Sistema de controle de acesso com três fatores de autenticação
Ponto de Controle 1

Mateus Felipe Massa Pereira e Victor Bastos I. Oliveira
Programa de Graduao em Engenharia Eletrnica, Faculdade Gama
Universidade de Braslia
Gama, DF, Brasil
email: mateusmassa7@gmail.com, victorbio101@gmail.com

I. JUSTIFICATIVA

O controle de acesso é definido como a prática de permitir a entrada e saída de um local apenas para pessoas autorizadas. O objetivo dessa prática é garantir a segurança do local o qual terá o acesso controlado, permitindo a entrada apenas dos indivíduos julgados como essenciais. Este tipo de tecnologia tem aplicação em qualquer tipo de local que necessite da filtragem no acesso das pessoas, seja por questões técnicas ou questões de segurança. Tomando como exemplo uma usina termonuclear, onde o acesso a certas partes críticas da planta deve ser estritamente controlado para evitar que pessoal não autorizado, geralmente sem conhecimento técnico e licenciamento, cause algum distúrbio e leve uma catástrofe à acontecer. Outro exemplo advém das aplicações governamentais e militares, onde segredos de Estado, arquivos de alto sigilo e equipamentos devem ser guardados com extrema cautela, com acesso liberado a apenas um seleto grupo de pessoas.

A motivação por trás desta proposta de projeto é realizar o controle eletrônico através de um dispositivo de segurança, mostrando que é possível criar um sistema complexo de autenticação e alerta que garante a eficiente filtragem do acesso de pessoal, a partir da combinação de diversos componentes e técnicas em eletrônica.

II. OBJETIVOS

Fazendo uso de uma placa Raspberry Pi, este projeto consiste no desenvolvimento de um sistema de controle de acesso com três fatores de autenticação, sendo estes a verificação de senha, checagem por RFID e reconhecimento facial por câmera. O sistema visa ser empregado em salas onde o acesso deve ser extremamente restrito, o que é relativamente comum no ramo de empresas laboratoriais, empresas de segurança, òrgãos governamentais de alto escalão e forças armadas, por exemplo.

III. REQUISITOS

O sistema proposto, a partir de uma perspectiva de requisitos, pode ser dividido em quatro partes principais:

- **Autenticação de segurança:** consiste na verificação de três fatores sendo o primeiro a senha fornecida pelo usuário através de um display touchscreen, o segundo a verificação do cartão de acesso pelo sistema RFID e o terceiro o reconhecimento facial do usuário.
- **Monitoramento de entrada:** consiste no recolhimento do horário de entrada e nome do usuário para serem salvos em algum meio, com o intuito de gerar dados de fluxo para monitoramento.
- **Envio de alerta:** consiste no envio de uma mensagem de alerta para o email cadastrado no sistema contendo a hora da falha, qual etapa da autenticação o invasor falhou e uma foto de quem tentou acessar o local.
- **Acionamento elétrico:** consiste no destravamento da tranca magnética e abertura automática da porta através de um motor de passo ou servo motor.

IV. BENEFÍCIOS

O sistema proposto possui alto grau de segurança devido à autenticação por três fatores realizada pelo sistema embarcado. Este tipo de autenticação faz com que a possibilidade de fraude e acesso de pessoas não autorizadas seja incrivelmente difícil, já que a quantidade de passos e os itens necessários para os testes são bem específicos. Ademais, o dispositivo também será capaz de emitir um alerta tanto sonoro quanto por email através da internet, para que as devidas medidas possam ser tomadas quanto à segurana do local, aumentando ainda mais a resiliência do sistema contra invasões físicas.

V. REVISÃO BIBLIOGRÁFICA

Alguns projetos semelhantes foram analisados para embasar o escopo da proposta realizada aqui. Um dos principais projetos analisados utiliza autenticação de dois fatores através de três estágios de verificação, sendo estes um sistema RFID, um número PIN de seis dígitos e um código aleatório de único-acesso enviado como mensagem para o celular [1]. Nota-se que o sistema apesar de ter três estágios de verificação é classificado apenas como tendo dois fatores de autenticação, devido à natureza dos testes realizados em cada estágio [2], diferentemente do sistema proposto.

Outro projeto na mesma área, publicado pela IEEE, propõe uma tranca eletrônica utilizando autenticação de um fator mas através de dois métodos diferentes. O usuário tem a opão de colocar a senha correta ou ter sua face reconhecida pela câmera que está conectada a Raspberry Pi. Se o usuário

não estiver cadastrado no banco de dados do dispositivo, uma foto é tirada do mesmo e mandada para o dono, que irá decidir dar a permissão de acesso ou não para o usuário [3][4].

No projeto Pi Lock, o foco está em uma autenticação de dois fatores através de senha e sistema RFID. Nesse sistema, deve-se validar o primeiro estágio atravs de um cartão magnético para leitura no RFID e em seguida colocar a senha correta para destravar a tranca magnética [5].

Por fim, foram pesquisadas referências no requisito de reconhecimento facial, onde foram encontradas duas principais fontes de informação, ambas com autenticação de apenas um fator. No projeto por Muhammad Aqib [6], o reconhecimento facial foi feito utilizando a câmera dedicada para Raspberry, com código na linguagem Python utilizando a biblioteca OpenCV. Em um artigo publicado pela IJCSN (International Journal of Computer Science and Network), foi feito o design e a implementação de um sistema de tranca utilizando reconhecimento facial para Linux embarcado na Raspberry Pi [7]. Nesse artigo, é proposto o desenvolvimento do dispositivo utilizando os mesmos recursos do projeto anterior, Python com biblioteca OpenCV, mas também é utilizado o classificador Haar Cascade como algoritmo para o reconhecimento de faces.

REFERENCES

[1] SWITCHED ON NETWORK. Build a Raspberry Pi Smart Door Lock Security System for your Smart Home. Disponível em: <https://www.switchedonnetwork.com/2017/11/10/build-the-ultimate-door-security-system-with-three-factor-authentication/>. Acesso em: 30 de Agosto de 2019.

[2] ROUSE, Margaret. Three-factor authentication (3FA). Disponível em: < https://searchsecurity.techtarget.com/definition/three-factor-authentication-3FA>. Acesso em: 30 de Agosto de 2019.

[3] HUSSEIN, Naser. MANSOORI, Inas. Smart Door System for Home Security Using Raspberry pi 3. Disponível em: <https://ieeexplore.ieee.org/abstract/document/8079785>. Acesso em: 30 de Agosto de 2019.

[4] MISHRA, Shwetank. SONI, Vivek. Smart Door System for Home Security Using Raspberry pi 3. Disponível em: < http://ijirt.org/master/publishedpaper/IJIRT146080_PAPER.pdf>. Acesso em: 30 de Agosto de 2019.

[5] BERNASCONI, Paolo. Pi Lock, an RFID solution for Access Control and Management. Disponível em: < http://www.pi-lock.com/>. Acesso em: 30 de Agosto de 2019.

[6] AQIB, Muhammad. How to Create a Facial Recognition Door Lock With Raspberry Pi. Disponível em: < https://maker.pro/raspberry-pi/projects/how-to-create-a-facial-recognition-door-lock-with-raspberry-pi>. Acesso em: 30 de Agosto de 2019.

[7] ROY, Sourav. UDDIN, Nasir, et al. Design and Implementation of the Smart Door Lock System with Face Recognition Method using the Linux Platform Raspberry pi. Disponível em: < http://ijcsn.org/IJCSN-2018/7-6/Design-and-Implementation-of-the-Smart-Door-Lock-System-with-Face-Recognition-Method-using-the-Linux-Platform-Raspberry-Pi.pdf>. Acesso em: 30 de Agosto de 2019.