Implementação de controle de acesso via Biometria e gestão de rotinas em ambientes microcontrolados

Rafael Ogayar Gomes[1], Alessandro André Mainardi de Oliveira[1]

[1]Centro Universitário Franciscano
Caixa Postal 97010-032 – Santa Maria – RS – Brasil

rafael.degomes@gmail.com, alessandroandre@unifra.br

Abstract. *The residential automation, increasingly present in daily life, aims to make life easier for users in repetitive tasks, thereby assisting in their activities. In this context, the work presented herein demonstrates the implementation of a fingerprint detection system for release of doors, carrying with it more safety and tranquility. In addition, the execution of activities registered by the user was developed to comfort and convenience of the user, thus bringing guidelines automation. Thereunto, the equipment used was an Arduino and biometric sensor interconnected in an Android application.*

Resumo. *A automação residencial, cada vez mais presente no cotidiano, tem como objetivo facilitar a vida de usuários em tarefas repetitivas, auxiliando assim em suas atividades. Neste contexto, o trabalho aqui apresentado demonstra implementação de um sistema de detecção de digitais para liberação de portas, trazendo com isto mais segurança e tranquilidade. Além disto, foi desenvolvida a execução de atividades cadastradas pelo usuário para melhor conforto e comodidade do mesmo, trazendo assim consigo diretrizes da automação. Para tanto, foram utilizados equipamentos como Arduino e sensor biométrico, interligados por uma aplicação Android.*

1. Introdução

A automação cada vez mais vem sendo utilizada em casas, escritórios e indústrias. Ela está baseada em três pontos: conforto, economia e segurança. Este último, é preocupação constante de boa parte da população, tanto no ambiente de trabalho como em suas residências.

Existem diversas soluções para que se tenha esse controle de acesso, um dos métodos utilizados é o reconhecimento biométrico, que pela implantação de um sistema que detectam a impressão digital é possível identificar digitais não reconhecidas entre as de indivíduos autorizados [Mocellin et al 2013].

A capacidade dos computadores reconhecerem pessoas é uma atividade que está sendo utilizada em diversos lugares, a impressão digital é uma delas, cada pessoa tem sua identificação através de suas diferenças. Através desses fatores é possível diferenciar cada indivíduo, podendo assim ser utilizado por exemplo em uma abertura de porta através da digital.

Pessoas tem suas rotinas em suas residências, e muitas vezes não conseguem cumpri-las, sendo por falta de tempo, dificuldade na realização, entre outros. Uma das

maneiras para melhor suprir essa necessidade um sistema de gestão de rotinas é uma ótima opção pois além de notificar o que deve ser feito também pode ser efetuado pelo sistema.

1.1. Justificativa

Há locais onde não se pode liberar acesso a qualquer indivíduo, por exemplo em uma residência, onde só deve ter acesso moradores ou convidados, pois a violência vem sendo a preocupação das pessoas, com isso, através de um sistema de biometria se pode ter registros de pessoas que podem ou não ter acesso trazendo assim mais segurança ao ambiente.

A facilidade com que o usuário final da tecnologia está utilizando a biometria demonstra o seu potencial para a expansão dessa área, do ponto de vista do cliente o uso dessa tecnologia é intuitivo e atende as necessidades. [Santos C. 2013].

1.2. Objetivos

O trabalho teve propósito de aumentar o nível de segurança em ambientes através do controle de acesso via identificação biométrica, além disto, pretende-se gerenciar automaticamente tarefas rotineiras de acordo com rotinas pré-cadastradas.

Para atingir o objetivo proposto, foram implementados os seguintes objetivos específicos:

- Desenvolvimento de um aplicativo para automação residencial;
- Estudo e desenvolvimento de algoritmo para Scanner biométrico GT-511C1R;
- Implementação através do Android e Arduino para controle de acesso através da impressão digital; e
- Desenvolvimento de um gerenciador de rotinas do usuário utilizando banco de dados SQLite.

Para a realização de testes, o aplicativo será implementado junto a um ambiente microcontrolado sendo ele uma maquete com Leds, Motores e Atuadores que foi construído e desenvolvido por [Gomes et al. 2013], onde o mesmo proporciona todas as especificações que foram solicitadas para realização do trabalho, que é ilustrado na Figura 1.

Figura 1. Ambiente Microcontrolado. Adaptado de: [Gomes et al. 2013].

1.3. Estrutura do trabalho

Este trabalho está assim dividido. O 1. Introdução apresenta o objetivo do trabalho e sua justificativa a Revisão Bibliográfica é dividida em: estudo sobre biometria 2.2. Reconhecimento Biométrico, histórico e informações sobre automação 2.1. Automação Residencial o restante do texto são informações sobre *softwares*, *hardware* e linguagem que serão utilizados para o desenvolvimento do projeto em questão e por fim seus resultados obtidos.

2. Revisão Bibliográfica

Nos próximos tópicos será demonstrado os conceitos de reconhecimento facial e as ferramentas utilizadas para seu desenvolvimento.

2.1. Automação Residencial

Também conhecida como *domótica,* vem demonstrando que aliado a principais características que são: conforto, segurança e sustentabilidade estão auxiliando usuários a realizarem atividades do cotidiano com mais facilidade e comodidade.

A automação é a integração de equipamentos eletromecânicos e eletroeletrônicos, que são utilizados para realizarem ações de acordo com o que o usuário deseja. Atualmente a preocupação no desenvolvimento dessa tecnologia concentram-se em baixo custo de dispositivos e segurança [Wortmeyer et al. 2005].

Como é vista como uma tecnologia nova, usuários tendem a supor que seja uma tecnologia cara, entretanto os benefícios que são disponibilizados são diversos, os serviços mais procurados são os na área da segurança residencial que são integrados a câmeras e sensores biométricos, esses são capazes de perceber pessoas que não são permitidas no ambiente, podendo assim haver mais controle de acesso em residências [Wortmeyer et al. 2005].

O controle de gastos com energia também é uma das vantagens, pois em um sistema de automação a energia só é utilizada quando necessário.

2.2. Reconhecimento Biométrico

O reconhecimento biométrico é um recurso que identifica pessoas através de suas diferenças genéticas tais como impressão digitais, contornos do rosto, reconhecimento de retina, íris e geometria da mão [Liu and Silverman 2001]. Esses tipos de reconhecimentos é feito através de algoritmos e de sensores que fazem a comparação dos traços da pessoa.

Grandes empresas utilizam a biometria, policias, empresas, banco, entre outros o sistema é confiável tendo a precisão de quase 99% de acerto, servindo assim para que violações e fraudes possas ser evitadas [Liu and Silverman 2001].

Existem certos fatores para que a leitura de características físicas seja caracterizada como biometria são elas:

- Universalidade: a pessoa deve ter a sua característica em estudo.
- Distinção: as características em estudo devem ser diferente de pessoa para pessoa.

- Permanência: as características não podem ser modificadas [Janes R. 2009].
- Desempenho: a velocidade de reconhecimento e precisão de todo o processo devem ser levados em consideração.
- Segurança: o sistema deve ter passado por vários testes para que não tenha fraudes e violações nas identificações [Matyáš and Říha 2010a].

2.2.1. Verificação Biométrica

Biometria pode ser efetuada por dois tipos de verificação.

Autenticação: é feita de maneira que o algoritmo receba números de identificação a partir de um teclado, código de barras, cartão magnético, em seguida recebe algum tipo de biometria, buscando então em um banco de dados e fazendo a associação dos números recebidos e imagem para determinar se são da mesma pessoa.

Verificação: o algoritmo recebe a imagem da biometria e pesquisa em um banco de dados se é existente, caso tenha cadastro o sistema envia um código para a identificação da pessoa para que possa acessar determinado local [Janes R. 2009].

2.2.2. Reconhecimento Biométrico de Digitais

Existem diversas técnicas de reconhecimento de impressão digital, através de captura de imagem, equipamento como scanner (Seção 2.2.3. Scanner de Impressão Digital GT-511C1), fazendo o cadastro dessas imagens armazenando para após identificar características [Janes R. 2009]. Dentre os tipos de leitores utilizados, os principais são:

Ópticos: o modo de captura deste equipamento é feito através de uma luz que é emitida sobre o dedo que é posicionado sobre um vidro, a imagem então é capturada. Ilustrado na Figura 2 à esquerda.

Capacitivos: é feito através da captura das minúcias que são detalhes do dedo através de uma pastilha de silício, transformando esses detalhes em imagens. Na Figura 2 à direita é mostrado o sensor.

Figura 2. À esquerda Sensor Óptico. À direita sensor capacitivo.

As desvantagens do Sistema de reconhecimento por impressão digital está na variação da leitura dos dedos causados por diversos fatores como mostrado na (Seção 2.2.2.1 Algoritmo de Impressão Digital), as vantagens são a rapidez da leitura e identificação e baixo custo da tecnologia. A escolha para a Biometria da Digital se dá ao

fato de que é uma tecnologia que está sendo utilizada em diversos lugares fazendo assim com que se possa avançar em estudos e o avanço do mercado nessa tecnologia.

2.2.2.1. Algoritmo de Impressão Digital

O algoritmo de biometria digital faz a verificação de todos os detalhes do dedo, o detalhamento é dividido em bifurcações, arcos, núcleo e terminação dos sulcos da minúcias que são locais descontínuos no padrão da impressão é mostrada na Figura 3.

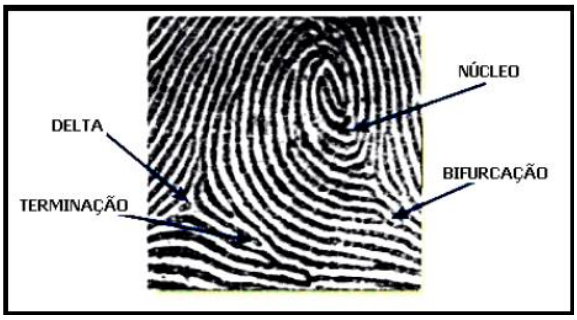

Figura 3. Caracteristicas da minúcia . Adaptado de: [Janes R. 2009].

Após a coleta da impressão ela é tratada (ver Figura 4) utilizando filtros para melhor verificação, o sistema faz a comparação dos pontos da minúcia com as impressões já cadastradas no banco de dados podendo assim definir se existem padrões entre as digitais.

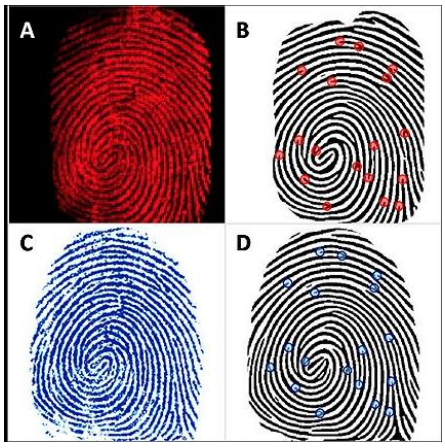

Figura 4. Tratamento da imagem. Adaptado de: [Janes R. 2009]

Problemas podem ocorrer nessa verificação, um deles é a qualidade da imagem que é coletada, podendo ser causada por rotações do dedo durante a leitura, cicatrizes após o cadastramento, ressecamento da pele, leitor com problemas, entre outros. Para que se possa solucionar esse problema os usuário devem não movimentar o seu dedo durante o cadastramento de sua digital e também ser periodicamente verificada e efetuado um novo recadastramento [Bolzani et al. 2006].

2.2.3. Scanner de Impressão Digital GT-511C1

O Scanner utilizado neste trabalho para coleta e tratamento de impressão digital é o GT-511C1 apresentado na Figura 5. É um sensor de integração com Arduino (ver seção 2.3.

Arduino) que faz a comunicação com a serial TTL. O Scanner faz desde a leitura até o reconhecimento através de um sensor ótico (Seção 2.2.2), podem ser cadastradas até 20 digitais no módulo, podendo também ser cadastrados *templates* das digitais em um banco de dados tendo assim mais digitais cadastradas.

Figura 5. Scanner de Impressão Digital GT-511C1

Fonte: https://www.robocore.net/upload/lojavirtual/558_1_H.png

Para funcionamento é necessário utilizar um conversor de nível analógico pois a comunicação das portas é 3.3V e do Arduino a saída é 5V. A facilidade com que o *scanner* é utilizado, grande disponibilidade de fórum e também o baixo custo foram fatores para que este tenha sido escolhido para o projeto.

2.3. Arduino

Arduino é uma placa de prototipagem eletrônica que integra *hardware* e *software* em sua placa a um microcontrolador chamado *Atmega* tem suporte para entrada e saída de dados.

É utilizado a linguagem de programação baseada em C que é denominada *Wring* um dos objetivos da criação do projeto, Arduino foi para que possa ser feito vários projetos com custos muito baixo e descomplicado de programar e manusear os componentes para que os projetos sejam feitos por pessoas que não conhecem a área da eletrônica e da programação [Arduino, 2012].

2.3.1. Shield Internet

Shield Internet é uma placa que é conectada ao Arduino, permitindo assim com que ele se conecte a *internet*, para executar determinada função. Ela oferece uma rede TCP ou UDP, pode ser inserido cartão de memória, em sua placa tem portas digitais e analógicas e utiliza a mesma programação do Arduino [Arduino, 2012].

2.4. Android

Android é um sistema operacional para dispositivos móveis, *Open Source* está atualmente na versão 5.1 que foi lançada em 2015.

Há diversas bibliotecas, fóruns e *APIs* que são disponibilizadas na *internet* portanto desenvolver nessa plataforma se torna eficiente, sendo utilizada em diversos projetos para diversas áreas.

2.5. Trabalhos Correlatos

A literatura traz uma série de trabalhos correlatos sendo alguns aqui apresentados. Em **"Trava com abertura biométrica ou remota"** [Mocellin. G *et al.* 2013] é apresentado um sistema de controle de acesso, um dos problemas comum em diversos tipos de ambiente, cuja trava é controlada por um sistema embarcado, que tem o controle tanto por impressão digital quanto por ações de um dispositivo remoto.

Outro trabalho, **"Biometric authentication – Security and Usuability**" [Matyáš and Říha 2010b] trata de um estudo sobre biometria na área de segurança trazendo consigo vantagens e desvantagens de sua utilização nos dias de hoje, também salienta a sistemática de como a biometria é efetuada, fazendo apenas um estudo como a tecnologia está sendo utilizada.

Por fim, [Janes R. 2009] **em "Estudo sobre sistemas de segurança em instalações elétricas automatizadas**", trata da utilização de sensores para a área de segurança de uma residência, tanto em relação ao acesso quanto a prevenção de incêndios. O autor faz o levantamento de vantagens e desvantagens de sistemas de segurança, o enfoque é nas tecnologias biométricas e a sua aplicação no controle de acesso. A implementação é de um controle de acesso em um ambiente educacional. Conclui que a utilização biométrica é uma tendência mundial, não sendo muito implementa hoje em dia pois pesquisadores levantam polêmica sobre a segurança de dados biométrico.

No entanto nem um dos trabalhos faz esse reconhecimento utilizando a placa de prototipagem Arduino junto com o Scanner de Impressão Digital GT-511C1 com aplicação para dispositivo móvel, utilizando a Shield Internet acoplada ao Arduino para fazer a conexão com a aplicação móvel, também utilizando um banco de dados que será hospedado em um servidor local na residência.

3. Metodologia

A demora para implementação de *software* fazia com que clientes ficassem insatisfeitos com os trabalhos solicitados, foi então que surgiram as metodologias ágeis. Elas propõem a solução para este problema, o aperfeiçoamento de métodos já existente além de também se adapta facilmente a diversos projetos [Barbosa *et al*. 2009].

Após o manifesto ágil surgiram as metodologias ágeis, dentre elas destacam-se, Extreme Programming (XP), SCRUM e Feature Driven Development (FDD), sendo que a Feature Driven Development (FDD) a escolhida para o desenvolvimento deste projeto, pois atende as necessidades do trabalho.

3.1. Feature Driven Development (FDD)

É uma metodologia incremental e iterativa, cada iteração é a implementação completa de um conjunto de funcionalidades, que devem ser apresentadas ao cliente para que o mesmo perceba a evolução. Essas iterações não devem ultrapassar duas semanas, caso isso aconteça ela deve ser dividida em mais partes, [Palmer and Felsing 2002].

Segundo [Palmer and Felsing 2002]. FDD é constituído por 5 processos.

- Desenvolver um modelo geral: que é a definição de requisitos e domínio do sistema para sua construção, documentação da especificação das funcionalidades;
- Construir lista de Funcionalidades: constitui na lista de funcionalidades, cada funcionalidade é revisada pelo cliente;
- Planejar por funcionalidade: criar funções sequenciais que são executadas de acordo com a sua prioridade;
- Projetar por funcionalidade e Construir por funcionalidade: constituiu na implementação de certa funcionalidade selecionada pelo grupo de desenvolvedores de acordo com sua prioridade, a implementação nesta etapa não deve ultrapassar 2 semanas.

3.2. Funcionamento do Software

O Sistema foi implementado, iniciando da montagem do circuito, onde o 2.2.3. Scanner de Impressão Digital GT-511C1 junto com Arduino e Shield Internet, formam o circuito na Figura 6, onde a Shield Internet é acoplada ao Arduino, após é ligado o Sensor ao Arduino iniciando assim o protótipo.

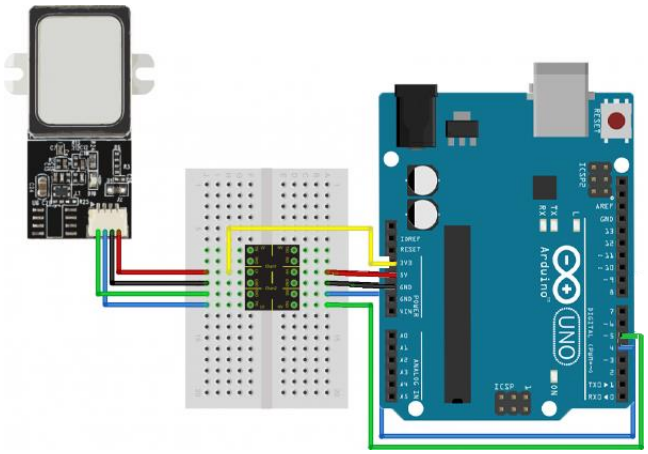

Figura 6. Circuito Scanner.

Após feito a montagem do protótipo foi iniciado a programação no ambiente Android Studio.

A tela inicial do sistema Figura 7 (A) o usuário informa seu *login* e senha cadastrados no sistema, o sistema então verifica junto ao banco de dados se os dados informados por parte do usuário estão corretos, caso os dados estejam incorretos o sistema apresenta na tela uma mensagem para o usuário verificar os campos digitados, caso os dados estejam corretos é aberta a tela de verificação de digital Figura 7 (B).

Na Figura 7 (B) o usuário seleciona a opção Iniciar Verificação, o sistema inicia um processo de verificação, que funciona da seguinte forma:

- É enviado o comando para o Arduino inicia a verificação;
- O usuário posiciona a sua digital cadastrada no leitor;

- Por fim o Arduino verificar a digital, retornando a resposta para o sistema onde o mesmo verifica se a digital é a do usuário que efetuou o *login*.

Os passos informados anteriormente utiliza a verificação por Autenticação para assim liberar acesso ao usuário, ou nega-lo, após essa verificação o usuário pode utilizar o menu do sistema podendo cadastrar, alterar, excluir usuários e suas atividades mostrados na Figura 7 (C).

No menu atividades, o usuário é cadastra a atividade registrando a hora, data e o equipamento escolhido para o mesmo Figura 7 (E), após efetuado o registro o sistema automaticamente inicia a verificação de atividades que funciona da seguinte forma:

- Caso a atividade esteja na hora e data registrado o sistema então envia uma notificação para o usuário
- O usuário clicar na notificação acionando assim a tela ilustrado na Figura 7 (D)
- É verificado a resposta do usuário, realizar a atividade ou não caso seja clicado em sim o sistema então envia para o Arduino a atividade para que seja efetuada por ele, caso seja clicado em não o sistema sai da aplicação.

Figura 7. Telas do Sistema.

O software final pode ser melhor visualizado na Figura 8, onde é mostrado o funcionamento do software implementado, o usuário informa seu login e senha no aplicativo Figura 8 (1) o usuário então posiciona a sua digital no sensor biométrico Figura 8 (2) o Arduino então faz o reconhecimento enviando para o Android se a digital está cadastra ou não, fazendo a liberação da porta ou não Figura 8 (3).

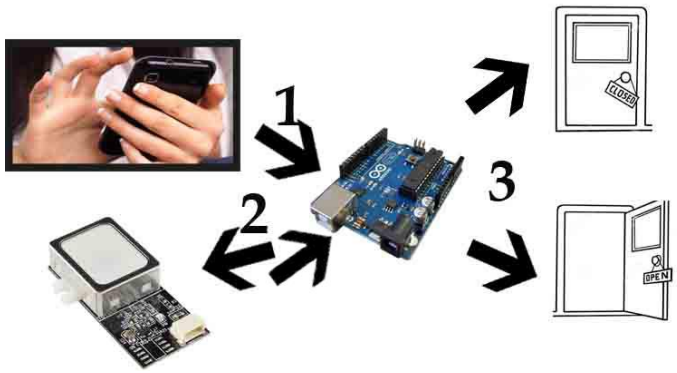

Figura 8. Funcionamento do Software.

4. Projeto

A seção a seguir demonstra os requisitos do sistema junto com diagramas de Domínio, Classes, Dados.

4.1. Funcionalidades do Sistema

As funcionalidades do *software*, são:

- Funcionalidade 1: Cadastrar, Alterar, Excluir, Pesquisar Usuários.
- Funcionalidade 2: Cadastrar, Alterar, Excluir, Pesquisas Atividades.
- Funcionalidade 3: Cadastrar, Alterar, Excluir Digitais.
- Funcionalidade 4: Verificar Digitais de acordo com usuário para liberação de portas.
- Funcionalidade 5: Verificar Atividades de acordo com usuário, para efetua-las caso aceito pelo usuário.

Essas são necessárias para que *software* efetue todas as necessidades encontradas para o êxito do projeto.

4.2. Análise e Levantamento de Requisitos

A análise e levantamento de requisitos traz uma melhor compreensão do *software,* é o estudo sobre o problema e o levantamento de requisitos, onde é descrito as informações e restrições que o sistemas deve seguir [Ramos 2006].

4.2.1 Requisitos Funcionais

Os requisitos funcionais são os que mostram o comportamento do sistema, as atividades que devem ser efetuadas durante seu funcionamento. É importante que o sistema atenda aos requisitos funcionais, pois quando bem definidos custos com manutenção do

sistema são diminuídos [Rezende 2005]. Na Tabela 1 são mostrados os requisitos funcionais do sistema.

Tabela 1. Requisitos Funcionais.

RF1 – Gerenciar Usuários	**Dependência:**	**Requisitos Relacionados:**	**Dificuldade**
Descrição: O sistema deverá permitir o cadastro, alteração, exclusão e a pesquisa de Usuários.	RNF4.		Médio
	Categoria	**Desejável**	**Permanente**
	Gerenciamento	X	X
RF2 – Gerenciar Digitais	**Dependência:**	**Requisitos Relacionados:**	**Dificuldade**
Descrição: O sistema deverá permitir o cadastro, alteração, exclusão e a pesquisa de Digitais.	RF1, RNF4.		Difícil
	Categoria	**Desejável**	**Permanente**
	Gerenciamento	X	X
RF3 – Gerenciar Atividades.	**Dependência:**	**Requisitos Relacionados:**	**Dificuldade**
Descrição: O sistema deverá permitir o cadastro, alteração, exclusão e a pesquisa de Atividades.	RF1, RNF4,		Dificil
	Categoria	**Desejável**	**Permanente**
	Gerenciamento	X	X
RF4 – Verificar Digitais.	**Dependência:**	**Requisitos Relacionados:**	**Dificuldade**
Descrição: O sistema deverá verificar a digital do usuário caso seja solicitado pelo mesmo.	RF1, RF2, RNF4.	RF2.	Dificil
	Categoria	**Desejável**	**Permanente**
	Gerenciamento	X	X
RF5 – Verificar Atividades.	**Dependência:**	**Requisitos Relacionados:**	**Dificuldade**
Descrição: O sistema deverá verificar a existência de atividades a cada minuto para que então sejam efetuadas.	RF1, RF3, RNF4.	RF3.	Dificil
	Categoria	**Desejável**	**Permanente**
	Gerenciamento	X	X
RF6 – Executar Atividades.	**Dependência:**	**Requisitos Relacionados:**	**Dificuldade**
Descrição: O sistema deverá executar as atividades que foram cadastradas pelo usuário.	RF1, RF3, RF5, RNF4.	RF5, RNF5.	Dificil
	Categoria	**Desejável**	**Permanente**
	Gerenciamento	X	X

4.2.2. Requisitos não Funcionais

Os requisitos não funcionais são relacionados a como será efetuado o uso do sistema como desempenho, manutenção, disponibilidade, o cliente nem sempre especifica-os, pois eles são as características mínimas para a qualidade do *software* ficando por conta do desenvolvedor efetuar esses requisitos [Rezende 2005].

Na Tabela 2 são mostrados os requisitos não funcionais do sistema.

Tabela 2. Requisitos não Funcionais.

RNF1 – Acesso Digital
Descrição: O Sistema deve liberar acesso apenas quando a digital do usuário for verificada e seus dados forem os mesmos cadastrados.
RNF2 – Linguagem de Programação JAVA
Descrição: O sistema deverá usar qualquer versão da linguagem de programação JAVA.
RNF3 – Banco de Dados SQLite.
Descrição: O sistema deverá usar qualquer versão do banco de dados SQLite a partir da 5.0.
RNF4 – Login de Usuários.
Descrição: Os usuários deverão estar ligados ao utilizar o sistema para quaisquer requisito.

4.3. Diagrama de Domínio

É a representação das classes conceituais ou objetos em um domínio do problema, deve conter compreensão ao qual o sistema irá gerenciar [Celepar Informatica do Paraná 2009]. A Figura 9 ilustra o diagrama de domínio da aplicação ao qual pode-se ver graficamente o esboço e uma compreensão do problema a ser resolvido no projeto.

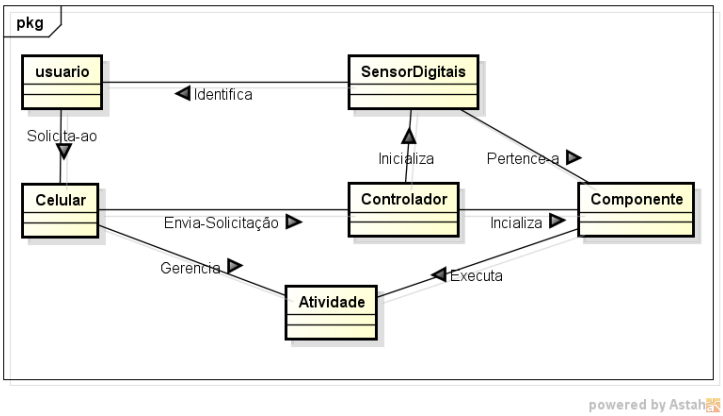

Figura 9. Diagrama de Domínio.

4.4. Diagrama de Classes

É a representação das classes e o relacionamento entre elas, também permite a análise de restrições, relacionamentos entre outros aspectos [Booch *et al*. 2006]. A Figura 10 ilustra as classes que foram implementadas no projeto onde as que estão na cor amarela são classes que a aplicação Android terá e a em azul será a que o Arduino irá utilizar, na classe em azul não será utilizado orientação a objetos será de forma estruturada. Sendo elas:

- funcaoBanco onde é gerenciado todas query relacionada ao banco. Os atributos existentes nos métodos inserir e alterar usuários são: String id,String nome, String senha, String datanascimento, String rg, String cpf, String telefone, String endereco, String cidade, String estado, String pais, String digital. No método alterar atividade e inserir atividade os atributos do método são: String id_atividade,String data, String hora, String local_equipamento, String id_usuario
- O diagrama representado na cor azul é a classe que está no Arduino, onde a função loop executa todas as funções do Arduino, e o método setup inicializa as variáveis.

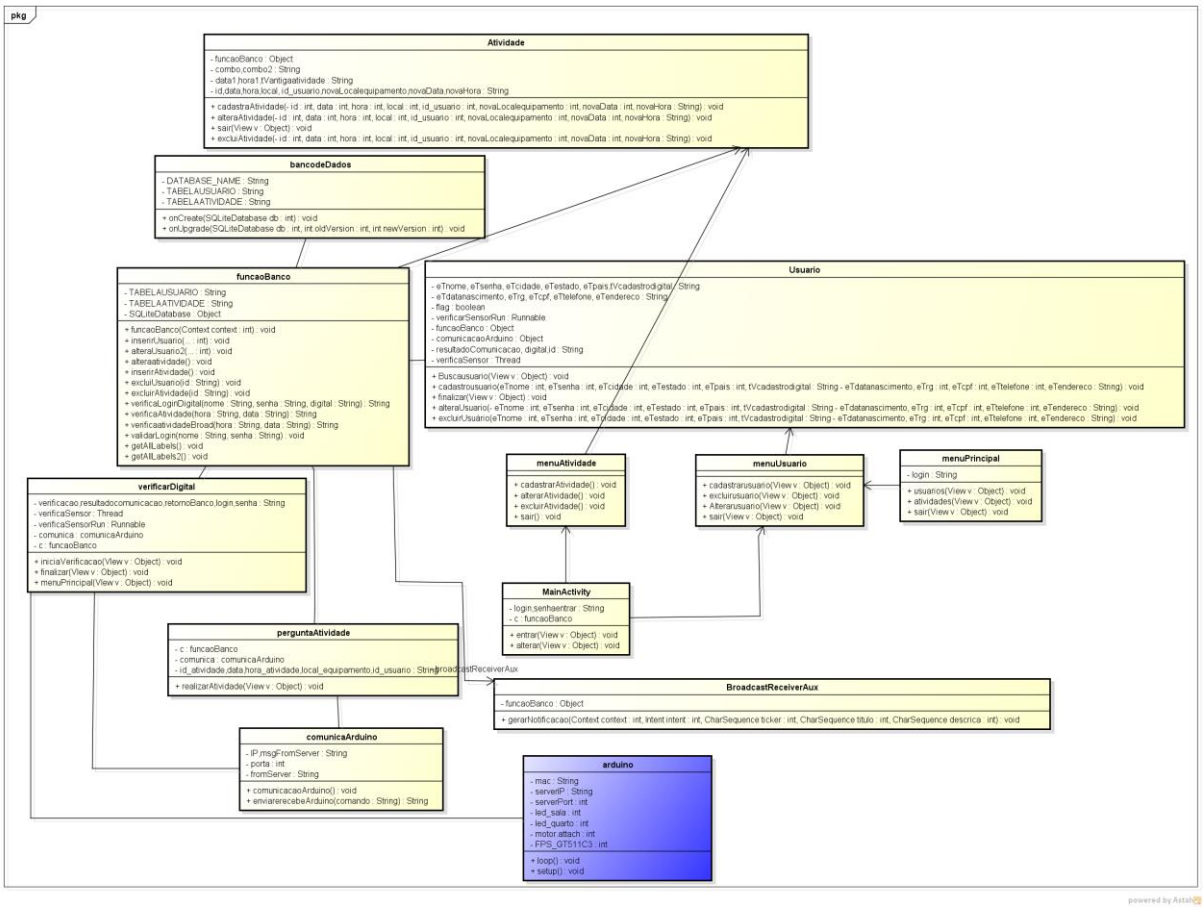

Figura 10. Diagrama de Classes.

4.5. Modelo Entidade Relacionamento (DER)

É o modelo utilizado para descrever objetos, atributos e como são relacionados entre si, este modelo representa a estrutura que o banco de dados irá possuir no *software* [Ozeas .2013].

A Figura 11 mostra estrutura do banco que será implementado utilizando o Gerenciados de Banco de Dados (MySQL) o banco de dados se encontra em um servidor local na residência.

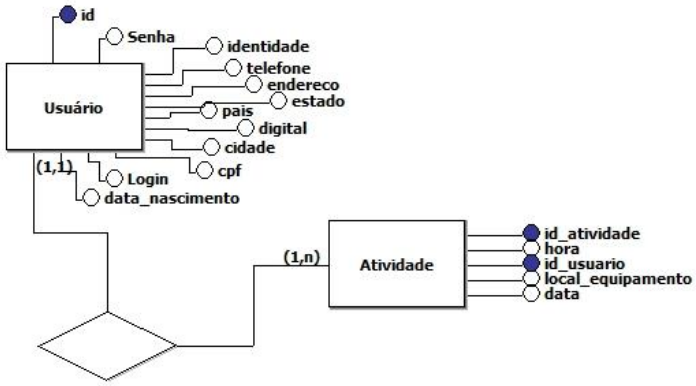

Figura 11. Modelo Entidade Relacionamento.

4.6. Trabalhos Futuros

Para trabalhos futuros pode-se realizar uma análise dos dados em que cada usuário registra sua atividade e utilizá-los para fazer uma mineração de dados criando assim perfis de usuário, onde se pode melhor ainda mais a comodidade não necessitando que o usuário cadastre a atividade.

Pode ser efetuado uma melhora para a velocidade de verificação de digital podendo ser utilizado diferentes equipamentos.

O sistema também pode ser testado em uma residência e não em uma maquete o que mostraria mais resultados na área segurança.

5. Conclusão

O trabalho mostra a implementação de um aplicativo para controle de acesso e também controle de atividades em ambientes microcontrolados. Faz uso de equipamentos como Arduino, sensores e atuadores, que irão disponibilizar dados a uma aplicação Android que será executada através do celular, ambos serão conectados à rede utilizando a Shield Internet.

A principal contribuição deste trabalho foi elevar a segurança em residências, e a melhor realização de atividades pelo usuário, utilizando equipamentos acessível e que se diferenciem dos trabalhos já concluídos. Com o estudo de caso efetuado em um ambiente microcontrolado foi analisado a melhora na segurança e na comodidade do usuário em utilizar todo o ambiente.

Foi escolhida a metodologia ágil Feature Driven Development (FDD) destaca-se nela as entregas frequentes e a busca do desenvolvimento por funcionalidade. No

capítulo 4. Projeto foram descritas as funcionalidades do sistema, junto com diagramas solicitados pela metodologia, seguindo assim todo o fluxo do Feature Driven Development (FDD) para a realização do trabalho.

O trabalho contribui para a segurança em ambientes microcontrolados e também a comodidade do usuário em realizar suas atividades trazendo assim diretrizes da automação.

6. Referências

ARDUINO (2012). An open-sourceelectronicsprototypingplatform. Disponível em: <http://www.arduino.cc>. Acessado em: 19 mai. 2015 .

Booch, G., Rumbaugh, J., Jacobson, I. (2006), "UML: Guia do Usuário", 2ª Edição. Rio de janeiro, RJ: Elsevier Editora ltda.

Barbosa, A., Azevedo, B., Pereira, B., Campos, P. and Santos, P. (2009). Metodologia Ágil : Feature Driven Development.

Bolzani, C. A. M., Montagnoli, C. and Netto, M. L. (2006). Domotics over IEEE 802.15.4 - A spread spectrum home automation application. In *IEEE International Symposium on Spread Spectrum Techniques and Applications*.

Celepar Informatica do Paraná (2009). Guia para elaboração do Modelo de Domínio Metodologia Celepar.

Janez, R. (2009). Estudo sobre sistemas de segurança em instalações elétricas automatizadas. São Paulo, 2009.

Gomes, R. O., Niederauer, A. R. and Alessandro A. M de Oliveira (2013). AMBIENTES MICROCONTROLADOS COMO ECONOMIZAR ENERGIA E CUSTOS COM DISPOSITIVOS. v. 1, p. 1–5.

Liu, S. and Silverman, M. (2001). Practical guide to biometric security technology. *IT Professional*, v. 3, p. 27–32.

Matyáš, V. and Říha, Z. (2010a). Security of biometric authentication systems. In *2010 International Conference on Computer Information Systems and Industrial Management Applications, CISIM 2010*.

Matyáš, V. and Říha, Z. (2010b). Security of biometric authentication systems. In *2010 International Conference on Computer Information Systems and Industrial Management Applications, CISIM 2010*.

MOCELLIN G, LAURA WOBETO, THAYSE MARQUES SOLIS, W. M. N. (2013). *TRAVA COM ABERTURA BIOMÉTRICA OU REMOTA*. CURITIBA: .

Ozeas, G. (2013). Modelagem de Domínio: os 7 maus cheiros de informação. Disponivel em: <http://www.infoq.com/br/articles/seven-modelling-smells> Acessado em 19 de mai. 2015.

Palmer, S. R. and Felsing, M. (2002). *A Practical Guide to Feature Driven Development*. p. 271

Ramos, R. A. (2006), "Treinamento Prático em UML", Digerati Books.

Rezende, D. A. (2005), "Engenharia de Software e Sistemas de Informação", 3ª Edição. Rio de Janeiro, RJ: Brasport Livros e Multimídia Ltda.

Wortmeyer, C., Freitas, F., Cardoso, L., Educacional, A. and Bosco, D. (2005). Automação Residencial : Busca de Tecnologias visando o Conforto , a Economia , a Praticidade e a Segurança do Usuário . Resumo. p. 1064–1067.

Santos C. (2013). Faturamento do mercado global de Biometria tem rápido crescimento. Disponível em: <http://convergecom.com.br/tiinside/seguranca/26/03/2013/faturamento-do-mercado-global-de-biometria-tem-rapido-crescimento/#.VQdg047F9UV> Acessado em: 16 de mar. 2015.