Fechadura Microcontrolada com Gerência Centralizada

Yuri M. Guedes, Marcelo C. P. Santos

Núcleo de Informática – Instituto Federal de Educação, Ciência e Tecnologia do Sudeste de Minas Gerais – Campus Juiz de Fora (IFSEMG)
Rua Bernardo Mascarenhas, 1283 - Fábrica – 36.080-001 – Juiz de Fora – MG – Brasil

yuri@megaguia.com.br, marcelo.santos@ifsudestemg.edu.br

Abstract. *This paper describes and specifies the construction of a remote management system of digital door locks based on Internet of Things concept, seeking an alternative to traditional model of locks, based on the use of individual local management. Wherever it is possible, we move the complexity of our device to a server that holds the entire system configuration and manage.*

Resumo. *Este trabalho descreve e especifica a construção de uma tranca eletrônica que será associada a um sistema de gerenciamento remoto de portas com trancas digitais. Esse sistema é baseado no conceito de Internet das Coisas, sendo uma alternativa ao modelo tradicional de trancas, baseado no uso de gerenciamento local individual. A complexidade do sistema, sempre que possível, foi movida para um servidor que detém toda a configuração e a gerência da solução.*

1. Introdução

1.1. Contextualização

Um dos grandes problemas da sociedade sempre foi relacionado à segurança de locais e em como manter um local seguro quando não se está nele ou próximo o suficiente para tê-lo em vista. Além disso, buscam-se formas de garantir que apenas determinados indivíduos ou grupos tenham acesso aos determinados setores. Embora existam várias soluções convencionais, como paredes, portas, travas, trincos, cadeados, fechaduras, essas soluções não necessariamente exercem esse tipo de controle.

A existência de um mecanismo de controle eletrônico centralizado constitui uma ferramenta que garante a proteção e a confidencialidade. Confidencialidade é a propriedade de que o recurso não esteja disponível a quem não tem autorização nem esteja credenciado. Tal propriedade envolve a classificação em graus de sigilo, o credenciamento de acesso e as medidas de proteção e de acesso em geral. Nesse contexto, a utilização de sistemas constitui uma alternativa em que as fechaduras se tornam componentes digitais gerenciáveis através da Internet, podendo ser acionadas por simples senha ou por sensores de presença. Isso possibilita até mesmo o uso de características biométricas do indivíduo, como impressão digital ou reconhecimento da face.

Apesar da grande variedade de produtos disponíveis no mercado atualmente, há ainda uma lacuna quando se pensa em dispositivos de instalação simples, baratos e com possibilidade de gerenciamento remoto centralizável.

O sistema proposto preocupa-se com a segurança nas transmissões, sempre criptografando os dados, adicionalmente à criptografia já utilizada no padrão IEEE 802.11 (*Wi-Fi - Wireless Fidelity*).

Deve-se atentar também que falhas na conexão podem ocorrer e, em virtude disso, foram desenvolvidos dois modos de operação, *on-line* e *off-line*, garantindo-se, assim, o funcionamento básico das trancas nos casos de falta de conexão com o servidor.

1.2. Internet das Coisas

A FMGC (Fechadura Microcontrolada com Gerência Centralizada) se encaixa no conceito de Internet das Coisas (*Internet Of Things – IoT)*, termo que se refere a sistemas de dispositivos conectados a sistemas na web que podem estar interconectados ou não [Nascimento 2015]. É um conceito de uso da conectividade pelos utensílios mais básicos do cotidiano, como um aparelho de ar condicionado, assim como por máquinas mais complexas, como caldeiras de indústrias. Segundos este novo paradigma, as coisas, objetos em geral, passarão a se comunicar, trocando informações e gerando dados para melhorar nossas vidas.

O conceito de IoT ainda é apenas parcialmente implementado, pois, de forma geral, conecta-se “coisas” a computadores. Espera-se que, no futuro, tenhamos mais “coisas” conectadas diretamente a outras “coisas”. Por exemplo, hoje temos aparelhos de ar condicionado que controlamos por meio do celular, que é um computador. Poderíamos ter um aparelho de ar condicionado que trocasse informações diretamente com um relógio que possuísse um termômetro com acesso à sua temperatura corporal, modificando a temperatura ambiente automaticamente dependendo dessa informação, maximizando o conforto do usuário.

1.3. Visão Geral deste Trabalho

A proposta deste trabalho é a criação de uma Fechadura Microcontrolada com Gerência Centralizada (FMGC), uma fechadura de instalação simples, com conexão baseada em redes sem fio e troca de informações com servidores baseada em protocolos de comunicação amplamente conhecidos e utilizados, que irão fornecer as configurações necessárias para autenticação dos indivíduos em cada fechadura, o que significa a garantia do acesso ou da negação do mesmo a determinado ambiente, podendo ser utilizados critérios como data, hora, evento, dentre outros. Ou seja, um indivíduo pode ter acesso a determinado ambiente, porém somente por um determinado prazo ou em determinados dias ou mesmo períodos do dia, tudo configurável por meio de um sistema centralizado, conforme podemos verificar na Figura 1.

As formas de acesso aos ambientes gerenciados podem ser configuradas para aceitar individualmente ou em conjunto um código de identificação, uma senha ou dados lidos de um dispositivo RFID (*Radio-Frequency IDentification*) [Viera et al 2007].

É importante salientar que a abrangência deste trabalho limita-se ao projeto do *hardware*, do *software* embarcado na fechadura e a construção de um protótipo que prove a viabilidade da ideia. Em [Pacheco 2016], é projetado um exemplo de servidor que complementa a aplicação.

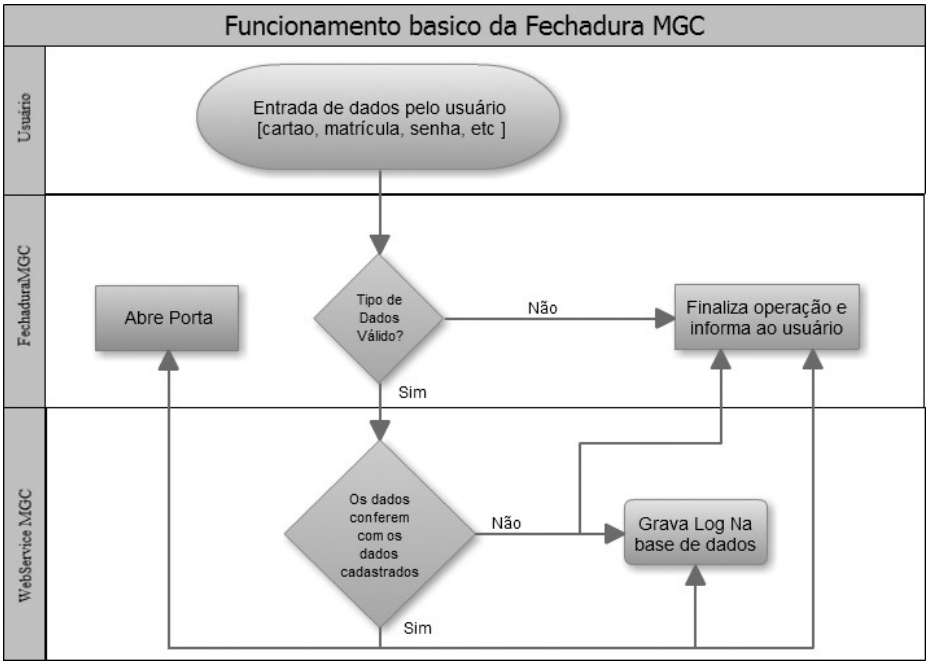

Figura 1. Funcionamento básico da fechadura MGC.

Desta forma, o nível de segurança de cada ambiente pode ser elevado de acordo com a necessidade. Por exemplo: um refeitório pode ser acessado com uma senha de conhecimento geral, uma sala pode ter acesso restrito e, assim, serem necessários para acesso a digitação de uma identificação de usuário (ID) e de uma senha, e um outro ambiente que tenha nível de segurança um pouco menor pode ser acessado pelo portador de um dispositivo RFID, sem necessidade de digitação de senha. O dispositivo RFID pode ser incluído, por exemplo, em crachás, tornando prática e simples sua utilização.

O sistema proposto trabalha com qualquer trava elétrica, magnética ou eletrônica atualmente disponível no mercado, e esses dispositivos normalmente não prejudicam a utilização da fechadura convencional, permitindo a abertura e trancamento com a chave.

No decorrer deste documento serão descritas as motivações para o mesmo, o material utilizado, o *hardware* e *software* desenvolvidos, bem como as ideias para melhoramentos futuros.

2. Revisão Bibliográfica

Em [Modesto and Sirotheau 2006], é sugerido um projeto de circuito para automatização de fechaduras por meio de computadores, no qual se pode passar uma senha em um teclado numérico para que seja liberado ou não o acesso. Os pontos fracos em relação ao projeto proposto neste documento seriam a comunicação com um computador através da porta serial que limita em muito o distanciamento do dispositivo e do computador, bem como foi proposto somente o uso de uma única senha para a abertura da porta.

Já em [Nunes et al 2007], o projeto contempla vários dispositivos conectados a um computador, também através da porta serial, mas contando com um aplicativo que promove a conexão com a internet e, com isso, disponibilizando a informação para

qualquer lugar que se possa estar. Comparando com proposta aqui apresentada, o trabalho sofre das mesmas limitações de distância já citadas para a comunicação serial, demanda a manutenção de um computador ligado 24 horas por dia, 7 dias por semana, para que o sistema esteja operacional. Além disso, por não utilizar o *Wi-Fi*, é de instalação muito mais cara e trabalhosa.

[Oliveira et al 2012] abordam uma proposta simples, mas bastante interessante, para resolver o problema de dificuldade de acesso a locais dentro de uma subestação da Eletronorte. Dentro da solução abordada, foi necessário utilizar fibra ótica devido às grandes dispersões eletromagnéticas geradas no local; por esse motivo, o projeto apresentado por este trabalho não se aplicaria, pois foi concebido para locais totalmente cobertos por acesso *Wi-Fi*. Fora isso, acrescentaram-se funcionalidades como teclado *touchscreen*, que permite uma enorme versatilidade ao protótipo.

Produtos comerciais como, por exemplo, a *Lockitron* [Lockitron] e *SmartLock* [SmartLock], apesar de ambos serem *Wi-Fi* e conectados à internet, possibilitando que de um celular se abra a porta de qualquer lugar do mundo, são descentralizados e são produtos voltados para residências e não para empresas.

3. O Sistema Embarcado

Sistemas embarcados são dispositivos com *hardware* e *software* elaborados e dimensionados com fins e propósitos específicos, diferentemente de um computador de uso geral, como um *desktop* ou um *notebook*. Um dispositivo com sistema embarcado tem, em geral, seus recursos limitados pensados exclusivamente para o seu objetivo. Já o computador de uso geral é geralmente superdimensionado para que se encaixe em uma gama maior de aplicações.

Pela sua especificidade, a maioria dos dispositivos com sistemas embarcados têm tamanhos reduzidos em relação a dispositivos de propósitos gerais, pois possuem periféricos que são projetados de acordo com as necessidades dos processos a serem executados, ficando, assim, bastante compactos.

O que se propõe neste documento é um sistema embarcado cuja principal característica é a simplicidade do *hardware*, movendo-se, sempre que possível, a complexidade para o *software*.

Exceto quanto às configurações básicas que possibilitem à fechadura a comunicação via rede, toda configuração da fechadura será enviada do servidor. O *software* embarcado, dependendo da configuração recebida do servidor, limitar-se-á a funções simples, como exibir uma mensagem, enviar um *login* digitado ou lido de um dispositivo RFID, acompanhado ou não de senha (dependendo da configuração) ao servidor e abrir ou não a porta, dependendo da resposta do servidor.

Como o sistema envolve a comunicação entre dispositivos heterogêneos, modelou-se a comunicação como um *Web Service* [Booth 2004]. *Web Services* utilizam um grupo de tecnologias: SOAP/XML, que fornece o padrão para a estrutura dos dados transmitidos e recebidos; WSDL, um descritor do serviço; UDDI, que fornece uma maneira de achar serviços na internet. Utilizamos o SOAP em todas as mensagens trocadas no sistema proposto.

A fechadura possui dois modos de operação: *on-line*, quando conectada ao servidor, e *off-line*, caso contrário.

Ao ligar a fechadura pela primeira vez ou após acionar o *hardreset*, deverá ser informada a identificação da fechadura, o endereço do servidor e, em seguida, a chave de criptografia para a comunicação de dados. A partir daí, o restante da configuração é feita por meio do servidor, que deverá enviar um pacote de informações para a fechadura contendo: data e hora atuais, os ID´s e senhas para login *off-line*, o modo de autenticação, o tempo máximo de espera por respostas do servidor (após esse tempo o sistema entra em modo *off-line*) e o tempo máximo sem comunicação, a partir do qual a fechadura dispara uma mensagem sem conteúdo apenas para checar se o servidor continua acessível.

Quando entrar em modo *off-line*, a fechadura para de enviar requisições de validação ao servidor e passa a fazê-lo nos seus registros internos. A cada nova tentativa de validação, com sucesso ou não, ocorrerá o registro em memória local da fechadura, para posterior envio ao servidor assim que for reestabelecida a comunicação. Após cada registro local, a fechadura tentará restabelecer a comunicação com o servidor.

Durante o modo *off-line*, assim que a fechadura receber um sinal de retorno de atividade do servidor, irá retornar ao modo *on-line* e iniciará o envio dos logs das atividades registradas durante o período *off-line*, se houver.

Tanto no modo *on-line* quanto no *off-line*, os dados informados pelo usuário para validação poderão ser diferentes em cada fechadura (ID de usuário, senha, cartão RFID). O funcionamento será totalmente interativo, com a solicitação ao usuário de cada informação pelo dispositivo.

4. Descrição do *Hardware* Desenvolvido

A FMGC é composta basicamente por três três módulos distintos. O LCD (*Liquid Cristal Display*), que fornece e recebe informações ao usuário através de sua interface gráfica com *touchscreen*, sendo assim possível pedir ao usuário que digite sua senha, imprimindo esta mensagem no LCD juntamente com um teclado e, depois, recebendo os números digitados através do *touchscreen*.

A placa CC3200 *LaunchPad* é responsável por centralizar todos processos, desde a impressão de uma mensagem no LCD, até o recebimento da resposta do servidor sobre a permissão ou não de entrada em determinado ambiente.

Entre o LCD e o modulo CC3200, temos uma placa criada especialmente para este trabalho. Esta placa é responsável por interligar o módulo CC3200 com seus periféricos, o LCD para exibir mensagens e receber *inputs* do usuário, o relê para acionar a tranca da porta, duas portas IO para utilização de sensores ou atuadores digitais, o módulo de leitura RFID e o *buzzer*.

4.1. CC3200 LaunchPad

O CC3200 LounchPad, conforme pode-se observar na Figura 2, é uma placa de testes e desenvolvimento, criada pela Texas Instruments, para o microcontrolador CC3200 um chip com um processador ARM Cortex-M4 com *Wi-Fi* embutida, propiciando um excelente custo benefício para aplicações voltadas para a IoT de baixo consumo. Esta placa possui uma interface de entrada e saída de dados composta por dois pares de

conectores de dez pinos cada, provendo, dessa forma, acesso a quarenta pinos para usos diversos, por exemplo: alimentação, comunicação serial, entradas e saídas digital e analógica e PWM (*Pulse Width Modulation*).

A placa conta com um gravador e depurador para o microcontrolador *on-board*, assim como outros periféricos que não serão utilizados neste trabalho.

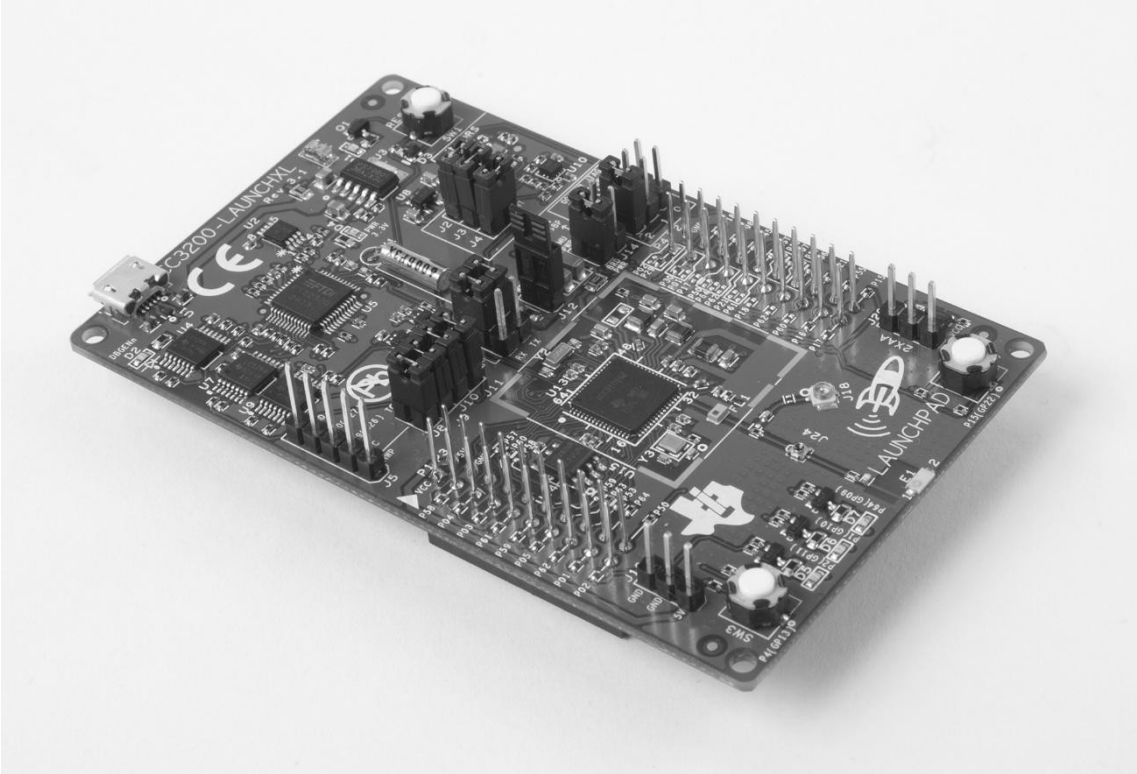

Figura 2. Foto do Módulo CC3200 LaunchPad.

4.1.1. Microcontrolador CC3200

O CC3200 foi criado especificamente para a IoT. Integra um processador ARM CortexM4 de alta performance, rodando com *clock* de 80MHz e 256Kb de SRAM.

O CC3200 possui outro microcontrolador embutido que implementa o padrão de comunicação Wi-Fi. Wi-Fi é uma marca registrada da Wi-Fi Alliance, que é utilizada por produtos certificados da classe de dispositivos de rede local sem fios (WLAN) baseados no padrão IEEE 802.11 [Molisch 2011]. O termo Wi-Fi é normalmente usado como um sinônimo para a tecnologia IEEE 802.11 e é uma abreviação do termo inglês Wireless Fidelity, que significa Fidelidade Sem Fio.

O padrão Wi-Fi opera em faixas de frequências que não necessitam de licença para uso o que o torna atrativo. Porém, no Brasil, para uso comercial, é necessária a certificação da Agência Nacional de Telecomunicações (Anatel).

Para se conectar a uma rede *Wi-Fi*, deve-se estar no raio de captação de um dispositivo de acesso e usar um aparelho, como celular, *notebook* ou similar com capacidade de comunicação sem fio, deixando o usuário do *Wi-Fi* bem à vontade sem a necessidade de fios para a conexão.

Atualmente, quase todos os celulares bem como os computadores portáteis vêm de fábrica prontos para se comunicarem com redes sem fio no padrão *Wi-Fi* (802.11 a, b ou g). A conexão sem fio, que já foi um acessório, está se tornando item obrigatório, principalmente devido à facilidade de implementação das redes sem fio, ocasionando sua larga utilização.

Além do *Wi-Fi*, o microcontrolador CC3200 conta com a pilha de protocolos TCP/IP embutido em seu cerne, o que significa utilização de redes sem fio com muita facilidade por parte do desenvolvedor. Sendo assim, foram utilizados no protótipo protocolos de comunicação HTTP, com criptografia WPA2 na conexão sem fio e RC4 [Rosen 2012] na composição dos dados transmitidos no corpo dos documentos.

Na Figura 3, pode-se observar a construção do CC3200, com seus barramentos, periféricos e seu subnúcleo para o processamento da comunicação *Wi-Fi*.

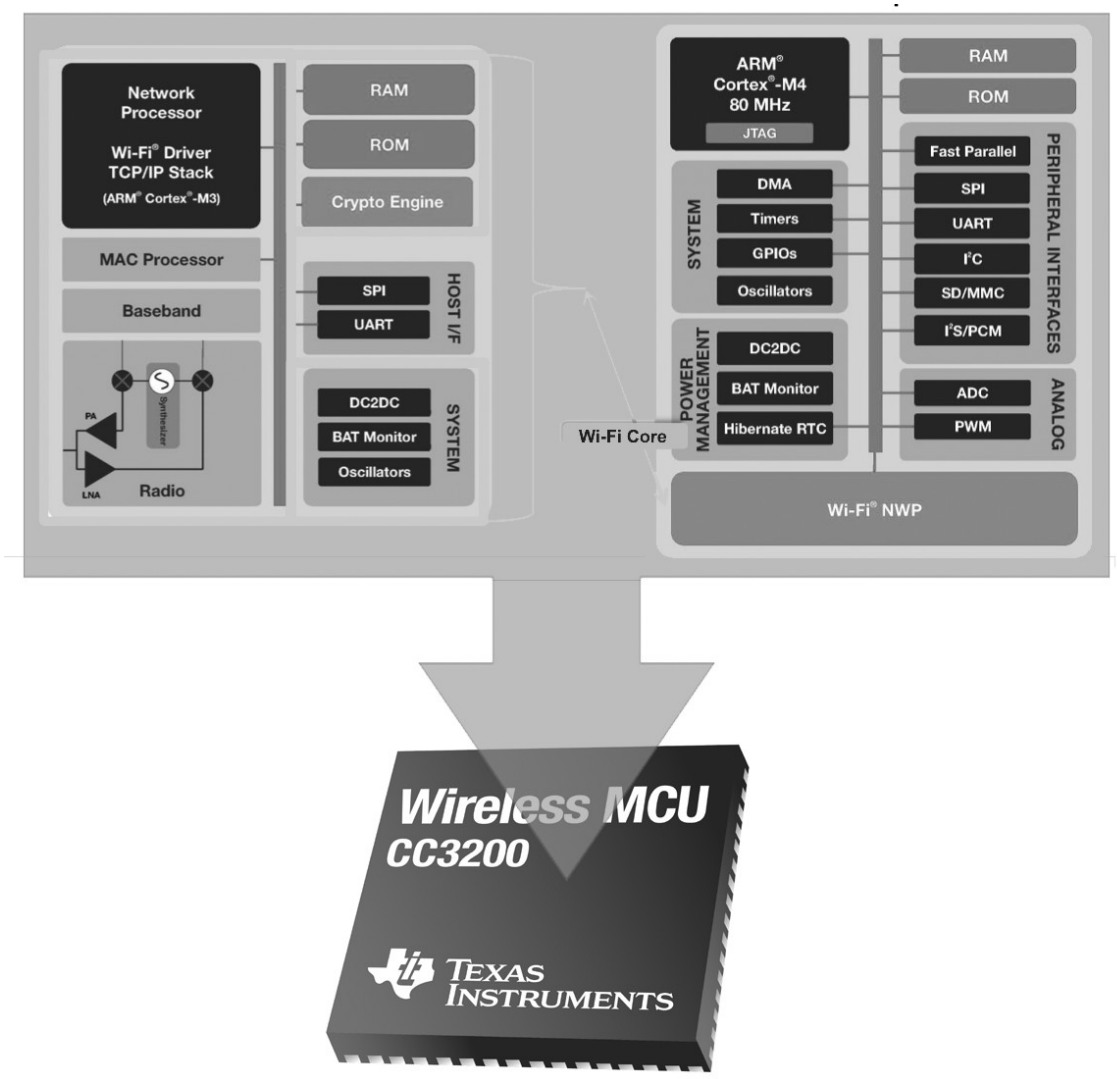

Figura 3. Microcontrolador CC3200 e seus periféricos.

4.2. LCD

A utilização do LCD, apresentado na Figura 4, como principal meio de entrada e saída de informações do sistema, deve-se à grande versatilidade obtida em seu uso. O mesmo dispositivo pode ser usado para exibir mensagens ou para *input* de número, letras ou ambos. Via *software* embarcado, desenha-se na tela o teclado virtual que melhor se adapte à situação. O tratamento dos toques na tela é feito inteiramente pelo *software* embarcado, livre de restrições. Caso seja necessário que se digite uma senha, basta que o processador desenhe um teclado numérico e aguarde a digitação na própria tela. Caso seja necessário que o usuário aproxime o cartão RFID do equipamento, mensagens de orientação podem ser exibidas no LCD.

Com o LCD, a utilização do sistema pode até mesmo ser ampliada de diversas formas. Avisos sobre o que está acontecendo no momento em uma sala podem ser exibidos no LCD, evitando-se interrupções indesejadas, ou participantes podem ser avisados do cancelamento ou realocação de uma reunião assim que tentarem entrar na sala inicialmente reservada para ela.

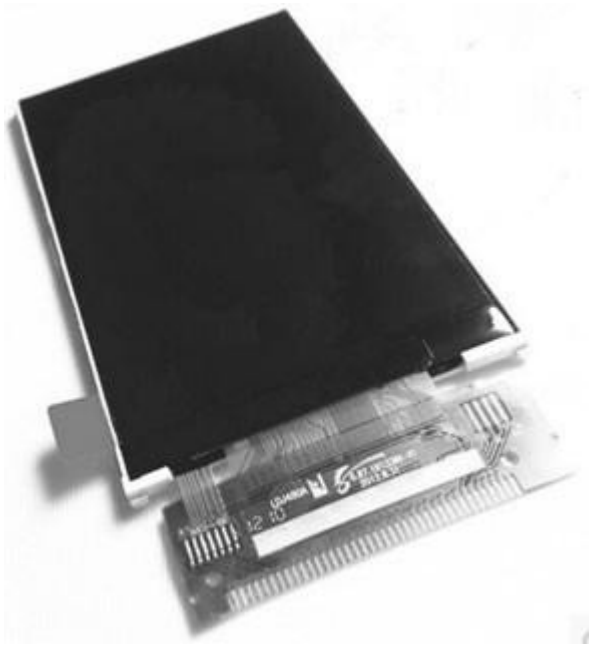

Figura 4. Foto do Módulo LCD ILI9327.

4.3. Placa de interface da conexão do CC3200 LaunchPad com o LCD

A conexão do LCD com a placa CC3200 se dá por uma interface desenvolvida para este protótipo. A interface faz a ligação dos pinos conforme a tabela 1. Nas figuras 5 e 6, podem-se observar, respectivamente, o esquemático e o *layout* da placa desenvolvida.

Periférico	Pinos	Pinos GPIO do LaunchPad
LCD - dados	D0 ~ D7	08 ~ 15
LCD - semáforos	Reset, CS, RS, RW e RD	00, 02, 05, 06 e 30
TouchScreen	02 e 03	03 e 04
Relé	-	23
Buzzer	-	28
Pinos IO livres	1 e 2	01 e 25
RFID	Entrada PWM e Saída de sinal	17 e 24
HardReset	-	22

Tabela 1. Conexão entre a LaunchPad e seus periféricos.

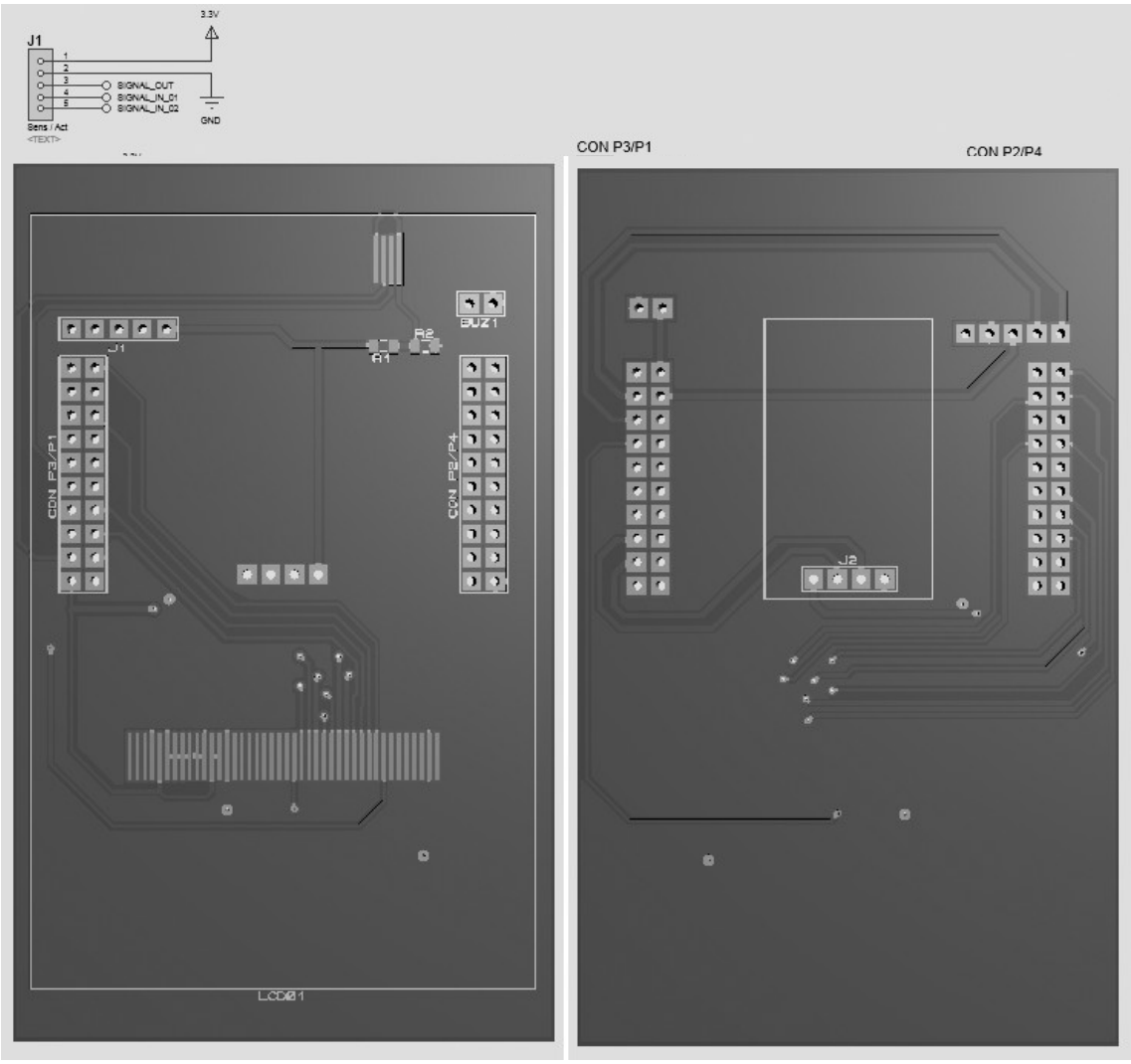

Figura 6. Visão 3D da placa Interface.

4.3.1. Relé

Nesta placa, há um relé que é responsável por acionar a tranca da porta. Este relé tem dois estágios, um normalmente aberto (NA), o que significa que seu circuito só é fechado quando o relé é acionado, e um normalmente fechado (NF), que tem seu circuito fechado enquanto o relé não for acionado, podendo ser utilizado o que for mais

conveniente dependendo da tranca adotada. Podemos adotar trancas que funcionem com pulso para abrir e, desta forma, serão ligadas a porta NA ou trancas que necessitem estar sempre com corrente, como trancas magnéticas e que serão ligadas à porta NF, pois precisam que o pulso cesse para que sejam acionadas.

4.3.2. Portas IO

Contamos com duas portas de entrada e saída (IO) destinadas ao uso com sensores digitais para, por exemplo, saber se a porta está fechada ou se há alguma presença no interior de um ambiente.

4.3.4. Botão *HardReset*

Este botão é responsável por resetar as configurações básicas para o padrão pré-instalação, para o caso, por exemplo, de a configuração do servidor ser corrompida, o que impossibilitaria a comunicação entre a fechadura e o servidor, inviabilizando a operação do aparelho instalado. Para resetar a configuração, será necessário retirar todas as fontes de energia da tranca e religar com o botão pressionado, de tal modo que a tranca reiniciará e, percebendo o botão pressionado, irá restaurar os padrões de fábrica, entrando em modo de configuração para que entrem os dados básicos, como chaves de segurança e endereço do servidor.

4.3.5. Buzzer

Buzzers são dispositivos que convertem energia elétrica em som (transdutor).

Neste trabalho, o *buzzer*, como se vê na Figura 7, é utilizado para emitir sinais sonoros de avisos do sistema, como, por exemplo, para alertar que os dados digitados estão incorretos ou que a fechadura entrou em modo *off-line* por estar há muito tempo sem receber resposta do servidor.

Figura 7. Foto de um *buzzer*.

4.4. Módulo RFID

Este módulo é responsável por ler as informações contidas no dispositivo RFID [Viera et al 2007] e enviá-las ao controlador para decodificar e validar os códigos contidos nela. Nas Figuras 8 e 9, podem-se ver o esquemático e o *layout* da placa, respectivamente.

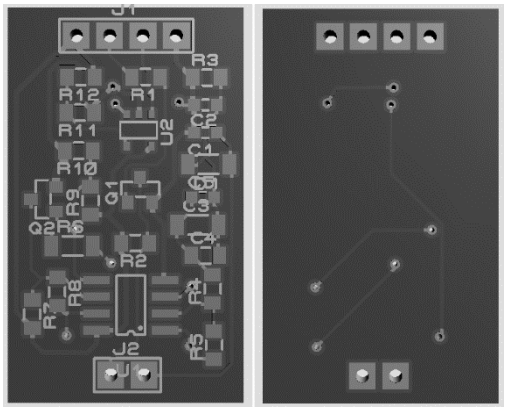

Figura 8. Esquemático do módulo RFID.

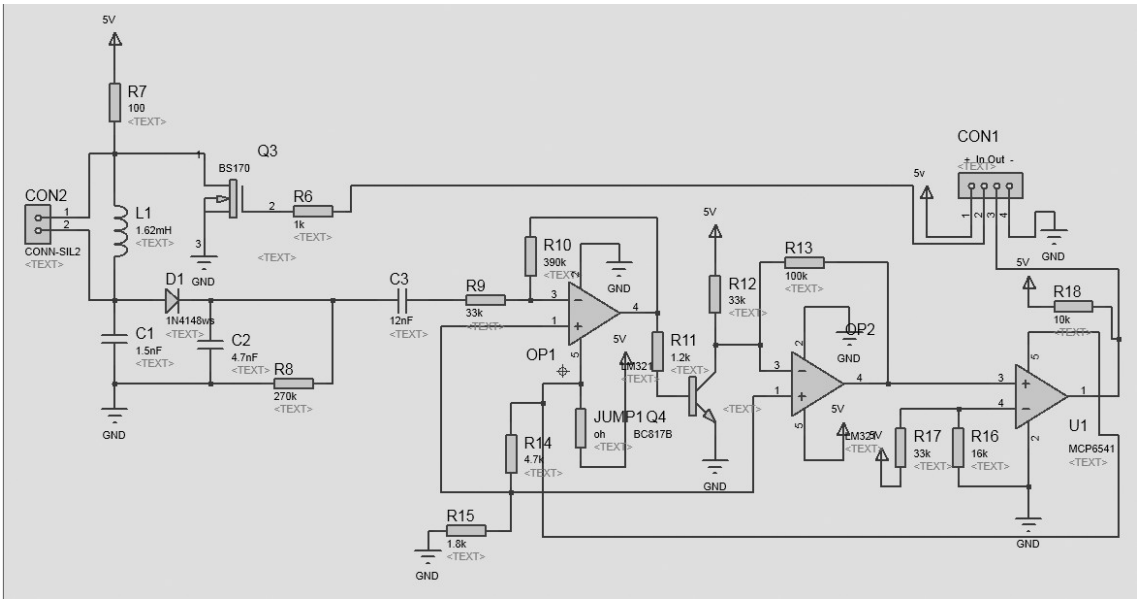

Figura 9. Visão 3D da placa do módulo RFID.

O módulo RFID possui uma antena em forma de bobina que gera um campo eletromagnético. Ao aproximarmos o dispositivo RFID do módulo, o circuito do dispositivo RFID é alimentado pela corrente induzida produzida pela bobina, e causa distorções no campo eletromagnético gerado. Essas distorções são utilizadas para modular informações contidas no dispositivo RFID. Este módulo foi projetado para usar o protocolo EM4100 [Design 2007]**.**

A fim de melhorar o *layout* do equipamento, optou-se por uma antena/bobina retangular nas exatas dimensões do LCD, economizando espaço e tornando mais prática a sua utilização, pois, dessa forma, aproximamos o dispositivo RFID do LCD para efetuarmos a leitura das informações nele contidas.

Para a confecção da antena, foi utilizado um fio esmaltado de 0,3 mm enrolado em uma base plástica de 6,0 x 8,7 x 0,3 cm (Largura x Comprimento x Altura – dimensões do LCD). Para calcularmos o número de espiras na bobina, utilizamos a Expressão 1 [Lee 2003], onde x, y e h são, respectivamente, largura, comprimento e altura da bobina, b é a espessura e L a indutância resultante.

Como colocou-se o LCD no interior da bobina, e a fórmula vista na expressão 1 foi concebida para bobinas sem núcleo, foi feito um ajuste empírico e chegamos a uma bobina com 85 voltas para gerar aproximadamente 1600uH (micro Henry) necessários para um funcionamento satisfatório do equipamento, com aproximadamente 100% de leituras corretas quando o dispositivo RFID é colocado a menos de 3cm da bobina.

$$L = \frac{0.0276\left((x+y+2h)N\right)^2}{1.908(x+y+2h)+9b+10h} \text{ em (uH)}$$

Expressão 1. Fórmula para cálculo da antêna do módulo RFID.

4.5. Tranca

Neste trabalho, utilizou-se uma tranca eletromagnética que não inutilize o sistema atual de segurança da porta, conforme pode-se observar na Figura 10. Assim, mantem-se a estrutura atual, somente acrescendo a nova forma de ingresso aos ambientes. A opção por este modelo em particular deu-se pela facilidade de encontrá-lo em lojas de ferragens e pelo seu baixo custo.

As fechaduras eletromagnéticas são atualmente amplamente utilizadas em ambientes com necessidade de fácil abertura, como portas de prédios residenciais. São adaptadas facilmente para utilização com sistemas de interfone, de forma a poderem ser acionadas a distância, de dentro dos apartamentos.

Figura 10. Foto de uma tranca eletromagnética.

5. Segurança

O aspecto de segurança é parte importante na adoção de sistemas computacionais de forma geral. No caso deste sistema, a segurança também é um dos objetivos a se alcançar.

Alguns dos conceitos de segurança da informação devem ser adotados para que se considere o sistema seguro. São eles: confidencialidade, integridade, disponibilidade e autenticidade. A confidencialidade limita o acesso à informação somente àqueles autorizados. A integridade garante que a informação, ao ser manipulada, não terá seu teor alterado, ou será provida uma rastreabilidade das mudanças. A disponibilidade garante que a informação estará sempre disponível aos autorizados. A autenticidade garante que o remetente da mensagem é realmente quem alega ser. No projeto apresentado, utilizou-se algoritmos de criptografia para atingir todos esses objetivos.

Como utilizamos comunicação sem fio e, portanto, os sinais estão “no ar”, disponíveis para qualquer pessoa que possua um receptor, a segurança baseada em criptografia torna-se ainda mais importante [Molisch 2011].

Além da criptografia de conexão WPA2, implementada em sistemas *Wi-Fi*, será utilizado o algoritmo de criptografia RC4, por ser computacionalmente leve e, portanto, bastante adequado para utilização com microcontroladores. O RC4 é um algoritmo de criptografia simétrica, ou seja, utiliza a mesma chave para criptografar e decifrar o código gerado. Consequentemente, supondo-se que os equipamentos envolvidos (servidor e fechadura) são mantidos seguros, a comunicação também o será.

Supondo a possibilidade de roubo de uma fechadura para análise e posterior tentativa de invasão, temos algumas possibilidades de defesa: O CC3200 possui um modo de operação que inviabiliza a leitura da memória interna por dispositivos externos, o que dificulta bastante a inspeção do código embarcado na busca por falhas de segurança, além disso, é de fácil implementação um dispositivo que apague todas as informações sensíveis caso o gabinete do equipamento seja aberto, conectando um sensor em uma das portas de uso genérico disponíveis.

6. Conclusão

O sistema projetado é voltado principalmente para o controle de um conjunto de fechaduras de instituições que necessitem de regras versáteis para abertura, independente do *hardware*. Os critérios encontram-se totalmente inseridos em um servidor que pode ser construído praticamente em qualquer ambiente computacional por utilizarmos padrões amplamente difundidos na indústria de *software* (*WebService*, SOAP, TCP/IP, dentre outros).

Foi construído um protótipo para demonstração da viabilidade da ideia. Embora o protótipo seja composto por circuitos genéricos e tenham sido implementadas apenas algumas das funcionalidades descritas neste documento, serve como base para a construção de um projeto de circuitos que atendam mais especificamente aos requisitos e a novas funcionalidades.

O *software* embarcado foi escrito preocupando-se com os principais conceitos de segurança vigentes e pode perfeitamente ser reutilizado para uma versão de produção do *hardware*.

7. Trabalhos Futuros

O protótipo construído não prevê uma fonte de alimentação própria. Em caso de falha da alimentação principal, o sistema ficará inoperante, podendo o ambiente ser acessado utilizando-se a chave convencional para abertura da porta. Uma extensão importante do *hardware* seria a incorporação de uma fonte de energia secundária (bateria) para a eventualidade de falha na fonte primária.

Há ainda a expectativa de que este trabalho seja estendido e incorpore outras formas de identificação como, por exemplo, identificação biométrica. Para tanto, necessitaríamos de alterações no *hardware* e no *software*.

O *software* pode facilmente ser adaptado para outras funções além da simples abertura condicional das fechaduras. Com pequenas adaptações, pode-se utilizar o sistema para ponto eletrônico, controle de ronda de vigias, controle de presença de alunos e para várias outras funções.

Referências

Booth, David (2004) "*Web Services Architecture*", W3C, https://www.w3.org/TR/ws-arch/, Acesso: janeiro/2016

Design, Priority 1 (2007) "*EM4100 Protocol description*". Disponível: http://www.priority1design.com.au/em4100_protocol.html. Acesso: agosto/2015.

Lee, Youbok (2003) "*Antenna Circuit Design for RFID Applications*" Revisão C, Microchip. Disponível: http://ww1.microchip.com/downloads/en/AppNotes/00710c.pdf. Acesso: agosto/2015.

Lockitron. Disponível: http://www.lockitron.com. Acesso: janeiro/2016.

Modesto, André Luiz; Sirotheau, Rafael de David (2006) "Sistema de Segurança Microcontrolado", Instituto de Estudos Superiores da Amazônia.

Molisch, Andreas F (2011) "*Wireless Communications*". 2ª Ed. Nova York, Wiley.

Nascimento, Rodrigo (2015) "O que, de fato, é internet das coisas e que revolução ela pode trazere?", http://computerworld.com.br/negocios/2015/03/12/o-que-de-fato-e-internet-das-coisas-e-que-revolucao-ela-pode-trazer. Acesso: janeiro/2016.

Nunes, Rafael Augusto Reis; Souza, Carlos Diego Pôjo de Brito; Neto, José Romualdo Carneiro de Figueiredo (2007) "Desenvolvimento de um sistema microcontrolado para segurança de prédios", Instituto de Estudos Superiores da Amazônia.

Oliveira, Andréa G. de; Anjos, Gisele B. dos; Lima, Wellington José F. (2012) "Sistema de Gerência Centralizada de Fechaduras Microcontroladas", Seminários de Trabalho de Conclusão de Curso do Bacharelado em Sistemas de Informação.

Pacheco, Tatiane Martins (2016) "Sistema de Gerência Centralizada de Fechaduras Microcontroladas", Seminários de Trabalho de Conclusão de Curso do Bacharelado em Sistemas de Informação.

Viera, Angel Freddy Godoy et al (2007) “Tecnologia de Identificação Por Rádio Frequência: fundamentos e aplicações em automação de bibliotecas”, R. Eletr. Bibliotecon. Ci. Inf., Florianópolis, n. 24, p. 183-202.

Rosen, Kenneth H. (2012) “*RC4 Stream Cipher and It´s Variants*”, Discrete Mathematics and its Applicationsl, Series Editor.

SmartLock. Disponível: http://august.com/products/august-smart-lock/. Acesso: janeiro/2016.