemente.	O *log* original permanece na *blockchain*. A função "Restaurar *Logs*" o reinsere no banco operacional.
Alteração de *Timestamp*	Um *UPDATE* no *SQL* pode reordenar eventos.	O *timestamp* do bloco sela a ordem cronológica. A alteração invalidaria o *hash* de toda a cadeia.
Ataque de Insider	Admin pode apagar seus próprios rastros.	Todas as ações administrativas são notarizadas, criando um registro imutável da atividade do administrador.
***Backup* Adulterado**	Restaurar um *backup* modificado pode inserir *backdoors.*	O *hash* do *Backup* é notarizado. O sistema compara os *hashes* antes de restaurar e aborta se houver divergência.

Tabela 1: Comparação de Mitigação de Ataques

5.2 Experimento: Performance e Segurança em Ambiente Isolado

Este experimento quantifica a latência da arquitetura e analisa os desafios de segurança e sustentabilidade inerentes à operação em uma rede *air-gapped*.

A viabilidade da arquitetura híbrida depende de sua capacidade de introduzir a camada de segurança sem comprometer a performance operacional. Para quantificar a latência, foram realizados os testes empíricos descritos na Seção 3.2.

A análise divide o processamento em duas fases. A primeira é a fase síncrona (Impacto na Operação), que representa o único *overhead* percebido pela operação de acesso. Os testes registraram uma latência média de 0,5ms ± 0,1ms. Este valor é imperceptível, validando que a camada operacional não sofreu degradação de performance.

A segunda fase é a fase Assíncrona (Notarização), o processo opera em paralelo e é composto pela transmissão para a rede (146,9ms ± 45,1ms) e pela mineração

(51,5ms ± 61,1ms). A latência total do processo assíncrono é de aproximadamente 198,4ms.

A tabela 2 consolida os resultados, demonstrando a clara separação entre a operação crítica e a garantia de integridade. A análise empírica valida que a sobrecarga introduzida não compromete os requisitos de tempo real do sistema.

Etapa do Processo	Característica	Latência Média (ms)	Desvio Padrão (ms)
Persistência Síncrona	Bloqueante	0,5	0,1
Notarização Assíncrona	Não Bloqueante	198,4	-

Tabela 2: Resumo das Latências Medidas

5.3 Limitações e Desafios

Embora os experimentos validem a eficácia e a performance da arquitetura, sua sustentabilidade a longo prazo depende da gestão de desafios inerentes à estrutura proposta. A análise crítica abrange três dimensões principais: as implicações do mecanismo de consenso adotado, as consequências do crescimento perpétuo do armazenamento e os requisitos para a manutenção da segurança criptográfica.

A principal implicação da escolha pela Prova de Trabalho (*PoW*) é o consumo de recursos de CPU constante, ainda que baixo. Esta escolha foi deliberada, priorizando a simplicidade de implementação e a natureza *trustless* (sem necessidade de confiança) do mecanismo. Em um sistema focado em auditoria forense, a validação de cada bloco através de uma prova matemática objetiva é uma vantagem fundamental sobre alternativas como a Prova de Autoridade (*PoA*), que introduzem uma camada de confiança nos nós validadores, um modelo considerado menos ideal para este contexto de segurança crítica (ZHAO, W. *et al*., 2025).

Em relação ao armazenamento, a natureza imutável da *Blockchain* tem como consequência um crescimento de dados linear e perpétuo, replicado em cada nó. Isso exige um planejamento de infraestrutura para ambientes de alto tráfego, onde o volume de dados pode atingir múltiplos gigabytes por ano. Adicionalmente, a sincronização de um novo nó ou a recuperação de um participante que esteve *offline* pode se tornar um processo operacionalmente complexo, especialmente em redes isoladas (*air-gapped*).

Por fim, a resiliência da solução está condicionada à robustez dos algoritmos criptográficos empregados. Embora a segurança do *SHA-256* seja considerada alta, a sustentabilidade de longo prazo demanda uma gestão rigorosa do ciclo de vida das chaves criptográficas privadas. O comprometimento de uma chave por um agente interno com acesso privilegiado ao servidor representa uma ameaça crítica, pois permitiria a falsificação de transações. Isso reforça a necessidade de políticas de rotação de chaves e de mecanismos de armazenamento seguro para as chaves criptográficas, que as isolem do próprio sistema operacional e as protejam contra o comprometimento do servidor (ZHAO, X. *et al.*, 2024).

6. CONCLUSÃO

Este trabalho apresenta contribuições originais na implementação e validação de uma arquitetura híbrida para resolver o problema fundamental da mutabilidade de *logs* em sistemas de controle de acesso biométrico. A integração de uma camada de notarização via *Blockchain* privada na plataforma Gestor de Acesso, um sistema original desenvolvido pelo autor, demonstrou ser uma solução robusta e eficaz. A arquitetura proposta preserva a agilidade operacional necessária para o reconhecimento facial em tempo real, enquanto incorpora uma camada de integridade irrefutável para todos os registros de acesso e auditoria.

A validação prática desta solução completa, desde a plataforma de gerenciamento até a camada de segurança distribuída, é um dos resultados centrais do estudo. Os experimentos realizados confirmaram a viabilidade da arquitetura: a análise de performance quantitativa demonstrou que o impacto na operação crítica é imperceptível (latência síncrona de ~0,5ms), enquanto o processo de notarização assíncrono é concluído eficientemente em segundo plano (~198ms). Adicionalmente, as simulações de tentativa de adulteração validaram a resiliência do sistema, comprovando a capacidade de detectar e reverter a supressão maliciosa de registros, reforçando a cadeia de custódia digital.

O sistema estabelece, portanto, um caso de estudo prático que valida o potencial da *Blockchain* como tecnologia fundamental para a próxima geração de sistemas de segurança biométrica confiáveis. Os resultados contribuem para o avanço da

segurança de dados de auditoria, fornecendo um modelo replicável para organizações que necessitam de integridade absoluta de registros históricos. A análise das limitações evidencia que a sustentabilidade de longo prazo desta robustez dependerá da gestão dos desafios operacionais de armazenamento, sincronização e da manutenção contínua das práticas criptográficas.

As direções para trabalhos futuros focam no aprimoramento da estrutura proposta. Recomenda-se a pesquisa de otimizações do mecanismo de Prova de Trabalho, como o ajuste dinâmico da dificuldade, para melhorar a eficiência energética.

O desenvolvimento de interfaces de consulta avançadas para análise forense e a integração com sistemas de detecção de anomalias baseados em aprendizado de máquina expandiriam significativamente as capacidades investigativas do sistema. Finalmente, o aprimoramento dos protocolos de gestão de chaves criptográficas, incluindo o desenvolvimento de mecanismos avançados para isolar e proteger as chaves privadas do sistema operacional, é um passo importante para fortalecer ainda mais a segurança da arquitetura contra ameaças internas.

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD).* Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 6 nov. 2025.

DAI, Y.; LU, G.; HUANG, Y. A Blockchain-Based Access Control System for Secure and Efficient Hazardous Material Supply Chains. *Mathematics*, v. 12, n. 17, p. 2702, 2024. Disponível em: https://www.mdpi.com/2227-7390/12/17/2702. Acesso em: 6 nov. 2025.

KARADUMAN, Ö.; GÜLHAS, G. Blockchain-Enabled Supply Chain Management: A Review of Security, Traceability, and Data Integrity Amid the Evolving Systemic Demand. *Applied Sciences*, v. 15, n. 9, p. 5168, 2025. Disponível em: https://www.mdpi.com/2076-3417/15/9/5168. Acesso em: 28 jul. 2025.

GHAFOURIAN, M.; SUMER, B.; VERA-RODRIGUEZ, R.; FIERREZ, J.; TOLOSANA, R.; MORALES, A.; KINDT, E. Blockchain and Biometrics: Survey, GDPR Analysis, and Future Directions. *arXiv preprint*, arXiv:2302.10883v3, 2025. Disponível em: https://arxiv.org/html/2302.10883v3. Acesso em: 6 nov. 2025.

RAJUROY, A.; JOHN, B. A Framework for Blockchain-Based Access Logs and Tamper-Proof Audit Trails. *ResearchGate*, 2025. Disponível em: https://www.researchgate.net/publication/392312120. Acesso em: 6 nov. 2025.

XING, H.; TAN, S. Y.; QAMAR, F.; JIAO, Y. Face Anti-Spoofing Based on Deep Learning: A Comprehensive Survey. *Applied Sciences*, v. 15, n. 12, p. 6891, 2025. Disponível em: https://doi.org/10.3390/app15126891. Acesso em: 6 nov. 2025.

MA, Y. et al. Algorithm of face anti-spoofing based on pseudo-negative features generation. Frontiers in Neuroscience, v. 18, p. 1362286, 2024. Disponível em: https://pmc.ncbi.nlm.nih.gov/articles/PMC11047124/ Acesso em: 09 nov. 2025.

NAKAMOTO, S. *Bitcoin: A Peer-to-Peer Electronic Cash System.* 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 6 nov. 2025.

PUNIA, A. et al. A Systematic Review on Blockchain-Based Access Control Systems in Cloud Environment. *Journal of Cloud Computing*, v. 13, n. 146, 2024. Disponível em: https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-024-00697-7. Acesso em: 6 nov. 2025.

SHARMA, S.; DWIVEDI, R. A Survey on Blockchain Deployment for Biometric Systems. *IET Blockchain*, v. 4, n. 1, p. 63-85, 2024. Disponível em: https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/blc2.12063. Acesso em: 6 nov. 2025.

ZHAO, X.; PENG, C.; TAN, W.; DING, H. Blockchain-based access control dynamic key authentication protocol in IoT. In: PROCEEDINGS OF THE 2024 7th INTERNATIONAL CONFERENCE ON BLOCKCHAIN TECHNOLOGY AND APPLICATIONS. ACM, 2024. p. 55-59. DOI: 10.1145/3708622.3708625. Disponível em: https://dl.acm.org/doi/10.1145/3708622.3708625. Acesso em: 2 nov. 2025.

ZHAO, W.; YANG, S.; LUO, X. Blockchain-Facilitated Cybersecurity for Ubiquitous Internet of Things with Space–Air–Ground Integrated Networks: A Survey. *Sensors*, v. 25, n. 2, art. 383, 2025. DOI: 10.3390/s25020383. Disponível em: https://doi.org/10.3390/s25020383. Acesso em: 6 nov. 2025.