josif 2025
17ª Jornada Científica e Tecnológica
14º Simpósio de Pós-Graduação
do IFSULDEMINAS
ISSN: 2319-0124
REALIZAÇÃO
INSTITUTO FEDERAL Sul de Minas Gerais
APOIO
CNPq
FAPEMIG

SISTEMA INTEGRADO DE CONTROLE DE ACESSO ÀS SALAS E LABORATÓRIOS DO IFSULDEMINAS UTILIZANDO TECNOLOGIAS IOT E MICROSSERVIÇOS

Matheus H. M. SILVA [1]; Filipe S. SILVA [2]; Gabriel F. G. GHETTI [3]; Thiago C.TAVARES[4]; Rodrigo L. ORTOLAN[5];

RESUMO

O controle de acesso no IFSULDEMINAS, dependente de chaves físicas, gera gargalos logísticos e riscos de segurança. Este trabalho descreve a arquitetura e a concepção de um sistema integrado para automatizar e centralizar o controle de acesso, visando otimizar a gestão, aumentar a segurança e permitir o monitoramento em tempo real. A solução proposta utiliza uma arquitetura de microsserviços para garantir escalabilidade, composta por um painel administrativo Web, um aplicativo móvel para abertura de portas validada por geolocalização e microcontroladores (ESP32/ESP8266) nos pontos de acesso. A comunicação entre os dispositivos de Internet das Coisas (IoT) e o backend é realizada pelo protocolo leve MQTT. A segurança é reforçada com autenticação integrada à API do SUAP, políticas de controle de acesso RBAC e DAC, e a segmentação da rede com uma VLAN dedicada. O sistema, gerenciado com contêineres Docker, resulta em uma solução robusta e replicável que automatiza o processo, gera logs de auditoria para todos os acessos e estabelece uma base tecnológica para futuras expansões.

Palavras-chave: Internet das Coisas; Arquitetura Distribuída; Segurança de Rede; Protocolo MQTT; Conteinerização.

1. INTRODUÇÃO

No Instituto Federal do Sul de Minas (IFSULDEMINAS), a ausência de um sistema digital e centralizado para o controle de acesso a salas e laboratórios representa um significativo gargalo logístico e de segurança. O método atual, que depende da entrega manual de chaves físicas por um funcionário, é propenso a atrasos, dificulta a rastreabilidade dos acessos e eleva os riscos associados à perda ou duplicação de chaves. Essa vulnerabilidade compromete não apenas a segurança de equipamentos, mas também a integridade de atividades acadêmicas e pesquisas.

Para solucionar este desafio, propõe-se o desenvolvimento e a implementação de um sistema integrado de controle de acesso, composto por um software de gestão, um aplicativo móvel e microcontroladores. A solução visa otimizar o fluxo de acesso, reforçar a segurança por meio de logs de auditoria detalhados, simplificar a gestão de permissões e permitir o monitoramento das portas em tempo real, utilizando tecnologias de Internet das Coisas (IoT), segurança de rede e uma arquitetura de microsserviços moderna e escalável. O presente artigo pretende detalhar a arquitetura planejada, as tecnologias selecionadas e a metodologia para a implementação. Por se tratar de um projeto em andamento, o foco é a concepção do sistema.

[1]Bolsista, IFSULDEMINAS – *Campus* Poços de Caldas. E-mail: matheus.moreno@alunos.ifsuldeminas.edu.br.
[2]Voluntário, IFSULDEMINAS – *Campus* Poços de Caldas. E-mail: filipe.silva@alunos.ifsuldeminas.edu.br.
[3]Bolsista, IFSULDEMINAS – *Campus Poços de Caldas*. E-mail: gabriel.ghetti@alunos.ifsuldeminas.edu.br.
[4]Orientador, IFSULDEMINAS – *Campus* Poços de Caldas. E-mail: thiago.tavares@ifsuldeminas.edu.br.
[5]Coorientador, IFSULDEMINAS – *Campus* Poços de Caldas. E-mail: rodrigo.ortolan@ifsuldeminas.edu.br.

2. FUNDAMENTAÇÃO TEÓRICA

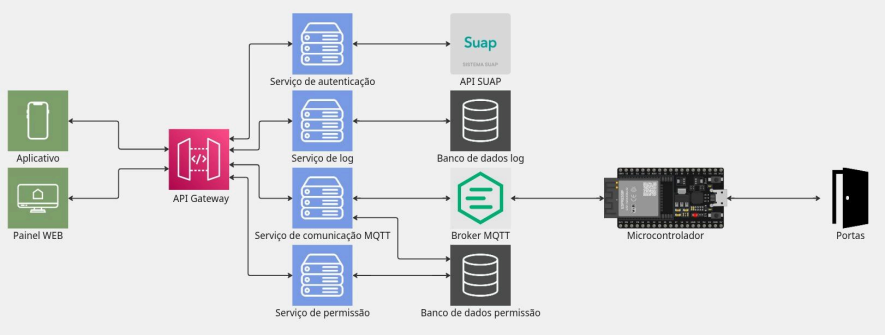
A base do sistema assenta-se em tecnologias e conceitos-chave para garantir sua funcionalidade, segurança e escalabilidade. A arquitetura de microsserviços foi adotada para dividir a aplicação em componentes menores e independentes, promovendo a manutenção e a escalabilidade otimizada (JARAMILLO; NGUYEN; SMART, 2016; APARECIDO; SANTOS, 2024). Cada serviço é empacotado em contêineres Docker, o que assegura a consistência e portabilidade entre diferentes ambientes (ANDERSON, 2015).

Na camada de hardware, foram selecionados os microcontroladores ESP32 e ESP8266 devido à sua conectividade Wi-Fi integrada e excelente relação custo-benefício. A comunicação entre estes dispositivos IoT e o backend é realizada através do protocolo MQTT (Message Queuing Telemetry Transport), um padrão leve e eficiente, ideal para redes com baixa largura de banda (YASSEIN *et al.*, 2017).

A segurança é tratada em múltiplas camadas. O controle de acesso combina os modelos RBAC (Role-Based Access Control), para permissões baseadas em funções, e DAC (Discretionary Access Control), para concessões pontuais (FERRAIOLO; BARKLEY; KUHN, 1999; SANDHU; MUNAWER, 1998). A autenticação dos usuários é integrada à API do SUAP, utilizando um sistema de tokens para proteger as comunicações. Adicionalmente, a segurança da rede é reforçada com a criação de uma VLAN (Virtual Local Area Network) exclusiva para os dispositivos IoT, isolando-os do restante da rede institucional (ANDRADE *et al.*, 2023).

3. MATERIAL E MÉTODOS

A metodologia do projeto foi estruturada em cinco fases sequenciais: análise de requisitos, design da arquitetura, desenvolvimento, testes e implantação. A arquitetura do sistema foi projetada no modelo de microsserviços, e os serviços incluem: Serviço de Autenticação, Serviço de Log, Serviço de Comunicação MQTT e Serviço de Permissões. A comunicação entre os componentes é orquestrada por uma API Gateway.



Fonte: auditoria própria (2025)

O *frontend* abrange um painel administrativo Web e um aplicativo móvel. O firmware dos microcontroladores será programado para se conectar à rede Wi-Fi e comunicar-se com o Broker MQTT para receber comandos de abertura e publicar o estado da porta (aberta/fechada) em tempo real, utilizando um sensor *Reed Switch*. A implantação de todos os serviços será gerenciada por contêineres Docker.

4. RESULTADOS E DISCUSSÃO

A implementação deste sistema resultará na substituição completa do obsoleto processo manual de controle com chaves físicas por uma plataforma digital, centralizada e auditável. O principal resultado esperado é um aumento significativo na segurança e na eficiência operacional do campus. A automação do processo de abertura de portas via aplicativo móvel, validado por geolocalização, eliminará os gargalos logísticos, especialmente durante a troca de aulas.

A geração automática de logs para cada tentativa de acesso, seja ela bem-sucedida ou negada, fornecerá uma trilha de auditoria completa, permitindo a rastreabilidade e a investigação de incidentes de segurança. A arquitetura de microsserviços, aliada ao uso de contêineres Docker, confere ao sistema a flexibilidade e escalabilidade necessárias para se adaptar a futuras demandas (ALSHUQAYRAN; ALI; EVANS, 2016; APARECIDO; SANTOS, 2024), como a expansão para outras unidades do IFSULDEMINAS ou a integração com outros sistemas de automação. A segmentação da rede por meio de VLANs isola os dispositivos IoT, mitigando riscos e protegendo a infraestrutura de rede da instituição contra possíveis ataques. Espera-se que a solução se torne uma base tecnológica sólida para futuras inovações no campus.

5. CONCLUSÃO

Este trabalho detalhou a arquitetura e o planejamento de um sistema integrado de controle de acesso que moderniza e fortalece a segurança do IFSULDEMINAS. Ao substituir o método manual por uma solução baseada em IoT e microsserviços (DMITRY; MANFRED, 2014), o projeto não apenas soluciona as vulnerabilidades existentes, como a falta de rastreabilidade e os riscos de segurança, mas também estabelece um novo padrão de gestão para a instituição. A arquitetura modular, a comunicação em tempo real via MQTT e as múltiplas camadas de segurança (autenticação SUAP, RBAC/DAC, VLANs) garantem uma solução robusta, escalável e eficiente. O sistema resolve um problema operacional imediato e fornece uma base tecnológica preparada para futuras expansões, alinhando o campus às demandas de uma instituição de ensino moderna e conectada.

REFERÊNCIAS

ALSHUQAYRAN, Nuha; ALI, Nour; EVANS, Roger. A systematic mapping study in microservice architecture. In: **2016 IEEE 9th international conference on service-oriented computing and applications (SOCA)**. IEEE, 2016. p. 44-51. Disponível em: https://ieeexplore.ieee.org/abstract/document/7796008. Acesso em: 13 jun. 2025

ANDERSON, Charles. Docker [software engineering]. **IEEE software**, v. 32, n. 3, p. 102-c3, 2015. Disponível em: https://ieeexplore.ieee.org/abstract/document/7093032. Acesso em: 15 jun. 2025.

ANDRADE ARENAS, Laberiano Matías et al. Information security: proposal for a VLAN network model. 2023. Disponível em: https://repositorio.utp.edu.pe/handle/20.500.12867/7192. Acesso em: 21 abr. 2025.

APARECIDO, João P. L.; SANTOS, Paulo C. dos. COMPARAÇÃO ENTRE ARQUITETURA MONOLÍTICA E DE MICROSSERVIÇOS: Análise de escalabilidade, manutenção e eficiência no desenvolvimento de software. In: **JORNADA CIENTÍFICA E TECNOLÓGICA DO IFSULDEMINAS**, 16., 2024. Disponível em: https://josif.ifsuldeminas.edu.br/ojs/index.php/anais/article/view/1952/1558. Acesso em: 23 set. 2025.

DMITRY, Namiot; MANFRED, Sneps-Sneppe. On micro-services architecture. **International Journal of Open Information Technologies**, v. 2, n. 9, p. 24-27, 2014. Disponível em: https://cyberleninka.ru/article/n/on-micro-services-architecture. Acesso em: 13 jun. 2025

FERRAIOLO, David F.; BARKLEY, John F.; KUHN, D. Richard. A role-based access 23 control model and reference implementation within a corporate intranet. **ACM Transactions on Information and System Security (TISSEC)**, v. 2, n. 1, p. 34-64, 1999. Disponível em: https://dl.acm.org/doi/abs/10.1145/300830.300834. Acesso em: 14 jun. 2025

JARAMILLO, David; NGUYEN, Duy V.; SMART, Robert. Leveraging microservices architecture by using Docker technology. In: **SoutheastCon 2016**. IEEE, 2016. p. 1-5. Disponível em: https://ieeexplore.ieee.org/abstract/document/7506647. Acesso em: 13 jun. 2025

SANDHU, Ravi; MUNAWER, Qamar. How to do discretionary access control using roles. In: **Proceedings of the third ACM workshop on Role-based access control**. 1998. p. 47-54. Disponível em: https://dl.acm.org/doi/pdf/10.1145/286884.286893. Acesso em: 14 jun. 2025

YASSEIN, Muneer Bani *et al.* Internet of Things: Survey and open issues of MQTT protocol. In: **2017 international conference on engineering & MIS (ICEMIS)**. Ieee, 2017. p. 1-6. Disponível em: https://ieeexplore.ieee.org/abstract/document/8273112. Acesso em: 16 jun. 2025.