IF Access: controle de acesso utilizando tecnologia RFID e microcontrolador

Pedro Luis Araújo Silva[1], George Sobral Silveira[1], Alfredo Rodrigo Sousa da Silva[1]

[1]Instituto Federal de Educação, Ciência e Tecnologia da Paraíba – Campus Campina Grande (IFPB-CG) – Campina Grande, PB – Brasil.

{pedro.araujo, george.silveira}@ifpb.edu.br,
alfredo.rodrigo@academico.ifpb.edu.br

Abstract. *With technological advances and the integration of various security systems, it is possible to prevent a person from accessing an environment without authorization. Due to the increased circulation of people in the IFPB Campus Campina Grande, greater control of access to the institution's environments was required. In this research project, an access control system was developed for IFPB Campus Campina Grande environments using RFID technology and microcontrollers. The system showed good results by correctly managing access times and correlating them with registered users, ensuring effectiveness, agility and security in access control to the institution's environments.*

Resumo. *Com os avanços tecnológicos e a integração de diversos sistemas de segurança, é possível evitar que uma pessoa acesse determinado ambiente sem autorização. Devido ao aumento da circulação de pessoas no IFPB Campus Campina Grande, passou-se a exigir um maior controle de acesso aos ambientes da instituição. Nesse projeto de pesquisa foi desenvolvido um sistema de controle de acesso para os ambientes do IFPB Campus Campina Grande utilizando tecnologia RFID e microcontroladores. O sistema mostrou bons resultados, gerenciando corretamente os horários de acesso e os correlacionando com os usuários cadastrados, garantindo a eficácia, a agilidade e a segurança no controle de acesso aos ambientes da instituição.*

1. Introdução

A necessidade de restringir o acesso de determinados ambientes de pessoas não autorizadas existe há muito tempo. Visando principalmente a segurança, buscamos sempre utilizar mecanismos, sejam eles fechaduras, correntes ou cadeados, que garantam que somente pessoas com autorização consigam acessar e utilizar algum espaço. Com a evolução da tecnologia, a utilização de controles de acesso eletrônicos ficou cada vez mais frequente. No Brasil eles são utilizados há mais de 20 anos. Com eles é possível garantir que somente pessoas previamente cadastradas e autorizadas acessem e utilizem determinado ambiente. Sistemas deste tipo são diretamente responsáveis pela segurança, não só patrimonial, mas também das pessoas que fazem uso destes espaços.

No IFPB Campus Campina Grande, o controle de acesso a ambientes como salas de aula, salas administrativas e laboratórios ainda é feito de forma manual. Apesar de possuir um setor dedicado ao controle de chaves destes locais, o processo gera uma

grande movimentação de pessoas no interior do campus até este setor. O atual modelo de controle de acesso utilizado na instituição não oferece facilidade de uso e praticidade aos diversos usuários da mesma, o que acaba, por sua vez, ocasionando falhas e atrasos.

Diante dessa perspectiva, se faz necessária a modernização do controle de acesso do campus, automatizando esse processo de forma a garantir a segurança dos ambientes do IFPB Campus Campina Grande, bem como levar praticidade e agilidade aos usuários destes ambientes.

O presente projeto consiste de um modelo automático de controle de acesso, que se divide em duas grandes etapas de desenvolvimento, que são as etapas de software e hardware. Com este sistema será possível gerenciar e controlar o acesso a determinados ambientes do IFPB Campus Campina Grande, sob a regência de regras, como estabelecimento de horários, regras de prioridade, entre outros. Tal sistema garantirá a segurança dos ambientes que, uma vez fechados e com o controle de acesso eletrônico, só poderá ser acessado por pessoal devidamente autorizado. O sistema se utilizará de tecnologia RFID (*Radio-Frequency Identification*) para realizar a autenticação das pessoas que possuem autorização para acessar determinado ambiente, onde cada pessoa possuirá o seu cartão RFID (a "chave" de acesso) individual.

2. Tecnologias utilizadas

Neste projeto, diversas tecnologias estão presentes. Antes de entrar no desenvolvimento do projeto, um estudo para determinar quais tecnologias seriam utilizadas se fez necessário. Então, é interessante que, antes de entendermos, neste artigo, como se deu o desenvolvimento do projeto, entendamos um pouco sobre as tecnologias empregadas no mesmo.

2.1. RFID

Tecnologias sem fio estão cada vez mais presentes em nosso dia a dia. Satélites, antenas transmissoras de rádio, TV, telefonia móvel, comunicação Bluetooth e Wi-Fi são algumas das tecnologias sem fio que podemos encontrar facilmente na maioria dos locais. Uma dessas tecnologias é o RFID (do inglês "*Radio-Frequency Identification*").

> A identificação por radiofrequência (RFID) é uma tecnologia capaz de captar, gerenciar, analisar e responder aos dados provenientes de sensores eletrônicos. (...) RFID é uma tecnologia de identificação que utiliza a radiofrequência para capturar os dados, permitindo que uma etiqueta RFID seja lida sem a necessidade de contato ou campo visual, através de barreiras e objetos tais como madeira, plástico, papel, entre outros. É um método de armazenamento e recuperação de dados de forma remota. Ele funciona como um sistema poderoso de aquisição de dados em tempo real, com a vantagem de eliminar as intervenções humanas manuais e visuais, dinamizando assim o tempo de transições e assegurando eficiência e eficácia no processo. (GREFF, 2009, p. 20).

A identificação por radiofrequência é um método de identificação automática através de sinais de rádio, onde um leitor coleta dados de um dispositivo denominado etiqueta RFID. Essa etiqueta (comumente chamada de "*tag*") é um transponder que pode ser colocado em diversos locais, ou até mesmo transportado por uma pessoa, e que contém chips e antenas que lhe permite se comunicar com uma base transmissora, através de ondas de radiofrequência. Tais *tags* podem ser lidas e/ou escritas, e podem ser utilizadas como alternativa aos códigos de barras, por exemplo.

As *tags* RFID são classificadas em quatro tipos, que variam de acordo com a sua fonte de energia e transmissão, a saber: passivas, semipassivas, ativas e semiativas. As *tags* passivas não possuem fonte de alimentação própria e funcionam a partir da energia enviada pelo sinal do leitor. É o tipo de *tag* RFID mais barata e de maior durabilidade. Já as *tags* semipassivas possuem uma bateria utilizada para alimentação do circuito e de sensores, mas dependem do leitor para realizar uma comunicação. Em contrapartida, as *tags* ativas possuem fonte de alimentação própria e permitem a emissão de sinais próprios, sem dependência do leitor. Esse tipo de *tag* RFID possui um maior alcance, mas sua durabilidade é reduzida, limitada à autonomia da bateria. Já as *tags* semiativas diferenciam-se das ativas somente pelo fato de que esta última está em atividade a todo momento, enquanto as semiativas só entram em atividade quando a mesma é ligada pelo leitor. Isso aumenta o tempo de vida da bateria e, consequentemente, da *tag* RFID.

A tecnologia RFID é utilizada em diversos setores, como indústria, comércio, serviços, entre outros. Tal tecnologia é empregada no rastreamento de produtos em uma linha de produção, no monitoramento do progresso em um processo de fabricação de objetos, em veículos para pagamento automático de pedágio, no rastreamento de objetos e de animais, em etiquetas antifurtos em lojas, no rastreamento de bagagens em aeroportos, nos controles de acesso, entre outras aplicações:

> O microchip contido na etiqueta permite armazenar inúmeros campos de informação nesta e ainda apagar esta informação e armazenar novos campos. Com isto tem-se um infinito campo de aplicações e soluções integradas numa única tecnologia. Tudo isto é feito sem contato físico de nenhuma espécie, não apresentando o inconveniente do código de barra que precisa ser lido individualmente e está sujeito a depredações ou danos. No caso da etiqueta de RFID ela pode ser inserida no interior de um livro e mesmo assim será lida sem nenhum problema. A única limitação tecnológica é quanto a itens metálicos, que podem vir a "blindar" ou bloquear os sinais de rádio impossibilitando a leitura (NOGUEIRA, 2002).

2.2. Microcontrolador

Microcontroladores são pequenos computadores em um único circuito integrado, ou seja, são circuitos integrados que contém todos os componentes de um computador, de forma a economizar tempo, espaço e, consequentemente, custos. Dotados de *Central Processing Unit* (CPU), memória, portas de entrada e saída, conversores analógico/digital e digital/analógico, entre outros, os microcontroladores são utilizados nas mais variadas aplicações microcontroladas, desde simples controles remotos para automação residencial até grandes sistemas de controles, sistemas de telefonia e em robôs industriais.

Os microcontroladores são fabricados em diversas linhas, e entre as principais fabricantes, podemos citar as marcas Atmel, Microchip, Texas Instruments, Intel, Motorola, entre outras, com destaque para a primeira, que é a principal fabricante de microcontroladores para a plataforma de prototipagem Arduino, que é a utilizada no projeto.

2.3. Sistema embarcado

Um sistema embarcado é um sistema microprocessado dedicado ao dispositivo ou sistema que se deseja controlar. Diferentemente dos computadores de propósito geral, um sistema embarcado realiza um conjunto de tarefas pré-definidas, com requisitos específicos. Os softwares para sistemas embarcados são chamados de firmwares, e são armazenados em uma memória ROM ou flash. Tais sistemas também são executados

com recursos computacionais limitados, por vezes, sem teclado, tela e com pouca memória.

Os sistemas embarcados são comumente encontrados em dispositivos que são especializados em alguma função, como por exemplo aparelhos de TV e máquinas de lavar: diferentemente de computadores pessoais, esses aparelhos executam tarefas pré-definidas, como exibir a transmissão de um canal de televisão ou lavar e enxaguar uma quantidade de roupas, por exemplo.

3. A escolha do RFID

Tecnologias sem fio garantem praticidade e agilidade no dia a dia de seus usuários, devido a facilidade em sua utilização, uma vez que o não uso de fios e cabos promovem mobilidade e conectividade. Atualmente vivemos cercados das mais diversas redes de comunicação, utilizadas para os mais diversos fins, como redes de telefonia móvel, TV e internet. A escolha pela tecnologia RFID em nosso projeto se justifica em três fatores principais: segurança, praticidade e custo. A utilização de tal tecnologia implica diretamente na segurança dos ambientes, já que cada usuário possuirá a sua *tag* RFID individual, associada ao seu usuário e aos seus dados. É prático, pois *tags* RFID são pequenas e leves, facilitando o seu transporte. Em formato de cartão ou chaveiro, as tags podem ser transportadas em carteiras ou em conjunto com outras chaves, por exemplo. Além disso, leitores e *tags* RFID são simples, possuem um baixo custo e uma grande durabilidade, o que facilita a sua aquisição ou troca, além de simplificar a manutenção do sistema.

3.1. Vantagens do RFID

Comparada a outras formas de coletas de dados, a tecnologia RFID possui uma série de vantagens (INTERMEC, 2007):

a) mais de mil leituras por segundo podem ser realizadas, garantindo grande precisão e proporcionando alta velocidade;

b) os dados das *tags* RFID podem ser alterados sempre que houve necessidade;

c) a tecnologia pode ser usada em conjunto como outras tecnologias, como Wi-Fi e código de barras.

Em relação ao tradicional código de barras, a tecnologia RFID possui as seguintes vantagens (HODGES, 2005):

a) o alcance de leitura da tecnologia RFID é maior, tendo em vista que não se necessita de uma leitura visual, como no código de barras;

b) a leitura pode ser efetuada em movimento;

c) a leitura pode ser efetuada em qualquer direção, desde que a *tag* RFID esteja dentro da amplitude de radiofrequência dos leitores;

d) *tags* RFID possuem maior capacidade de armazenamento de dados, podendo chegar até 64kB, enquanto que os códigos de barras estão limitados a 100B (FINKENZELLER, 2003).

3.2. Desvantagens do RFID

Apesar de contar com uma série de vantagens, algumas tecnologias ainda superam a RFID em alguns aspectos. Estes são alguns pontos negativos da utilização da identificação por radiofrequência (LOUREIRO, 2015):

a) o sistema RFID pode sofrer interferências magnéticas causadas por materiais metálicos;

b) apesar de ser de baixo custo em relação à outras tecnologias sem fio, a RFID possui um custo maior do que o sistemas de código de barras;

c) obstáculos no espaço entre a *tag* e o leitor RFID podem impedir a leitura.

4. IF Access

O projeto, que conta com duas grandes etapas de desenvolvimento (software e hardware), é um sistema que visa automatizar o controle de acesso aos ambientes do IFPB Campus Campina Grande. Sistemas de controle de acesso automáticos estão sendo cada vez mais utilizados no mundo inteiro, pois garantem segurança e agilidade aos ambientes e aos usuários. Na Figura 1, podemos ver o esquema do sistema de controle de acesso desenvolvido neste projeto:

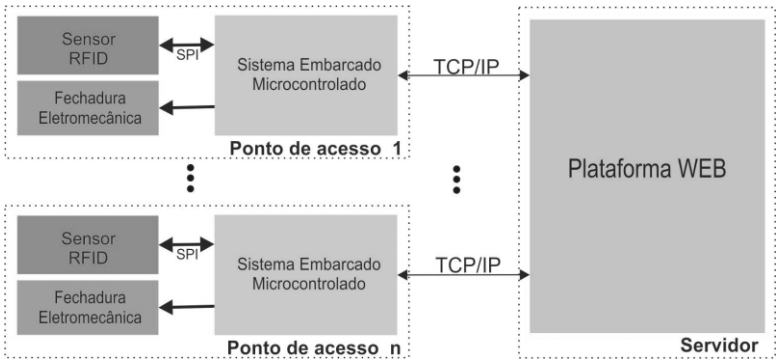

Figura 1. Esquema do sistema de controle de acesso

Cada ponto de acesso é constituído de um sistema embarcado em um microcontrolador, de um sensor RFID e de uma fechadura eletromecânica. Os pontos de acesso serão instalados em cada ambiente da instituição, e se comunicarão via rede, utilizando o protocolo TCP/IP, com o servidor, que conterá o software responsável por toda a gerência do sistema. Os pontos de acesso – o hardware principal do sistema – contarão com um sistema de baterias, que visará suprir as necessidades energéticas do sistema em caso de interrupção do fornecimento de energia elétrica.

A utilização do sistema dar-se-á da seguinte forma: após o registro do usuário no servidor, é feita a correlação dele com os ambientes aos quais terá acesso. O servidor, por sua vez, transferirá essas informações, previamente armazenadas em um arquivo do tipo *Comma Separated Values* (CSV) (ver seção 4.1.1), para todos os pontos de acesso correlacionados com o usuário. Esse envio se faz necessário para caso a rede lógica fique inoperante. Uma vez com o arquivo CSV, o ponto de acesso será capaz de realizar a autenticação de qualquer usuário cadastrado no sistema, mediante a leitura da *tag* RFID do usuário. Ao aproximar a *tag* do leitor, o sistema efetuará a leitura do código da *tag*, e consultará se o mesmo se encontra cadastrado para utilização daquele ambiente naquele horário. Em caso positivo, o acesso ao ambiente é liberado, para o que o usuário

possa realizar o uso do mesmo. Em caso negativo, o usuário não consegue acessar o ambiente.

4.1. Software

O software aplicativo do servidor foi desenvolvido utilizando a linguagem de programação Python, juntamente com o framework para desenvolvimento para aplicações web Django. Também foram utilizadas as tecnologias SQLite3, CSS3, JavaScript e HTML5. O sistema conta com os módulos de cadastro de usuários, ambientes, pontos de acesso e as funcionalidades para identificar, autenticar e auditar os eventos dos registros de acesso. Cada página HTML lida diretamente com o usuário: são elas que aparecem na interface web do sistema para que o utilizador possa inserir os dados necessários no mesmo.

As páginas HTML desenvolvidas estão divididas em dois principais grupos: edição e registro, onde as do grupo de edição são responsáveis por editar os dados do sistema (usuários cadastrados, horários preenchidos, entre outros), e também por sua remoção, enquanto que as do grupo de registro são responsáveis por alimentar o sistema com novos dados. Há ainda as páginas que estão destinadas somente à exibição de dados. Estas somente efetuam consultas ao banco de dados e exibem os resultados na tela para o usuário, como por exemplo os horários reservados para um utilizador em um determinado ambiente. Abaixo, na Figura 2, temos a lista com todas as páginas HTML desenvolvidas:

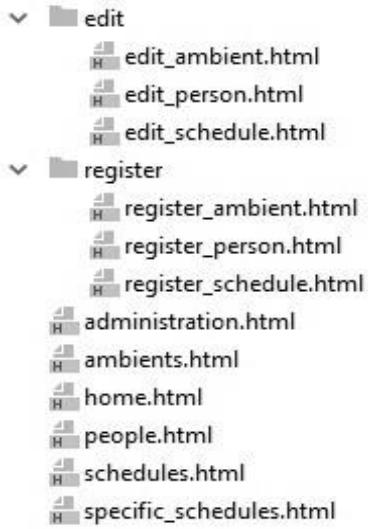

Figura 2. Páginas HTML desenvolvidas no projeto

Cada página HTML possui o seu modelo, seu formulário e a sua *view*. Os modelos são as tabelas que existem no banco de dados, enquanto que os formulários são os responsáveis por capturar as informações inseridas em uma página HTML pelo usuário. Já as *views* compõem a lógica da aplicação. Elas são responsáveis pela interação entre as páginas HTML e seus formulários com o banco de dados, ou seja, elas enviam informações do formulário de uma página HTML para o banco de dados, e também recuperam informações do banco de dados para serem exibidas em uma página HTML.

Abaixo, na Figura 3, podemos ver a página inicial da plataforma web do IF Access:

Figura 3. Página inicial da plataforma web do IF Access

O sistema conta com quatro páginas principais, a saber: página inicial, pessoas, ambientes e horários. Nas páginas pessoas e ambientes, é possível cadastrar, remover e editar os dados dos usuários cadastrados e dos ambientes, respectivamente. Já na página horários é possível gerir todos os horários disponíveis para acesso aos ambientes e determinar quais usuários podem ou não acessar os ambientes em determinados horários.

Cada entidade (pessoa, ambiente e horário) possui cadastrada uma série de informações acerca dos mesmos. Para cadastrar uma entidade "pessoa", informa-se o nome, a matrícula e o número da *tag* RFID (ver seção 3.2) que o usuário possui. Já para a entidade "ambiente", informa-se o tipo de ambiente (predefinido como coordenação, sala ou laboratório), o nome, o ID (pequeno código utilizado para facilitar o reconhecimento de ambientes), o IP do ponto de acesso (ou seja, do ambiente) e a máscara de sub-rede daquele ponto. Por fim, para a entidade "horário", é feita uma correlação entre o ambiente, o usuário e o horário de permissão de acesso. Para tal, informa-se o dia da semana, a hora de entrada e a hora de saída em que será permitido que determinado usuário use o ambiente, além do nome da pessoa e do ambiente, ambos previamente cadastrados.

Todos estes dados serão utilizados na geração do arquivo CSV, responsável por armazenar todas as informações inerentes ao funcionamento do sistema e por correlacionar os ambientes com seus respectivos horários e usuários. Tais dados são armazenados de forma segura, uma vez que a permissão de alteração destes dados só é concedida a administradores, os quais só conseguem efetuar mudanças no sistema mediante autenticação, entrando com seu usuário e senha.

O cadastro de novos usuários no sistema, bem como o agendamento de horários para utilização dos ambientes é feito por um coordenador de curso, ou qualquer outro usuário administrador. Para deixar de ser um usuário comum e passar a ser um usuário administrador, um coordenador deve acessar o sistema e dar esse direito ao usuário em questão.

4.1.1. Arquivo *Comma Separated Values*

O formato de arquivo *Comma Separated Values* (CSV), ou Valores Separados por Vírgula, é um formato em que, basicamente, cada registro corresponde a uma linha do arquivo, e em cada registro, campos diferentes são delimitados por vírgulas.

> O formato de arquivo CSV (*Comma Seprated Values*) é geralmente usado para trocar dados entre aplicativos diferentes. O formato de arquivo, como é usado no Microsoft Excel, tornou-se um pseudopadrão em toda a indústria, mesmo entre plataformas não-Microsoft. (REPICI, [20--], tradução nossa).

Tal formato de arquivo foi escolhido para ser utilizado no projeto pois mantém os dados organizados, tal como numa planilha, além de ocupar pouco espaço na memória, por armazenar somente texto.

4.2. Hardware

O sistema conta com a instalação de um ou mais pontos de acesso, integrados pelo software hospedado em um servidor web. Essa integração só é possível, dentre outros fatores, por causa do hardware empregado nos pontos de acesso do projeto. Para se permitir ou não a entrada de pessoas nos ambientes mediante autenticação, se faz necessário o uso de um hardware que faça a abertura e o fechamento dos ambientes, bem como o reconhecimento do pessoal autorizado e a conexão dos pontos de acesso com o servidor.

O hardware pensado para o projeto envolve as tecnologias anteriormente citadas na seção 2 deste artigo, que são as tecnologias RFID, microcontrolador e sistema embarcado. Abaixo, na Figura 4, podemos ver o hardware que será utilizado no projeto para efetuar a autenticação dos usuários:

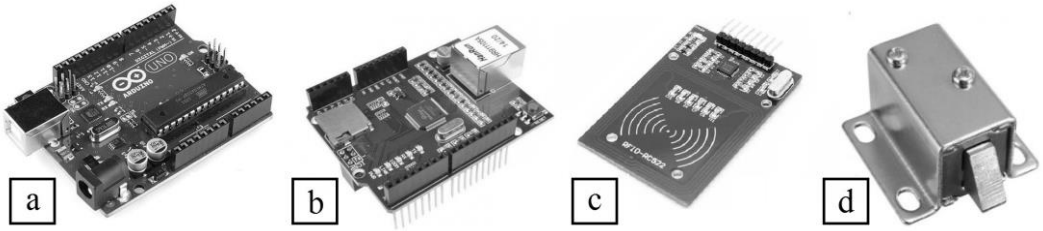

Figura 4. Hardware utilizado no IF Access. (a) Arduino Uno. (b) Ethernet Shield W5100. (c) Leitor RFID MFRC522. (d) Fechadura eletromecânica (exemplo)

Cada usuário do sistema será equipado com uma *tag* RFID, de uso individual, que poderá ser um cartão ou um chaveiro, conforme mostrados na Figura 5:

Figura 5. *Tags* RFID. (a) Cartão RFID. (b) Chaveiro RFID

Essas *tags* serão previamente configuradas no software hospedado no servidor web, com informações acerca do usuário proprietário da *tag*, como nome, CPF, matrícula e informações dos ambientes e horários em que o usuário pode acessar tais ambientes. Essas *tags*, uma vez configuradas, quando aproximadas do leitor RFID serão lidas pelo ponto de acesso, que verificará se determinado usuário tem permissão para

acessar aquele ambiente naquele horário. Essas informações são enviadas pelo servidor web ao ponto de acesso durante a configuração, e ficam no mesmo permanentemente, até que uma nova configuração seja realizada.

No projeto, o Arduino Uno foi a plataforma de prototipagem escolhida para o sistema microcontrolado dos pontos de acesso. Essa plataforma conta com o microcontrolador Atmel ATmega328P, que opera com um *clock* de 16MHz, possui 6 portas de entrada analógicas, 14 portas de entrada/saída digitais e 6 portas *Pulse Width Modulation* (PWM). A escolha do Arduino Uno para o projeto tem como base o seu custo, sua quantidade de portas e seu consumo energético. Dentre as placas de prototipagem Arduino existentes no mercado, o Arduino Uno é uma das que possui melhor custo benefício, pois ela é suficiente para a maioria dos projetos microcontrolados, e pode ser adquirida por um preço acessível. Além disto, o Arduino Uno possui uma quantidade satisfatória de portas de entrada e saída, o que possibilita a conexão de vários Shields e periféricos, ao mesmo tempo que possui um baixo consumo energético, considerando que a mesma opera com um nível de tensão de 5 volts.

O Arduino, no projeto, opera com um sistema embarcado que é responsável por toda a lógica que tem como finalidade liberar ou não o acesso aos ambientes. No Arduino, um algoritmo efetua o confrontamento dos dados lidos pelo leitor RFID com as informações contidas em sua memória e checa se o usuário que tentou efetuar a autenticação naquele momento está autorizado a entrar no ambiente. Uma vez autenticado, o Arduino sinaliza para a fechadura eletromecânica que ela deve se mover para a posição “aberto” e o ambiente é devidamente liberado ao acesso. O Arduino ainda realiza o registro de um histórico de todos os usuários que fizeram uso de determinado ambiente, bem como de todos os horários dessas utilizações.

O módulo Ethernet Shield W5100 é responsável por manter o Arduino e, consequentemente, o ponto de acesso conectados à rede, para que os mesmos possam se comunicar com o servidor web. Ele dispõe, ainda, de um slot para o uso de um cartão de memória do tipo micro SD. Tal módulo se conecta com o servidor por meio do protocolo de rede TCP/IP e recebe do servidor os pacotes com as informações de cadastro dos usuários do sistema, armazenados em um arquivo CSV, além de enviar para o servidor web o histórico de utilização dos ambientes.

4.2.1. Software embarcado do projeto

O sistema embarcado foi desenvolvido utilizando a linguagem de programação Arduino, que é muito similar à linguagem de programação C++. O código fonte é responsável por especificar o comportamento e a interação do microcontrolador com seus respectivos periféricos. É neste código fonte que se encontram especificadas as instruções de funcionamento para o microcontrolador, para o módulo Ethernet Shield, para o leitor RFID e para a fechadura eletromecânica.

O código se utiliza de quatro bibliotecas: MFRC522, que disponibiliza, dentre outras, as funções de leitura e escrita de *tags* RFID; SPI, que especifica a comunicação entre o microcontrolador e o leitor RFID, utilizando a interface Serial Peripheral Interface (SPI) e o protocolo de comunicação SPI; Ethernet, que provê a comunicação entre o Arduino e a Ethernet Shield, bem como a comunicação de todo o ponto de acesso com a rede; SD, que provê as funções necessárias para a leitura e escrita em cartão de memória.

5. Testes

O software web para o servidor foi devidamente implementado, e o mesmo foi submetido a uma série de testes, onde foram introduzidos dados a fim de analisar o comportamento do sistema. O software do projeto necessita coletar os dados dos usuários, sob demanda, e os armazenar em um arquivo do tipo CSV, de forma organizada. Tal arquivo, quando pronto, é enviado aos pontos de acesso.

Dados fictícios de professores, coordenadores e demais usuários dos ambientes do campus foram inseridos no sistema, o qual pôde gerar o arquivo com os dados referentes a horários, ambientes e usuários com permissão de acesso. Com estes dados, o sistema foi capaz de confrontar as informações, quando uma tentativa de autenticação foi feita, e pôde liberar ou não o acesso a determinado usuário ao ambiente.

A etapa de hardware do projeto não se encontra concluída, então os testes de hardware foram limitados. A fechadura eletromecânica foi simulada com o auxílio de dois LEDs, um da cor verde e um da cor vermelha, que emitiram sinais luminosos referentes ao comportamento do sistema. Quando se tentou autenticar uma *tag* RFID que se encontrava cadastrada no sistema, um sinal luminoso verde constante foi emitido, sinalizando ao usuário que o acesso dele àquele ambiente estava liberado. Na situação contrária, quando foi feita uma tentativa de acesso com uma *tag* RFID que não estava cadastrada no sistema, um sinal luminoso vermelho intermitente foi emitido, sinalizando ao usuário que o seu acesso àquele ambiente foi negado.

6. Resultados

O IF Access define uma modernização no controle de acesso aos ambientes do campus através de um processo automático que fornece maior segurança, praticidade e agilidade aos usuários desses ambientes. Tal sistema se mostra eficiente no controle de acesso, e demonstra a garantia da segurança necessária para os ambientes do campus. Com o controle de acesso automático, falhas na segurança do sistema antigo deixam de existir, como a perda de chaves, por exemplo.

O sistema web do IF Access consegue realizar com êxito o cadastro de usuários, ambientes e horários, e ainda os correlacionar, além de gerar, de forma correta, o arquivo CSV com as informações necessárias para serem enviadas aos pontos de acesso.

Abaixo, na Figura 6, podemos observar um exemplo deste arquivo CSV gerado, onde constam os dados dos horários de acesso, com os nomes dos dias, os horários de entrada e de saída, a matrícula do usuário cadastrado e o código do ambiente, separados por vírgula:

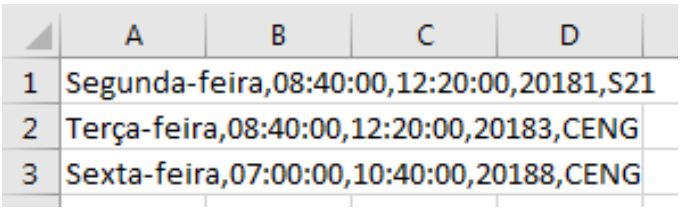

Figura 6. Recorte de exemplo do arquivo CSV gerado pelo software web do IF Access

Fazendo os testes com o hardware de forma a realizar uma simulação do real comportamento do sistema, pôde-se perceber que o mesmo se comportou de forma adequada e desejada, acendendo o LED verde para sinalizar que o usuário teve o acesso

liberado ao ambiente, ou o LED vermelho para sinalizar que o usuário teve o acesso negado. Como mencionado, posteriormente tais LEDs serão substituídos por uma fechadura eletromecânica, onde os atuais sinais luminosos corresponderão aos sinais de "aberto" e "fechado" da fechadura. Abaixo, na Figura 7, podemos ver a montagem do circuito com o atual hardware, bem como também os testes que foram realizados com as *tags* em formato de cartão e de chaveiro.

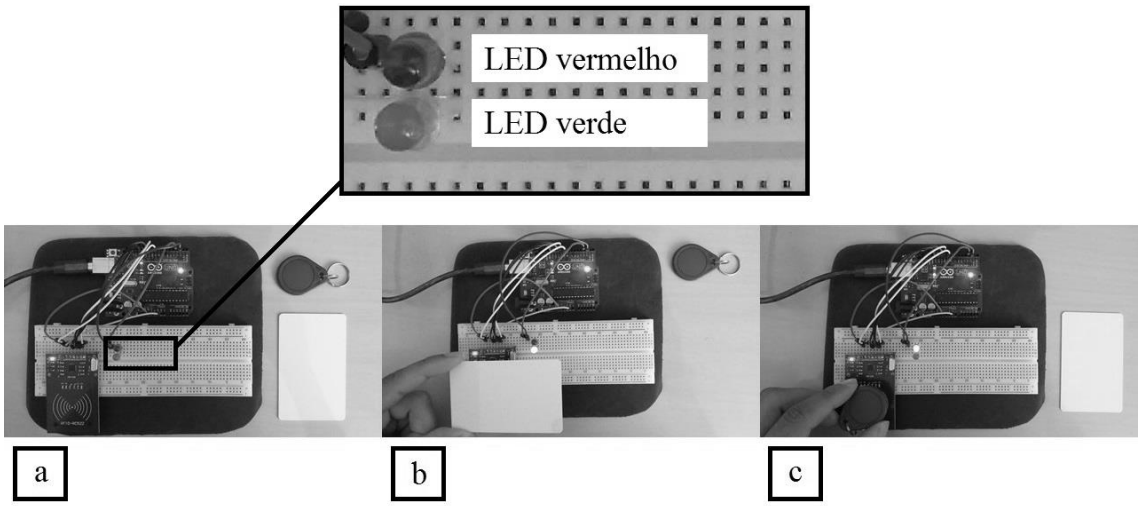

Figura 7. Teste realizado com o circuito. (a) Demonstração do circuito. (b) Teste com o cartão RFID. (c) Teste com o chaveiro RFID

7. Conclusões

Devido à crescente circulação de pessoas do IFPB Campus Campina Grande no setor de chaves, o atual modelo de controle de acesso a ambientes é sujeito a inúmeras falhas, além de não ser prático e ágil. Diante dessa perspectiva, a utilização de um sistema eletrônico de controle de acesso se fez necessária. Neste artigo, vimos como se deu o desenvolvimento do projeto IF Access, passando por todas as suas etapas, explanando o desenvolvimento do software web do projeto, bem como as tecnologias utilizadas em todo o sistema de controle de acesso.

De acordo com os resultados preliminares, o sistema proposto possui grandes chances de atingir o seu objetivo. Apesar da etapa de hardware não estar concluída, o software funciona de forma satisfatória.

O IF Access é de fácil implementação e manutenção. Além da garantia de segurança e agilidade que ele fornece, o sistema, que é de baixo custo, possui componentes de hardware de fácil aquisição no mercado, e o arcabouço de ferramentas e softwares utilizados é totalmente gratuito, o tornando, assim, uma excelente alternativa para o controle de acesso a ambientes.

Referências

ALMEIDA, R. M. a.; MORAES, C. H. V.; SERAPHIN, T. F. P. "Programação de sistemas embarcados - Desenvolvendo software para microcontroladores em linguagem C". Elsevier, 2016.

ANDRADE, F. S. D.; Oliveira, A. S. D. Sistemas Embarcados - Hardware e Firmware na Prática. Érica, 2010.

FINKENZELLER, Klauss. RFID Handbook Fundamentals and Applications in Contactless Smart Cards and Identification. 2 ed. England: John Wiley & Sons Ltd., 2003.

_____. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication. 3 ed. Chippenham: Wiley, 2010. 462 p.

GAO RFID Inc. RFID Solutions for ID Badges and Access Control. Disponível em: <http://gaorfid.com/access-control-rfid-system/>. Acesso em: 27 fev. 2018.

GREFF, Ponciano de Almeida. Especificação de um Sistema para Monitoramento de Atividades de Natação usando RFID. Dissertação (Tecnólogo)–Curso Superior de Tecnologia em Sistemas de Telecomunicações, Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina - Campus São José, São José - SC, 2009.

HODGES, Steve; MCFARLANE, Duncan. Radio frequency identification: technology, applications and impact. Cambridge University UK, Auto-ID Lab, September, 2005.

LOUREIRO, G. S. M.; SOUZA, I. Q.; LOPES, M. G. M.; Identificação por Radiofrequência. 2015. Trabalho apresentado como requisito parcial para aprovação na Disciplina Redes de Computadores I, Escola Politécnica da Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2015.

MARCONDES, José Sérgio. Controle de acesso físico, como medida de segurança física. 2015. Disponível em: <https://www.gestaodesegurancaprivada.com.br/controle-de-acesso-fisico/>. Acesso em: 03 mar. 2018.

NOGUEIRA, Isabel Cristina. Gerenciando a biblioteca do amanhã: tecnologias para otimização e agilização dos serviços de informação. In: SEMINÁRIO NACIONAL DE BIBLIOTECAS UNIVERSITÁRIAS, 12., 2002, Recife. Anais... Recife: UFPE, 2002.

PALA, Zeydin; INANÇ, Nihat. Smart Parking Applications Using RFID Technology. IEEE, RFID Eurasia. 2007. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4368108&tag=1>. Acesso em: 27 fev. 2018.

REPICI, Dominic John. The Comma Separated Value (CSV) File Format. [20--]. Disponível em: <http://www.creativyst.com/Doc/Articles/CSV/CSV01.htm>. Acesso em: 14 ago. 2019.

SEAL TELECOM. Todo o poder das soluções de segurança. Disponível em: <http://blog.sealtelecom.com.br/solucoes-de-seguranca> Acesso em: 03 mar. 2018.

SHARMA, Meenakshi; SIDDIQUI, Adil. RFID Based Mobiles: Next Generation Applications. In: 2nd IEEE International Conference on Information Management and Engineering (ICIME), 2010. Disponível em: <https://ieeexplore.ieee.org/document/5477641>. Acesso em: 27 fev. 2018.