DOI: 10.53660/CLM-1758-23L07

A system for access control in students' leaving times at childhood education units

Um sistema para controle de acesso nos horários de saída de estudantes em unidades escolares do ensino infantil

Received: 2023-07-03 | Accepted: 2023-08-05 | Published: 2023-08-11

Alextian Bartholomeu Liberato
ORCID: https://orcid.org/0000-0001-8592-455X
Instituto Federal do Espírito Santo, Brasil
E-mail: alextian@ifes.edu.br
Keverson Soares de Oliveira
ORCID: https://orcid.org/0009-0007-0657-9147
Instituto Federal do Espírito Santo, Brasil
E-mail: keversonsoares.ti@gmail.com
Sanderson Gurgel
ORCID: https://orcid.org/0009-0004-4976-5925
Instituto Federal do Espírito Santo, Brasil
E-mail: sangurgel@gmail.com
Julio Cesar Nardi
ORCID: https://orcid.org/0009-0004-0644-2624
Instituto Federal do Espírito Santo, Brasil
E-mail: julionardi@ifes.edu.br
Giovany Frossard Teixeira
ORCID: https://orcid.org/0009-0004-8159-5313
Instituto Federal do Espírito Santo, Brasil
E-mail: giovany@ifes.edu.br
Octavio Cavalari Júnior
ORCID: https://orcid.org/0000-0001-8063-5484
Instituto Federal do Espírito Santo, Brasil
E-mail: cavalarioc@ifes.edu.br
Eduardo Meireles
ORCID: https://orcid.org/0000-0002-6711-6572
Universidade do Estado de Minas Gerais, Brasil
E-mail: eduardo.meireles@uemg.br

ABSTRACT

Releasing students on leaving school times is a process that requires full attention. In some kindergarten schools, private or public, it is possible to find a specific professional to carry out this mission, however, it is not uncommon to see teachers or even other servers performing this service. Regardless of who is responsible, releasing a student to an unauthorized person or even a stranger represents a terrible security breach for educational institutions. This error can generate trauma and sequelae for the life of the student and their family members. Thus, this work presents a system to help kindergarten schools in the task of controlling students when they leave school. For system validation, we consider the implementation of a prototype integrated with RFID and biometrics (fingerprint) technologies. Three scenarios were considered in order to demonstrate the functioning of the system. The results show that it is possible to control the release of students when they leave school, simplifying the future implementation of integrated security protocols in a teaching unit.

Keywords: School safety; Fingerprint; RFID.

RESUMO

A liberação de estudantes na saída escolar é um processo que exige total atenção. Em algumas escolas do ensino infantil, sejam privadas ou públicas, é possível encontrar um profissional específico para a realização desta missão, todavia, não é incomum visualizarmos docentes ou mesmo outros servidores acumulando este serviço. Independentemente de quem seja o responsável, a liberação de um estudante para uma pessoa não autorizada ou até mesmo para um desconhecido, representa uma terrível falha de segurança para as instituições de ensino. Esse erro pode gerar traumas e sequelas para a vida do estudante e seus familiares. Deste modo, neste trabalho é apresentado um sistema para auxiliar as escolas do ensino infantil na tarefa de controle dos alunos no horário de saída escolar. Para validação do sistema, consideramos a implementação de um protótipo integrado com as tecnologias RFID e biometria (impressão digital). Três cenários foram considerados para evidenciar o funcionamento do sistema. Os resultados demonstram que é possível controlar a liberação dos discentes no horário de saída da escola, simplificando a futura implementação de protocolos integrados de segurança em uma unidade de ensino.

Palavras-chave: Segurança escolar; Impressão digital; RFID.

INTRODUÇÃO

Pais e responsáveis, ao deixarem suas crianças nas escolas e creches, realizam um ato de confiança, na plena certeza de reencontrá-los no momento em que retornarem no ambiente escolar para retirá-los. Contudo, é possível encontrar em veículos de notícias, dezenas de casos no Brasil e no mundo de crianças que são entregues, por engano, a pessoas não autorizadas, gerando situações de extrema gravidade.

Tendo como escopo o apoio no controle de acesso nos horários de saída em unidades escolares do Ensino Infantil (crianças de 01 a 05 anos), a responsabilidade sobre tal controle deve ser prioridade, pois erros podem gerar gravíssimas consequências, como traumas e sequelas de ordem física e/ou psíquica para os estudantes e familiares. Relatos de profissionais que trabalham em unidades escolares dizem que os eventos de insegurança na liberação dos estudantes são comuns, o que requer soluções a fim de minorar situações de risco.

Dentre algumas situações, podem-se destacar: os pais ou responsáveis chegam para buscar as crianças e precisam se identificar à algum colaborador da escola. Entretanto, este procedimento, por vezes, não se apresenta eficaz ou seguro, pois: i) pai/responsável não leva a carteirinha de identificação (produzida pela própria unidade de ensino, onde constam o nome do responsável e o nome do estudante); ii) os pais/responsáveis pedem a uma outra pessoa para buscar o estudante sem a devida carteirinha; e/ou iii) alguns pais possuem restrições de ordem judicial para não estar junto aos filhos, dentre outras.

A cada instante, surgem inovações que facilitam e operacionalizam diversos procedimentos e atividades cotidianas. De modo especial, na área de Segurança, inovações podem evitar erros humanos por displicência, imprudência ou negligência.

Neste contexto, uma importante alternativa para a identificação dos pais/responsáveis de forma automática é a biometria, que foi utilizada em uma solução computacional visando atenuar a ocorrência de erros humanos, promovendo melhorias para o processo de controle de saída dos estudantes em unidades escolares. Assim, com o objetivo de ampliar o nível de segurança no momento da saída dos estudantes nas unidades de ensino infantil, foi proposto o desenvolvimento e a implantação de um sistema intitulado **TagBiometrick**.

Tal sistema foi construído sobre a plataforma Raspberry PI e implementado utilizando-se a linguagem C# e Phyton. O sistema conta com uma base de dados para armazenar informações dos estudantes e respectivos pais/responsáveis autorizados. A partir dessas informações, ele pode verificar o pai/responsável autorizado a ter acesso à unidade escolar e ao respectivo estudante.

Para identificação e validação foram realizadas coletas de impressões digitais e de leitores de cartões/etiquetas RFID para controle. O sistema deverá ficar na saída da unidade de ensino para que quando os responsáveis cheguem, autentiquem-se como pais ou responsáveis, através da biometria, desse modo, o colaborador confirmará as informações no monitor sobre o respectivo estudante relacionado com seu cadastro no sistema.

Pessoas não cadastradas no sistema, mas de posse do cartão RFID, deverão ser checadas por um funcionário da unidade de ensino. Cada unidade deverá utilizar protocolos criados por ela própria para esta verificação, como por exemplo: entrar em contato com os pais/responsáveis cadastrados no sistema, para certificar se a pessoa que foi buscar o estudante realmente foi autorizada para retirar a criança da unidade de ensino.

O restante deste artigo está estruturado da seguinte forma: na Seção 2 é apresentada a fundamentação teórica, o objetivo desta seção é discutir aspectos teóricos importantes para compreensão do trabalho. Em seguida, na Seção 3 é apresentado o protótipo com descrição dos principais componentes utilizados. Além disso, também é discutida a implementação técnica e os recursos de software utilizados. Na Seção 4 como prova de conceito, são apresentados e debatidos alguns cenários e os resultados obtidos desses experimentos. Por fim, na Seção 5 são tecidas as considerações finais e direcionamento dos trabalhos futuros.

RERERENCIAL TEÓRICO

Nesta seção, são apresentados aspectos teóricos importantes para a fundamentação da pesquisa, bem como soluções correlatas àquela apresentada neste trabalho.

Sistemas biométricos

Os sistemas biométricos tiveram início na década de 70, devido à grande necessidade de agilizar o processamento de reconhecimento de características únicas do indivíduo. Tipicamente, um sistema biométrico pode ser definido como um conjunto de tecnologias capaz de realizar várias tarefas para captar, processar, armazenar, recuperar e comparar dados biológicos.

Segundo Pinheiro (2008), sistemas biométricos podem ser definidos como um conjunto de hardware e software que realizam o reconhecimento de padrões com um propósito específico. Assim, realizam o reconhecimento de características e extraem um modelo/padrão previamente armazenado em memória e usando determinadas características para comparação. Estes padrões adquiridos servem, pois, de base para comparação e reconhecimento. O reconhecimento pode se dá, por exemplo, na comparação da impressão digital fornecida com uma impressão digital anteriormente modelada e armazenada em um banco de dados.

Biometrias são características físicas que diferenciam indivíduos uns dos outros e podem ser usadas para individualizar uma pessoa em meio a uma multidão. Esta individualização pode se dar por meio de leitura facial, leitura da digital, da íris ou da identificação vocal. De acordo com Garen (2022), a biometria começou a ficar ainda mais conhecida no Brasil a partir de 2008, nas eleições, quando começou a ser testada em três municípios brasileiros no pleito daquele ano para identificar o eleitor. Um simples toque com o dedo indicador dava acesso ao leitor para votação. De lá para cá, ela se popularizou, e está presente tanto no acesso a bancos, *notebooks*, *smartphones*, veículos, dentre outros.

Para Santos (2007), a biometria facial é um sistema menos intrusivo, pois podem-se utilizar imagens fotográficas amplas para realizar a identificação. A biometria digital é a mais utilizada no mundo, pois é extremamente segura, eficaz e barata. A biometria por íris é uma das mais caras e tem limitação, pois a fotografia deve ser feita, em média, a uma distância de 25 cm. A biometria vocal não é tão confiável como as demais, pois ruídos ou sons no ambiente podem se misturar à voz, alterando o padrão de reconhecimento.

Leitores biométricos são poderosas ferramentas tecnológicas utilizadas para evitar fraudes e buscar segurança. Leitores biométricos fisiológicos lêem as características físicas dos indivíduos (GAREN, 2022). São exemplos: (i) leitores de íris, (ii) leitores de impressões digitais, (iii) leitores do formato de orelhas, (iv) leitores de DNA, (v) leitores de impressões de veias sanguíneas das mãos, e (vi) leitores de face / rostos. Os leitores biométricos comportamentais são aqueles que lêem as características comportamentais dos indivíduos (RESENDE, 2007). São

exemplos: (i) leitores de voz, (ii) leitores de marcha/caminhada e (iii) leitores de assinaturas manuais.

Dentre os vários leitores biométricos, o mais comum é o leitor biométrico de impressão digital, o qual é de uso simples e tem o melhor custo benefício (COSTA, 2001) (PINHEIRO, 2008). Tais leitores são utilizados desde em agências bancárias até em novas gerações de *smartphones* (GAREN, 2022). A biometria digital utiliza as diferentes formas das linhas que as pessoas possuem nas pontas dos dedos a fim de identificá-las unicamente (AQUINO, 2014).

As impressões digitais são encontradas na derme, que é o tecido conjuntivo sobre o qual se apoia a epiderme, que é a porção superficial da pele (AQUINO, 2014). Na derme encontram-se as papilas, dispostas em uma série de linhas separadas por sulcos. A impressão digital de cada ser humano, se forma durante o sexto mês de gestação e durante o envelhecimento, apesar de ocorrer mudanças como tamanho, o formato permanece inalterado durante toda a vida do indivíduo (ABE, 2005) (SILVA, 2006).

O método de captura da impressão digital leva em conta, pois, a análise das irregularidades (chamadas de sulcos ou minúcias). A aquisição da imagem é essencial para o reconhecimento do indivíduo, mas para que isso ocorra é importante também que haja um sensor de boa qualidade. Existem, basicamente, dois tipos de métodos de leituras (VIGLIAZZI, 2006)(MARCONDES, 2022): (i) óptico (baseia-se no princípio da reflexão da luz) e (ii) não-óptico (baseia-se no princípio de impulsos elétricos).

O método óptico é o mais recomendado para o uso em leitores biométricos. Entretanto, a escolha do tipo de leitor dependerá da complexidade de atuação onde o dispositivo será empregado. O preço e a qualidade dos leitores podem variar consideravelmente. Os modelos mais simples custam, em média, R$ 140,00; já os modelos com melhor qualidade podem custam, em média, R$ 620,00.

Radio frequency identification (RFID)

A tecnologia RFID (*Radio Frequency Identification*), surgiu em meados dos anos 1940 e permite a captação de dados de diferentes objetos, sendo a leitura desses dados realizada por etiquetas eletrônicas (*tags*). No sistema RFID existem antenas leitoras que emitem sinais de energia por radiofrequência para as *tags*. Tais sinais alimentam o circuito interno do microchip da *tag* e retornam a informação armazenada. As antenas leitoras, por sua vez, recebem a informação e enviam para um banco de dados acessível via sistema, podendo este ser um computador ou um microcontrolador, sendo possível comunicar com diferentes plataformas locais e distribuídas (THOMAZINI, 2020).

Na área de controle de acesso, o RFID pode ser aplicado em vários contextos como, por exemplo, em ingressos de eventos, dificultando a falsificação dos mesmos, pois sua identificação

é única no sistema. Também pode ser aplicado em crachás de acesso de funcionários e visitantes, em prédios e convenções, dentre outros.

A Figura 1 apresenta um kit RFID contendo um módulo de leitura e dois cartões de acesso: um em formato de cartão de crédito e outro em formato de chaveiro.

Figura 1 - Módulo RFID MFRC522 Mifare.

Fonte: https://www.filipeflop.com.br, (2022).

Raspberry

Desenvolvido e registrado pela Raspberry Pi *Foundation*, uma instituição sem fins lucrativos do Reino Unido, esta plataforma consiste em um computador de pequeno porte, inicialmente criado com objetivo de ensinar programação para crianças.

Sua estrutura de *hardware* passou por modificações. Atualmente, possui um processamento semelhante aos computadores tradicionais. A estratégia do fabricante era ter um *hardware* flexível e possível de realizar atividades simples e ter acesso aos componentes principais que um computador possui, porém utilizando dispositivos pequenos de circuitos integrados a um preço acessível. Na Figura 2 é apresentado o Modelo Raspberry PI 3 Model B V1.2, com memória de 1GB RAM, 4 portas USB e uma interface Ethernet.

Em termos de linguagem de programação, os dispositivos Raspberry são na maioria das vezes programados utilizando as linguagens Scratch e Python, além da tradicional linguagem C, que é utilizada em muitas plataformas de prototipagem (MANENTE, 2019 e ROVEDA, 2020).

Figura 2 - Raspberry PI 3.

Fonte: www.raspberrypi.com, (2022).

Soluções de software para controle de acesso

A fim de apresentar uma visão geral do estado da técnica sobre soluções de software existentes para controle de acesso, foi realizado um levantamento dos registros de programas de computador existentes na base de dados do INPI (Instituto Nacional de Propriedade Industrial).

Na etapa de busca, utilizaram-se as palavras-chave “acesso” e “controle”. Ambas as palavras deveriam constar no título dado ao programa de computador registrado. Foram encontrados 60 (sessenta) registros em uma busca realizada em 11 de julho de 2023, os quais foram analisados. Por questões de espaço, no Quadro 1, são apresentados apenas um subconjunto de todos os registros analisados.

Considerando as informações fornecidas nas páginas do INPI pode-se observar que alguns desses registros são versões atualizadas de programas já registrados (p.ex., BR 51 2015 000865 0 e BR 51 2018 051998 9) ou mesmo módulos de uma mesma solução, que foram registradas separadamente (p.ex., BR 51 2022 000404 6, BR 51 2022 000403 8, BR 51 2022 000402 0, BR 51 2022 000393 7). Assim, não há, necessariamente, uma relação única direta de cada registro para uma solução existente de controle de acesso. De todo modo, as informações obtidas dão uma boa noção do tipo de solução de controle de acesso que vem sendo desenvolvida e o histórico de registros ao longo das últimas 4 (quatro) décadas.

Quadro 1 - Resultados da busca por registros de programas de computador no INPI.

Pedido	Depósito	Título	Aplicação
BR 51 2023 001681 0	14/06/2023	ACRA - Sistema de controle de Acesso de Pedestre e Veículos em estabelecimento residencial e empresarial	Controle de acesso de pedestres e veículos
BR 51 2023 000585 1	10/03/2023	Controle de Acesso - 2023	Controle de acesso (genérico ou não especificado)

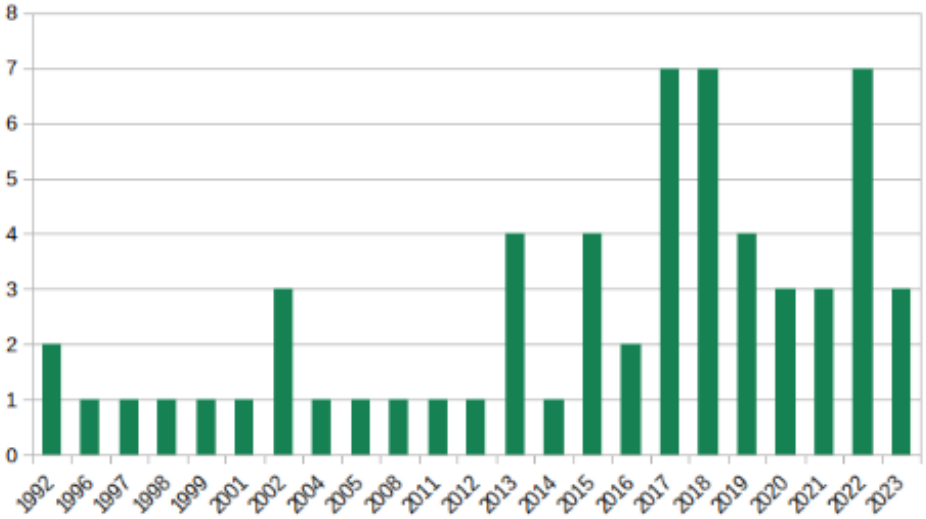
BR 51 2023 000577 0	10/03/2023	Controle de Acesso Externo - 2023	Controle de acesso (genérico ou não especificado)
BR 51 2022 002668 6	23/09/2022	Controle de Acesso Inteligente CTI	Controle de acesso (genérico ou não especificado)
BR 51 2022 002411 0	31/08/2022	SICAAM - Sistema de Controle de Acesso Armamento e Munições	Controle de acesso a armamento e munições
BR 51 2022 000605 7	20/03/2022	Tellus - Sistema de Gestão de Equipamentos e Controle de Acesso	Controle de acesso (genérico ou não especificado)
BR 51 2022 000404 6	22/02/2022	faceum-backoffice (1.5.0-3) DT FACEUM Controle de Ponto e de Acesso por Reconhecimento Facial	Controle de acesso e ponto
BR 51 2022 000403 8	22/02/2022	faceum-web (2.3.0-2) DT FACEUM - Controle de Ponto e de Acesso por Reconhecimento Facial	Controle de acesso e ponto
BR 51 2022 000402 0	22/02/2022	faceum-api (2.3.0-2) DT FACEUM - Controle de Ponto e de Acesso por Reconhecimento Facial	Controle de acesso e ponto
BR 51 2022 000393 7	22/02/2022	faceum-app (2.3.0-9) DT FACEUM - Controle de Ponto e de Acesso por Reconhecimento Facial	Controle de acesso e ponto
BR 51 2021 002608 0	09/11/2021	Otimização Do Sistema IoT de Controle de Acesso ao Laboratório de Desenvolvimento Tecnológico da Unc - Unidade de Marcílio Dias	Controle de acesso a laboratório
BR 51 2021 000224 5	12/02/2021	Gestão *mobile* de processamento de projetos: Sistema de controle de pessoal e atividades com acesso remoto e gerenciamento de equipes	Controle de acesso remoto/online para gerenciamento de equipes
BR 51 2021 000030 7	12/01/2021	Sistema de Controle de Acesso para Equipamentos Industriais baseado em Reconhecimento Facial com Aprendizado de Máquina	Controle de acesso a equipamentos industriais
BR 51 2020 002031 3	29/09/2020	Controle de acesso temporário de Pedestre por QR-Code utilizando Visão Computacional	Controle de acesso de pedestre
BR 51 2020 001636 7	13/08/2020	Sistema de Controle de Acesso por Biometria (Impressão Digital)	Controle de acesso (genérico/não especificado)
BR 51 2020	22/04/2020	iiPedágio - Sistema de Gestão de Cobrança	Controle de acesso

000728 7		e Controle de Acesso a Praça de Pedágio	a praça de pedágio

Fonte: Elaborado pelos autores.

A fim de estabelecer uma análise temporal dos registros encontrados, a Figura 3 apresenta um histograma organizando o número de registros de programas de computador realizados por ano. Pode-se observar uma curva acentuada nos anos 2017 e 2018, decrescendo, em seguida, nos anos 2019, 2020 e 2021. Em 2022, novamente, houve um crescimento. Entretanto, ao se analisar, cuidadosamente, os registros deste ano, nota-se que esse pico em 2022 se dá por ter havido vários registros, em separado, de módulos/subsistemas de uma mesma solução (a DT FACEUM), como pode ser observado no Quadro 1. No ano de 2023, tendo a busca sido realizada ao final do primeiro semestre, acredita-se que possa haver ainda um crescimento atingindo patamares acima dos registrados nos anos de 2019, 2020 e 2021.

Figura 3 - Histograma com registros de programas de computador no INPI.



Fonte: Elaborado pelos autores.

Considerando o conjunto de registros de programa de computador obtidos e as informações disponibilizadas nas páginas do INPI, pode-se identificar, pelo menos, 5 (cinco) soluções que, explicitamente, manifestaram usar biometria na solução de controle de acesso. Tais soluções são BR 51 2020 001636 7, BR 51 2014 001173 9, BR 51 2021 000030 7, BR 51 2018 001145 4 e a solução composta pelos registros BR 51 2022 000404 6, BR 51 2022 000403 8, BR 51 2022 000402 0 e BR 51 2022 000393 7. É neste contexto que este trabalho se insere e busca contribuir na construção de novas soluções de controle de acesso via biometria. É importante destacar que o registro do programa de computador do TagBiometrick será solicitado ao INPI, garantindo segurança jurídica para a criação.

RESULTADOS: O SISTEMA TAGBIOMETRICK

Esta seção apresenta o protótipo do sistema TagBiometrick. Ademais, também é descrito nesta seção o projeto e a implementação de uma proposta para autenticação e liberação para estudantes do ensino infantil.

Arquitetura de alto nível

O TagBiometrick, ilustrado na Figura 4, foi idealizado como sistema de autenticação e liberação dos estudantes do ensino infantil, sua infraestrutura é prototipada por: (A) Leitor biométrico, (B) Software desenvolvido na linguagem C# para leitura da digital, (C) Protocolo MQTT Mosquitto Broker, (D) Banco de Dados Microsoft SQL Server Express, (E) Telas para inserção dos dados dos responsáveis pelos discentes no Sistema (Front-End), (F) Raspberry PI 3 Model B, (G) Leitor RFID e (H) Monitor para apresentar saída das informações para o funcionário da escola.

Figura 4 - Visão geral do sistema proposto.

Fonte: Elaborado pelos autores.

Ainda na Figura 4, é possível obter uma visão geral do protótipo, as conexões entre os componentes físicos (hardware) e o aplicações (software), indicado pelas setas na cor vermelha e azul, ademais, é ilustrada a comunicação entre as aplicações via protocolo MQTT, representando a troca de dados entre os componentes (C). O TagBiometrick utiliza 2 (dois) elementos de leitura, sendo um leitor RFID para o cartão de identificação, representado na legenda (G) e o outro o leitor biométrico para captura da digital dos pais/responsáveis (A). Todo processamento para leitura de dados do cartão de identificação via RFID é realizado no Raspberry Pi (F). O Quadro 3 apresenta uma breve descrição das tecnologias utilizadas no desenvolvimento do sistema.

Quadro 3 - Descrição complementar das tecnologias utilizadas no TagBiometrick.

Tecnologias	Descrição/Justificativa
MQTT Mosquitto Broker	O protocolo MQTT (*Message Queuing Telemetry Transport*), desenvolvido pela IBM no final dos anos 90, é um protocolo de rede baseado em TCP/IP (CORRÊA et al. 2016 e SONI, 2017). Este protocolo permite transportar informações de maneira leve e flexível, ideal para aplicações da Internet das Coisas - IoT (LIGHT, 2017). Optou-se por utilizar este protocolo, devido à sua flexibilidade para se adaptar a diversos tipos de ambientes, incluindo dispositivos restritos, que são aqueles com recursos como CPU, memória e potência limitados.
Banco de Dados Microsoft SQL Server Express	É um SGBD (Sistema de Gerenciamento de Banco de Dados) que utiliza a linguagem SQL e suporta uma ampla variedade de processamento de transações e operações, *business intelligence* e aplicações analíticas em ambientes corporativos (MICROSOFT BRASIL, 2012). Utilizou-se o SQL Server Express por se tratar de uma edição gratuita de sistema de gerenciamento de banco de dados avançado, além disso é confiável e fornece um repositório de dados para sites leves e aplicativos para área de trabalho.
Linguagem C#	A linguagem de programação C#, foi desenvolvida no início de 1999, para ser a nova linguagem para a plataforma .NET (INFOESCOLA, 2022). O C# foi selecionado por ser uma ferramenta essencialmente imperativa, que utiliza o paradigma de orientação a objetos, tornando a uma linguagem dinâmica, de fácil implementação e segura.
Linguagem Python	Criada no início da década de 1990 com foco em produtividade e legibilidade. A linguagem possui ampla versatilidade, atendendo aplicações na área comercial ou em áreas mais específicas como desenvolvimento científico e em aplicações mobile (SOUZA SILVA, 2019). Optou-se pelo Python por ser uma linguagem de alto nível, modular, dinâmica, multiplataforma e orientada a objetos.

Fonte: Elaborado pelos autores.

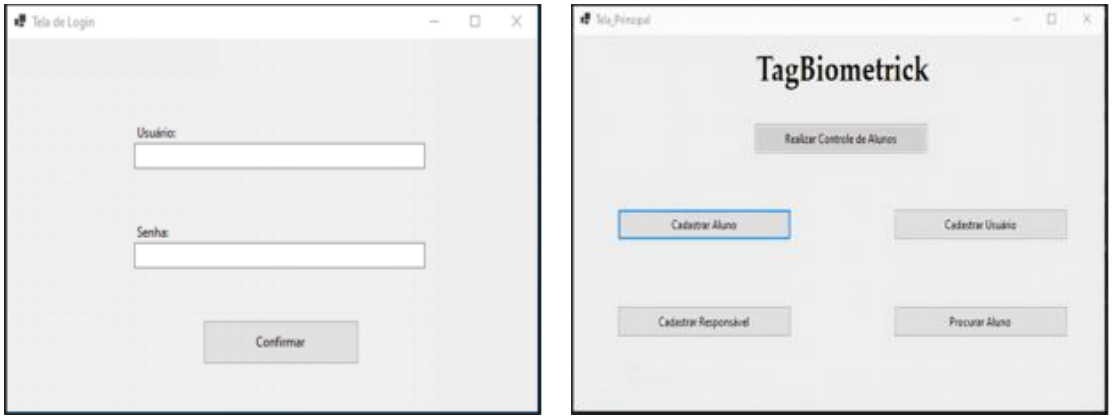
A linguagem de programação C#, que faz interação com o bancos de dados (D), ademais, é utilizada para integração dos módulos de *software* no TagBiometrick. A inserção dos dados pelo usuário no TagBiometrick é representada pelo monitor (E). Para visualização dos resultados da consulta dos estudantes e pais/responsáveis é utilizado o monitor (H).

Descrição das funcionalidades

O TagBiometrick foi idealizado com o objetivo de ser uma ferramenta de apoio para a equipe escolar no horário de saída. Assim, foram implementadas funcionalidades administrativas para o cadastro, alteração e exclusão de pais/responsáveis, além das funcionalidades de controle de acesso, que integram a dupla camada de autenticação (biometria digital e cartão de identificação). A seguir são descritas as funcionalidades do sistema por meio da apresentação das telas.

Para ter acesso ao TagBiometrick, conforme a Figura 5(a), o usuário precisa informar as credenciais de login (nome de usuário e senha). A partir do acesso correto, os usuários terão acesso às funcionalidades, como: cadastro dos alunos(as), usuários, pais/responsáveis, controle de acesso e busca por nome do aluno(a), como ilustrado na Figura 5(b).

Figura 5 - Tela de *login* (a) e tela principal (b).

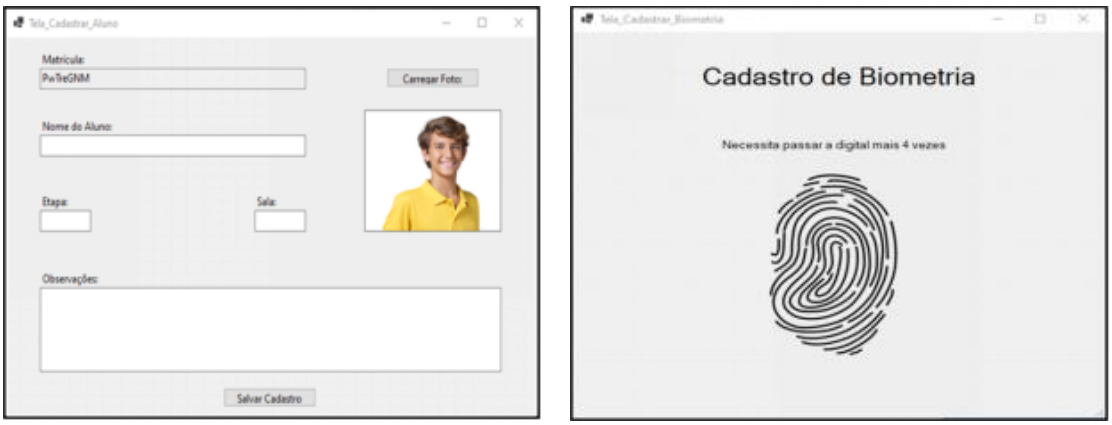


(a) **(b)**

Fonte: Elaborado pelos autores.

A Figura 6(a) apresenta a tela de Cadastro dos Alunos(as). Nesta tela o usuário informa: matrícula; nome completo do aluno(a) e responsáveis; foto para identificação visual; série/etapa; e número da sala de aula. Ademais, está disponível nesta tela um campo para inserção das observações particularidade do(a) aluno(a). A Figura 6(b) ilustra a tela para Cadastro da Biometria. Por questões de segurança são cadastradas no mínimo duas digitais por responsável.

Figura 6 - Tela de cadastro dos discentes (a) e Tela para cadastro da biometria (b).

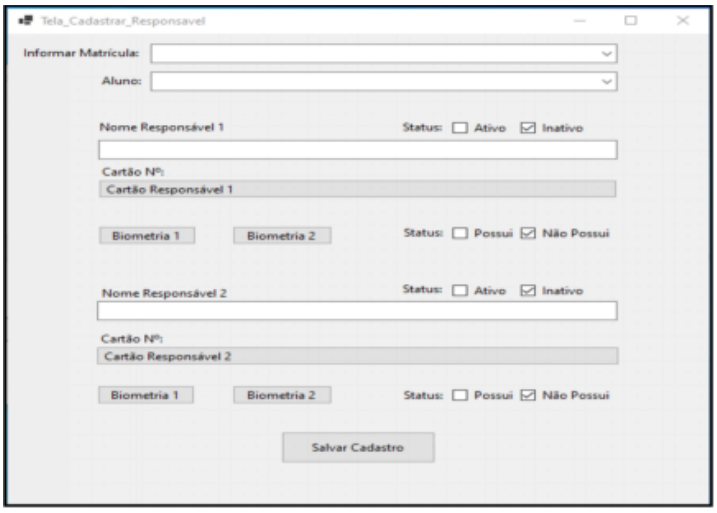


(a) **(b)**

Fonte: Elaborado pelos autores.

A Figura 7 apresenta a tela de Cadastro dos pais/responsáveis. Nesta tela é realizada a associação entre o aluno(a) com os pais/responsáveis, para isso o usuário do sistema deve informar o nome, o código da tag RFID e a biometria. Ademais, também é necessário habilitar o responsável como "Ativo" no sistema. Em algumas situações, em decorrência da síndrome de Nagali (MELDAU, 2009) o responsável não possui digital, portanto, nesta etapa o usuário deverá informar no registro, desabilitando a coleta das digitais do responsável.

Figura 7 - Tela para cadastro dos pais e responsáveis.

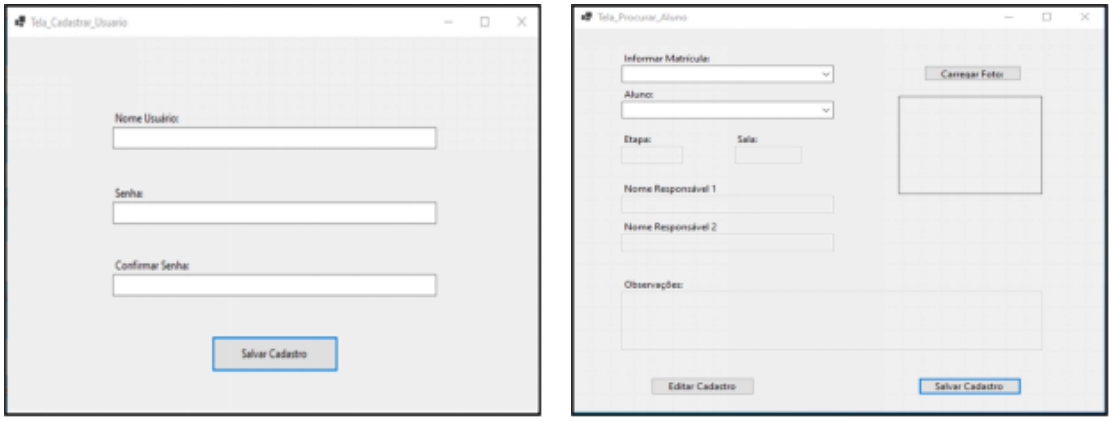


Fonte: Elaborado pelos autores.

A Figura 8(a) apresenta a tela para Cadastro dos Usuários. Por questões de simplificação no desenvolvimento do sistema, optou-se por não implementar um controle de funcionalidades por usuário, deste modo, todos os usuários possuem o mesmo acesso no sistema, sendo necessário apenas informar usuário e a respectiva senha.

Na Figura 8(b) é apresentada a tela de Procura do Aluno(a). Nesta tela o usuário informa o número de matrícula ou o nome do aluno(a), o sistema busca informações no banco de dados e apresenta o resultado na tela incluindo a foto do aluno(a) com as observações inseridas no registro.

Figura 8 - Tela para cadastro dos usuários (a) e Tela para consulta dos alunos (b).



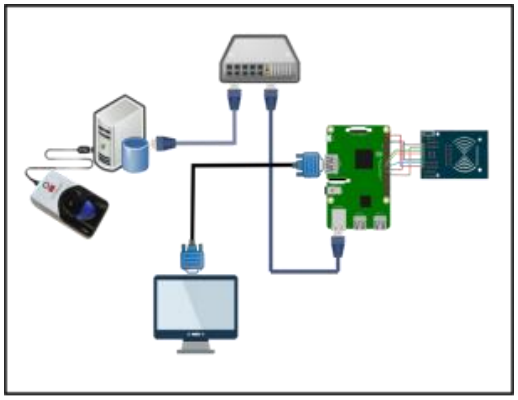
(a) **(b)**

Fonte: Elaborado pelos autores

Componente físicos do sistema

Na Figura 9 é apresentado o modelo esquemático de conexão entre os dispositivos (hardware) no TagBiometrick. O leitor RFID é conectado diretamente com o Raspberry via jumpers flexíveis, o leitor biométrico é conectado no servidor de aplicação. Para comunicação entre o Raspberry e o servidor de aplicação é utilizado um comutador Ethernet com 08 (oito) portas via cabo para transmissão de dados.

Figura 9 - Modelo esquemático de conexão.

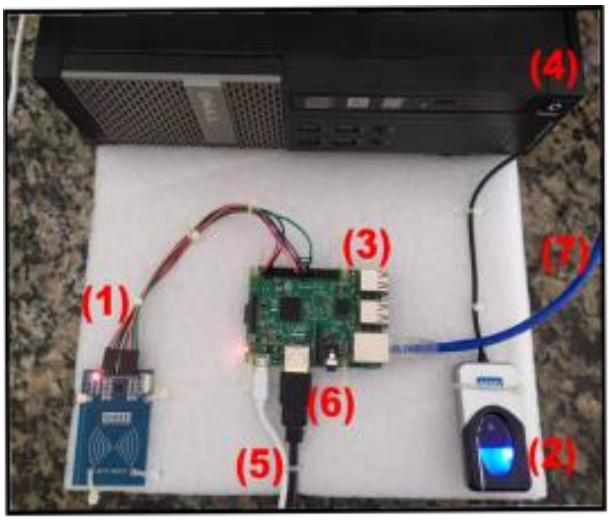


Fonte: Elaborado pelos autores.

Na Figura 10 são ilustrados todos os componentes utilizados no protótipo do sistema: (1) Leitor RFID para leitura do cartão de identificação; (2) Leitor biométrico; (3) Raspberry PI 3; (4) Servidor de aplicação, onde o sistema TagBiometrick encontra-se instalado; (5) Alimentação DC

5v; (6) Cabo para vídeo HDMI; e (7) cabo para transmissão de dados MultiLan categoria 5e sem blindagem.

Figura 10 - Visão geral dos dispositivos físicos utilizados no protótipo computacional.



Fonte: Elaborado pelos autores.

O módulo de leitura de radiofrequência utilizado para a leitura dos cartões de identificação foi o MFRC522 com frequência de operação em 13.56 Mhz. Para cadastro e leitura da biometria foi utilizado o leitor biométrico Digital Persona 4500 Fingerprint Reader (HID), conforme ilustrado na Figura 10. Este equipamento tem alto nível de durabilidade e confiabilidade, contendo um revestimento de silicone que permite ler uma grande variedade de impressões digitais com precisão e rapidez, independente do ângulo de posicionamento. O gabinete metálico de alta qualidade resiste a movimentos não intencionais, ademais, a relação custo x benefício é razoável.

O mini-computador utilizado foi o Raspberry PI 3 Modelo B, com processador Broadcom BCM2837 64bit ARMv8 Cortex-A53 Quad-Core Clock 1.2 GHz, com memória RAM: 1GB, adaptador Wifi 802.11n integrado, Bluetooth 4.1 BLE integrado, conector de vídeo HDMI, com 4 portas USB 2.0, conector Ethernet, *slot* para cartão micro SD, conector de áudio, vídeo e GPIO de 40 pinos (vide Figura 10).

VALIDAÇÃO EXPERIMENTAL

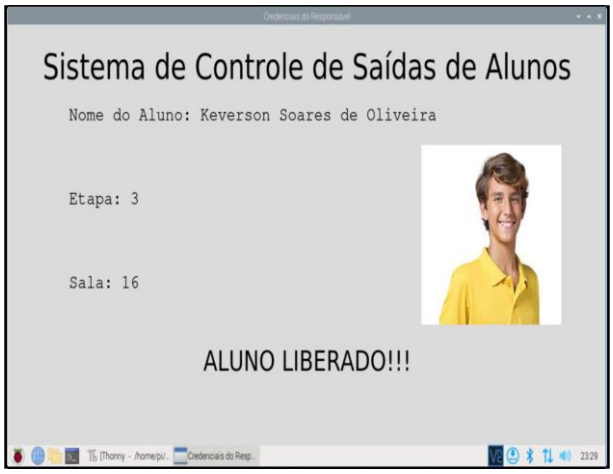
Para realizar a validação experimental do TagBiometrick foi necessário inserir os dados relacionados ao usuário de *login*, inserção de cadastro das IDs TAGs, cadastro de biometria, cadastro de alunos(as) e seus respectivos pais/responsáveis. Todo processo foi realizado no

servidor de aplicações. Nesta etapa foram considerados 03 (três) cenários, estes foram selecionados de acordo com as prioridades descritas pelos colaboradores de uma escola municipal.

Cenário 1: RFID e biometria cadastrados

Neste cenário a tag e a biometria dos respectivos responsáveis estão cadastradas no TagBiometrick. Assim, o sistema informa através do monitor, conectado ao Raspberry a seguinte mensagem: “ALUNO LIBERADO”, ademais, são apresentados os dados cadastrais como o nome do(a) aluno(a), série/etapa, número da sala, foto e observações. Na Figura 11 é apresentada a tela visualizada pelo funcionário da escola. O processo de liberação dos(as) alunos(as) inicia-se com a leitura da tag RFID e a biometria do responsável pelo aluno(a) no sistema.

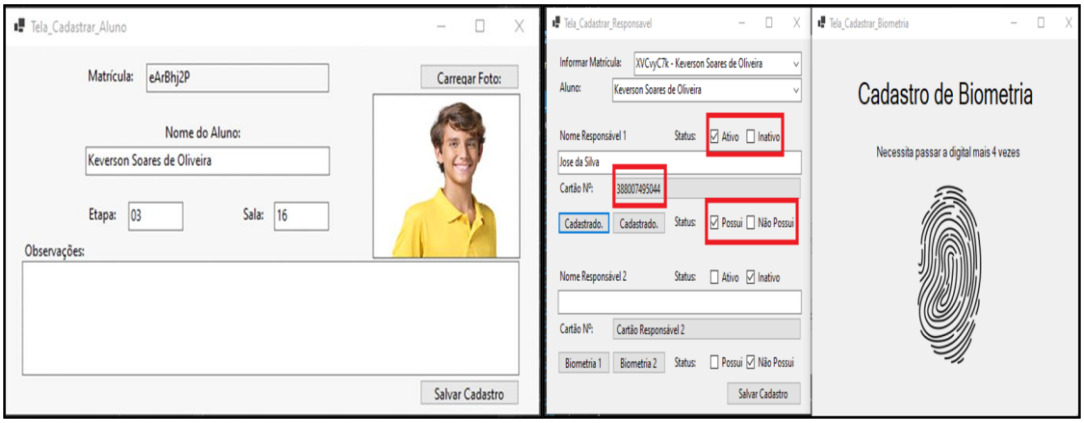
Figura 11 - Tela de liberação do estudante via TagBiometrick.



Fonte: Elaborado pelos autores.

Na Figura 12(a) é apresentada as informações cadastradas no sistema sobre o estudante. Na Figura 12(b) são ilustrados os parâmetros do cadastro dos responsáveis, em destaque, o status “ativo”, o código da tag e a biometria ativada, indicando que possui cadastro da digital no TagBiometrick. Por questões de privacidade, os dados e imagens são meramente ilustrativos.

Figura 12 - Tela de cadastro do estudante (a) e Tela com os parâmetros do responsável.



(a) **(b)**

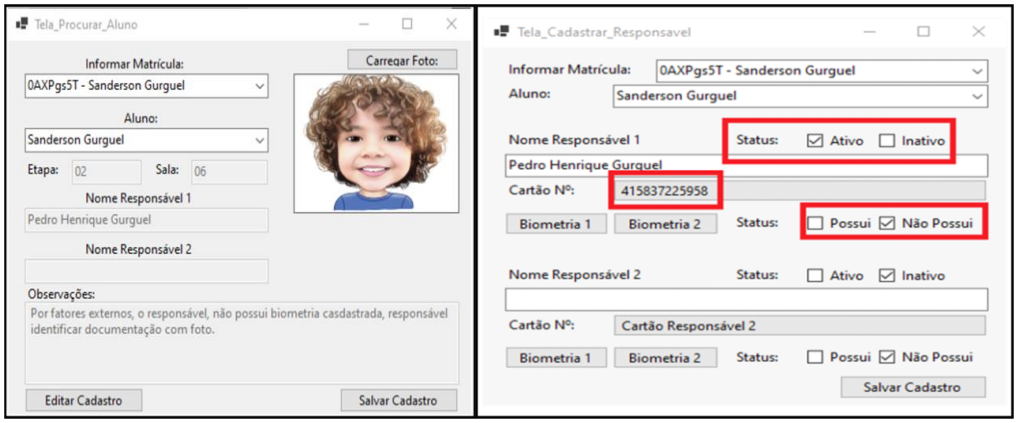
Fonte: Elaborado pelos autores.

Cenário 2: RFID cadastrado e biometria não cadastrada

Para o cenário 2 foi considerado a seguinte situação: o responsável não possui digital, deste modo, o sistema deverá permitir que o responsável utilize apenas o cartão RFID para identificação do responsável, neste caso não será possível cadastrar a biometria dos pais/responsáveis.

Na Figura 13(a) são apresentadas as informações sobre o estudante cadastrado no sistema. Ainda nesta tela é possível notar, no campo observação, sobre a impossibilidade de cadastro da digital dos pais/responsáveis. Na Figura 13(b) são ilustrados os atributos cadastrados dos pais/responsáveis, em destaque, o status "ativo", o código da tag do cartão de identificação RFID e a biometria selecionando o campo "Não possui", indicando que o responsável não terá o cadastro da digital no TagBiometrick.

Figura 13 - Tela de cadastro do estudante (a) e Tela com os parâmetros do responsável (b).

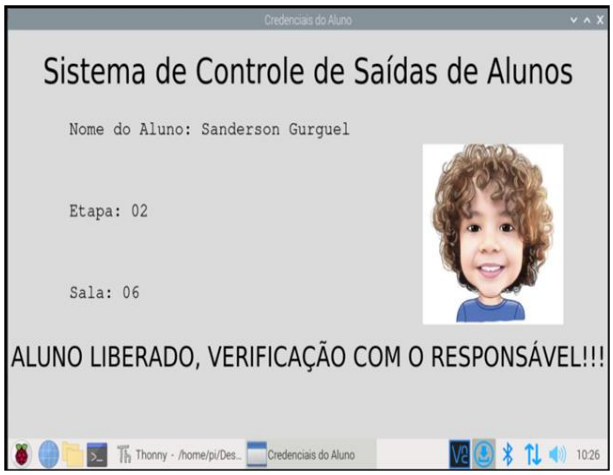


(a) **(b)**

Fonte: Elaborado pelos autores.

O processo de liberação do estudante inicia-se normalmente, com a leitura da tag RFID, como o responsável não possui a biometria cadastrada no TagBiometrick a liberação só será permitida quando o responsável apresentar uma documentação com foto para sua identificação, encerrando assim o processo de liberação do estudante, conforme ilustrada na Figura 14.

Figura 14 - Tela com o status de liberação do estudante sem biometria cadastrada.

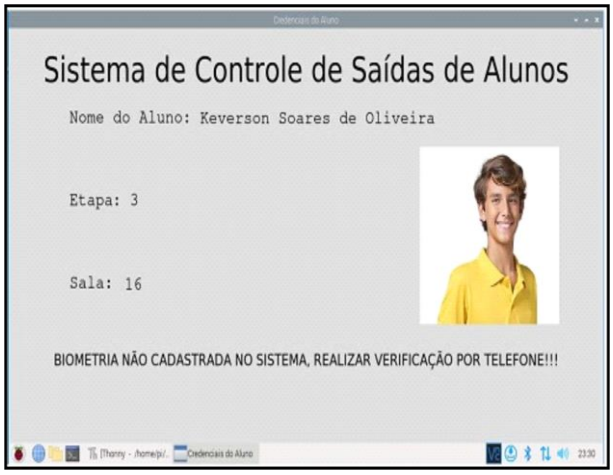


Fonte: Elaborado pelos autores.

Cenário 3: RFID em posse de terceiros

Neste terceiro cenário temos os mesmos requisitos do Cenário 1, ou seja, tag e biometria cadastrados, todavia, o cartão de identificação RFID está de posse de uma outra pessoa. Esta pessoa pode ser algum familiar como: irmã, tio, avô, avó ou até mesmo um desconhecido. Deste modo, quando a pessoa tentar retirar a criança da escola, ele deverá aproximar o cartão RFID, em seguida, o TagBiometrick solicitará a verificação da biometria. Como a digital não está cadastrada para aquele estudante, o sistema apresentará uma mensagem de alerta, ilustrada na Figura 15, orientando o funcionário da escola para não liberar o estudante e que uma ligação telefônica deve ser realizada para os pais/responsáveis. Após o contato com os responsáveis e respectiva autorização, o estudante será liberado e o processo encerrado.

Figura 15 - Tela orientando o funcionário para realizar contato com o responsável.



Fonte: Elaborado pelos autores.

Os cenários apresentados não esgotam todas as possíveis situações, todavia, evidenciam o uso do TagBiometrick no apoio à equipe escolar.

CONCLUSÃO E TRABALHOS FUTUROS

Neste trabalho foi apresentado o sistema TagBiometrick: um arcabouço composto por programas de computador e dispositivos de baixo custo (de biometria digital e tecnologia RFID) utilizado no controle da saída de estudantes em unidades escolares do Ensino Infantil.

No processo de análise e levantamento dos requisitos, foram consideradas as seguintes atividades: (i) reunião com alguns membros setor pedagógico e colaboradores de uma unidade municipal de ensino infantil, (ii) leitura de artigos científicos, material de apoio e busca por registros de programas de computador no INPI, (iii) estudos preliminares de utilização de leitores RFID e leitores biométricos digitais; (iv) projeto e desenvolvimento de um protótipo utilizando plataforma Raspberry PI, v) implementação de um sistema em linguagem de programação C#, e (vi) validação experimental em uma bancada de laboratório.

Os resultados obtidos demonstram que é possível melhorar o nível de segurança por meio do uso do sistema proposto. Ademais, foi possível observar que o TagBiometrick pode atuar como uma ferramenta de desenvolvimento institucional, apoiando o treinamento dos profissionais que atuam em unidades de ensino infantil. A inserção de um procedimento operacional padrão (POP) alinhado ao uso do sistema poderia reduzir a sobrecarga da equipe: na ausência de um colaborador responsável pela tarefa de liberação dos estudantes no horário de saída escolar, outro funcionário treinado poderia exercer tal função a partir das rotinas implementadas pelo sistema, reduzindo assim os riscos de eventuais falhas.

Como maior desafio no desenvolvimento da solução, pode-se destacar a fase de implementação do sistema, que se deu pelo desenvolvimento e integração dos programas de

computador e pela dificuldade de integrar diferentes bibliotecas de software com os diversos dispositivos físicos (*hardware*) utilizados no TagBiometrick.

Como trabalhos futuros, espera-se realizar mais experimentos com a solução proposta, colocando-a disponível em um cenário real. A curto prazo, planeja-se colocar o sistema, sob supervisão, para funcionar em, pelo menos, duas unidades escolares municipais. A médio prazo, planeja-se desenvolver um aplicativo *mobile* (APP) para que pais e responsáveis possam realizar, de maneira *online*, a liberação do estudante nos horários de saída escolar.

REFERÊNCIAS

ABE, R. C. **Dispositivos Biométricos com Comunicação USB**. São Paulo. Faculdade de Engenharia de Sorocaba, 2005.

AQUINO, E. D. N. **Sistemas automáticos de impressões digitais integrando Java e Arduino**. Pernambuco: Editora Principia, 2014.

CORREA, R. P. S.; CUNHA, M. J.; ALMEIDA, M. B.; MORAES, J. S. **Simulação de aplicações utilizando o protocolo de comunicação MQTT com aplicações em ambientes industriais**. In: CONFERÊNCIA DE ESTUDOS EM ENERGIA ELÉTRICA, 14, 2016, Uberlândia. Uberlândia: Universidade Federal de Uberlândia - UFU, 2016. Disponível em: <https://www.peteletricaufu.com/static/ceel/doc/artigos/artigos2016/ceel2016_artigo108_r01.pdf> Acesso em 14/06/2022.

COSTA, Silvia Maria Farani. **Classificação e Verificação de impressões digital**. 2001. Dissertação de Mestrado em Engenharia Elétrica – Escola Politécnica da Universidade de São Paulo, São Paulo, 2001. Disponível em: . Acesso em: 20/07/2022.

GAREN, Automação. **Leitores Biométricos**, 2020. Disponível em: <https://garen.com.br> Acesso em: 20/07/2022.

INFOESCOLA – **Navegando e Aprendendo. Linguagem de Programação C#**. Disponível em: <https://www.infoescola.com/informatica/c-sharp/> Acesso em 01/07/2022.
LIGHT, Roger A. et al. Mosquitto: server and client implementation of the MQTT protocol. **J. Open Source Software**, v. 2, n. 13, p. 265, 2017.

MANENTE, Luis Otávio; CRESPO, Pedro Moreno. **Desenvolvimento de um sistema de controle de acesso com armazenamento de dados em nuvem**. TCC - UTFPR, Ponta Grossa, 2019. Disponível em 22 v.6 n.1 2022 . Acesso em 01/07/2022.

MARCONDES, José S. **Biometria, Sistema Biométrico: O que é, Como Funciona?** Disponível em: <https://gestaodesegurancaprivada.com.br/biometria-sistema-biometrico-o-que-e-como-funciona> Acesso em 01/06/2022.

MELDAU, Débora Carvalho. **Site InfoEscola - Síndrome de Nagali**. Disponível em: <https://www.infoescola.com/doencas/sindrome-de-nagali/> 2022. Acesso em 15/07/2022.

MICROSOFT, Microsoft®. **SQL Server® 2019 Express**. Disponível em <https://www.microsoft.com/pt-br/download/details.aspx?id=101064> Acesso em 09/07/2022.
PINHEIRO, J. M. **Biometria nos Sistemas Computacionais Você é a Senha**. 1. ed. Rio de Janeiro: Ciência Moderna, 2008.

RESENDE, Pedro Antonio de Dourado. **Por que biometria, e para quê?** Entrevista a Carlos Antônio de Oliveira, Para publicação no Jornal da Comunidade, Brasília. Universidade de Brasília Fevereiro de 2007. Disponível em: . Acesso em: 20/07/2022.

ROVEDA, Ugo. **O que é Python, para que serve e por que aprender?** Kenzie Academy, 2020. Disponível em: <https://repositorio.ufpe.br/handle/123456789/16367> Acesso em: 26/07/2022.

SANTOS, Alfredo Luiz dos. **Gerenciamento de identidades**. 2007. Rio de Janeiro, Editora Brasport. <https://www.google.com.br/books/edition/Gerenciamento_de_Identidades/ACFU300zVGUC?hl=pt-BR&gbpv=1&dq=leitura+biom%C3%A9trica+digital+e+iris&pg=PA30&printsec=frontcover > Acesso em 13/07/2022.

SONI, Dipa; MAKWANA, Ashwin. **A survey on mqtt: a protocol of internet of things (iot)**. In: International Conference On Telecommunication, Power Analysis And Computing Techniques (ICTPACT-2017). 2017.

THOMAZINI, D.; ALBUQUERQUE, P. Urbano Braga de. **Sensores Industriais**. 9 ed. São Paulo: Érica, 2020.

VIGLIAZZI, Douglas. **Biometria: Medidas de Segurança**. 2. ed. Florianópolis: Visual Books, 2006.

ZAGONEL, Mateus Victorio; MACHADO, Cristian Cleder et al. **Tecnologia RFID: Um estudo de caso para controle de acesso em escolas**. Departamento de Engenharias e Ciência da Computação, URI, Campus Frederico Westphalen - RS, 2017. Disponível em: <http://revistas.fw.uri.br/index.php/recet/article/download/2247/pdf_1> Acesso em 13/07/2022.