Controle de acesso e automação de ambientes com Artificial Intelligence of Things

Robson Pires Borges[1], Ronaldo Pires Borges[1]

[1]Programa de Pós-Graduação em Ciência da Computação - Universidade do Estado do Rio Grande do Norte (UERN)/Universidade Federal Rural do Semi Árido (UFERSA)

{robson.borges, ronaldo.borges}@alunos.ufersa.edu.br

Resumo. *Em muitos casos, o acesso a salas e laboratórios em locais controlados se torna dispendioso devido ao uso de fichas de controle de acesso, chaves e à necessidade de pessoal para abrir e fechar esses ambientes. Este trabalho apresenta uma solução que utiliza dispositivos IoT operando de maneira autônoma, eliminando a necessidade de usuários portarem quaisquer dispositivos de acesso ou acessórios; a presença do usuário no local é suficiente, além de geração de relatórios automatizados. O sistema proposto é composto por quatro componentes principais de IoT como uma solução para o problema. Em sua versão de testes, o sistema mostrou-se eficiente e capaz de atender às necessidades de um controle de acesso autônomo.*

Abstract. *In many cases, access to rooms and laboratories in controlled locations becomes expensive due to the use of access control sheets, keys and the need for personnel to open and close these environments. This work presents a solution that uses IoT devices operating autonomously, eliminating the need for users to carry any access devices or accessories; the presence of the user on site is sufficient, in addition to generating automated reports. The proposed system is composed of four main IoT components as a solution to the problem. In its test version, the system proved to be efficient and capable of meeting the needs of autonomous access control.*

1. Introdução

No mundo moderno em que vivemos o uso de tecnologias e soluções que realizam tarefas de forma automatizada está cada vez mais presente em diversos ambientes, seja ele doméstico ou empresarial. O amplo emprego da Internet abriu espaço para agregar novas fontes de informação: objetos e máquinas também podem ser conectados a essa rede de big data. Nesse contexto, a Internet das Coisas (IoT) está sendo definida como conectar todas as coisas à Internet, incluindo aspectos como conectividade, manipulação de dados e serviços [Alberti et al. 2019].

O surgimento de novas tecnologias para redes de todos os tipos (nomeadamente, redes sem fios) e os avanços em miniaturização e tecnologia de sensores possibilitam a coleta de informação espaço-temporal nos mais diversos domínios, com um nível de detalhe antes impensável [FACELI, K.; LORENA, A.C.; GAMA, J.; AL, E. 2021]

O uso de Inteligência Artificial (IA) já é uma realidade e se encontra presente em diversos sistemas, seja ele software ou hardware. O uso de IA já está presente em soluções para atendimento ao consumidor, veículos, monitoramento de trânsito, segurança pública, em muitos aplicativos para smartphones, desktops e eletrônicos diversos, mostrando que a adoção de tecnologias está cada vez mais presente propiciando maior conforto, praticidade e eficiência.

Com o advento e evolução das tecnologias de comunicação digital, hoje é comum o acesso a redes de ótima qualidade, propiciando cada vez mais a presença da *Internet of Things (IoT)*, ou Internet das Coisas, é um conceito que une diversas áreas, como sistemas embarcados, eletrônica e comunicação, áreas essas que vêm evoluindo rapidamente nos últimos anos [Luís Gustavo Maschietto et al. 2021]. Todo esse progresso leva a um intenso aprimoramento da IoT, intensificando seu uso por parte dos profissionais em diversos âmbitos. Atualmente estão disponíveis no mercado vários modelos de dispositivos prontos que se integram, cujos consumidores apenas realizam a instalação de forma fácil, como por exemplo os assistentes pessoais que permitem controlar dispositivos como lâmpadas, TVs, entre outros equipamentos domésticos através de comandos de voz. Por outro lado, existem algumas necessidades específicas que necessitam de soluções mais personalizadas.

Em se tratando de controle de acesso a ambientes públicos ou privados, é possível utilizar novas tecnologias para gerenciar a utilização e a presença de pessoas autorizadas de maneira mais eficiente, discreta e automatizada. Um exemplo claro disso é o uso de laboratórios em escolas e universidades. Em muitos casos, o controle é feito de forma manual e dispendiosa, com a necessidade de um profissional se deslocar para fechar as portas e verificar se equipamentos e luzes foram desligados após a utilização. Isso pode levar mais tempo e gerar desperdícios, especialmente em instalações de grandes dimensões. A solução proposta neste trabalho busca endereçar essas ineficiências através do uso de tecnologias de reconhecimento facial e dispositivos IoT para automatizar o controle de acesso e a verificação de uso. Aplicando as tecnologias citadas, é proposto um sistema capaz de identificar e permitir a entrada de usuários autorizados, controlar o uso de equipamentos e iluminação, verificar a presença de pessoas e manter um registro de entradas e saídas de forma autônoma.

2. Fundamentação Teórica

Esta fundamentação é baseada em três pilares principais: a identificação de pessoas através do reconhecimento facial, a biblioteca de programação *OpenCV* e o *framework Face Recognition*. Além disso, é importante destacar o algoritmo Classificador em cascata de Viola e Jones, que tem sido amplamente utilizado para detecção de objetos.

2.1. Identificação de pessoas

O reconhecimento facial consiste em identificar e isolar a área referente a face em uma imagem digital, que pode ser realizada com base em vários atributos: formato do rosto ou cabeça, aparência da face, ou a combinação destes [Santos et al. 2021]. O algoritmo rastreia e mapeia os padrões de uma face humana em formatos geométricos e logarítmicos, para então identificar as suas características únicas. Ao processar a imagem o algoritmo gera uma codificação (*encoder*) que pode ser armazenada em um arquivo de texto e tornando computacionalmente viável realizar comparações de forma mais rápida. É por meio da predição que o reconhecimento facial determina a probabilidade de um rosto ser o mesmo que foi apresentado em um documento ou armazenado em uma base de dados.

OpenCV (Open Source Computer Vision) é uma biblioteca de programação, de código aberto e inicialmente desenvolvida pela Intel com o objetivo de tornar a visão computacional mais acessível a desenvolvedores e "*hobbystas*" [Nguyen et al. 2021]. Atualmente possui mais de 500 funções, pode ser utilizada em diversas linguagens de programação (C++, Python, Ruby, Java…) e é usada para diversos tipos de análise em imagens e vídeos, como detecção, tracking e reconhecimento facial, edição de fotos e

vídeos, detecção e análise de textos etc. Na biblioteca OpenCV, existem diversos algoritmos com técnicas diferenciadas de detecção e tratamento de imagens. A figura 1 mostra a classificação e aplicação dos algoritmos de reconhecimento facial utilizados neste trabalho.

2.2. Face Recognition

Face Recognition[1] é um *framework* para a biblioteca *Dlib*, que usa *deep learning* na resolução de problemas. Pode ser usada também integrado a *OpenCV*. O *framework* é especializado em reconhecimento facial e conecta facilmente classes para a linguagem Python e C++, sendo que o modelo tem uma precisão de 99,38% no reconhecimento de faces [Adam Geitgey 2022]. Usando alguns métodos disponíveis no framework é possível analisar imagens, gerar os *face encodings* e fazer as comparações.

2.2.1. Algoritmo Classificador em cascata de Viola e Jones

A detecção de objetos usando classificadores em cascata baseados em recursos de *Haar* é um método eficaz de detecção de objetos proposto por Paul Viola e Michael Jones em seu artigo "Detecção rápida de objetos usando uma cascata impulsionada de recursos simples" em 2001. É uma abordagem baseada em aprendizado de máquina em que uma função cascata é treinada a partir de muitas imagens positivas e negativas. Em seguida, é usado para detectar objetos em outras imagens [Nguyen et al. 2021].

Esse algoritmo passou a ser mais difundido a partir de 2012 devido ao poder computacional mais acessível. Mesmo se tratando de um algoritmo de 2021 é considerado muito eficiente no reconhecimento de rostos e uma imagem, por usar somas e subtrações nos processamentos de imagens tendo baixo custo computacional.

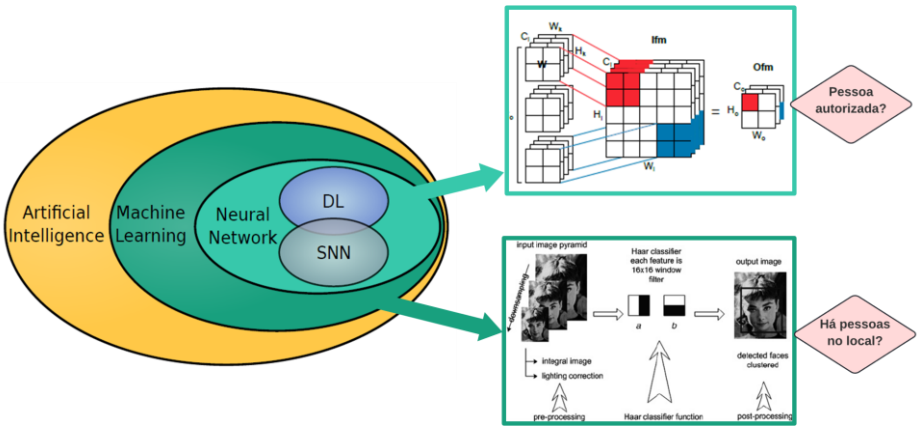

Figura 1. Tecnologias de reconhecimento facial dentro do diagrama de classificalção da IA. *Face Recognition* usa tecnologias de *Deep Leanning* para identificar idivíduos enquanto o Classificador apenas detecta se há pessoas na imagem usando tecnologias de *Machine Leanning*. Fonte: Capra (2020) e OpenCV Documentation.

3. Problema

[1] Disponível em https://pypi.org/project/face-recognition/

Tomando como estudo de caso os Institutos Federais do Piauí (IFPI), em suas mais de 20 unidades distribuídas pelo estado, o controle de acesso às salas de aula e laboratórios é feito por servidores com o apoio dos profissionais de segurança patrimonial dos *campi*. No caso dos laboratórios, somente servidores têm acesso e para isso devem ser registrados nome, horário de entrada e de saída em um livro para cada laboratório, porém é comum que ocorram desencontros e as chaves não voltem para o seu devido local, causando longos deslocamentos na busca delas. De forma semelhante o acesso às demais salas de aula é controlado por um servidor — o assistente de alunos — que, de posse das chaves e controles remotos de condicionadores de ar, visita cada uma das salas abrindo e ligando os aparelhos e fazendo o contrário quando as salas não estão em uso. Ocasionalmente as salas ficam ociosas, abertas e com equipamentos ligados, causando desperdícios.

Casos como esse podem ser simplificados com o uso de tecnologias. A combinação de reconhecimento facial e dispositivos IoT podem otimizar de forma discreta e autônoma o controle de acesso aos ambientes, fazendo a verificação de presença de pessoas nos ambientes e após seu uso realizar o desligamento de diversos equipamentos como ar-condicionado e iluminação, além do fechamento da porta. Consequentemente, um relatório contendo o nome (ou outros dados pertinentes como documento de identificação e matrícula por exemplo) da pessoa responsável que acessou o ambiente, data e horário de entrada e saída podem ser gerados automaticamente pela solução tecnológica.

4. Proposta de Solução

Este trabalho apresenta uma proposta e demonstração prática do uso de dispositivos de AIoT (*Artificial Intelligence of Things*) e algoritmos de reconhecimento facial para solução do problema apresentado em apenas um ambiente, podendo o modelo ser replicado para outros *n* ambientes e integrado a um sistema unificado de monitoramento e controle.

A proposta de solução visa estabelecer um funcionamento autônomo do sistema, eliminando a necessidade de os indivíduos portarem qualquer tipo de dispositivo de acesso ou acessórios, tais como chaves, cartões, tokens, entre outros. Nesse contexto, a autenticação ocorrerá unicamente com base na presença e movimentação dos usuários dentro do ambiente controlado.

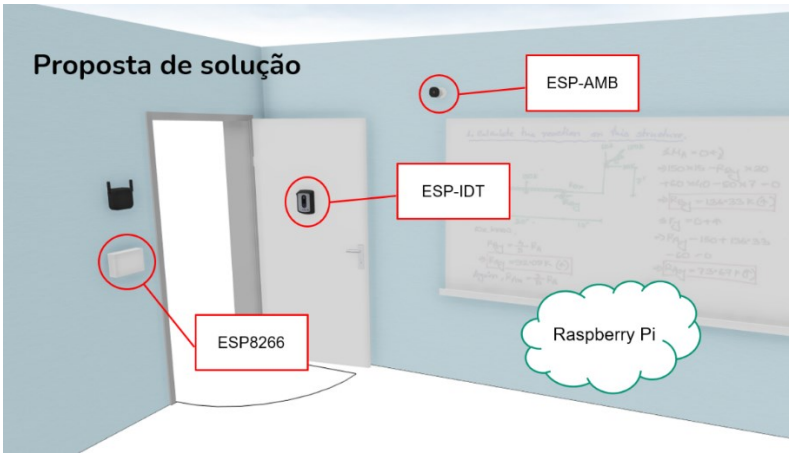

Figura 2. Disposição dos dispositivos AIoT no modelo proposto. Fonte: Autoria própria.

4.1. Hardware

Um fator relevante para escolha dos dispositivos é o consumo elétrico, visto que estes permanecerão ligados de forma contínua durante os turnos de funcionamento do ambiente controlado. Outro fator relevante é o custo financeiro para que a implementação do projeto se torne viável para as mais diversas instituições.

Para a captura das fotografias do responsável pelo acesso e monitoramento do ambiente optou-se pelo uso do AI Thinker ESP32-CAM por possuir câmera integrada, comunicação com redes WiFi e terminais de entrada e saída de propósito geral (GPIO), que possibilitam o acionamento de equipamentos elétricos/eletrônicos. Na Figura 2 é apresentada uma forma de disposição dos dispositivos em um ambiente de aulas.

Para executar os algoritmos de reconhecimento facial e detecção de pessoas, optou-se pelo Raspberry Pi 3 B por possuir poder de processamento suficiente e boa eficiência energética. Considerou-se, também, a possibilidade de expansão do controle para mais de um ambiente, o que levou à exclusão do uso das GPIOs do Raspberry Pi e como forma de garantir a automação do maior número de dispositivos no ambiente, optou-se por usar um NodeMCU ESP8266, que também possui comunicação com redes WiFi e um número maior de GPIOs. Na Figura 3 são apesentados os protótipos dos dispositivos e os seus circuitos.

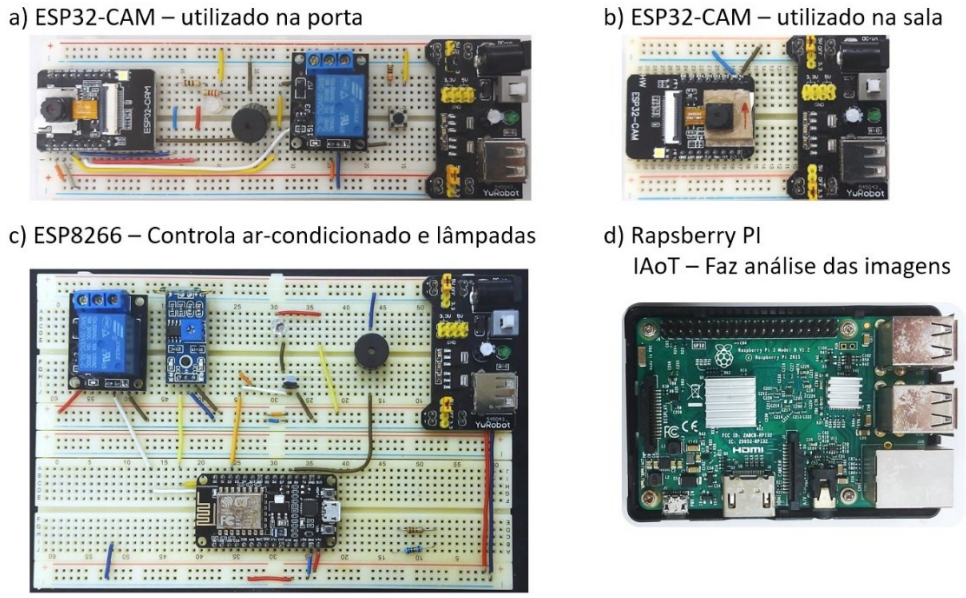

Figura 3. Conjunto de protótipos dos dispositivos IoT e AIoT. Fonte: Autoria própria.

As especificações e consumo elétrico dos dispositivos são listados na Tabela 1.

Tabela 1 Especificações dos componentes de hardware do projeto

Características	AI Thinker ESP32-CAM	Raspberry Pi 3 B	NodeMCU ESP8266

Microcontrolador Processador	Dual core Xtensa® 32-bit 240 MHz	ARM Quad Core 1.2GHz Broadcom BCM2837 64bit CPU	32-bit Tensilica Xtensa 80 MHz
Memória RAM	520 KB interno + PSRAM externo de 8 MB	1GB DDR	64KB
Armazenamento	SPI Flash 4MB	Cartão Micro SD	Flash QSPI 4MB
Conectividade	IEEE 802.11 b/g/n Bluetooth 4.2 BR/EDR e BLE	IEEE 802.11 b/g/n Fast Ethernet Bluetooth 4.1	IEEE 802.11 b/g/n
GPIOs	9 (5 utilizáveis)	28	17
Sistema Operacional	FreeRTOS	Raspberry PI OS (Linux)	FreeRTOS
Programação	Framework Arduino	Python, PHP e C/C++	Framework Arduino
Consumo de pico	310mA@5v (**1.55w/h**)	300mA@5v (**1.5w/h**)	300mA@5v (**1.5w/h**)
Outros	Câmera OV2640 2MP	-	-
Custo médio[2]	de R$ 5,00 a R$ 180,00	U$ 35,00 (site oficial)	de R$ 10,00 a R$ 80,00

4.2. Regras de acesso aos ambientes (salas de aula e/ou laboratórios e uso geral)

Partindo do princípio de que há sempre um responsável pela utilização dos ambientes e para que não seja necessário identificar todos os presentes na sala, apenas o responsável, como por exemplo um professor ou técnico de laboratório, será suficiente para autorizar seu uso. Para isso faz-se necessário um cadastro prévio dos responsáveis autorizados, para que a solução tecnológica consiga identificar o responsável e permitir o acesso.

4.3. Identificação de responsáveis

O cadastro de pessoas autorizadas é feito por um módulo a parte para capturar fotos da pessoa e assim gerar seu face encode para diretório de encodes conhecidos no Raspberry PI. Para o acesso, será usado um dispositivo IoT (ESP32-IDT) localizado na porta de sala, que em conjunto com os outros dispositivos, fará a identificação por reconhecimento

[2] Valores consultados no primeiro semestre de 2022.

facial, liberando ou não o acesso ao ambiente e fazendo o devido registro no arquivo log.html.

O algoritmo de reconhecimento facial usado é o da API para Python *Face-recognition* que usa redes neurais convolucionais (CNNs) e aprendizado profundo no núcleo do seu algoritmo, sendo considerado muito eficiente na identificação facial. Algoritmos que utilizam CNNs são considerados dentro do campo da IA, e sendo na solução executada em um dispositivo de IoT, no caso Raspberry PI. Na Figura 1 é apresentado um diagrama classificando o algoritmo usado dentro do campo da IA como um todo.

O dispositivo a ser localizado na porta possui um botão de solicitação de entrada que quando acionado captura uma fotografia que será enviada ao dispositivo AIoT (Raspberry PI), via HTTP POST para verificar se a pessoa da foto está em sua lista de pessoas autorizadas. Em caso positivo o Raspberry PI enviará por protocolo MQTT os comandos "abrePorta()" para o ESP32-IDT onde um led verde e sinal sonoro sinalizará que o acesso foi autorizado e abrirá a porta. Ainda nesse momento o Raspberry PI envia ao ESP8266 os comandos para acionamento dos equipamentos, no caso, lâmpadas e ar-condicionado ("ligaIlumincao()", "ligaArCondicionado()"). Em caso negativo, um led vermelho e outro sinal sonoro indicarão acesso negado, não liberando a porta, voltando a aguardar solicitação de identificação.

4.4. Verificação de pessoas no ambiente

Em caso positivo para liberação de acesso à sala, será feito o registro com dados de acesso (Data, horário, responsável e status) pelo Raspberry PI, no arquivo log.html e iniciado o monitorado por outro dispositivo IoT (ESP32-CAM-AMB) dentro da sala, que enviará para o Raspberry PI em intervalos programados, fotos da sala para fazer a detecção de pessoas no ambiente.

O algoritmo de análise de imagens para essa situação é o *haarcascade* que faz parte da biblioteca OpenCV para Python. Esse algoritmo é mais apropriado por identificar rostos em imagens de plano aberto com maior rapidez e precisão. Na Figura 1 é apresentado um diagrama que categoriza o algoritmo em discussão dentro do contexto abrangente da IA.

Caso não haja pessoas detectadas nas imagens, o Raspberry PI enviará comandos para o controlador ESP8266 para realizar o desligamento do ar-condicionado e lâmpadas da sala e fará a verificação do fechamento da porta, que se aberta, aguardará um tempo e voltará a verificar presença de pessoas no ambiente e fazendo o registro no log. Quando a porta estiver detectada como fechada será registrado o término de uso da sala pelo responsável com os dados de data e horário no arquivo de log.

O diagrama da Figura 4 representa o fluxo de controle de um ambiente.

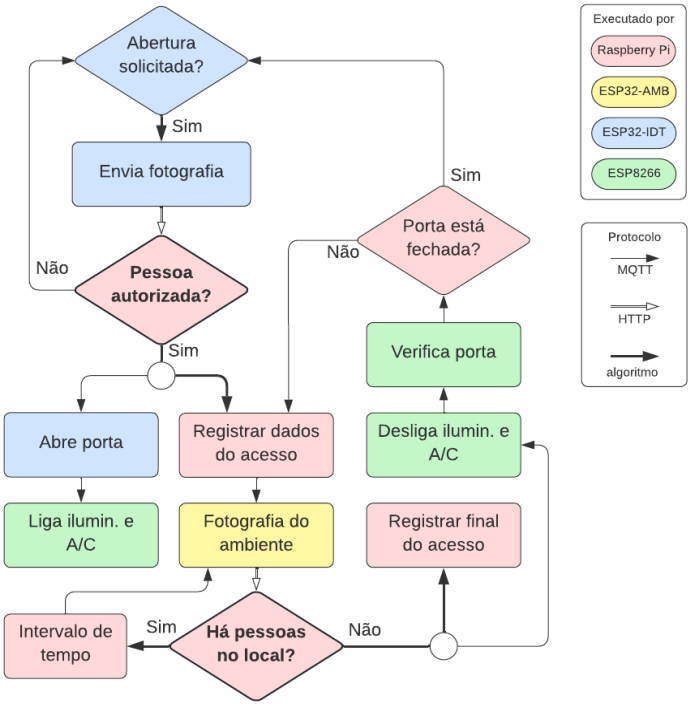

Figura 4. Fluxograma de funcionamento da solução proposta. Fonte: Autoria própria.

5. Considerações

Nesta seção, serão abordados os principais aspectos observados ao longo deste estudo, incluindo problemas identificados e sugestões de melhorias. O desenvolvimento e implementação do sistema trouxeram à tona uma série de considerações relevantes para a eficácia e aprimoramento do projeto.

5.1. Problemas encontrados

Confiabilidade dos dispositivos ESP32 CAM são duvidosos talvez por falta de um controle de qualidade do fabricante ou não garantia de qualidade dos componentes, uma vez que foi observado funcionamento diferente em dispositivos adquiridos de fornecedores diferentes.

O método de detecção de rostos *haarscascades* dentro da OpenCV é impreciso e detecta rostos apenas de forma frontal gerando falsos resultados de ambiente vazio ou o inverso, resultados de ambiente ocupado falsos devido a detecção de rostos em objetos. Sobreo a API *Face-recogniton* para *Dlib*, foram encontradas fragilidades quanto a segurança, pois caso se utilize uma foto de uma pessoa com autorização a IA de reconhecimento não consegue distinguir se é uma foto ou a pessoa na imagem.

Faz-se necessário testes com tipos de lentes diferentes na captura de imagens e testes com outros algoritmos de detecção facial para propósitos diferenciados.

5.2. Sugestões de melhorias

Ampliar testes para validação dos algoritmos de reconhecimento facial e detecção de presença de pessoas além de testar outros algoritmos. Refinamento de mensageria entre os dispositivos por MQTT beneficiando-se do modelo *half-duplex* de comunicação. Criação de aplicação para o cadastro de pessoas autorizadas. Implementar paralelismo nos scripts Python, pois o sistema requer comunicação síncrona e assíncrona entre os

dispositivos. Adicionar banco de dados para modularização da solução e fácil escalabilidade do modelo de dados gerado. Para melhorar a segurança, usar um dispositivo adicional após o reconhecimento facial, como, por exemplo, um PIN a ser informado em um teclado numérico.

6. Referências

Adam Geitgey (2022). Face Recognition Documentation. https://face-recognition.readthedocs.io/en/latest/history.html.

Alberti, A. M., Santos, M. A. S., Souza, R., et al. (2019). Platforms for Smart Environments and Future Internet Design: A Survey. *IEEE Access*, v. 7, p. 165748–165778.

FACELI, K.; LORENA, A.C.; GAMA, J.; AL, E. (2021). *Inteligência Artificial - Uma Abordagem de Aprendizado de Máquina*. Grupo GEN. v. 2ª edição

Luís Gustavo Maschietto, Anderson Luiz Nogueira Vieira, Fernando Esquírio Torres, et al. (2021). *Arquitetura e Infraestrutura de IoT*. 1ª edição ed. Editora: Grupo A. v. 1

Nguyen, L., Cao, T. N. M., Huynh-Anh, L. and Dang-Ngoc, H. (21 dec 2021). An Embedded Machine Learning System For Real-time Face Mask Detection And Human Temperature Measurement. In *2021 8th NAFOSTED Conference on Information and Computer Science (NICS)*. IEEE. https://ieeexplore.ieee.org/document/9701494/, [accessed on Jun 17].

Santos, E. O., Moitinho, L. C. C., De Almeida, W. T. and Benicasa, A. X. (2021). Reconhecimento de Faces e Identificação de Regiões de Interesse em Cenas para o Acompanhamento Baseado na Movimentação de Servomotores e Inteligência Artificial. p. 10.