Revista Eixos Tech
e-ISSN: 2359-1269 | DOI: 10.18406/2359-1269
V. 5 | N° 2 | 2018

Sistema de controle de acesso utilizando Arduino e Android

Gabriel Morais Silveira. IFSULDEMINAS – campus Inconfidentes. E-mail: gabrielmorais72@gmail.com

Italo de Rezende. IFSULDEMINAS – campus Inconfidentes. E-mail: italoeji@hotmail.com

Igor Oliveira Lara. IFSULDEMINAS – campus Inconfidentes. E-mail: igor.lara@ifsuldeminas.edu.br

Resumo. O uso de chaves em fechaduras por muitas vezes pode se tornar incômodo e inseguro. É de conhecimento geral que uma chave comum é algo que pode ser clonado por diferentes métodos. Além disso, outros dispositivos de segurança como keypads e cartões magnéticos, podem ser ineficientes, inseguros e caros. Com isso um mecanismo (tendo como base o microcontrolador Arduino) foi desenvolvido para facilitar e proporcionar de forma simples gerenciamento e controle do acesso a ambientes, de forma que o mecanismo trabalhe em conjunto com um smartphone, onde é realizada uma verificação com duas possibilidades, utilizando um mecanismo biométrico de autenticação ou um mecanismo lógico (PIN/senha).

Palavras-chave: Chave. Microcontrolador. Biometria. Smartphone.

INTRODUÇÃO

Embora nos dias de hoje as pessoas vivam em uma era digital, ainda existem mecanismos que não utilizam da tecnologia disponível para o aprimoramento de suas funções. Um exemplo são as chaves físicas que praticamente não evoluíram desde o mecanismo lançado em 1840 pelos britânicos Robert Barron e Joseph Bramah, baseado em molas e cilindros (Cordeiro, 2017).

Atualmente existe um número massivo de chaves para tudo que se possa acionar, abrir e fechar todos os dias, como as portas de casas e carros, alarmes, entre outros. Dentre as diversas vertentes de chaves existem diversos dispositivos, vários não são tão seguros como aparentam ser ou não são economicamente viáveis.

As chaves físicas atualmente utilizadas são incômodas e barulhentas e podem facilmente ser perdidas, roubadas, adulteradas e copiadas. Mesmo quando são escolhidas vertentes mais modernas de chaves, como fechaduras eletrônicas, ainda existem barreiras como o preço, segurança e praticidade. A tabela 1 mostra a comparação do projeto com alguns dos mecanismos já existentes no mercado:

Tabela 1 – Análise dos concorrentes

	Projeto	Bloqueio de Teclado	Cartões Magnéticos
Prós:	-Fácil gerenciamento. -Preço acessível. -Maior segurança com filtro MAC. -Pode ser utilizado em qualquer ambiente.	-Bom para ser usado em hotéis. -Os hóspedes não são bloqueados caso não tenham uma chave física.	-Pode ser desativado caso perca ou seja roubado. -Bom para ser usado em hotéis.
Contras:	-Difícil aceitação do público, pois ainda é um projeto novo e em fase de testes.	-O código de acesso pode ser descobertos por terceiros.	-O chip do cartão pode ficar sujo e parar de funcionar. -O cartão quebra facilmente por ser de plástico.
*Preço médio:	**R$180,00	R$800,00	R$550,00
1 *Média de preços feita com base nos preços encontrados no site: https://www.buscape.com.br/.			
2 **Média feita a partir dos componentes comprados para montagem do projeto.			

Fonte: Elaborada pelos autores.

Esse projeto desenvolve uma solução para esses problemas expostos, sendo executada a criação de um aplicativo móvel para smartphones, com controle e segurança lógica, e uma fechadura física junto com uma placa microcontroladora Arduino para bloqueios e desbloqueios de portas. O projeto também pode ser implementado em qualquer ambiente desde que o ambiente utilize chaves e possa ser automatizado.

No projeto foi desenvolvido um aplicativo que faz o cadastro do usuário, tendo ele duas opções, a biometria e o padrão, que pode ser caracterizado como uma espécie de desenho (caso o usuário não deseje a biometria ou o celular não seja compatível). Após esse cadastro, o usuário irá fazer o pareamento com a placa arduino que controla a fechadura, assim então podendo abrir a porta desejada.

Além da identificação biométrica (dermatoglifia) ou uso do padrão, outros métodos de segurança foram testados e utilizados, como um cadastro do endereço físico do *smartphone* (endereço MAC Bluetooth) pelo aplicativo, ou por uma página WEB

(que foi feita como uma solução em caso de perda ou roubo do *smartphone*). Diretivas básicas de segurança da informação no uso de senhas serão avisadas aos usuários, assim como a periodicidade nas trocas de senhas.

Outra contribuição relevante, além da possibilidade de oferecer uma solução para os problemas relacionados à acessibilidade e controle de acesso de dispositivos e ambientes com uso de chaves físicas, é proporcionar aos envolvidos a chance de aplicar e desenvolver conhecimentos relacionados à automação básica e ao uso do Arduino, ao desenvolvimento de aplicativos para dispositivos móveis e à aplicação de princípios e teorias da segurança da informação de modo prático.

FUNDAMENTAÇÃO TEÓRICA

Foi utilizado para esse projeto o microcontrolador arduino, que segundo a definição do site oficial, é uma plataforma de prototipagem eletrônica open-source que se baseia em hardware e software flexíveis e fáceis de usar. É destinado a artistas, designers, hobbistas e qualquer pessoa interessada em criar objetos ou ambientes interativos (Arduino, 2017), desta definição, pode-se abstrair que a plataforma Arduino foi criada para facilitar o desenvolvimento de vários tipos de projetos eletrônicos, podendo ser utilizada em várias áreas. Seus criadores foram Massimo Banzi, David Cuartielles, Tom Igoe, Gianluca Martino e David Mellis.

O Arduino possui características próprias, como uma interface de desenvolvimento e o uso de microcontroladores específicos. Segundo a descrição do site oficial do projeto, o microcontrolador na placa é programado com a linguagem de programação Arduino, baseada na linguagem Wiring, e o ambiente de desenvolvimento Arduino, baseado no ambiente Processing (Simula um caderno de notas e uma linguagem de comunicação no contexto de artes visuais). Os projetos desenvolvidos com o Arduino podem ser autônomos ou podem comunicar-se com um computador para a realização da tarefa, com uso de software específico (ex: Flash, Processing, MaxMSP) (Arduino, 2017).

O meio de transmissão é o Bluetooth, uma tecnologia de transmissão de dados local e sem fio definida no padrão IEEE 802.15. O protocolo é amplamente difundido atualmente, sendo utilizados em smartphones de todas as faixas de preço, desde os mais simples até os mais complexos, e com o passar dos anos seu alcance foi melhorado. Conforme descrito em IEEE (2005) o bluetooth pode interoperar entre diferentes plataformas.

Segundo Costa (2001), a biometria pode ser expressa de duas formas, sendo a primeira por identificadores fisiológicos que incluem impressões digitais, geometria de mão, retina, características faciais e formato de unha. Enquanto a segunda forma consiste em identificadores de procedimento onde destaca-se a voz e a assinatura.

Análise do reconhecimento de voz e assinatura geralmente são considerados menos conclusivos porque eles estão sujeitos a limitações devido a enfermidades ou imitações.

Impressão digital é a captação das linhas da impressão digital por meio de um leitor biométrico que impulsiona o sistema a compará-lo com seu banco de dados. Hoje em dia tem sido o meio mais viável, pois é o que oferece melhor segurança pelo menor preço. Por este motivo a biometria foi escolhida para este projeto. Além dessas características a impressão digital é o meio mais rápido dentre os outros tipos de biometria, palavra que tem origem do grego, *bios* (vida) e *metron* (medida) e pode ser caracterizada como um meio de reconhecimento individual a partir de medidas biológicas. A seguir será exemplificado o funcionamento da biometria de impressão digital com um trecho em texto do livro Handbook of Fingerprint Recognition (MALTONI; MAIO; JAIN; PRABHKAR, 2003) e de Costa (2001).

Figura1 – Biometria e impressão digital

Fonte: <http://www.linhadecodigo.com.br/artigo/1162 /biometria-processamento-de-imagens-capturadas-em-leitores-de-impressao-digital.aspx>. Modificado. Acesso em 24 abril de 2017.

A análise consiste em verificar posição das minúcias, tais com bifurcações e terminações dos sulcos, e também verificar os arcos e voltas que aparecem no dedo (demonstradas na figura 1), utilizando para isso algoritmos. Grande parte dos algoritmos trabalha com o princípio de extração dos pontos de minúcias ou pontos característicos. Após a extração, são calculadas as relações entre as distâncias desses pontos; cada algoritmo possui a sua base de cálculo, seja por análise dos pontos em si ou por agrupamentos de pontos para análise de semelhanças de triângulos com os ângulos internos (MALTONI; MAIO; JAIN; PRABHKAR, 2003).

As aplicações das impressões digitais destinam-se ao aumento de segurança e agilidade em operações empresariais, governamentais ou institucionais, tais como: Forças Armadas, governo, repartições públicas, transações eletrônicas, controle de ponto, controle de acesso e presença (COSTA, 2001).

O dicionário de Cambridge diz que *smartphone* é “um telefone móvel que pode ser usado como um pequeno computador e que se conecta a internet” (CAMBRIDGE, 2017), e segundo a Fundação Getúlio Vargas, o uso de *smartphone*s no Brasil só tende a aumentar, como se pode ver na tabela 2, representada abaixo.

Tabela 2 – Uso de dispositivos informáticos

Data	Tipo de Dispositivo	Dispositivos em uso	Densidade (Dispositivos em uso/ Habitantes)
Maio/2018	Computadores*	174 milhões	5 computadores para cada 6 habitantes.
Maio/2018	Dispositivos conectados a internet	394 milhões(Computadores 174 milhões, Smarphones 220 milhões)	1,9 dispositivo por habitante.
2019	Dispositivos conectados a internet	420 milhões(Computadores 185 milhões, Smarphones 235 milhões)	2 dispositivos por habitante
Maio/2018	Dispositivos Móveis**	306 milhões(Móveis 86 milhões, Smarphones 220 milhões)	1,5 dispositivo por habitante.
*Desktops, notebooks e tablets.			
**Notebooks e tablets.			
Fontes: Fundação Getúlio Vargas-EAESP-GVcia, Anatel, CGI.br, IBGE, Cartner, IDC, ITU, Teleco e World Bank.			

Modificado e disponível em:
<https://eaesp.fgv.br/sites/eaesp.fgv.br/files/pesti2018gvciappt.pdf>.
Acesso em 18 de Maio de 2018.

Segundo termo definido pela IBM (2017) “Android é a plataforma de computador e comunicações remota e *wireless* frequentemente discutida da Google.”, como visto em Gartner (2018) o Android é um dos sistemas mais utilizados no mundo. Nosso projeto visa desenvolver uma aplicação para essa plataforma. Utilizaremos a interface de desenvolvimento oficial do sistema, o Android Studio, que utiliza as lin guagens Java, C e C++.

Uma pesquisa publicada por Phil Nickinson (2016) e traduzida por Renato Santino (2016), demonstra que os leitores de impressão digital estão melhorando a segurança do sistema Android por causa de sua agilidade. Com base nessa pesquisa, a

implementação desse tipo de segurança em portas de residências ou de hotéis, pode ser bem aceita pelas pessoas, além de oferecer uma segurança maior:

O relatório do Google compara os aparelhos da família Nexus. Os modelos 5x e 6p (de 2015) tem um uso 64% maior de telas de bloqueio do que os modelos 5 e 6 (de 2013 e 2014, respectivamente). Nestes modelos mais recentes, a tela de bloqueio está ativada em 91% dos casos (SANTINO, 2016).

O detalhe, discretamente incluído no documento que analisa a segurança do Android em 2015 mostra que, se as ferramentas forem simples, o público está disposto a se proteger. Bloquear a tela do celular é a medida mais básica de segurança do dispositivo que pode ser tomada, e todos deveriam fazê-lo, mas as senhas, padrões e PINs ainda deixavam muitos inseguros em relação ao custo e benefício de ter que destravar o aparelho a cada vez que querem abrir um aplicativo. O leitor de impressão digital, felizmente, elimina boa parte do atrito neste processo, incentivando as pessoas cuidar melhor de suas informações (SANTINO, 2016).

Atualmente, dados e informações são gerados e armazenados de maneira prática e rápida, porém estão sujeitos a diversos tipos de manipulações e furtos por parte de terceiros, e para se proteger dessas ameaças existe a modalidade de segurança da informação. Segundo Peltier (2001), o propósito do programa de segurança da informação é proteger os preciosos recursos de informação de uma empresa. Entre a seleção e aplicação de apropriadas políticas, padrões e procedimentos, um programa de segurança universal ajuda a empresa a estabelecer seus objetivos empresariais (...) são necessárias políticas, padrões e procedimentos bem escritos (PELTIER, 2001, p.13).

Em um artigo científico sobre os cinco últimos anos de pesquisa em biometria foi constatado que segundo Oliveira e Santos (2015), acredita-se que, com a necessidade de maior segurança em eventos importantes que ocorreram e ocorrerão no Brasil, tais como Olimpíadas, Copa do Mundo e Eleições, é um grande incentivo para novas pesquisas e aplicações de sistemas biométricos (OLIVEIRA; SANTOS, 2015).

MATERIAL E MÉTODOS

Os materiais utilizados foram voltados a montagem da parte física do projeto e do aplicativo desenvolvido no Android Studio, fazendo com que ele seja disponível para qualquer aparelho que possui sistema operacional Android. Segue a tabela dos materiais (tabela 3), a ilustração dos materiais utilizados e em baixo de cada figura uma breve explicação sobre ele (Figuras de 2 a 11):

Tabela 3 – Tabela dos materiais utilizados

1	Módulo bluetooth HC-05	1
2	Fonte 12 voltz	2
3	Modulo Rele	1
4	Protoboard	1
5	Kit Resistores 2K	1
6	Kit Jumpers	1
7	Arduino Uno R3	1
8	Mini Trava Solenoide	1

Fonte: Elaborada pelos autores.

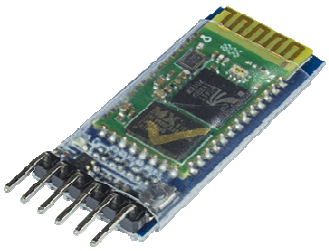
Figura 2 – Fechadura Eletrônica

Fonte: <https://images-americanas.b2w.io/produtos/01/00/sku/8648/8/8648810SZ.jpg>. Acesso em: 18 de Maio de 2018.

A fechadura foi utilizada para demonstrar o acionamento remoto e sem fios do mecanismo, sendo ela um meio visual de autenticação e a base do projeto, visto que

precisamos de uma fechadura elétrica para o acionamento da mesma pelo aplicativo. Em termos práticos a fechadura está conectada a um relé, que por sua vez é gerenciado pelo arduino, desta forma, podemos controlar em quais momentos o relé será acionado/desativado e por quanto tempo (Figura 2).

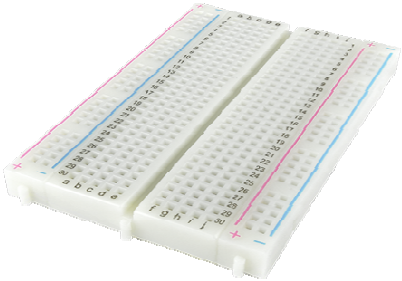
Figura 3 - Módulo Bluetooth HC-05



Fonte: <https://s3-sa-east-1.amazonaws.com/robocore-lojavirtual/1025/images/1025_1_H.png?20180515115424>. Acesso em 18 de Maio de 2018.

O módulo *bluetooth* é um dos itens essenciais do projeto, ele permite a conectividade sem fio de maneira simples, com um custo menor e de maneira ágil, não consumindo tantos recursos do arduino e podendo ser amplamente explorado. Com ele conseguimos fazer o controle de MAC, usando um controle lógico no arduino e no smartphone (Figura 3).

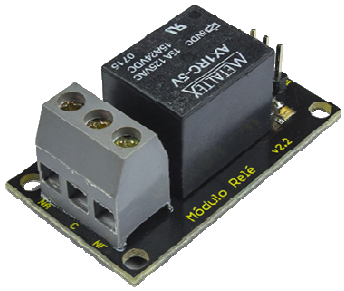
Figura 4 - Protoboard



Fonte: <https://s3-sa-east-1.amazonaws.com/robocore-lojavirtual/985/images/985_1_H.png?20180515164049>. Acesso em 18 de Maio de 2018.

Ferramenta de prototipagem utilizada para conexões rápidas e testes de eletrônica. Foi utilizada para interligar o arduino aos módulos e para controlar a tensão do módulo *bluetooth* (Figura 4).

Figura 5 – Módulo Relé



Fonte: <https://s3-sa-east-1.amazonaws.com/robocore-lojavirtual/258/images/258_1_H.png?20180509122404>. Acesso em 18 de Maio de 2018.

O relé é um componente eletrônico utilizado para abrir e fechar circuitos. Foi utilizado para o acionamento da fechadura elétrica (Figura 5).

Figura 6 – Fonte Chaveada

Fonte: <https://s3-sa-east-1.amazonaws.com/robocore-lojavirtual/533/images/533_1_H.png?20180426170337>. Acesso em 18 de Maio de 2018.

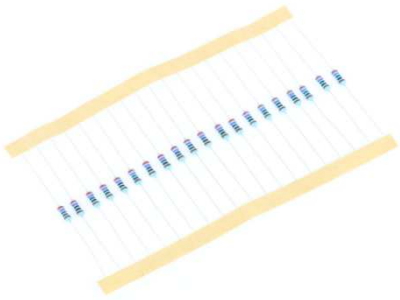
Fonte de 12 volts e 1 ampere utilizada para fornecer energia ao arduino e/ou fechadura (Figura 6).

Figura 7 - Jumpers

Fonte: <https://www.filipeflop.com/wp-content/uploads/2017/09/IMG_5106.png>. Acesso em 18 de Maio de 2018.

Utilizado para conectar componentes e módulos a *protoboard*. Foram utilizados tanto conectores macho-macho quanto macho-fêmea (Figura 7).

Figura 8 - Resistores

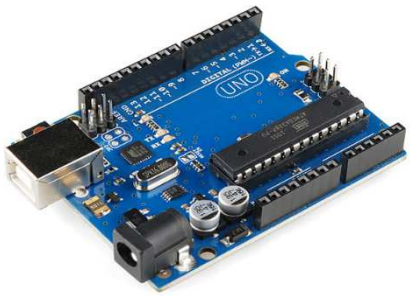


Fonte: <https://www.filipeflop.com/wp-content/uploads/2017/07/Resistor_270R.png>. Acesso em 18 de Maio de 2018.

Componentes utilizados para controlar a tensão/corrente de dispositivos eletrônicos (Figura 8).

Revista Eixos Tech
e-ISSN: 2359-1269 | DOI: 10.18406/2359-1269
V. 5 | N° 2 | 2018

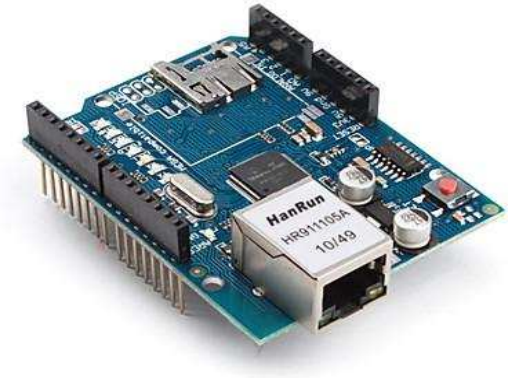
Figura 9 - Arduino Uno



Fonte: <https://www.filipeflop.com/wp-content/uploads/2017/07/Arduino_Uno_R3.png>. Acesso em 18 de Maio de 2018.

Foi o modelo de arduino utilizado no projeto por ser amplamente conhecido, de fácil desenvolvimento e ter um custo acessível, fazendo com que o valor final do projeto tenha um custo reduzido. Com ele foi possível controlar os componentes eletrônicos pela linguagem de programação C/C++ (Figura 9).

Figura 10 – Ethernet Shield



Fonte: <http://luthortronics.com.br/wp-content/uploads/2015/10/qnfgjz1339666028684.jpg>. Acesso em 18 de Maio de 2018.

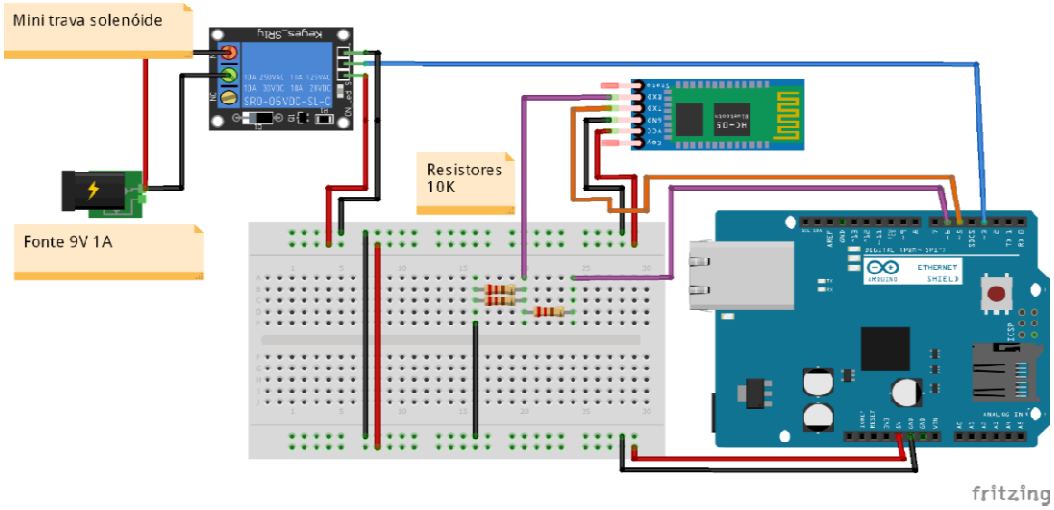
É um módulo disponível para Arduino que faz com que a placa microcontroladora possa ter conexão com a rede local e com a internet, com ela podemos acessar sites externos e montar um servidor web local por exemplo. O projeto a utilizou para criar um *WebServer* capaz de enviar comandos ao microcontrolador através de uma interface simples e assim gerenciar os componentes (Figura 10).

Revista Eixos Tech
e-ISSN: 2359-1269 | DOI: 10.18406/2359-1269
V. 5 | N° 2 | 2018

O projeto foi dividido em etapas, sendo que a primeira consistiu em pesquisas exploratórias sobre o funcionamento do Arduino, desenvolvimento de aplicativo para o sistema Android, eletrônica básica e conceitos de segurança da informação.

A segunda etapa ocorreu concomitante com a primeira e consistiu no começo do desenvolvimento do algoritmo responsável pelo gerenciamento e controle do dispositivo, além de montar o mecanismo físico (como no esquema a seguir) e o desenvolvimento do aplicativo para *smartphones* utilizando o Android Studio.

Figura 11 – Esquema elétrico



Fonte: Elaborada pelos autores.

Na terceira etapa foram pesquisados, durante o desenvolvimento do arduino, diversos métodos para realizar a comunicação entre o ele e a aplicação. Com isso foi encontrado um método para unir a simplicidade necessária para tornar a comunicação ágil e a funcionalidade de ter uma comunicação precisa usando métodos de comparação do que é recebido pelo módulo e o que é enviado pela aplicação. No desenvolvimento da parte física tomamos cuidado para entregar a corrente DC necessária em cada dispositivo para melhorar a longevidade dos componentes. Já no módulo bluetooth é necessário um cuidado especial, visto que tensões superiores podem danificar o aparelho fazendo com que ele não tenha conexão ao smartphone ou não receba os dados de maneira adequada, alterando assim um dos pilares da CID (Confidencialidade, Integridade e Disponibilidade), que devem ser mantidos a todo custo.

A quarta etapa foi a finalização do desenvolvimento da aplicação. Nesse processo para cada funcionalidade proposta foi feito um aplicativo externo para o estudo do desenvolvimento daquela função. No final, todo o conhecimento adquirido fazendo os aplicativos externos foram unidos em um único para deixá-lo com as funcionalidades desejadas.

A quinta etapa foi voltada a busca de falhas e erros no software e no hardware do esquema montado no arduino. Foram feitos vários testes para garantir a conectividade, a recepção correta dos dados transmitidos, a velocidade de recepção de dados, a distância e alguns testes de invasão que são amplamente descritos no relatório em anexo, ele envolveu buscas em portas de serviços oferecidos pelo servidor e tentativas de conexão utilizando senhas conhecidas.

A sexta etapa assim como a anterior serviu para a busca de falhas e erros, porém, desta vez, voltados ao aplicativo. Os testes foram feitos para garantir que o aplicativo não apresentasse erros em sua execução, fizesse um envio correto dos dados e cumprisse com as suas funcionalidades.

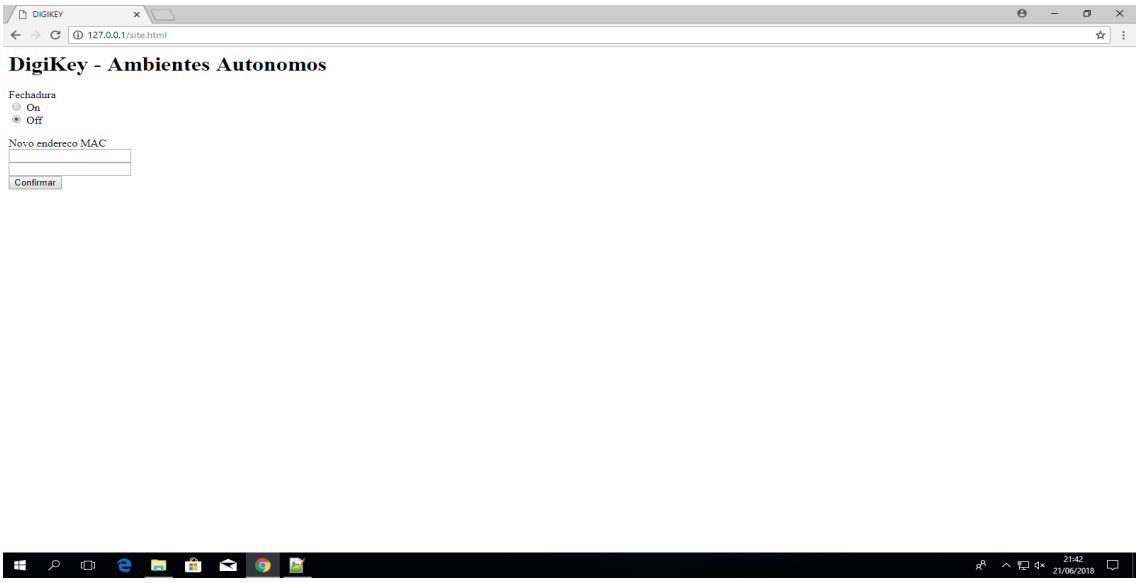
Na sétima etapa, com os testes das partes isoladas já feitas, o foco foi deixar um projeto apresentável, e fazer os testes com o público para garantir a facilidade de seu uso.

RESULTADOS E DISCUSSÕES

O projeto desenvolvido apresentou bons resultados. O acionamento da trava pelo aplicativo acontece de forma instantânea. A interface WEB é fluida e simples, podendo ser utilizada por qualquer usuário. Esta possui uma tela simples para fácil entendimento, como demonstrado na figura 12, possuindo apenas dois campos, sendo um para desligar e ligar o dispositivo e o outro para o envio de endereço físico, tendo tudo apresentado de maneira clara. Apesar dos bons resultados durante a execução do projeto foi percebido que o shield ethernet HANRUN tem grande elevação de temperatura durante o seu funcionamento, o que causa instabilidades após o uso prolongado entre compilações da sketch e acessos ao site, isto foi verificado manualmente. Como solução podem ser acoplados alguns dissipadores de calor. No algoritmo utilizado, o uso de variáveis no microcontrolador é grande, sendo assim o uso de recursos adicionais aos já oferecidos necessitam de algoritmos simplificados. Como exemplo a integração de fechaduras é um recurso interessante, porém necessita de mais poder de processamento e, consequentemente, variáveis.

Revista Eixos Tech
e-ISSN: 2359-1269 | DOI: 10.18406/2359-1269
V. 5 | N° 2 | 2018

Figura 12 – Site do projeto



Fonte: Elaborada pelos autores.

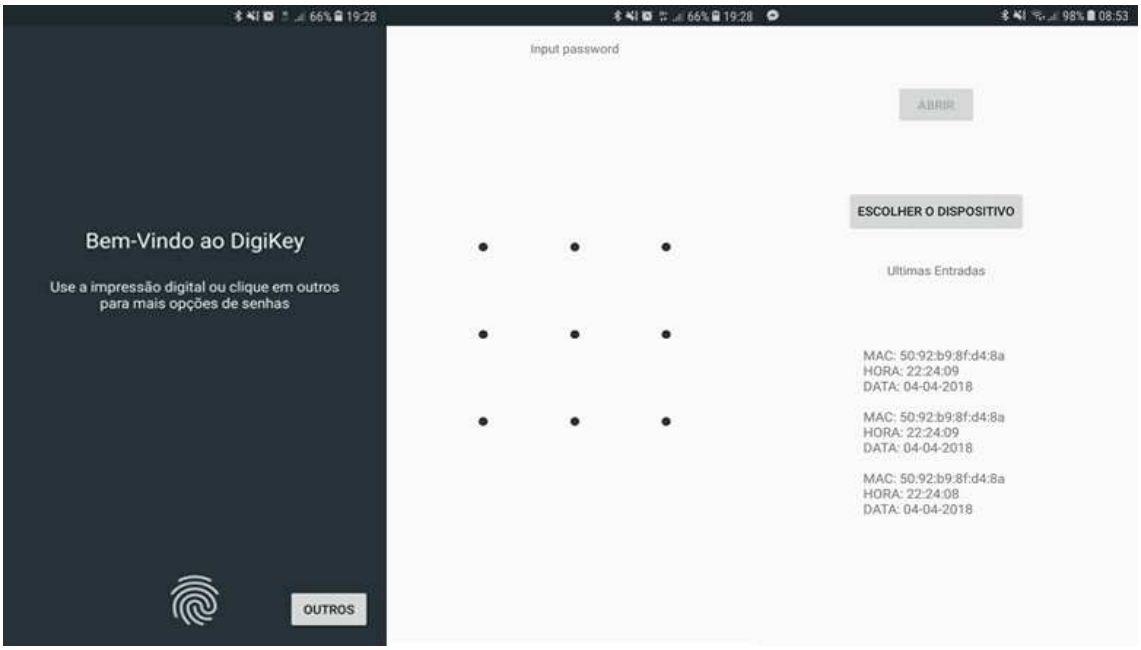
CONCLUSÕES

O objetivo do trabalho foi desenvolver tanto uma fechadura aliada a um microcontrolador que permitisse um acesso rápido, seguro e prático ao ambiente desejado, quanto um aplicativo utilizado no celular do usuário que utiliza a comunicação via Bluetooth para acionar a fechadura. Para garantir o alcance dos objetivo, foram realizados testes de tentativas de invasão à interface web e aos métodos de segurança apresentados pelo projeto, com os alunos do curso de Tecnologia em Redes de Computadores do Instituto Federal campus Inconfidentes. Eles usaram seus próprios métodos de tentativa de invasão como, ataque de força bruta, sniffer de pacotes de rede e engenharia social, entretanto nenhum foi bem sucedido. Durante essa série de testes não foram utilizadas ferramentas como exploits ou malwares, mas em contrapartida um *pentest* foi aplicado, e este demonstrou que o dispositivo não apresenta vulnerabilidades aparentes e a comunicação entre a aplicação e o Arduino não apresentou instabilidades. Além disso, o desenvolvimento da aplicação foi feito com base na opinião de usuários e foi elogiada durante os testes, garantindo assim a facilidade em seu uso. Contudo o dispositivo demonstrou ser promissor, tendo sua segurança forte, sua praticidade alta e seu custo atraente.

O aplicativo final apresentou as seguintes funcionalidades: uma tela de *login* para autenticação pela digital ou por padrão(desenho), uma segunda tela com um botão para abrir as opções de dispositivos *bluetooth* para se conectar, e nessa mesma tela, quando o dispositivo é escolhido, um botão para acionar o arduino, assim abrindo a fechadura, além de fazer o registro da última vez em que a fechadura foi aberta. A

figura 13 demonstra as telas de login e principal do aplicativo, com as funcionalidades descritas neste parágrafo:

Figura 13 – Telas do aplicativo



Fonte: Elaborada pelos autores.

REFERÊNCIAS

Arduino PLAYGROUND - HOMEPAGE. Ano: 2017. Disponível em: <http://playground.Arduino.cc/Portugues/HomePage> Acesso em: 24 Abril 2017.

CAMBRIDGE UNIVERSITY. Significado de "smartphone" no Dicionário de Inglês. Disponível em: <https://dictionary.cambridge.org/pt/dicionario/ingles/smartphone>. Acesso em: 26 nov. 2017.

CORDEIRO, Tiago. Como surgiu a chave? 2017. Disponível em: <https://mundoestranho.abril.com.br/ciencia/como-surgiu-a-chave/>. Acesso em:07 Jun. 2017.

COSTA, S. M. F. Classificação e verificação de impressões digitais. 2001. 123 f. Dissertação (Mestrado em Engenharia Elétrica) – Escola Politécnica, Universidade de São Paulo, São Paulo, 2001.

FARIA, Alexandre. BIOMETRIA: PROCESSAMENTO DE IMAGENS CAPTURADAS EM LEITORES DE IMPRESSÃO DIGITAL. Ano: 2017. Disponível em:<http://www.linhadecodigo.com.br/artigo/1162/biometria-processamento-de-imagens-capturadas-em-leitores-de-impressao-digital.aspx> Acesso em: 24 Abril 2017.

FUNDAÇÃO, Getulio Vargas. 27ª Pesquisa Anual do Uso de TI. Disponível em: <http://eaesp.fgvsp.br/sites/eaesp.fgvsp.br/files/pesti2016gvciappt.pdf>. Acesso em: 28 abr. 2017.

GARTNER (Org.). Gartner Says Worldwide Sales of Smartphones Recorded First Ever Decline During the Fourth Quarter of 2017: Worldwide Smartphone Sales to End Users by Operating System in 2017 (Thousands of Units). 2018. Disponível em: <https://www.gartner.com/newsroom/id/3859963>. Acesso em: 22 fev. 2018.

GOOGLE, Recursos do Android Studio | Android Studio. Disponível em: <https://developer.android.com/studio/features.html>. Acesso em: 28 abr. 2017.

IBM. Desenvolver Aplicações Android com o Eclipse. Disponível em: <https://www.ibm.com/developerworks/br/library/os-eclipse-android/>. Acesso em: 28 abr. 2017.

IEEE (Org.). IEEE 802.15 Working Group for Wireless Personal Area Networks. Disponível em: <http://www.ieee802.org/15/about.html>. Acesso em: 29 set. 2017.

MALTONI, D., MAIO, D., JAIN, A.K., PRABHAKAR, S., “Handbook of Fingerprint Recognition”, Springer, 2003.

NICKINSON, Phil. The most important news from the Android Security recap had nothing to do with malware. 2016. Disponível em:<http://www.androidcentral.com/most-important-news-android-security-had-nothing-do-malware>. Acesso em: 03 abr. 2017.

OLIVEIRA, Magda Vieira da Silva; SANTOS, Melina Rossi. ÚLTIMOS CINCO ANOS DE PESQUISA EM BIOMETRIA: UM ESTUDO DAS PRINCIPAIS UNIVERSIDADES NO BRASIL. Forscience: Revista científica do IFMG, Formiga, v. 2, n. 3, p.39-55, jul. 2015.

PELTIER, Thomas R. Introduction. In: PELTIER, Thomas R. Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. [S.l.]: Auerbach, 2001. p. 13-14. Disponível em: <https://books.google.com.br/books?id=mM_LsS-W4f4C&printsec=frontcover#v=onepage&q&f=false>. Acesso em: 28 abr. 2017.

SANTINO, Renato. Leitores de impressão digital estão melhorando segurança do Android. 2016. Disponível em:<https://olhardigital.uol.com.br/fique_seguro/noticia/leitores-de-impressao-digital-estao-melhorando-seguranca-do-android/57544>. Acesso em:03 abr. 2017.