SISTEMA *MOBILE* EMBARCADO PARA CONTROLE DE ACESSO

Gustavo Souza Azevedo, Luciene Cristina Alves Rinaldi
Departamento de Ciências da Computação, Centro Universitário FEI
gu.ve.13@gmail.com, lucienerinaldi@fei.edu.br

Resumo: *Este trabalho apresenta uma solução para controle de acesso de ambientes em tempo real como casas, escritórios, centros comerciais, fábricas (controle de ponto), laboratório de pesquisa (controle de perfil de alunos e professores do laboratório de IoT da VIVO), salas de aula (controle de acesso de alunos), ou qualquer outro ambiente que precise de controle de acesso. Será construído um aplicativo mobile multiplataforma e site web via rede wi-fi para auxiliar no controle e monitoração do ambiente para a redução de custos dos recursos humanos (eliminação da lista de presença).*

1. Introdução

A Internet das Coisas (*Internet of Things* - IoT) é um novo paradigma no cenário de telecomunicações. Este conceito envolve o cruzamento de informações ao redor de ambientes inteligentes internos e externos juntamente com sensores como: ultrassônicos, atuadores, de presença, *RF-ID* entre outros; que são capazes de interagirem uns com os outros para atingirem um objetivo em comum, com o intuito de tornar a vida mais fácil e confortável [1]. Estes dispositivos também irão trazer à tona o que chamamos de computação ubíqua que é a onipresença da informática no cotidiano das pessoas.

Anteriormente, o termo controle de acesso, era associado somente com a segurança física de um ambiente através de métodos mecânicos como trancas e tramelas, porém, com a evolução da computação surgiu muitas preocupações tais como a segurança e a privacidade digital. Para sanar algumas preocupações em nossa instituição, este projeto visa a criação de um dispositivo embarcado de segurança que irá autenticar as pessoas em ambientes como a sala de aula sem a necessidade das mesmas lembrarem-se de senhas, assinarem lista de presença, gastar papel e recursos humanos; pois, irá fornecer alternativas para a proteção do ambiente através da padronização da forma de acesso de alunos e docentes ao ambiente, além de inviabilizar a entrada de pessoas não autorizadas em locais pré-determinados. Este sistema também poderá ser utilizado em estabelecimentos como empresas e em qualquer outro local onde o acesso seja restrito.

2. Metodologia

- Levantamento bibliográfico de informações para montagem do dispositivo embarcado (*hardware*);
- Montagem do dispositivo embarcado;
- Elaboração de relatórios (parcial e final);
- Testes e análise dos resultados;
- Construção do aplicativo para rodar em *smartphone*, computadores, *notebooks* e *tablets* (sistema multiplataforma);
- Escrita da monografia, pôster e resumo para a SICFEI e artigo externo;
- Escrita de um tutorial e vídeo didático para ensinar como foi feito o projeto para a aprendizagem de alunos, além disso, que possa dar continuidade e ser melhorado por outros alunos de pesquisa.

3. Projeto

O cenário deste trabalho visa à automatização do controle da lista de presença de alunos e controle de acesso (perfil) de alunos e professores ao laboratório de IoT (também pode ser usado para controle de acesso/ponto de condomínios, *shoppings* ou qualquer outra empresa) auxiliando no monitoramento em tempo real e na redução dos recursos financeiros e humanos (principalmente em mão de obra de pessoas com relação a tempo, erro humano e reclamações tanto de alunos como funcionários).

O protótipo inicial é um dispositivo embarcado que utiliza um Arduino Mega com um sensor *RF-ID* (sensor de radiofrequência) que foi instalado na entrada do laboratório de IoT para testes de perfil de alunos e professores (depois será instalado na sala de aula) onde o aluno passa seu cartão da biblioteca (que possui algumas informações, por exemplo, sua identificação e uma *tag* que responde ao *RF-ID*) e um módulo gravador de som. O projeto visa também o estudo e comparação de vários sensores (como a câmera para reconhecimento facial, sensor biométrico, teclado para senha, *QR Code*, GPS, entre outros).

O problema a ser analisado é a de "*um aluno que pode se passar por outro*" com o cartão da biblioteca no dispositivo embarcado sem que o mesmo esteja na universidade. Sendo assim, foi pensado inicialmente em um sistema com a combinação ou fusão de vários sensores como o *RF-ID*, leitor biométrico, teclado para digitação de senha, câmera para reconhecimento facial, entre outros. Depois dos testes, pode-se analisar e escolher quais soluções são as mais adequadas dependendo do problema.

Está sendo utilizado para a comunicação sem fio *WI-FI* na transmissão de informações dos sensores para o servidor, o módulo ESP8266. As informações podem ser monitoradas em tempo real através do aplicativo multiplataforma ou da *web* utilizando computadores, *notebook*, *tablets* e *smartphone*. Também pode-se utilizar essas informações cruzadas transmitidas através da rede como turmas, disciplinas, horários e salas de

aula para análises e previsões de comportamento utilizando técnicas de *Big Data* e IA.

O mesmo sistema pode ser utilizado para monitoramento de dados de entrada de alunos na universidade, caso isso seja pensado futuramente. Pode-se utilizar o mesmo cartão da biblioteca para entrar na universidade através de catracas ou apenas o GPS do *smartfone* do aluno. Com isso, ao saber quando o aluno entra/sai da faculdade, também teria-se informações de quando ele está em sala de aula e cruzando as informações, pode-se comparar quanto tempo ele está em aula X, quanto tempo ele não está na aula X e o período que ele está dentro da faculdade. Ao saber que X alunos estão em aula, nas Y salas no Prédio K, a área de *Facilities* terá informação de, por exemplo, prever a partir dos dados, quando limpar e abastecer (com produtos pertinentes) os banheiros. As informações de monitoramento permitirão que esse *big data* faça análises e previsões baseado no comportamento dos alunos no campus.

Todas as informações no aplicativo podem ser monitoradas e podem ser modificadas em tempo real pela *web* (acessado pelo *browser* de computadores, *notebooks* ou *smartfone* de qualquer sistema operacional) pelos funcionários, que precisam estar cadastrados e ter permissão para fazer modificações, consultas ou mexer nas configurações. O sistema conterá *log* para auditoria e *compliance*.

O esquema elétrico atual do *hardware* e suas principais ligações são apresentadas na Figura 1.

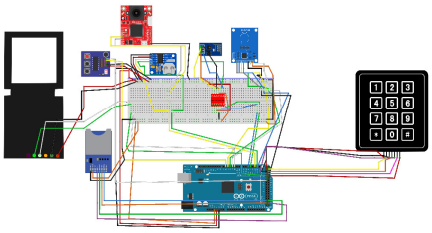

Figura 1 - Protótipo atual do projeto

Está sendo utilizado na construção do aplicativo multiplataforma o Cordova (atualmente modificado para o PhoneGap). Ele usa o ponto forte da *web* de ter linguagens padronizadas, o navegador *web* e pode-se construir aplicativos instaláveis híbridos da plataforma escolhida, mas que foram construídos em *HTML*, *CSS*, *JavaScript* e *JS* com *API*s que funcionam em todo lugar. Mas, não são instaláveis como *APP*s, e não integram com recursos avançados dos equipamentos móveis (*smartphones e tablets*).

A escolha do aplicativo híbrido é o menor custo de desenvolvimento e um único código que serve todas as plataformas. Não será necessário ter equipes específicas de programadores em Java e Android para dar manutenção na linguagem, banco de dados, servidor, entre outros.

Foi criado um servidor virtual no laboratório de IoT da VIVO utilizando o *VMware* com o sistema operacional *Ubuntu*. O servidor foi programado em *Node JS* e o banco de dados instalado foi o *MongoDB*. A comunicação de dados entre o dispositivo embarcado e o servidor foi feito utilizando o módulo ESP8266.

A arquitetura do projeto está dividida em 4 partes e organizada em 4 camadas:

Aplicações: nesta camada se encontram as aplicações como o navegador *web*, o aplicativo gerado e o *site* desenvolvido. Os principais módulos do aplicativo móvel são: módulo com as regras de negócio, módulo *WI-FI*, módulo de notificações e o módulo que realiza a comunicação com o *backend* utilizando *webservices*.

***Framework* de Aplicações:** expõe diversos recursos do sistema operacional para os desenvolvedores utilizarem na programação.

Bibliotecas: contém todo código que disponibiliza os principais suportes para a aplicação, por exemplo, o banco de dados (MongoDB).

***Kernel* do Linux:** é o *kernel* no qual o projeto é baseado. Essa camada possui todos os *drivers* de baixo nível dos componentes de *hardware* como: *WI-FI*, ultrassônico, infravermelho, *display*, relé, entre outros

4. Considerações Finais

Este projeto está em desenvolvimento e apresenta um estudo de aplicação de IoT aplicado ao controle de acesso/ponto. Como prova de conceito, foi utilizado como ambiente o laboratório de IoT da universidade com um dispositivo embarcado na entrada contendo o módulo *RF-ID*. Além disso, os alunos e professores para o teste de perfil com um cartão que possui a *tag* para a leitura no módulo *RF-ID*. O projeto já tem uma publicação internacional indexada B1 [2] como resultado inicial.

Uma arquitetura foi aplicada nesse cenário onde está sendo feito simulações com a transferência de informações através da rede *WI-FI* com a conexão dos sensores e servidor, visando o correto funcionamento do *hardware* (dispositivo embarcado) e *software* (aplicativo *mobile*) para validar a proposta.

As novas tecnologias de IoT podem trazer benefícios no controle e monitoramento de ambientes internos para a redução de custos de recursos financeiros, como a eliminação da lista de presença, o tempo, erro humano e reclamações, tanto de alunos, como funcionários.

5. Referências

[1] ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. The internet of things: A survey. Computer networks, v. 54, n. 15, p. 2787-2805, 2010.

[2] Rinaldi, Luciene C. A. et al. Academic Research Internet of Things. 13th International Conference for Internet Technology and Secured Transactions (ICITST - 2018), University of Cambridge, Cambridge, UK, 2018 (to appear).

Agradecimentos

À Telefônica/Vivo pelos recursos financeiros fornecidos aos projetos do laboratório de IoT e ao Centro Universitário FEI pela bolsa de Iniciação Científica concedida através do programa PIBIC ao aluno Gustavo Souza Azevedo.