LetMeIn - Sistema de Controle de Acesso Para Ambientes Educacionais.

Eike D. Santiago[1], Diogo F. Bento[1], Breno J. D. Costa[1]

[1]Coordenação de Informática (CINFO) – Instituto Federal de Alagoas (IFAL)
CEP 57.020-600 – Maceió – AL – Brazil

{eikesantz, diogofb93}@hotmail.com, brenojac@ifal.edu.br

Abstract. *The physical key still traditionally used in many institutions, having disadvantages as: (a) manual key`s access control (using paper and signatues), (b) possible failures of security (can simply create a copy of the key), (c) and other problems. This way, the LetMeIn was designed as an alternative to the use of keys, adapting the traditional door lock to an access control system that uses devices such as Raspberry Pi, Smartphones and a Virtual Private Server, all connected trough a Virtual Private Network (VPN). In addition, was designed a RESTful API to integrate possible external bases, allowing multifactorial authentication modes.*

Resumo. *A chave física ainda é tradicionalmente usada em muitas instituições, possuindo inconvenientes como: (a) o controle das chaves manualmente (usando papéis e assinaturas), (b) possíveis brechas de segurança (pode-se simplesmente copiar a chave), (c) entre outros problemas. Desta forma, o LetMeIn foi concebido como uma alternativa ao uso de chaves, adaptando as fechaduras tradicionais a um sistema de controle de acesso que utiliza dispositivos como o Raspberry Pi, Smartphones e um Servidor Virtual Privado, todos conectados por uma Rede Virtual Privada (VPN). Além disso, foi concebida uma API RESTful para integrar possíveis bases externas, permitindo modos de autenticação multifatoriais.*

1. Introdução

As organizações sempre estão em busca de melhoras quando o assunto é segurança. Para Tonin et al (2015) o uso da automação durante o processo de modernização tem como objetivo gerar um maior bem-estar às pessoas, e a segurança é uma das bases para este bem-estar.

A Internet das Coisas (IOT) tem um grande peso no processo de automação. A aplicação da mesma no âmbito do controle de acesso em ambientes educacionais como salas de aulas, bibliotecas e laboratórios, de acordo com Tonin et al (2015) e Felix (2018) traz maior segurança, flexibilidade e controle dos indivíduos, assegurando os ambientes, informações e bens moveis presentes.

Geralmente o controle de acesso aos ambientes educacionais são por meio da chave física, a qual tem um grande potencial de risco. Em um estudo de Jeong (2016) são citados três destes riscos: ela pode ser facilmente roubada, perdida ou copiada.

Com o intuito de prover uma maior segurança a estes tipos de ambientes, foi proposto um modelo onde as pessoas que necessitem ter acesso aos ambientes, precisem

apenas ter seu smartphone consigo e possuir as credenciais válidas, tendo em vista que eles estão presentes com maioria das pessoas. Coutinho (2015) comenta que é cada vez mais comum a incorporação de práticas mobile ao cotidiano das pessoas, através da utilização das redes sociais ou de qualquer outro aplicativo ou ferramenta existente nestes dispositivos.

2. Metodologia

Durante a construção deste trabalho foi realizado uma revisão sistemática da literatura (RSL). A RSL buscou os dispositivos mais utilizados para o controle de acesso em ambientes educacionais, assim como, suas vantagens e desvantagens. Foi possível observar que os dispositivos mais utilizados são Arduino e Raspberry Pi, pois possuem baixo custo, fácil implementação, ampla comunidade, linguagem de programação de fácil aprendizagem e entradas digitais de fácil acesso. Junto as vantagens, foi possível observar que estes dispositivos são comumente atrelados a outras tecnologias, como fitas RFID, leitores de biometria, smart-cards, entre outros. Nas subseções seguintes será explanado dispositivos e tecnologias utilizadas para a concepção do modelo proposto.

2.1. Raspberry Pi

Na elaboração do modelo, foi decidido o uso do Raspberry Pi. Além das vantagens apontadas na RSL, este dispositivo, por ser um microcomputador, já possui um sistema operacional em si, além de conexão à internet sem necessidade de módulos extras, o que foi um ponto decisivo em sua escolha.

De acordo com a Raspberry Pi Foundation (2015), o Raspberry Pi é um microcomputador, que executa um sistema operacional Linux através de um SD card, semelhante ao usados em câmeras digitais. Seu objetivo é incentivar o uso da programação. O tamanho do Raspberry é de aproximadamente um cartão de crédito, e tem aplicabilidade nas mais diversas áreas.

2.2. NAT

O Network Address Translation (NAT) é uma solução ao compartilhamento de internet por vários endereços de uma rede local através de um único endereço IP roteável na internet ou um pool de endereços. Desta forma, o roteador gateway possui uma tabela mapeando o endereço IP local, porta e endereço requisitado. Assim, ao receber a resposta de requisição, ele pode encaminhar corretamente ao dispositivo que a requisitou (BEZERRA; REDES DE COMPUTADORES, 2008).

2.3. VPN

Devido ao uso de NAT nas redes de computadores atuais, um endereço IP presente na internet não consegue alcançar endereços IP das redes locais. O uso de túnel VPN é uma alternativa para quem necessita realizar requisições da internet a uma rede local, ou entre duas redes locais de forma segura.

A VPN (Virtual Private Network) utiliza a internet no lugar das linhas privadas, que possuem um alto custo financeiro; a segurança é um dos principais pontos de uma VPN. Uma VPN se comunica através de um protocolo de tunelamento, que é o encapsulamento de um protocolo dentro de outro. Os requisitos básicos desejáveis para

aplicação de uma VPN são: autenticação de usuários, gerenciamento de endereço, criptografia de dados, gerenciamento de chaves e suporte a múltiplos protocolos (CHIN, 1998).

3. Modelo Proposto

Com o intuito de trazer uma maior segurança aos ambientes educacionais e como alternativa ao uso da chave física, foi proposto um modelo, sua arquitetura pode ser observada na figura 1, exposta abaixo.

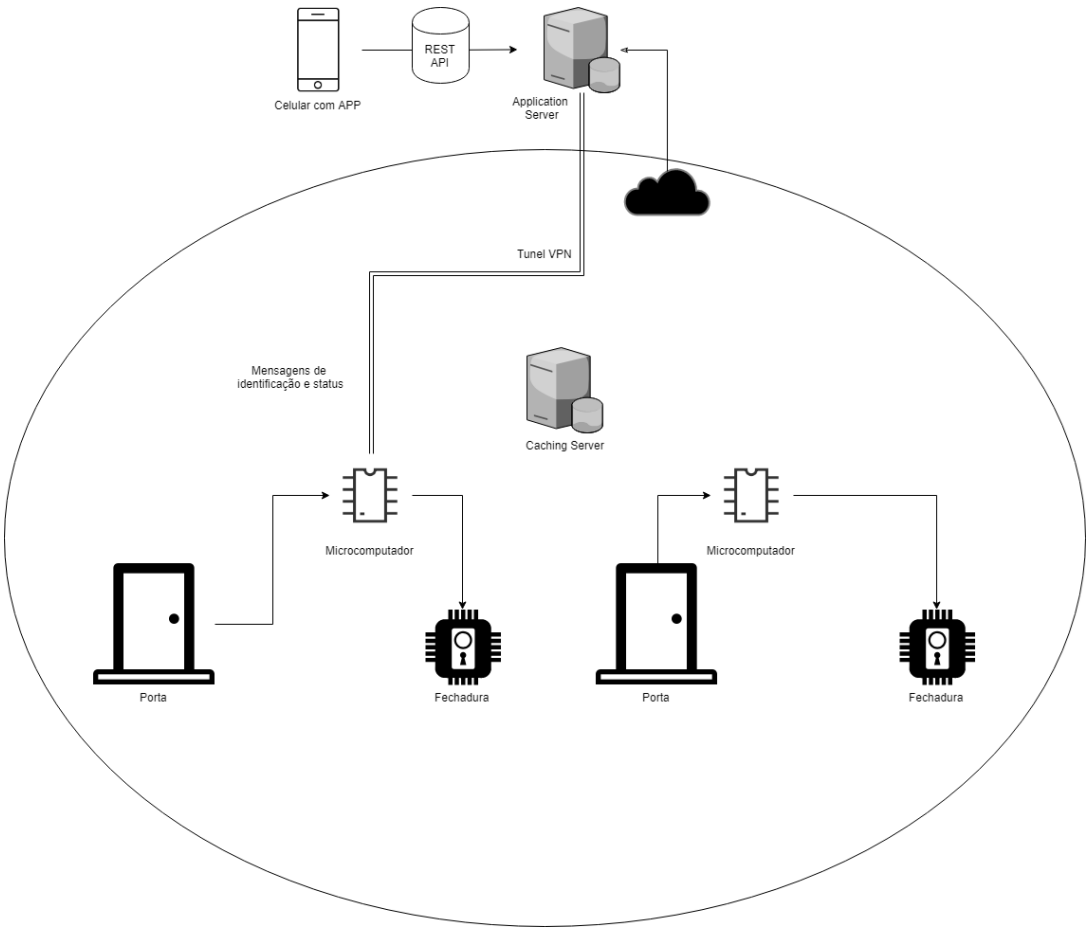

Figura 1. Arquitetura do modelo proposto.

A região delimitada pelo retângulo representa o ambiente educacional, a região sem delimitação seria a internet.

O fluxo para que um agente com credenciais válidas realize o destrancamento da fechadura do ambiente educacional é da seguinte forma:

1) O agente, através de seu smartphone, irá acessar o aplicativo a ser desenvolvido e solicitará a abertura da fechadura de um determinado ambiente.
2) Uma API RESTful se encarregará de validar a solicitação e a encaminhar para o Application Server. O Application server deverá conter as informações dos dispositivos Raspberry Pi conectados a ele através de um túnel VPN.

3) Após a análise da requisição o Application Server irá enviar uma requisição para o Raspberry Pi responsável pela fechadura do ambiente solicitado pelo agente. Como o Application Server necessita enviar uma outra requisição ao Raspberry Pi que se encontra em uma rede local, e sua conexão à internet é por meio de NAT, é necessário o uso de um túnel VPN para garantir a comunicação entre ambos.
4) Ao receber a requisição do Application Server o Raspberry Pi enviará um sinal elétrico para realizar o destravamento da fechadura, e assim, permitir que o agente realize o acesso ao ambiente pretendido.

Além de ser responsável pela liberação das portas o Raspberry Pi também enviará constantes mensagens ao Application Server, informando detalhes sobre si, como sua identificação e status, semelhante a um broadcast, assim alimentando a base de dados do server.

4. Conclusão

Este trabalho buscou apresentar o modelo proposto do LetMeIn, um sistema para controle de acesso aos ambientes educacionais. O sistema conta com a aplicação do Raspberry Pi para controlar as fechaduras dos ambientes. Além disso o usuário irá realizar o processo de solicitação de acesso ao ambiente através de seu smartphone. O modelo faz uso de uma VPN como alternativa de trafego seguro de dados, e para lidar com o problema em que um endereço IP da internet não consegue se comunicar diretamente com um endereço IP de uma rede local devido ao NAT. Esse sistema tem o intuito de ser uma alternativa ao uso de chaves físicas que possuem falhas de segurança.

5. Referências

Bezerra, R. M.; Redes de Computadores, I. I. (2008). A Camada de Rede.

CHIN, L. K. (1998). Rede privada virtual–VPN. Rede Nacional de Ensino e Pesquisa (RNP).

COUTINHO, G. L. (2015). A Era dos Smartphones: Um estudo Exploratório sobre o uso dos Smartphones no Brasil.

FELIX, D. S. A. (2018). Tecnologias para controle de acesso em sistemas de monitoramento em espaços urbanos inteligentes.

JEONG, J. I. (2016). A study on the IoT based smart door lock system. In Information Science and Applications (ICISA) 2016(pp. 1307-1318). Springer, Singapore.

Raspberry Pi Foundation, Raspberry Pi Foundation. Disponível em: <https://www.raspberrypi.org/about/>. Acesso em: 17 mar. 2019

TONIN, F. S.; CITTOLIN, G. F.; SOUZA, V. D. (2015). Desenvolvimento de um sistema web de controle de acesso. (Bachelor's thesis, Universidade Tecnológica Federal do Paraná).