Universidade Federal do Pampa
Silvio E. Quincozes

Uma Arquitetura Segura Baseada na Computação Ubíqua para Recuperação de Registros Médicos

Alegrete
2015

Ficha catalográfica elaborada automaticamente com os dados fornecidos
pelo(a) autor(a) através do Módulo de Biblioteca do
Sistema GURI (Gestão Unificada de Recursos Institucionais) .

Q7a Quincozes, Silvio
Uma Arquitetura Segura Baseada na Computação Ubíqua para Recuperação de Registros Médicos / Silvio Quincozes.
89 p.

Trabalho de Conclusão de Curso(Graduação)-- Universidade Federal do Pampa, ENGENHARIA DE SOFTWARE, 2015.
"Orientação: Juliano Kazienko".

1. Arquitetura. 2. Segurança. 3. Recuperação de Prontuário Eletrônico. 4. Computação Ubíqua. 5. Near Field Communication. I. Título.

Silvio E. Quincozes

Uma Arquitetura Segura Baseada na Computação Ubíqua para Recuperação de Registros Médicos

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia de Software da Universidade Federal do Pampa como requisito parcial para a obtenção do título de Bacharel em Engenharia de Software.

Orientador: Prof. Juliano F. Kazienko, Dr.

Alegrete

2015

Silvio E. Quincozes

Uma Arquitetura Segura Baseada na Computação Ubíqua para Recuperação de Registros Médicos

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia de Software da Universidade Federal do Pampa como requisito parcial para a obtenção do título de Bacharel em Engenharia de Software.

Trabalho de Conclusão de Curso defendido e aprovado em 9 de Julho de 2015.

Banca examinadora:

Prof. Juliano F. Kazienko, Dr.
Orientador

Prof. Daniel Welfer, Dr.
UNIPAMPA

Prof. Edgar Gonzaga Souza dos Santos, Dr.
UNIPAMPA

Agradecimentos

Primeiramente eu agradeço a Deus por iluminar meu caminho e nele abrir portas e oportunidades que viabilizaram chegar onde eu cheguei. Agradeço por cada escolha certa que fiz durante toda minha jornada até esse momento único na vida que também é a realização do sonho.

Agradeço a todos os professores que me passaram ensinamentos ao decorrer do curso, em especial ao meu orientador Juliano F. Kazienko que apostou em mim como orientando e me deu a oportunidade trabalhar em cima de assuntos de nosso interesse, gerando ótimos resultados e assim agregando conhecimento em minha formação.

Gostaria também de agradecer os funcionários do Hospital de Caridade de Jaguari pela ótima recepção, em especial ao administrador Ruderson Mesquita, o qual nos permitiu realizar os experimentos práticos e contribuiu no alance dos resultados desse trabalho.

Aos colegas e amigos da empresa na qual trabalhei praticamente todo o período da minha graduação, a Acesso Informática, em especial ao sócio-diretor Paulino Neto, que flexibilizou meus horários e foi compreensivo nos momentos que precisei de maior dedicação aos estudos.

Por fim, quero agradecer as pessoas mais importantes para mim, que sempre me apoiaram e incentivaram a alcançar meus objetivos: minha mãe Tarzi Isabel Ereno Quincozes, meu pai Oneides Quincozes, meu irmão Vagner Ereno Quincozes e minha avó Neuza Ereno. Além deles, não poderia deixar de agradecer aos parentes e amigos Leonir Ereno, Iara Terezinha, Cláudia Quincozes e Cezar Nereu dentre tantos outros que me apoiaram nesse período de estudos.

Resumo

Sistemas de Registros Médicos são ferramentas importantes para facilitar o acesso e manutenção de dados de pacientes, como seu histórico de internações e exames médicos. Atualmente, médicos, enfermeiros e técnicos em enfermagem precisam de um acesso rápido e seguro aos registros médicos, evitando a burocracia e imprecisões no processo de recuperação dessas informações. A computação ubíqua e pervasiva pode contribuir na superação desses desafios, entretanto o problema da personificação de dispositivos deve ser tratado cuidadosamente para não haver comprometimento de informações particulares ou adulteração em qualquer tipo de registros. A fim de mitigar esse problema, este trabalho apresenta uma arquitetura segura, baseada na computação ubíqua e pervasiva para a recuperação e manutenção de registros médicos. Tal arquitetura depende da tecnologia de Comunicação por Campo de Proximidade, do inglês, Near Field Communication (NFC). Dessa forma, um mecanismo de autenticação foi desenvolvido para garantir a autenticidade dos dispositivos envolvidos. A arquitetura é avaliada no Hospital de Caridade de Jaguari (HCJ). Os resultados da análise e validação mostram que o mecanismo é eficiente e promissor, estabelecendo a autenticação mútua. Adicionalmente, outras importantes propriedades de segurança são alcançadas, como a proteção anti-repetição e anti-rastreio de dispositivos.

Palavras-chave: Arquitetura, Segurança, Recuperação de Prontuário Eletrônico, Computação Ubíqua, *Near Field Communication*.

Abstract

Medical Records systems are important tools for easy access and maintenance of patient data, such as its history of hospitalizations and medical exams. Currently, physicians, nurses and technicians need a quick and secure access to medical records, avoiding bureaucracy and uncertainties in the process of recovery of this information. The ubiquitous and pervasive computing can help in overcoming these challenges, however the problem of impersonation devices should be handled carefully to be no compromise private information or tampering in any kind of records. In order to mitigate this problem, this paper presents a secure architecture based on ubiquitous and pervasive computing to the restoration and maintenance of medical records. This architecture depends on the Near Field Communication technology (NFC). Thus, an authentication mechanism is designed to ensure the authenticity of the devices involved. The architecture is evaluated in Hospital de Caridade de Jaguari (HCJ). The results of analysis and validation shows that the mechanism is effective and promising, establishing mutual authentication. In addition, other important security properties are achieved, as the anti-replay protection and anti-tracking.

Key-words: *Architecture, Security, Health Records Retrieval, Ubiquitous Computing, Near Field Communication..*

Sumário

Lista de Siglas

- NFC - Near Field Communication
- HCJ - Hospital de Caridade de Jaguari
- CFM - Conselho Federal de Medicina
- HL7 - Health Level 7
- OSI - Open Systems Interconnection
- ANSI - American National Standards Institute
- RIM - Reference Information Model
- CVX - Codes for Vaccines Administered
- mHealth - Mobile Health
- PHR - Personal Health Records
- EHR - Electronic Health Records
- EPR - Electronic Patient Records
- MD2 - Message Digest 2
- MD4 - Message Digest 4
- MD5 - Message Digest 5
- SHA - Secure Hash Algorithm
- MAC - Message Authentication Code
- KDC - Key Distribution Center
- BAN - Burrows-Abadi-Needham
- UWB - Ultra wideband
- RFID - Identificação por Radiofrequência
- LAN - Local Area Network
- Wi-Fi - Wireless Fidelity
- NDEF - NFC Data Exchange Format

- RTD - Record Type Definition
- URI - Uniform Resource Identifiers
- PICC - Proximity Inductive Coupling Card
- SE - Secure Element
- RF - Radiofrequência
- JIS - Japanese Industrial Standards
- UI - Circuito Integrado
- AES - Advanced Encryption Standard
- PIN - Personal Identifier Number
- SIM - Subscriber Identifier Module
- EMV - Europay, Mastercard and Visa
- T - Tag
- S - Servidor
- M - Dispositivo Móvel
- UC - Caso de Uso
- IDE -Integrated Development Environment
- SGBD - Sistema Gerenciador de Banco de Dados
- EE - Enterprise Edition
- SE - Standard Edition

1 Introdução

Nas últimas décadas, os hospitais brasileiros vêm demonstrando maior interesse na utilização de sistemas de informações hospitalares como meio de apoio ao atendimento robusto e com qualidade. Tais sistemas, além de promover a gerência de procedimentos hospitalares, também oferecem suporte ao armazenamento de informações pessoais dos pacientes em bancos de dados. Com o crescimento do uso de dispositivos móveis no cotidiano das pessoas, o acesso a esses sistemas através dos seus dispositivos pessoais parece ser uma ideia atraente para os usuários. Dessa forma a informação está disponível em qualquer lugar e a qualquer momento, facilitando a recuperação e manutenção das mesmas. Além disso, os sistemas de informações apóiam a gestão de registros médicos, resultando na redução de erros e negligências por parte do usuário, assim os dados ganham maior consistência (SETHIA et al., 2014) (MIORANDI et al., 2012) (ABOELFOTOH; HASSANEIN, 2014).

Dessa forma, por se tratar de informações particulares, é de suma importância que a privacidade dessas informações seja mantida. Para tal, devem ser satisfeitas as propriedades de confidencialidade, autenticidade e integridade dessa informação. Além disso, deve existir um controle de acesso com a autenticação dos dispositivos envolvidos (STALLINGS, 2008) (MENEZES; OORSCHOT; VANSTONE, 2010). Invasores ou mesmo meros visitantes, não devem ser capazes de ler ou alterar o diagnóstico ou prescrição de medicamentos de um paciente, por exemplo.

Suponha que um paciente possui registros de abuso de drogas ou de porte de doenças sexualmente transmissíveis. Ao aproximar seu *smartphone*, um atacante não deve ser capaz de acessar tais informações confidenciais. É importante que nem mesmo o próprio paciente seja capaz de efetuar alterações em seus próprios registros. A adulteração dos registros pode ser usada para modificar resultados de exames, como o a detecção de abuso do uso de drogas, por exemplo (ABOELFOTOH; HASSANEIN, 2014) (LAHTELA; HASSINEN; JYLHA, 2008).

Para assegurar que os dados não serão perdidos em caso de problemas físicos com o dispositivo que contém a informação, pode ser considerada a possibilidade de manter-se uma sincronização dos dados do sistema em um servidor ou sob controle de um provedor de serviços e armazenamento online (Nuvem). Todavia, com o envolvimento de terceiros, surge mais uma preocupação em torno da privacidade dos dados. Independente do ambiente onde são mantidas as informações do paciente, o mesmo deve haver mecanismos que previnam contra o vazamento de dados. Nem mesmo o administrador do provedor de serviço ou equipe de manutenção devem ser capazes de acessar informações pessoais

armazenadas sobre pacientes.

Além do armazenamento seguro, a transmissão também requer cuidado especial, principalmente quando o mesmo ocorre em meio sem fio. A tecnologia de campo de proximidade, do inglês, *Near Field Communication* (NFC), por exemplo, utiliza um formato de troca de mensagens que não oferece proteção limitada contra a manipulação indevida dos dados (ROLAND; LANGER, 2010) (SETHIA et al., 2014).

Atualmente, existem algumas propostas de sistemas e arquiteturas na literatura que buscam maior facilidade nos procedimentos hospitalares com apoio da computação ubíqua e pervasiva. Entretanto, muitos desses sistemas carecem de atenção para os aspectos de segurança. Assim, os sistemas atuais que não tratam adequadamente essas questões, estão vulneráveis a ataques como a personificação de dispositivos e invasão às informações particulares de pacientes (ABOELFOTOH; HASSANEIN, 2014), (RODRIGUES EDGAR T. HORTA; RODRIGUES, 2014), (IGLESIAS et al., 2009), (SETHIA et al., 2014).

1.1 Problema de Pesquisa Estudado

O estudo do acesso eficiente e seguro a registros médicos busca acelerar o processo de recuperação e atualização de informações, de maneira que as mesmas possuam a devida proteção contra o acesso indevido. Uma das maneiras utilizadas por atacantes para obter o acesso aos dados confidenciais consiste na personificação de dispositivos computacionais.

Esse trabalho se concentra em estudar o problema da personificação de dispositivos em sistemas de registros de saúde eletrônicos. Assim, dispositivos de atacantes não devem ser capazes de se passar por um dispositivo legítimo e consequentemente não poderão acessar informações pessoais que somente tal dispositivo tem acesso.

1.2 Objetivo

1.2.1 Objetivo Principal

O presente trabalho tem por objetivo propor uma arquitetura segura de registro e recuperação de dados hospitalares, especialmente através da comunicação por campo de proximidade. A segurança reside principalmente na autenticação entre dispositivos a fim de resolver o problema da personificação de dispositivos, garantindo outras propriedades relevantes de segurança, como a confidencialidade, proteção contra a reprodução de mensagens e o anti-rastreio. A proposta será embasada na computação ubíqua e pervasiva, assim a interação entre humano e computador se da de forma mais natural e é introduzida no cotidiano dos usuários (WEISER, 1991) (HANSMANN, 2003).

A arquitetura foi implantada no Hospital de Caridade de Jaguari (HCJ), onde os usuários fizeram a avaliação de sua experiência com o sistema bem como sua validação.

1.2.2 Objetivos Específicos

- Estudar os sistemas de registros médicos;
- Estudar os sistemas ubíquos e pervasivos, especialmente a comunicação sem fio e a tecnologia NFC;
- Rever as propriedades e os mecanismos da segurança da informação;
- Elaboração de um mecanismo de autenticação usando a tecnologia NFC;
- Propor uma arquitetura eficiente e segura para a recuperação de registros médicos;
- Implementar um protótipo de tal arquitetura proposta;
- Avaliar o mecanismo de segurança da arquitetura utilizando métodos formais;
- Avaliar a arquitetura proposta, através da implantação do protótipo desenvolvido, no HCJ.

1.3 Organização do Documento

O restante do documento está organizado como segue: No Capítulo 2 é apresentada a fundamentação teórica. Em seguida, apresenta-se a revisão da literatura, no Capítulo 3. Tal capítulo aborda sistemas médicos existentes, na Seção 3.1, e propostas relacionadas a segurança no NFC, na Seção 3.2. Em seguida, no Capítulo 4 é apresentada a Arquitetura para Recuperação Segura de Registros Médicos, proposta nesse trabalho. Um importante componente dessa arquitetura consiste em um mecanismo para prover a troca de informações de forma segura através da comunicação por campo de proximidade. Tal mecanismo é apresentado na Seção 4.3.1 . O Capítulo 5 apresentada a validação e análise do mecanismo proposto, bem como a avaliação experimental. Por fim, as conclusões e trabalhos futuros são apresentadas no Capítulo 6.

2 Fundamentação Teórica

Neste capítulo, serão abordados alguns conceitos fundamentais e termos comuns na área da saúde e ambiente hospitalar, na Seção 2.1, além de conceitos da área da segurança da informação, na Seção 2.2. Por fim, na Seção 2.3, são apresentados fundamentos da Computação Ubíqua e Pervasiva.

2.1 Conceitos Médicos

Nesta seção serão introduzidos alguns conceitos utilizados na tecnologia da informação voltada para a área médica.

2.1.1 Prontuários Médicos

Segundo a resolução do Conselho Federal de Medicina (CFM) nº 1.638/2002, um prontuário médico é um documento valioso para o paciente, médico e instituição de saúde. Estão nele contidas: informações, sinais e imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada. Esses dados são de caráter legal, sigiloso e científico. O propósito de um prontuário médico é possibilitar a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada a o indivíduo. Compete ao médico, instituição de saúde ou ambos, o dever de manter o prontuário de cada paciente atendido, preservando a qualidade das informações nele contidas. O artigo 5º dessa resolução define os itens que deverão constar obrigaróriamente em um prontuário, seja eletrônico ou manuscrito. As informações a seguir foram extraídas desse artigo (ANDRADE; SILVA, 2002).

Como dados de identificação do paciente, os seguintes registros devem estar presentes: o nome completo, data de nascimento (dia, mês e ano com quatro dígitos), sexo, nome da mãe, naturalidade (cidade e estado de nascimento), endereço completo (nome da via pública, número, complemento, bairro/distrito, município, estado e CEP (ANDRADE; SILVA, 2002).

Prontuários devem conter dados tais como: Anamnese - que consiste em um interrogatório do médico ao paciente a fim de contribuir no diagnóstico - além de exames físicos, exames complementares solicitados e seus respectivos resultados, hipóteses diagnósticas, diagnóstico definitivo e tratamento efetuado (ANDRADE; SILVA, 2002).

A evolução diária do paciente, com data e hora, discriminação de todos os procedimentos aos quais o mesmo foi submetido e identificação dos profissionais que o realizam deve também estar presente em um prontuário. Nos casos em que o prontuário é elabo-

rado ou armazenado em meio eletrônico, como é o caso da presente proposta, os dados sobre a evolução diária do paciente devem ser assinados eletronicamente. A guarda e manuseio dos prontuários, cabem ao médico assistente, à chefia da equipe, à chefia da Clínica e à Direção técnica da unidade (ANDRADE; SILVA, 2002).

2.1.2 Health Level 7

A "Saúde Nível-7"ou *Health Level 7* (HL7), é um conjunto internacional de normas para transferência de dados clínicos e administrativos entre sistemas de informações na área médica. Essas normas são direcionadas à sétima camada de rede do modelo de Interconexões de Sistemas Abertos, do inglês, *Open Systems Interconnection* (OSI), que se refere a camada de aplicação. O HL7 mantém uma semântica de nomenclatura de registros relacionados aos conhecimentos da área da saúde. Seu objetivo é promover a interoperabilidade para a troca de dados médicos (TAN; PAYTON, 2009).

A primeira versão do HL7 (1.0) foi publicada em 1987 pelo Instituto Americano de Normas Nacionais, do inglês, *American National Standards Institute*(ANSI). Essa versão foi responsável pelo escopo e formato do padrão HL7. Em 1988 a versão 2.0 foi lançada, dois anos depois, em 1990 a versão 2.1 foi adotada em escala global. Em 1997, o HL7 passou por uma completa revisão, que foi baseada no Modelo Referência de Informação, do inglês, *Reference Information Model* (RIM) (TAN; PAYTON, 2009) (LOPEZ; SETOLA; WOLTHUSEN, 2012).

O padrão HL7 é o conjunto de especificações mais largamente adotado em sistemas de saúde. A principal motivação para seu uso é a troca de conjuntos definidos de informações administrativas e clínicas entre sistemas de informações. Dados administrativos tendem a ser universalmente suportado através do padrão HL7, e seus segmentos são definidos de maneira mais uniforme. Os dados clínicos consistem na definição de tipos mais específicos de mensagens requeridas através do uso de um vocabulário de dados padrão e conjuntos de códigos para aqueles domínios de práticas clínicas, como, por exemplo, os Código de Vacina Administrada, do inglês, *Codes for Vaccines Administered* (CVX) (EDIDIN; BHARDWAJ, 2014).

2.1.3 Registros Médicos Eletrônicos

O acesso a dados sobre a saúde de pacientes muitas vezes pode ser recuperado ou alterado por dispositivos móveis tais como *laptops*, *smartphones* ou *tablets*. Essas aplicações são categorizadas como Saúde Móvel, do inglês, *Mobile Health* (mHealth). Usuários podem utilizar seus dispositivos móveis para prover monitoramento contínuo (RODRIGUES EDGAR T. HORTA; RODRIGUES, 2014) (IGLESIAS et al., 2009), ou para acompanhar seus registros pessoais de saúde (ABOELFOTOH; HASSANEIN, 2014).

Quando o responsável pela operação do sistema é o próprio paciente, esse sistema é categorizado como Registro de Saúde Pessoal, do inglês, *Personal Health Record* (PHR). Este é diferente do Registro Eletrônico de Saúde, do inglês, *Electronic Health Record* (EHR), o qual é mantido pela instituição responsável pelos cuidados médicos (MAGNUSON; FU, 2014). Outra categoria similar ao EHR, é o Registro Eletrônico do Paciente, do inglês, *Electronic Pacient Record* (EPR). Este por sua vez foca apenas nas informações mais relevantes, não cobrindo as rotinas do paciente nem cuidados odontológicos, alternativos ou comportamentais (SLEE; SLEE; SCHMIDT, 2009).

2.2 Segurança da Informação

Nesta seção serão discorridas as propriedades (2.2.1), mecanismos (2.2.2), juntamente com alguns conceitos acerca da segurança da informação.

2.2.1 Propriedades da Segurança da Informação

Existem algumas propriedades importantes para a segurança da informação. A confidencialidade, integridade, disponibilidade, autenticidade, auditoria, tempestividade, anti-reprodução, entre outras (STALLINGS, 2008). A seguir, as responsabilidades de algumas dessas propriedades serão discutidas.

Confidencialidade consiste na propriedade que se concentra em garantir que dadas informações possam ser acessadas apenas por indivíduos, processos ou sistemas autorizados. A propriedade integridade se preocupa com a garantia de que determinadas informações não tenham sofrido nenhuma alteração. Isto é, os as características originais devem ser preservadas no que diz respeito ao seu significado, completude, utilização pretendida, e correlação com a sua representação. A propriedade disponibilidade garante que a informação possa ser acessada a qualquer momento e sem interrupções.

Para se estabelecer autenticidade, deve ser possível verificar se uma entidade ou processo que está tentando acessar informações ou serviços é realmente quem afirma ser. O furto de identidades alheias pode ensejar um ataque de personificação, onde uma entidade se passa por outra. Isso pode ser alcançado através da utilização de falsos credenciais (CPF, RG, Nome, IDs, etc.), portanto sistemas de autenticação buscam robustez a fim de mitigar tais ataques. Entretanto, essa não é uma tarefa simples (SCHNEIER, 2009).

A propriedade auditoria consiste na possibilidade de responsabilizar e rastrear o responsável por uma ação. A autenticidade e auditoria requerem um meio de identificar uma entidade dentre as outras. O atributo de identificação provê esse recurso, atribuindo uma identidade única para cada entidade (LOPEZ; SETOLA; WOLTHUSEN, 2012). A tempestividade está relacionada à disponibilidade de uma informação em tempo hábil para seu uso, e a propriedade anti-reprodução consiste na prevenção da reprodução de

informações. A propriedade anti-rastreio consiste em utilizar identificadores dinâmicos para uma entidade. Dessa forma, atacantes não são capazes de identificar dispositivos através da captura desta informação.

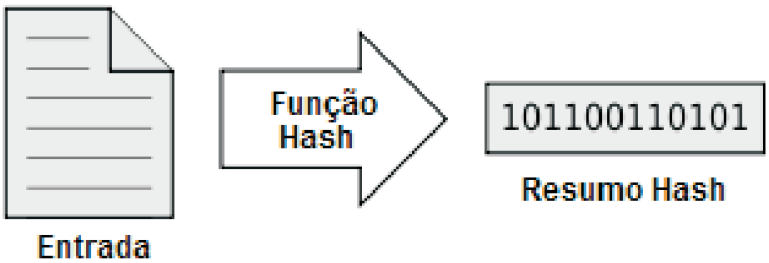
O sistema proposto contempla a propriedade de autenticação mútua, o que restringe o acesso às informações por atacantes. Essa restrição é importante para o alcance de outra propriedade, a confidencialidade. A integridade das mensagens é garantida através da inserção do resumo *hash* do conteúdo de uma mensagem nessa mesma mensagem, conforme ilustra a Figura 1. O contador concatenado às mensagens trocadas, antes do cômputo do resumo *hash*, resulta no estabelecimento de Anti-Reprodução.

2.2.2 Mecanismos de Segurança

Para alcançar as propriedades discutidas anteriormente, se faz necessário a utilização de alguns mecanismos e métodos de proteção. A seguir serão discorridos alguns conceitos e serviços utilizados em prol da segurança da informação:

Um algoritmo *hash* é uma função matemática unidirecional, ou seja, a função inversa não pode ser computada. Através da aplicação desse algoritmo, é possível obter um resumo do conteúdo passado como entrada. Independente do tamanho da entrada, o resultado da função *hash* tem sempre tamanho fixo. O uso desse algoritmo serve para fazer a verificação de integridade de um conteúdo, bem como na assinatura de arquivos. Ao assinar um documento, o leitor pode verificar se o mesmo não sofreu alterações. Se uma simples letra modificada, isso acarretaria em um resumo *hash* totalmente diferente do original. Outra utilização do *hash* é em logins de sistemas, a fim de verificar a igualdade de senhas (TIPTON; KRAUSE, 2012).

Figura 1 – Funcionamento do algoritmo *hash*



Existem diferentes algoritmos *hashes*. Alguns deles consistem em: *Message Digest-Algorithm* 2 (MD2), *Message Digest-Algorithm* 4 (MD4) e *Message Digest-Algorithm 5* (MD5). Ambos resultam em resumos *hashes* de 128-bit. O MD2 é o menos seguro, seguido do MD4, onde identificaram-se falhas. O algoritmo MD5 é a versão mais atual

dentre eles. O MD5 foi sucedido pelo *Secure Hash Algorithm* 1 (SHA-1), que produz um resumo de 160-bit (TIPTON; KRAUSE, 2012). Entretanto comparado ao algoritmo SHA-1 e seus sucessores mais robustos SHA-256, SHA-384 e SHA-512, ele é o mais rápido (THORSTEINSON; GANESH, 2003). O algoritmo escolhido para geração de *hashes* neste trabalho foi o MD5, entretanto qualquer outro algoritmo poderia ser usado.

A Função de Dispersão Chaveada, do inglês, *Keyed Hash Function*, também conhecido como Código Autenticador de Mensagem, do inglês, *Message Authentication Code* (MAC) consiste na combinação de uma chave simétrica e algum algoritmo de cifra de bloco, por exemplo um dos algoritmos *hashes* discutidos anteriormente. Tradicionalmente esse mecanismo é utilizado na conversação entre entidades, onde se deseja validar a integridade e autenticidade de uma informação transmitida. O propósito do MAC é autenticar a fonte de uma mensagem com base em sua chave secreta que é inserida (PATEL, 2008) (KUROSE; ROSS, 2010).

Um *nonce* consiste em um valor que é utilizado uma única vez em determinado contexto, geralmente para prevenir ataques de repetição (*replay attacks*). Esse termo é bastante utilizado em protocolos de segurança, e também é conhecido como número aleatório (*random number*) em um protocolo desafio-resposta. Com o uso de *nonces*, os mecanismos de segurança podem prover a garantia de unicidade à mensagem que o carrega. O recebimento de mais de uma mensagem com o mesmo *nonce* indica a detecção de um ataque de repetição (PATEL, 2008) (KUROSE; ROSS, 2010). Outra alternativa bastante semelhante consiste na substituição de *nonces* por contadores.

Quando utilizados mecanismos destinados ao estabelecimento de autenticação, a parte que está sendo autenticada precisa provar sua autenticidade. Para tal, as mesmas podem utilizar chaves secretas que seja de conhecimento restrito. Existem dois tipos de criptografia que podem ser utilizadas para esse fim: criptografia de chave simétrica e criptografia de chave assimétrica(STALLINGS, 2008).

A criptografia simétrica exige que as partes tenham uma chave secreta em comum compartilhada entre as mesmas. Tal abordagem impõe a necessidade de uma distribuição segura das chaves simétricas, onde muitas vezes é necessária o envolvimento de uma terceira parte confiável. Um Centro de Distribuição de Chaves, ou *Key Distribution Center* (KDC) (MENEZES; OORSCHOT; VANSTONE, 2010), tem como propósito a distribuição segura de chaves simétricas.

A criptografia assimétrica, também conhecida como criptografia de chave pública, é um método de criptografia onde as partes utilizam um par de chaves: uma chave pública e uma chave privada. A cifragem de dados é feita com base na chave pública de uma entidade, onde a mesma é capaz de decifrar esses dados por meio da utilização de sua chave privada (STALLINGS, 2008).

2.2.3 Lógica BAN

A lógica *Burrows-Abadi-Needham* (BAN) foi proposta em (BURROWS; NEEDHAM, 1990), onde os autores têm por objetivo o estabelecimento de uma verificação formal de protocolos, buscando por falhas ou brechas de segurança e antecipando passos de um possível ataque a ser executado por um invasor. Com base nessa verificação, é possível afirmar se um protocolo atinge os objetivos propostos, e se é seguro contra ataques como espionagem, por exemplo.

A análise de protocolos por essa lógica, é dividida em três etapas: Idealização, Levantamento de Suposições e Postulado. Na primeira fase da validação, as mensagens são reescritas de forma padronizada, conforme estabelecido pela notação da Lógica BAN. A próxima fase consiste na definição de premissas, crenças ou suposições iniciais. Essas suposições também devem respeitar a sintaxe proposta pela Lógica BAN. A última fase da validação consiste na aplicação de regras a fim de inferir conclusões a cerca dos objetivos atingidos pelo mecanismo. Essas regras consistem em afirmativas que são assumidas como verdadeiras quando uma condição for aceita. Por exemplo, se a entidade P acredita que o o nonce X é fresco - gerado recentemente - e P também acredita que Q disse X, então assume-se que P acredita que Q acredita em X.

2.3 Computação Ubíqua e Pervasiva

A computação ubíquoa e pervasiva, propõe a possibilidade de acesso a informações em qualquer lugar a qualquer momento pelos dispositivos computacionais envolvidos. O foco da computação ubíqua e pervasiva consiste na disponibilização de serviços de forma contínua, em dispositivos que possuam um software embarcado. Tais dispositivos normalmente se encontram dispersos no ambiente para prover apoio as atividades e rotinas dos usuários. Eles não são necessariamente móveis, mas sim onipresentes, ou seja, seu serviço pode ser oferecido em qualquer lugar a qualquer momento. Os componentes envolvidos na computação ubíqua e pervasiva têm baixo custo e se comunicam entre si por meio de redes sem fio (SISTEMAS. . . , 2011) (COULOURIS et al., 2013).

Segundo (PERSPECTIVAS. . . , 2003), o crescimento da computação ubíqua suscita numerosas questões relacionadas a confiança, proteção da privacidade, segurança da informação, fidedignidade, funcionalidade e garantia de funcionamento. Este trabalho se concentra no controle do acesso indevido a informação, mitigando ataques que exploram as brechas de segurança nas transmissões de dados no meio sem fio. A seguir, na Seção 2.3.1, serão apresentadas as tecnologias de comunicação sem fio utilizadas na computação ubíqua e pervasiva.

2.3.1 Comunicação sem Fio

Para a troca de dados entre dois ou mais dispositivos, é necessário que alguma tecnologia seja utilizada. Padrões tecnológicos como *ZigBee*, *Bluetooth*, UWB (ultra-wideband), NFC ou RFID (Identificação por Radiofrequência, do inglês, *Radio Frequency Identification*) são os padrões utilizados em serviços de proximidade. Entende-se por serviço de proximidade, aquele serviço que pode ser obtido através da aproximação física de dispositivos, máquinas ou objetos (IGLESIAS et al., 2009).

Um dos padrões mais comumente utilizados em redes locais, ou *Local Area Network* (LAN), é o padrão (802.11, 2014), também conhecido como "fidelidade sem fio", do inglês, *Wireless Fidelity* (Wi-Fi). A comunicação Wi-Fi dispensa a necessidade de cabeamento para interconexão de computadores e *notebooks* de uma mesma rede, além de possibilitar a integração de dispositivos como *smartphones* e *tablets* nessa mesma rede.

O NFC tem chamado atenção devido a algumas vantagens que apresenta. Não é necessária nenhuma configuração inicial, diferente do *Bluetooth* que necessita de pareamento, por exemplo. Devido ao seu menor alcance, essa tecnologia também é considerada mais segura comparada ao RFID tradicional. *Tags* NFC têm baixo custo, tornando possível a criação de novas interfaces com usabilidade potencializada (QUINCOZES; KAZIENKO, 2014) (IGLESIAS et al., 2009). Neste trabalho será adotada a tecnologa NFC aliada ao Wi-Fi para a comunicação de dados.

2.3.2 Near Field Communication (NFC)

A tecnologia de Comunicação por Campo de Proximidade, do inglês, *Near Field Communication* (NFC), surgiu em 2002 através de uma parceria entre a Sony e a Philips. Até poucos anos atrás, a tecnologia NFC estava presente em apenas uma minoria dos aparelhos celulares (JUELS, 2006). Atualmente muitos *smartphones* já possuem um chip NFC integrado, como é o caso dos dispositivos Sony Xperia M, Nokia Lumia 720, Samsung Galaxy S5 e o mais recente lançamento que aderiu a tecnologia: Apple iPhone 6 (INFOMONEY, 2014).

O NFC possibilita a troca de mensagens entre dispositivos, desde que possuam um chip integrado. Além de *smartphones*, alguns dispositivos como *notebooks*, *tablets*, cartazes, etiquetas e crachás também podem conter a tecnologia NFC embutida. Com a fixação de *tags* NFC em objetos, por exemplo, pode-se estabelecer uma interação desses objetos com os dispositivos citados anteriormente. Algumas padronizações como (ISO/IEC, 2011) são empregadas na regulamentação das aplicações baseadas na comunicação NFC.

Tal tecnologia de comunicação sem fio utiliza ondas de rádio de alta frequência, tradicionalmente 13,56 MHz, com um alcance aproximado de até 10 centímetros. A taxa de transmissão pode ser 106, 216, ou 424 kbit/s (MULLINER, 2009). A norma

(COMMISSION et al., 2013) define os modos de operação e interface de comunicação do NFC, requisitos para a modulação, taxas de bits e codificação bits.

O NFC tem diversas aplicações, como na área da saúde, transporte e pagamentos eletrônicos. O tempo de configuração, comparado à tecnologia *Bluetooth*, por exemplo, é menor. Assim como o alcance das ondas de rádio, comparado ao RFID, por exemplo. Por esse motivo é considerado mais seguro, visto que é mais difícil do sinal ser interceptado por atacantes (EUN; LEE; OH, 2013)(COSKUN; OZDENIZCI; OK, 2013).

2.3.2.1 Formato de Mensagens

O formato *NFC Data Exchange Format* (NDEF) é um conjunto de padrões para o armazenamento de informações independente do dispositivo, que foi estabelecido pelo (NFC-FORUM, 2006). Uma mensagem NDEF é organizada em registros, onde cada mensagem possui um ou mais registros.

O tamanho do espaço reservado ao conteúdo da mensaqem (*payload*) para cada registro NDEF é limitado à $2^{32} - 1$ *bytes*. Entretanto, registros podem ser encadeados através de uma mensagem para obter-se longos *payloads*. Teoricamente não há limites para o tamanho de uma mensagem NDEF, então isso dependerá das capacidades de cada dispositivo (JEPSON; COLEMAN; IGOE, 2012). A Figura 2 ilustra a estrutura de uma mensagem nesse formato.

Registros podem ser classificados de acordo com seu tipo ou formato de dados. *NFC Record Type Definition*(RTD): Especifica o tipo e regras para criação de registros a serem usados por aplicações compatíveis com o formato de dados NDEF (NFC-FORUM, 2014).

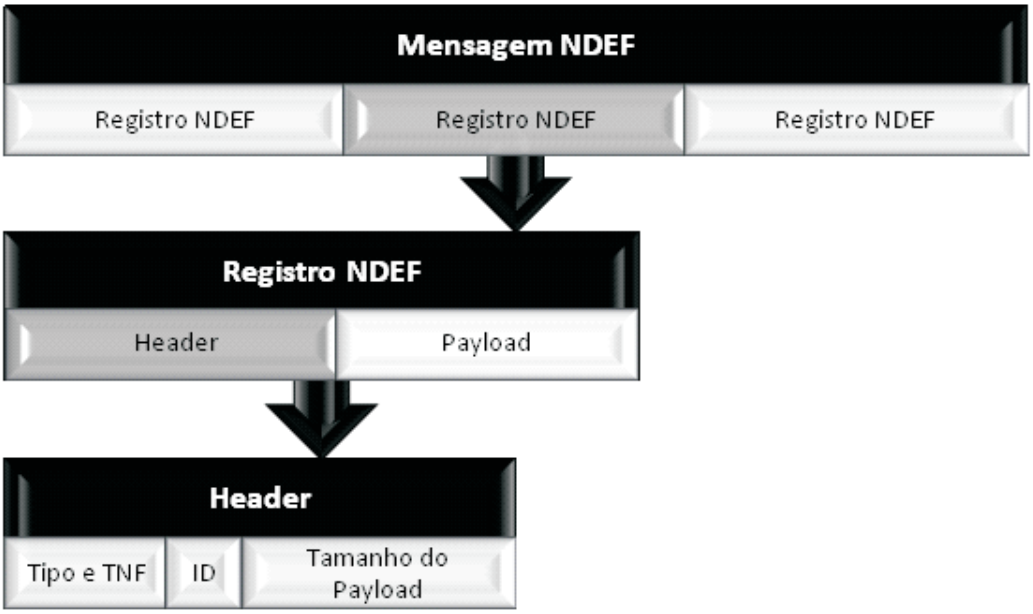
- *NFC Text RTD*: É utilizado para gravar informações em formato de texto (*strings*).

- *NFC URI RDT*: Serve para armazenar Uniform Resource Identifiers (URI). Existem aplicações onde são programadas funções, cada URI representa uma função que será ativa quando uma *tag* é aproximada.

- *NFC Smart Poster RDT*: É utilizada em cartazes inteligentes. Ao aproximar um dispositivo ativo de um cartaz inteligente (com uma *tag* NFC), pode-se capturar endereços de sites (URLs), número de telefone ou mensagens de texto. Esse formato utiliza os formatos *URI RDT e Text RDT*.

- *NFC Signature RDT*: Essa especificação possui um conjunto de algoritmos de assinatura que podem ser utilizados para assinar um ou múltiplos registros NDEF.

Figura 2 – Formato de Troca de dados NFC (NDEF)



O campo de carga de dados (*payload*) carrega o conteúdo da mensagem transmitida, enquanto o cabeçalho (*header*) carrega informações sobre essa mensagem, tais como tipo, tamanho e a identificação.

2.3.2.2 Modos de Operação

Existem três modos em que os dispositivos NFC podem operar, são eles: Modo de Emulação de Cartão (*Card Emulation Mode*), Par a Par (*Peer-To-Peer*, ou apenas P2P) e o modo de Leitura/Escrita (*Reader/Writer*) (COSKUN; OZDENIZCI; OK, 2013)(MULLINER, 2009). A seguir cada um deles é detalhado:

No modo de emulação de cartão, o dispositivo NFC age como um Cartão de Acoplamento Indutivo de Proximidade, do inglês, *Proximity Inductive Coupling Card* (PICC). Esse modo é bastante utilizado em aplicações de pagamento eletrônico, onde o cliente pode usar um *smartphone* como cartão de créditos, por exemplo. Para operar no modo de emulação de cartão um dispositivo deve possuir um Elemento Seguro (*Secure Element*, ou SE). O SE é um componente físico responsável por executar operações criptográficas e também por fazer o armazenamento seguro de dados.

Através do modo P2P, dois dispositivos ativos podem trocar mensagens de forma bidirecional. O Campo radiofrequência (RF) é gerado por ambos os dispositivos alternadamente. O dispositivo iniciador gera um campo RF para enviar sua mensagem ou requisição, o outro dispositivo deve gerar seu próprio campo (HASELSTEINER; BREITFUSS, 2006) no momento em que for responder.

No modo de Leitura/Escrita, dispositivos ativos podem ler e escrever dados em

dispositivos compatíveis com a tecnologia NFC, como *tags* por exemplo. Durante a leitura e escrita, o dispositivo responsável por gerar o campo RF deve ser um dispositivo ativo. No modo de leitura, o dispositivo passivo usa o sinal recebido para energização do próprio dispositivo e transmissão de dados.

2.3.2.3 Dispositivos NFC

Os dispositivos NFC estão classificados de acordo com a presença ou não de uma fonte de energia integrada e consequentemente possuir maior ou menor poder computacional, como dispositivos passivos ou ativos.

São considerados ativos os dispositivos que possuem uma fonte de energia integrada. Dispositivos ativos comuns podem ser, por exemplo: *smartphones*, *tablets*, *notebooks* e leitores portáteis NFC. Esses dispositivos podem gerar seu próprio campo de radiofrequência (RF), logo podem ser os iniciadores da comunicação. Dispositivos ativos podem conversar entre si através do modo de operação P2P ou no Modo de Emulação de Cartão, e podem também se comunicar com dispositivos passivos no modo de Leitura/Escrita (JEPSON; COLEMAN; IGOE, 2012).

Os dispositivos que utilizam a própria energia do sinal RF recebido para se energizar, a fim de executar operações e enviar mensagens são considerados dispositivos passivos. Esses dispositivos se caracterizam por ter um baixo poder computacional, requerendo uma atenção especial em sua programação. São exemplos de dispositivos passivos as *tags* NFC, *smartcards* e cartazes inteligentes (*smartpostes*). O espaço de armazenamento varia de acordo com o modelo e fabricante, mas é geralmente na unidade de *bytes* ou até alguns poucos *Kbytes*.

Dentre os dispositivos passivos, existem diferentes tipos de *tags*. Os tipos mais utilizados são os baseados no padrão ISO-14443 A. Essas *tags* possuem um espaço de armazenamento de 96 bytes, expansível para até 4K dependendo do tipo. As *tags* pertencentes à família Mifare, do fabricante Philips/NXP, incluem os modelos Mifare Ultralights, Mifare Classic 1K, Mifare Classic 4k e Classic Mini. Existe também um tipo de *tag* NFC baseada na norma industrial japonesa (JIS) X 6319-4. Estas têm memória inferior à 1 Kbyte. *Tags* Sony FeliCa são representantes desse tipo (JEPSON; COLEMAN; IGOE, 2012).

Os quatro tipos de *tags* reconhecidas pelo Forum-NFC são os seguintes:

Tipo 1: Esse tipo é baseado na ISO / IEC 14443A e permite leitura e re-escrita. A memória dessas *tags* pode ter o seu tamanho entre 96 bytes e 2 Kbytes e pode ser protegida contra gravação. A velocidade de comunicação com a *tag* é de 106 kbit / s. As *tags Innovision Topaz* são representantes desse tipo.

Tipo 2: Assim como o tipo 1, esse também é baseado na ISO / IEC 14443A

e permite leitura, re-escrita e proteção gravação. A diferença é que essas podem ter o tamanho da memória entre 48 bytes e 2 Kbytes. A velocidade de comunicação é a mesma velocidade do anterior. São exemplos de *tags* pertencentes ao Tipo 2 as *tags NXP Mifare Ultralight*, *NXP Mifare Ultralight* e NTAG203.

Tipo 3: Esse é o único tipo que não se baseiam na ISO / IEC 14443A, e sim na Norma Industrial Japonesa, do inglês, *Japaneses Industrial Standard* (JIS) X 6319-4. *Tags* do tipo 3 são pré-configuradas em fábrica para ser passível de leitura e re-escrita ou somente leitura. O tamanho da memória pode ser de até 1 Mbyte e a velocidade de comunicação com a *tag* é de 212 kbit / s. *Tags Sony Felica* fazem parte desse tipo.

Tipo 4: Esse tipo não é baseado, mas é compatível com a ISO / IEC 14443 (A B). Assim como o tipo 3, esse também é pré-configurado em fábrica para ser somente leitura ou leitura e re-escrita. Dentre as *tags* mencionadas, as com menor espaço de memória são as desse tipo, sendo de até 32 KBytes. A velocidade de comunicação com a *tag* é de 106 kbit / s. As *tags NXP Desfire e NXP SmartMX* são enquadradas nesse tipo.

As *tags Mifare Classic* não são compatíveis com o Fórum NFC, mas a sua leitura e a escrita é suportada pela maioria dos dispositivos NFC, já que os mesmos carregam um chip também do fabricante NXP. *Tags MIFARE Ultralight* possuem circuítos integrados (UI) de baixo custo, as *MIFARE Ultralight C* foram considerados os primeiros UI de baixo custo a oferecer criptografia aberta *Triple DES*.

3 Trabalhos Relacionados

Neste capítulo será feito o levantamento de trabalhos relacionados relevantes a fim de definir o estado da arte. A composição desse, se divide em duas seções: Sistemas Médicos (Seção 3.1) e Segurança no NFC (Seção 3.2).

3.1 Sistemas Médicos

Nesta seção serão apontados alguns trabalhos na área da tecnologia da informação aplicada à saúde. As vantagens e limitações de cada proposta são apresentadas nos próximos parágrafos.

O trabalho de (ABOELFOTOH; HASSANEIN, 2014) consiste na proposta de um sistema onde o paciente é capaz de acessar seus registros pessoais de saúde através de um dispositivo móvel. O sistema proposto estabelece uma conexão entre o dispositivo móvel do paciente e um sistema PHR, mantendo a sincronia dos registros. A verificação de integridade de dados é contemplada, usando a chave do médico para assinar os registros inseridos. O padrão de assinatura utilizado é o W3C XML. Os médicos podem encriptar os seus registros usando o algoritmo *Advanced Encryption Standard*(AES), para que o paciente tenha acesso a esses registros somente após a consulta. A autenticação do usuário perante o sistema se da através do uso de um *smartcard*. O limitado espaço de armazenamento no *smartphone* pode ser um problema no uso desse sistema. Além disso, médicos que não são usuários do mesmo sistema PHR em que o paciente é assinante, não serão capazes de ter acesso aos seus registros, então pode se fazer necessário o manuseio do *smartphone* do paciente pelo médico. Uma vez que o *smartphone* possui outros dados particulares como fotos, mensagens de texto ou contatos, por exemplo, esse procedimento pode expor a privacidade do paciente.

O trabalho (BENHARREF MOHAMED ADEL SERHANI, 2014) propõe um mecanismo para ser usado em aplicações que se auto-ajustam de acordo com as mudanças no ambiente. Para isso, são coletadas medidas sobre a disponibilidade de rede e uso de bateria de forma contínua. Com isso a sincronização de dados coletados através de biosensores com *smartphones*, se torna menos custosa. O meio de comunicação para a sincronização pode variar, podendo ser, por exemplo, através da rede 3G, *Wi-Fi* ou *Bluetooth*. No entanto, como já mencionado anteriormente, o *Bluetooth* pode não ser seguro o suficiente. Além disso, o trabalho não trata em nenhum momento de questões ligadas a segurança da comunicação ou armazenamento de informações.

No trabalho de (RODRIGUES EDGAR T. HORTA; RODRIGUES, 2014) a tec-

nologia de rede de sensores corporais é utilizada para a coleta de dados de pacientes em ambientes assistidos. A solução apresentada consiste no processamento de dados coletados por sensores para prever situações de perigo ou doenças, reduzindo a necessidade de acompanhamento presencial de um profissional da saúde. A comunicação de dados entre os sensores e o dispositivo receptor é via *Bluetooth* e nenhuma medida adicional de segurança é mencionada. Segundo (MUTCHUKOTA; PANIGRAHY; JENA, 2011), a chave criptográfica resultante a partir do PIN de quatro dígitos envolvido no pareamento de dispositivos não é forte o suficiente para oferecer a devida proteção contra a espionagem. Por se tratar de dados pessoais e sensíveis, é importante que haja um mecanismo específico para assegurar contra o acesso indevido a esses dados.

O trabalho de (IGLESIAS et al., 2009) propõe um sistema de monitoramento da saúde de pacientes debilitados ou idosos, onde através da validação com usuários, a usabilidade é avaliada. Usuários dessa aplicação podem se identificar através da aproximação de um dispositivo com NFC habilitado, onde informações são coletadas e associadas ao usuário identificado. Essas informações são enviadas a um rádio-receptor conectado a um computador via USB, e podem ser acessadas mais tarde de forma remota. O foco desse trabalho é a usabilidade do sistema. Entretanto, aspectos de segurança na comunicação e armazenamento dos registros capturados, bem como a autenticação entre a *tag* que identifica o usuário e leitor, não são considerados.

O trabalho (SETHIA et al., 2014) traz a proposta de um sistema EHR. Tal sistema é apoiado por dispositivos móveis com NFC e *Bluetooth* ou *tags* NFC, ambos com Elemento Seguro, do inglês, *Secure Element* (SE). O SE é responsável pelo armazenamento seguro de credenciais e dados confidenciais. As informações básicas são transmitidas via NFC e uma versão mais estendida dos registros pode ser transmitida via *Bluetooth*, onde podem haver vulnerabilidades de segurança (MUTCHUKOTA; PANIGRAHY; JENA, 2011). Nesse trabalho os medicamentos contém *tags* NFC, permitindo assim a sua autenticação antes de sua administração. Os autores propõem um Cartão de Saúde, do inglês, *Healthcard* baseado em dispositivos NFC, tais como *tags MIFARE Classic 1 K*, por exemplo, ou *smartphones*.

O *Healthcard* tem como objetivo o armazenamento dos registros do paciente. O método utilizado por (SETHIA et al., 2014), visando o estabelecimento de segurança para o sistema, consiste na autenticação mútua, onde são envolvidas chaves públicas e privadas de médicos e pacientes. Ao acessar os registros do paciente, o *smartphone* do médico passa por um processo de autenticação antes de poder ler e escrever dados, assinando com sua chave privada na escrita. No entanto, essas chaves são atualizadas somente de forma manual, pelo administrador do sistema. O processo de atualização de chaves deve ser repetido para cada uma das *tags*. Isso pode ser inviável no ponto de vista de escalabilidade, já que além dos leitos de pacientes, os medicamentos também possuem *tags*

de identificação. Além disso, um servidor de criptografia é necessário para a geração, verificação e armazenamento de chaves, e dispositivos de baixo poder computacional podem estar sujeitos a não atender aos requisitos necessários para utilização de criptografia assimétrica.

A proposta deste Trabalho de Conclusão de Curso também faz o uso de *tags* em medicamentos, mas além da autenticação dos mesmos, os profissionais de saúde poderão incluí-los nos registros dos prontuários médicos através da captura de sua identificação via NFC. Uma melhoria também é aplicada na renovação das chaves, onde as chaves simétricas passam a serem renovadas a cada autenticação bem sucedida de forma automática. Em relação a segurança, o mecanismo contemplado pela presente proposta foi projetado para rodar inclusive em dispositivos NFC de baixo poder computacional.

3.2 Autenticação no NFC

Em (CHEN et al., 2010), é proposto um mecanismo para estabelecer a autenticação de dispositivos NFC e permitir transações financeiras. Foram aproveitadas as primitivas criptográficas da tecnologia GSM, utilizando o cartão *Subscriber Identity Module* (SIM) de celulares para identificá-los. Nesse trabalho, as chaves são atualizadas dinamicamente a cada autenticação. Como a operadora de telefonia participa na geração da chave compartilhada, o uso do mecanismo fica limitado a dispositivos da mesma operadora.

O trabalho de (EUN; LEE; OH, 2013) propõe um método de privacidade condicional para proteger a privacidade do usuário usando pseudônimos. Essa proposta exige um terceiro confiável para a solicitação de um conjunto de pseudônimos. Com essa renovação o problema de rastreabilidade é controlado. Porém, essa abordagem requer aparelhos equipados com *Secure Element* (SE), o que inviabiliza o uso seguro dos demais dispositivos, como etiquetas NFC, por exemplo. Além disso, existe um custo computacional adicional para a solicitação de novos pseudônimos. Segundo os autores, um conjunto de 1000 pseudônimos exigira um espaço de 146,484 *Kbytes* em memória.

A especificação Europay, MasterCard e Visa (EMV) serve como a especificação global para o uso de cartões inteligentes para aplicações de crédito e débito em todo o mundo (ATKINS, 2003). Esse padrão propõe a autenticação de cartões de créditos pelos leitores, nos pontos de comércio. A segurança do EMV é construída por *hashes* sobre os dados da transação e autenticação *off-line* do cartão usando criptografia de chave pública. A cópia e clonagem de cartões são protegidas através da inclusão da identificação do cartão e de um *nonce* no resumo *hash*. A autenticidade e integridade de cartões são garantidas ao terminal, entretanto não é estabelecida nenhuma autenticação do terminal pelo cartão nas especificações publicadas em (EMV. . . , 2014). Dessa forma a autenticação mútua não existe. Isso significa que terminais têm a garantia de que estão

trocando informações com cartões autênticos, mas cartões estão vulneráveis a leitura por terminais falsos, viabilizando assim ataques como a captura de dados. Com isso, atacantes podem, por exemplo, pagar suas compras pela internet utilizando os dados de cartões de créditos das vítimas.

No trabalho (CEIPIDOR et al., 2012) são apontados alguns problemas de segurança existente no EMV aliado ao NFC, como segue: uma vez que o celular pode emular um *smartcard* (cartão inteligente), as informações sobre tal cartão podem ser lidas por qualquer atacante usando um leitor portátil que pode ser comprado por £7 (aproximadamente 28,00 reais) na Internet, segundo os autores. Mesmo quando o dispositivo se encontra desligado, um leitor ainda pode interagir com o chip NFC. Baseado nessas questões, é proposta uma solução que provê autenticação mútua e gera uma chave de sessão para a segurança da troca de informações. Todavia essa solução, assim como as discutidas anteriormente, depende de um terceiro confiável agindo como entidade certificadora. Cabe ressaltar que não é utilizada a certificação digital devido ao baixo poder computacional dos cartões - que não poderiam verificar a data de validade do certificado por não possuir um relógio, por exemplo. A proposta nesse trabalho conta com o apoio de uma terceira parte confiável que é conhecedora das chaves privadas dos dispositivos legítimos. Dessa forma, essa terceira parte é capaz de personificar quaisquer dispositivos, através do uso de suas chaves. Além disso, o número total de mensagens trocadas durante a autenticação (7 mensagens) é superior ao da presente proposta (5 mensagens).

O trabalho (QUINCOZES; KAZIENKO, 2014) consiste em um estudo inicial sobre a segurança na comunicação NFC, onde é apresentado um mecanismo para a autenticação de dispositivos. A principal diferença é que em (QUINCOZES; KAZIENKO, 2014) o foco consiste na segurança da comunicação NFC de dispositivos ativos como *Smartphones* e *Notebooks*. A autenticação de *Tags* NFC passivas não foi alcançada nesse estudo inicial, dessa forma o mecanismo proposto anteriormente não é apropriado para o cenário da proposta atual.

Os trabalhos mencionados anteriormente são comparados na Tabela 1.

Tabela 1 – Propriedades dos Mecanismos.

	Gerência de Chaves	Autenticação	Mensagens	Atende *Tags*
(CHEN et al., 2010)	Envolve Terceiros	Mútua	> 10	Não
(EUN; LEE; OH, 2013)	Envolve Terceiros	Mútua	6	Não
(EMV..., 2014)	Envolve Terceiros	Uma Via	> 10	Não
(CEIPIDOR et al., 2012)	Envolve Terceiros	Mútua	7	Não
(QUINCOZES; KAZIENKO, 2014)	Auto-Suficiente	Mútua	3	Não
Mecanismo Proposto Neste TCC	Auto-Suficiente	Mútua	5	Sim

4 Arquitetura Proposta

Este capítulo apresenta a arquitetura proposta e processo de desenvolvimento de seus componentes. O principal objetivo dessa arquitetura é o provimento de um sistema EHR de acesso seguro a registros médicos em ambientes hospitalares usando a comunicação sem fio, especialmente através da comunicação por campo de proximidade. Tal sistema baseou-se nos requisitos levantados através de uma entrevista com profissionais da saúde, onde deseja-se validar o sistema proposto.

4.1 Visão Geral da Arquitetura

A arquitetura proposta nesse trabalho visa prover o acesso seguro com inserção e recuperação dos dados armazenados em prontuários eletrônicos de pacientes de um hospital. Uma visão geral de toda a arquitetura é apresentada na Figura 3. Os componentes que envolvem essa arquitetura são apresentados na Seção 4.1.1.

4.1.1 Componentes

- *Smartphones*. Eles são usados para manutenção e recuperação de dados no sistema. Através destes dispositivos, os médicos, enfermeiros e técnicos de enfermagem são capazes de modificar e recuperar dados do servidor;
- Um servidor. Ele é responsável pelo armazenamento de registros do paciente, como exames, diagnósticos e prescrições médicas.
- Um Roteador Wi-Fi. A fim de estender a área de cobertura do sistema, esta proposta sugere que a comunicação entre *Smartphones* e o Servidor seja viabilizada via tecnologia Wi-Fi.
- *Tags* NFC: Elas armazenam uma pista - um *hash* - para a recuperação da identificação do paciente, que está armazenada no servidor. As *tags* são anexas às camas do pacientes. Na presente proposta, considera-se o uso de *tags* passivas com capacidade de leitura e escrita pelo fato das mesmas terem menor custo. Nas *tags* passivas, o transponder recebe energia por indução magnética a partir das mensagens transmitidas pelo leitor, que é ativo. Então, uma *tag* responde a um dispositivo leitor, como um *Smartphone* ou *Notebook*, desde que esse possua um adaptador NFC.
- Uma Aplicação Desktop: Essa aplicação é executada no servidor e/ou na estação utilizada pelo recepcionista ou médico. Através dessa aplicação é possível gerenciar internações e prescrições de medicamentos, por exemplo.

- Uma Aplicação para Plataforma Android: Uma aplicação para o sistema operacional Android que executa nos *smartphones*. Isso permite que técnicos em enfermagens, usando seus *smartphones*, sejam capazes de registrar os medicamentos administrados aos pacientes.

- Um mecanismo de autenticação. Um último e importante componente da presente arquitetura proposta consiste em um Mecanismo de Autenticação. Isso garante principalmente a autenticação mútua, a fim de mitigar a personificação de dispositivos. O mecanismo provê autenticação mútua entre o Servidor S e o Dispositivo M (Smartphone) baseado em um segredo compartilhado entre ambos. Adicionalmente, S pode também autenticar um Dispositivo T (Tags), identificando as quais não pertencem ao sistema.

De acordo com (STEELE; MIN; LO, 2012), sistemas são caracterizados como local, remoto ou hybrido. O sistema apresentado nesta Seção consiste em um sistema local. Ele não necessita de conexão à Internet. No entanto, depende de um servidor ligado à rede hospitalar uma vez que os dados são armazenados dentro das dependências hospitalares. A equipe do hospital é capaz de enviar e receber informações a este Servidor a partir de *Smartphones*, através de um ponto de acesso sem fio usando Wi-Fi (802.11, 2014).

4.1.2 Metodologia

Nesta seção serão discutidos as ferramentas e métodos utilizados no desenvolvimento.

Para o desenvolvimento da aplicação desktop, foi utilizado a linguagem de programação Java juntamente com a ferramenta Java *Standart Edition* - ou Java SE. O Ambiente de Desenvolvimento Integrado, do inglês, *Integrated Development Environment* (IDE) utilizado para essa aplicação foi o *NetBeans*. Como banco de dados, utilizou-se o sistema gerenciador de banco de dados (SGBD) *MySQL*, apoiado pela ferramenta *MySQL WorkBench*.

O aplicativo desenvolvido para rodar no sistema operacional android foi implementado na linguagem de programação Java, onde a ferramenta de suporte foi o Java *Enterprise Edition* - ou Java EE. O IDE utilizado foi o *Eclipse Juno*. O banco de dados conta com o SGBD SQLLite.

4.1.3 Procedimento de Internação

O primeiro procedimento que deve ocorrer quando um paciente precisa ser internado no hospital é a verificação de seu cadastro Passo (1) da Figura 3. Os dados cadastrais são carregados de um servidor Passo (2) que está conectado, via cabo de rede,

com o computador utilizado. Nesse momento novos pacientes podem ser cadastrados e os que já possuem cadastro podem ter o mesmo atualizado caso haja necessidade. O procedimento subsequente é o registro da internação do paciente Passo (1), onde é preenchido o formulário de internação. Nesse mesmo passo, também ocorre a associação da identificação do paciente à uma *Tag* NFC. Essa *Tag* é acoplada ao leito do paciente no Passo (3). Com isso é possível identificar um paciente de forma facilitada usando-se um *smartphone* ou *tablet*, por exemplo, conforme o Passo (4).

Os procedimentos descritos anteriormente são executados pelo setor administrativo do hospital, onde o recepcionista é o responsável pela operação do sistema no momento da internação. Os próximos procedimentos visam auxiliar os profissionais de saúde (médicos, enfermeiros e técnicos em enfermagem) em suas atividades de cuidados e acompanhamento de pacientes já internados.

Primeiramente, o profissional de saúde deve aproximar seu *smartphone* da *Tag* NFC que estará fixada no leito do paciente. Assim, uma pista para a obtenção da identificação do paciente pode ser recuperada via NFC Passo (4), da Figura 3. Com isso, o profissional pode ler e inserir registros médicos no prontuário do paciente Passo (5) via comunicação *Wi-Fi* de forma segura, devido ao uso do mecanismo apresentado na Seção 4.3.1.

4.2 Análise

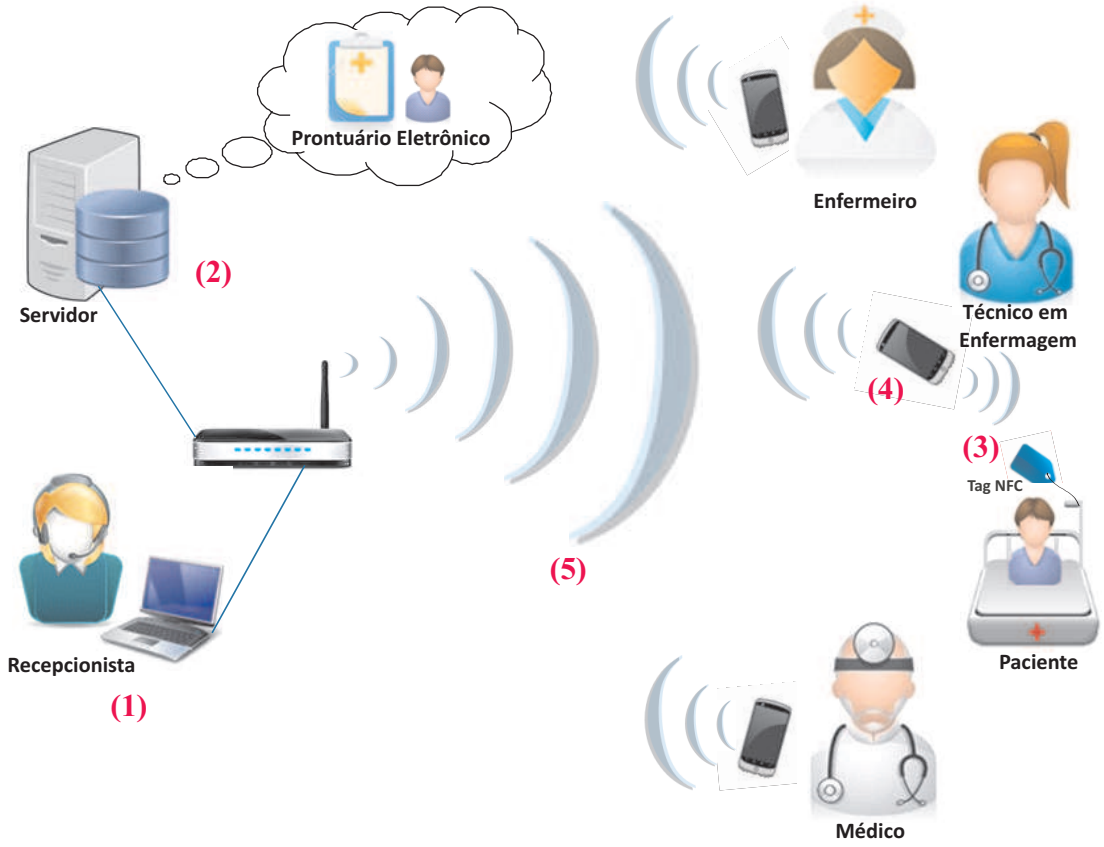
A fim de abstrair as rotinas executadas em ambiente hospitalar, executou-se uma entrevista com os profissionais da área da saúde que trabalham no HCJ. Dessa forma, iniciou-se o levantamento de requisitos do sistema proposto. Os atores responsáveis por manter os prontuários dos pacientes são seguintes: Recepcionista, Técnicos de Enfermagem, Enfermeiros e Médicos. Conforme já discutido na Seção 2.1, o prontuário médico é constituído por uma série de documentos que são atualizados por esses profissionais. Na Seção 4.2.3, é apresentada uma descrição do papel e funções de cada um desses profissionais. Os requisitos que foram levantados divididos entre funcionais e não funcionais. Tais requisitos são listados a seguir.

4.2.1 Requisitos Funcionais

Nesta Seção são elencados os requisitos Funcionais que foram levantados na análise.

- RF 01 – O recepcionista deve ser capaz de cadastrar pacientes;
- RF 02 – O recepcionista deve ser capaz de efetuar buscas por pacientes;
- RF 03 – O recepcionista deve ser capaz de alterar o cadastro de pacientes;

Figura 3 – Arquitetura do Sistema.



Visão Geral da Arquitetura.

- RF 04 – O recepcionista deve ser capaz de fazer o cadastro de medicamentos;
- RF 05 – O recepcionista deve ser capaz de fazer buscas por medicamentos;
- RF 06 – O recepcionista deve ser capaz de alterar o cadastro de medicamentos.
- RF 07 – O recepcionista deve ser capaz de registrar internações de pacientes;
- RF 08 – O recepcionista deve ser capaz de fazer buscas por internações;
- RF 09 – O recepcionista deve ser capaz de registrar altas de pacientes;
- RF 10 – O médico deve ser capaz de inserir o diagnóstico de um paciente;
- RF 11 – O médico deve ser capaz de visualizar o diagnóstico de um paciente;
- RF 12 – O médico deve ser capaz de alterar o diagnóstico de um paciente;
- RF 13 – O médico deve ser capaz de prescrever medicamentos à pacientes;
- RF 14 – O médico deve ser capaz de visualizar os medicamentos prescritos;

- RF 15 – O médico deve ser capaz de cancelar prescrições;
- RF 16 – O médico deve ser capaz de inserir uma Conduta Médica;
- RF 17 – O médico deve ser capaz de visualizar uma Conduta Médica;
- RF 18 – O médico deve ser capaz de atualizar uma Conduta Médica;
- RF 19 – O médico deve ser capaz de inserir notas ao documento de Evolução diária do paciente;
- RF 20 – O médico deve ser capaz de visualizar o documento de Evolução diária do paciente;
- RF 21 – O médico deve ser capaz de inserir prescrições de exames;
- RF 22 – O médico deve ser capaz de cancelar prescrições de exames;
- RF 23 – O médico deve ser capaz de alterar prescrições de exames;

4.2.2 Requisitos Não Funcionais

Esta Seção lista os requisitos Funcionais que foram levantados na análise.

- RFN 01 – O recepcionista deve ser capaz de operar o sistema a partir de um computador com o sistema operacional Windows 7 (ou superior) instalado;
- RFN 02 – O recepcionista deve ser capaz de operar o sistema a partir de um computador com o sistema operacional Windows 7 (ou superior) instalado;
- RFN 03 – O recepcionista deve ser capaz de operar o sistema a partir de um computador com o sistema operacional Windows 7 (ou superior) instalado;
- RFN 04 - O médico deve ser capaz de cadastrar diagnósticos em um computador com o sistema operacional Windows 7 (ou superior) instalado;
- RFN 05 - O médico deve ser capaz de alterar diagnósticos em um computador com o sistema operacional Windows 7 (ou superior) instalado;
- RFN 06 - O médico deve ser capaz de visualizar diagnósticos em um computador ou notebook com o sistema operacional Windows 7 (ou superior);
- RFN 07 - O médico deve ser capaz de prescrever medicamentos em um computador com o sistema operacional Windows 7 (ou superior) instalado;
- RFN 08 - O médico deve ser capaz de prescrever medicamentos em um computador com o sistema operacional Windows 7 (ou superior) instalado;

- RFN 09 - O médico deve ser capaz de prescrever medicamentos em um computador ou notebook com o sistema operacional Windows 7 (ou superior) instalado;
- RFN 10 - O médico deve ser capaz de inserir condutas médicas em um computador com o sistema operacional Windows 7 (ou superior) instalado;
- RFN 11 - O médico deve ser capaz de alterar condutas médicas em um computador com o sistema operacional Windows 7 (ou superior) instalado;
- RFN 12 - O médico deve ser capaz de visualizar condutas médicas em um computador ou notebook com o sistema operacional Windows 7 (ou superior) instalado;
- RFN 13 - O médico deve ser capaz de identificar um paciente via NFC quando utilizar um dispositivo móvel com sistema operacional Android;
- RFN 14 - O médico deve ser capaz de atualizar a Evolução Diária em um computador com o sistema operacional Windows 7 (ou superior) instalado;
- RFN 15 - O médico deve ser capaz de visualizar a Evolução Diária em um computador com o sistema operacional Windows 7 (ou superior) instalado;
- RFN 16 - O médico deve ser capaz de prescrever exames em um computador com o sistema operacional Windows 7 (ou superior) instalado;
- RFN 17 - O médico deve ser capaz de cancelar exames em um computador com o sistema operacional Windows 7 (ou superior) instalado;
- RFN 18 - O médico deve ser capaz de visualizar exames prescritos em um computador ou notebook com o sistema operacional Windows 7 (ou superior).

4.2.3 Escopo, Usuários e seus Papéis

Esta Seção detalha o fluxo de rotinas realizadas diariamente no HJC, bem como os respectivos responsáveis por sua execução. As informações aqui apresentadas foram colhidas por meio de uma entrevista com funcionários do hospital.

4.2.3.1 Recepcionista

O recepcionista é responsável pela manutenção dos cadastros de pacientes e medicamentos além da gerência de internações. Para tal, o mesmo fará uso de uma estação composta por um computador conectado à rede.

Para os Casos de Uso UC01, UC02 e UC03 foram elencados, respectivamente, os requisitos presentes nas Tabelas 2, 3 e 4.

Figura 4 – Diagrama de Caso de Uso - Ator Recepcionista.

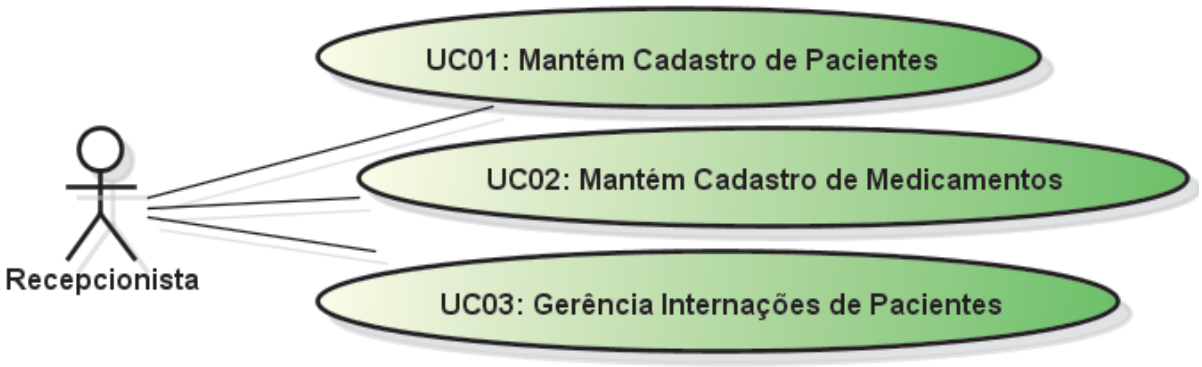


Tabela 2 – Caso de Uso 01 – Mantém Cadastro de Pacientes

UC01 – Mantém Cadastro de Pacientes
Pré-Condições: O usuário deve pertencer ao grupo de usuários "Administradores".
Ator: Recepcionista
Requisitos Funcionais
RF01 – O recepcionista deve ser capaz de cadastrar pacientes; RF02 – O recepcionista deve ser capaz de efetuar buscas por pacientes; RF03 – O recepcionista deve ser capaz de alterar o cadastro de pacientes;
Requisitos Não Funcionais
RNF01 – O recepcionista deve ser capaz de operar o sistema a partir de um computador com o sistema operacional Windows 7 (ou superior) instalado.
Pós Condições: Pacientes têm seu cadastro atualizado no sistema.

4.2.3.2 Médico

O médico deve fazer o diagnóstico da enfermidade de um paciente, além de registrar a prescrição de medicamentos e exames, definir a conduta médica e manter a Evolução Diária Resumida. A Evolução Diária Resumida se difere das demais Evoluções Diárias por ser mais sintética, por exemplo: "O paciente continua com dor".

As rotinas do sistema que são executada por médicos estão elencadas nos Casos de Usos UC04, UC05, UC06, UC07 e UC08 da Figura 5. Esses Casos de Usos são detalhados nas Tabelas 5, 6, 7, 8 e 9, respectivamente.

4.2.3.3 Técnicos em Enfermagem

A segunda versão da Evolução Diária do Paciente é bastante semelhante à primeira, porém nessa são registrados todos os eventos e sintomas presenciados pelos Técnicos de Enfermagem. Os técnicos também devem registrar os atendimentos prestados, bem como

Tabela 3 – Caso de Uso 02 – Mantém Cadastro de Medicamentos

UC02 – Mantém Cadastro de Medicamentos
Pré-Condições: O usuário deve pertencer ao grupo de usuários "Administradores".
Ator: Recepcionista
Requisitos Funcionais
RF04 – O recepcionista deve ser capaz de fazer o cadastro de medicamentos; RF05 – O recepcionista deve ser capaz de fazer buscas por medicamentos; RF06 – O recepcionista deve ser capaz de alterar o cadastro de medicamentos.
Requisitos Não Funcionais
RNF02 – O recepcionista deve ser capaz de operar o sistema a partir de um computador com o sistema operacional Windows 7 (ou superior) instalado.
Pós Condições: Medicamentos têm seu cadastro atualizado no sistema.

Tabela 4 – Caso de Uso 03 – Gerência Internações de Pacientes

UC03 – Gerência Internações de Pacientes
Pré-Condições: O usuário deve pertencer ao grupo de usuários "Administradores".
Ator: Recepcionista
Requisitos Funcionais
RF07 – O recepcionista deve ser capaz de registrar internações de pacientes; RF08 – O recepcionista deve ser capaz de fazer buscas por internações; RF09 – O recepcionista deve ser capaz de registrar altas de pacientes;
Requisitos Não Funcionais
RNF03 – O recepcionista deve ser capaz de operar o sistema a partir de um computador com o sistema operacional Windows 7 (ou superior) instalado.
Pós Condições: Os pacientes são vinculados a internações, as quais têm o seu status atualizado no sistema.

os cuidados realizados e medicamentos administrados, segundo a prescrição dos médicos e enfermeiros. Além disso, os técnicos devem verificar os sinais vitais como pressão arterial, temperatura corporal, frequência respiratória e frequência cardíaca, a fim de efetuar o registro. Os Casos de Usos UC09, UC10, UC11, e UC12, da Figura 6, são detalhados nas Tabelas 10, 11, 12 e 13, respectivamente.

Figura 5 – Diagrama de Casos de Uso - Ator Médico.

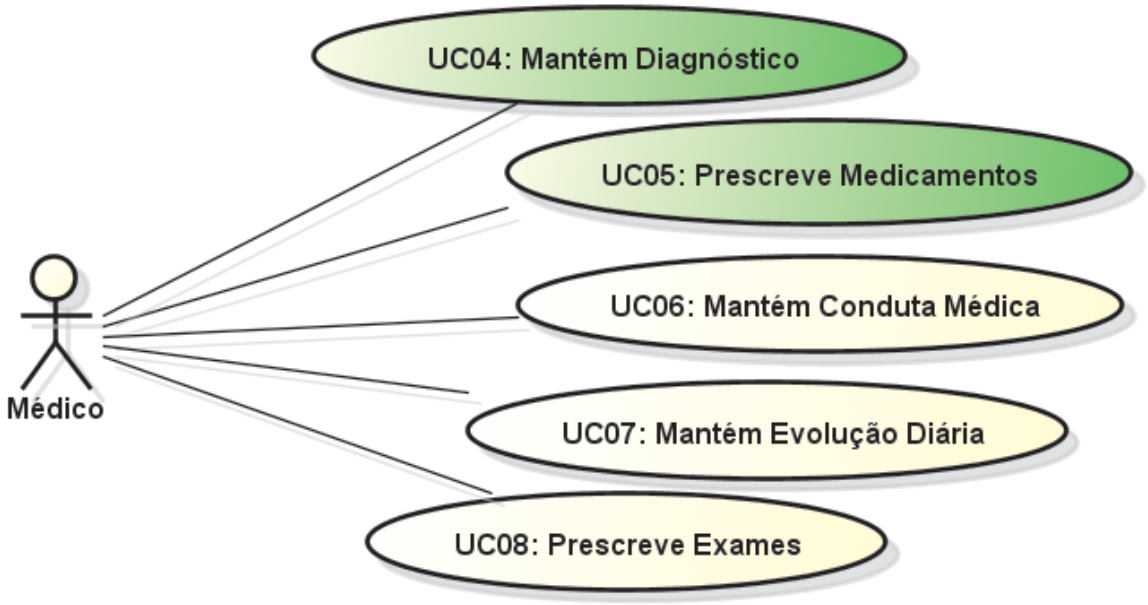


Tabela 5 – Caso de Uso 04 – Mantém Diagnósticos de Pacientes

UC04 – Mantém Diagnóstico
Pré-Condições: O usuário deve pertencer ao grupo de usuários “Médicos”.
Ator: Médico
Requisitos Funcionais
RF10 – O médico deve ser capaz de inserir o diagnóstico de um paciente; RF11 – O médico deve ser capaz de visualizar o diagnóstico de um paciente; RF12 – O médico deve ser capaz de alterar o diagnóstico de um paciente.
Requisitos Não Funcionais
RNF04 - O médico deve ser capaz de cadastrar diagnósticos em um computador com o sistema operacional Windows 7 (ou superior) instalado; RNF05 - O médico deve ser capaz de alterar diagnósticos em um computador com o sistema operacional Windows 7 (ou superior) instalado; RNF06 - O médico deve ser capaz de visualizar diagnósticos em um computador ou notebook com o sistema operacional Windows 7 (ou superior).
Pós Condições: O paciente possui seu diagnóstico atualizado.

4.2.3.4 Enfermeiros

Enfermeiros fazem a avaliação do paciente através de exames físicos e prescrevem cuidados. Além disso, todo evento percebido por enfermeiros são inseridos no documento de Evolução Diária Detalhada. Existem duas versões desse documento: a primeira deve ser

Tabela 6 – Caso de Uso 05 – Prescreve Medicamentos para Pacientes

UC05 – Prescreve Medicamentos
Pré-Condições: O usuário deve pertencer ao grupo de usuários "Médicos". O respectivo paciente e medicamentos devem estar cadastrados.
Ator: Médico
Requisitos Funcionais
RF13 – O médico deve ser capaz de prescrever medicamentos à pacientes; RF14 – O médico deve ser capaz de visualizar os medicamentos prescritos; RF15 – O médico deve ser capaz de cancelar prescrições.
Requisitos Não Funcionais
RNF07 - O médico deve ser capaz de prescrever medicamentos em um computador com o sistema operacional Windows 7 (ou superior) instalado; RNF08 - O médico deve ser capaz de prescrever medicamentos em um computador com o sistema operacional Windows 7 (ou superior) instalado; RNF09 - O médico deve ser capaz de prescrever medicamentos em um computador ou notebook com o sistema operacional Windows 7 (ou superior) instalado.
Pós Condições: Os enfermeiros e técnicos podem visualizar as prescrições para registrar as administrações de medicamentos.

Tabela 7 – Caso de Uso 06 – Mantém Conduta Médica

UC06 – Mantém Conduta Médica
Pré-Condições: O usuário deve pertencer ao grupo de usuários "Médicos". O paciente relacionado a conduta deve estar cadastrados e deve existir uma internação vinculada a este.
Ator: Médico
Requisitos Funcionais
RF16 – O médico deve ser capaz de inserir uma Conduta Médica; RF17 – O médico deve ser capaz de visualizar uma Conduta Médica; RF18 – O médico deve ser capaz de atualizar uma Conduta Médica;
Requisitos Não Funcionais
RNF10 - O médico deve ser capaz de inserir condutas médicas em um computador com o sistema operacional Windows 7 (ou superior) instalado; RNF11 - O médico deve ser capaz de alterar condutas médicas em um computador com o sistema operacional Windows 7 (ou superior) instalado; RNF12 - O médico deve ser capaz de visualizar condutas médicas em um computador ou notebook com o sistema operacional Windows 7 (ou superior) instalado.
Pós Condições: Os enfermeiros e técnicos podem visualizar as condutas médicas para efetuar os cuidados para aos pacientes.

Tabela 8 – Caso de Uso 07 – Mantém Evolução Diária

UC07 – Mantém Evolução Diária
Pré-Condições: O usuário deve pertencer ao grupo de usuários "Médicos". O paciente relacionado a Evolução Diária deve estar cadastrados e deve existir uma internação vinculada a este.
Ator: Médico
Requisitos Funcionais
RF19 – O médico deve ser capaz de inserir notas ao documento de Evolução diária do paciente; RF20 – O médico deve ser capaz de visualizar o documento de Evolução diária do paciente;
Requisitos Não Funcionais
RNF13 - O médico deve ser capaz de identificar um paciente via NFC quando utilizar um dispositivo móvel com sistema operacional Android; RNF14 - O médico deve ser capaz de atualizar a Evolução Diária em um computador com o sistema operacional Windows 7 (ou superior) instalado; RNF15 - O médico deve ser capaz de visualizar a Evolução Diária em um computador com o sistema operacional Windows 7 (ou superior) instalado;
Pós Condições: Os enfermeiros e médicos podem visualizar o histórico das Evoluções de pacientes.

Tabela 9 – Caso de Uso 08 – Prescreve Exames

UC08 - Prescreve Exames
Pré-Condições: O usuário deve pertencer ao grupo de usuários "Médicos". O paciente relacionado ao exame a ser prescrito deve estar cadastrados.
Ator: Médico
Requisitos Funcionais
RF21 – O médico deve ser capaz de inserir prescrições de exames. RF22 – O médico deve ser capaz de cancelar prescrições de exames. RF23 – O médico deve ser capaz de alterar prescrições de exames.
Requisitos Não Funcionais
RNF16 - O médico deve ser capaz de prescrever exames em um computador com o sistema operacional Windows 7 (ou superior) instalado; RNF17 - O médico deve ser capaz de cancelar exames em um computador com o sistema operacional Windows 7 (ou superior) instalado; RNF18 - O médico deve ser capaz de visualizar exames prescritos em um computador ou notebook com o sistema operacional Windows 7 (ou superior).
Pós Condições: Os enfermeiros e médicos podem visualizar o histórico das prescrições de exames para pacientes.

Figura 6 – Diagrama de Casos de Uso - Ator Técnico.

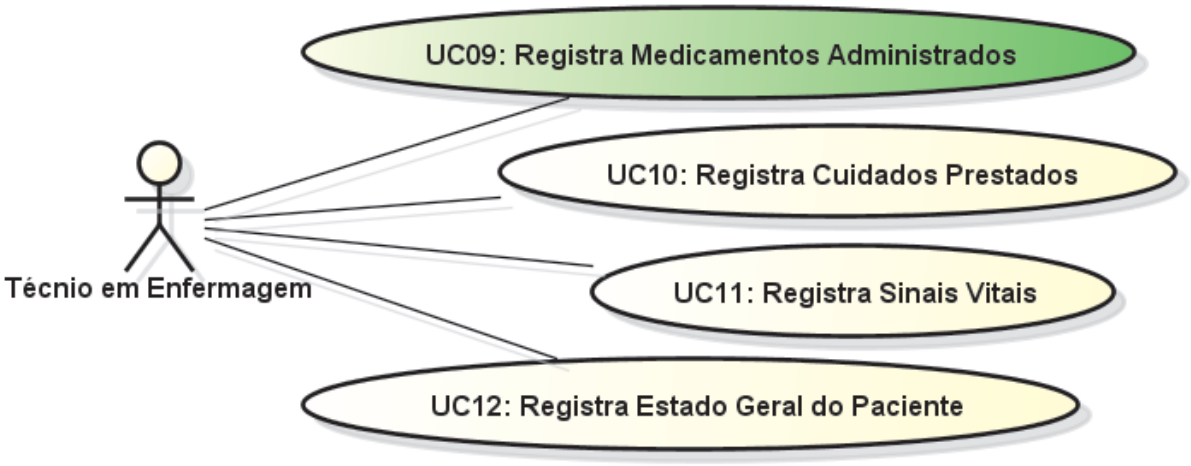


Tabela 10 – Caso de Uso 09 – Registra Medicamentos Administrados

UC09 - Registra Medicamentos Administrados
Pré-Condições: O usuário deve pertencer ao grupo de usuários “Técnicos”. O medicamento deve estar prescrito para o paciente.
Ator: Técnico de Enfermagem
Requisitos Funcionais
RF22 – O técnico deve ser capaz de consultar as prescrições de medicamentos. RF23 – O técnico deve ser capaz de registrar as administrações de medicamentos.
Requisitos Não Funcionais
RNF13 - O técnico deve consultar prescrições através de um dispositivo móvel com sistema operacional Android 4.2 (ou superior). RNF14 - O técnico deve registrar administrações de medicamentos através de um dispositivo móvel com sistema operacional Android 4.2 (ou superior).
Pós Condições: As administrações concluídas têm seu status atualizado e não aparecem mais na lista de administrações pendentes.

inserida por enfermeiros. Essa versão contém informações que dão origem aos cuidados que serão prescritos pelos próprios enfermeiros. O diagrama de casos de uso está representado na Figura 7. A descrição detalhada dos casos de usos UC13, UC14 e UC15 é apresentada, respectivamente, nas tabelas 14, 15 e 16.

4.3 Modelagem e Projeto

Através da análise da seção anterior, é possível definir algumas propriedades a fim de construir uma representação da modelagem das classes que o farão parte do sistema proposto, bem como suas associações e interações. Para complementar os requisitos

Tabela 11 – Caso de Uso 10 - Registra Cuidados Prestados

UC10 - Registra Cuidados Prestados
Pré-Condições: O usuário deve pertencer ao grupo de usuários "Técnicos". O paciente deve estar cadastrado e vinculado a uma internação.
Ator: Técnico de Enfermagem
Requisitos Funcionais
RF23 – O técnico deve ser capaz de consultar as prescrições de cuidados. RF24 – O técnico deve ser capaz de registrar os cuidados prestados.
Requisitos Não Funcionais
RNF01 - O técnico deve consultar cuidados através de um dispositivo móvel com sistema operacional Android 4.2 (ou superior).
RNF02 - O técnico deve registrar cuidados prestados através de um dispositivo móvel com sistema operacional Android 4.2 (ou superior).

Tabela 12 – Caso de Uso 11 - Registra Cuidados Prestados

UC11 - Registra Sinais Vitais
Pré-Condições: O usuário deve pertencer ao grupo de usuários "Técnicos". O paciente deve estar cadastrado e vinculado a uma internação.
Ator: Técnico de Enfermagem
Requisitos Funcionais
RF25 – O técnico deve ser capaz de registrar os sinais vitais de um paciente, tais como pressão arterial, frequência respiratória, frequência cardíaca e temperatura corporal.
Requisitos Não Funcionais
RNF01 - O técnico deve registrar os sinais vitais através de um dispositivo móvel com sistema operacional Android 4.2 (ou superior).

levantados na análise, o fluxo de rotinas do HCJ foi mapeado como segue.

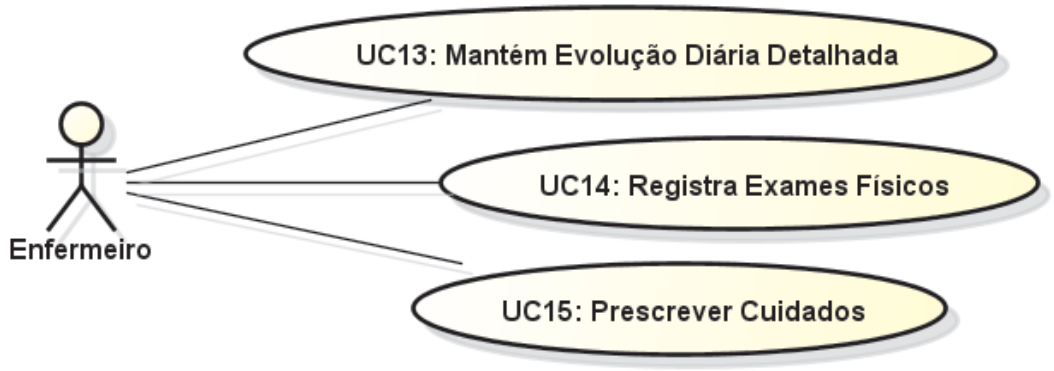
O fluxo de rotinas é iniciado a partir do momento em que ocorre a internação de um paciente. Nesse momento, o recepcionista deve verificar se o mesmo já possui cadastro e fazê-lo quando não houver. No cadastro do paciente são gravados inicialmente os dados pessoais tais como Nome, CPF e Endereço. Uma relação completa dos dados cadastrais pode ser visualizada na Figura 10.

A partir do momento em que um paciente chega no hospital e já está cadastrado, é gerada então uma ficha onde o médico deve escrever o Diagnóstico do Paciente. Essa operação pode ser embasada em exames, nesse caso os resultados dos exames serão armazenados e vinculados ao cadastro da entidade examinada. Após a internação de um

Tabela 13 – Caso de Uso 12 - Registra Estado Geral do Paciente

UC12 - Registra Estado Geral do Paciente
Pré-Condições: O usuário deve pertencer ao grupo de usuários “Técnicos”. O paciente deve estar cadastrado e vinculado a uma internação.
Ator: Técnico de Enfermagem
Requisitos Funcionais
RF26 – O técnico deve ser capaz de registrar o estado de saúde de um paciente.
Requisitos Não Funcionais
RNF01 - O técnico deve registrar informações sobre o estado de um paciente, através de um dispositivo móvel com sistema operacional Android 4.2 (ou superior).

Figura 7 – Diagrama de Casos de Uso - Ator Enfermeiro.



paciente, existem alguns documentos que são atualizados periodicamente.

Com base no diagnóstico inicial, o médico deverá decidir por uma conduta a ser tomada. A conduta consiste em uma resposta de ação ao diagnóstico. A conduta é atualizada toda vez que o diagnóstico sofrer alterações. Podemos então concluir que um exame pode acarretar na alteração de um diagnóstico, e consequentemente a conduta.

Ao fazer a abstração dessas informações, é possível montar o diagrama de clases do sistema. Esse diagrama é exibido na Figura 10. Além disso, o diagrama de Entidade Relacionamento é exibido na Figura 8. Nesse diagrama estão representadas as tabelas onde são armazenados os registros a cerca dos cadastro de pacientes *TBL_PACIENTES*, cadastro de medicamentos *TBL_MEDICAMENTOS*, internações *TBL_INTERNACOES* e prescrições de medicamentos a pacientes internados *TBL_PRESCRICOES*.

Assim, a *TBL_INTERNACOES* depende da existência da *TBL_PACIENTES*, pois somente um paciente cadastrado pode ser internado. Seguindo essa mesma lógica, a tabela *TBL_PRESCRICOES* depende também da tabela *TBL_PACIENTES*, e da tabela *TBL_INTERNACOES*, já que para que um medicamento possa ser prescrito para

Tabela 14 – Caso de Uso 13 – Mantém Evolução Diária Detalhada dos Pacientes

UC13 – Mantém Evolução Diária Detalhada
Pré-Condições: O usuário deve pertencer ao grupo de usuários "Enfermeiros", e também o respectivo paciente deve estar cadastrado e internado no hospital.
Ator: Enfermeiro
Requisitos Funcionais
RF27 – O Enfermeiro deve ser capaz de acrescentar informações ao documento de Evolução Diária do Paciente; RF28 – O Enfermeiro deve ser capaz de visualizar o documento de Evolução Diária do Paciente;
Requisitos Não Funcionais
RNF01 - O enfermeiro deve ser capaz de identificar um paciente via NFC quando utilizar um dispositivo móvel com sistema operacional Android; RNF02 - O Enfermeiro deve ser capaz de efetuar todos os procedimentos de manutenção de Evolução Diária do Paciente através de um dispositivo móvel com sistema operacional Android 4.2 (ou superior).
Pós Condições: Os médicos e enfermeiros podem visualizar o histórico de evoluções diárias de um paciente.

Tabela 15 – Caso de Uso 14 – Registra Exames Físicos

UC14 – Registra Exames Físicos
Pré-Condições: O usuário deve pertencer ao grupo de usuários "Enfermeiros", e também o respectivo paciente deve estar cadastrado e internado no hospital.
Ator: Enfermeiro
Requisitos Funcionais
RF29 – O Enfermeiro deve ser capaz de acrescentar informações ao documento de Registro de Exames Físicos; RF30 – O Enfermeiro deve ser capaz de visualizar o documento de Registro de Exames Físicos;
Requisitos Não Funcionais
RNF01 - O enfermeiro deve ser capaz de identificar um paciente via NFC quando utilizar um dispositivo móvel com sistema operacional Android; RNF02 - O Enfermeiro deve ser capaz de efetuar todos os procedimentos de manutenção de Registro de Exames Físicos através de um dispositivo móvel com sistema operacional Android 4.2 (ou superior).
Pós Condições: Os médicos e enfermeiros podem visualizar o histórico de exames físicos de um paciente.

um paciente o mesmo deve estar cadastrado e também internado. Adicionalmente, outra tabela essencial para uma prescrição consiste na tabela onde ficam os medicamentos

Tabela 16 – Caso de Uso 15 – Prescreve Cuidados ao Paciente

UC15 – Prescreve Cuidados
Pré-Condições: O usuário deve pertencer ao grupo de usuários "Enfermeiros", e também o respectivo paciente deve estar cadastrado e internado no hospital.
Ator: Enfermeiro
Requisitos Funcionais
RF31 – O Enfermeiro deve ser capaz de acrescentar informações ao documento de Prescrição de Cuidados do paciente; RF32 – O Enfermeiro deve ser capaz de visualizar o documento de Registro de Prescrição de Cuidados do paciente;
Requisitos Não Funcionais
RNF01 - O enfermeiro deve ser capaz de identificar um paciente via NFC quando utilizar um dispositivo móvel com sistema operacional Android; RNF02 - O Enfermeiro deve ser capaz de efetuar todos os procedimentos de manutenção de Registro de Prescrição de Cuidados através de um dispositivo móvel com sistema operacional Android 4.2 (ou superior).
Pós Condições: Os Técnicos de Enfermagem podem visualizar as prescrições de cuidados.

cadastrados *TBL_MEDICAMENTOS*.

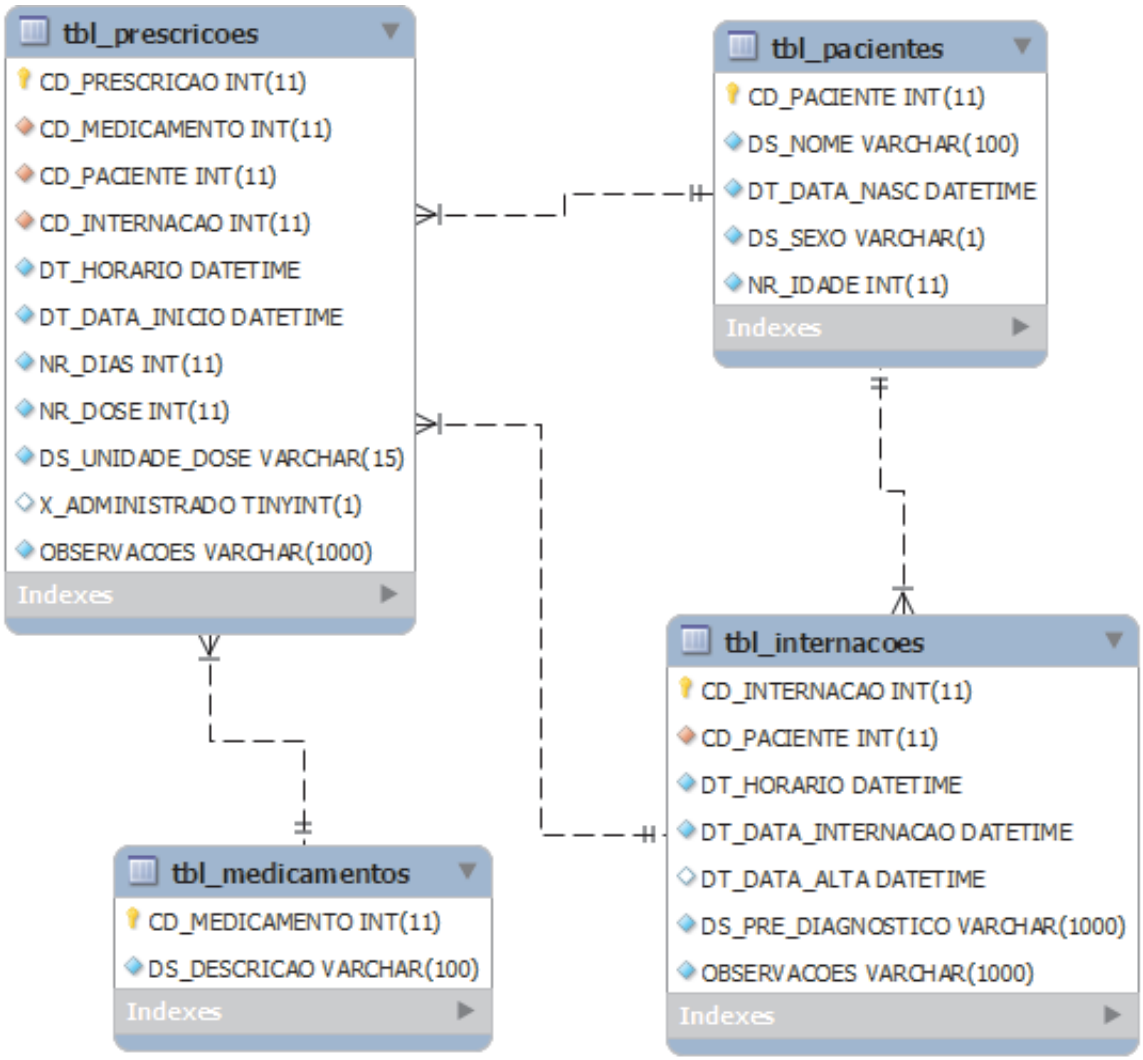
4.3.1 Mecanismo de Autenticação

A identificação dos pacientes vinculada ao seu prontuário serve de base para muitos procedimentos de cuidados médicos, bem como para ao acesso as informações confidenciais de pacientes. Assim, a captura ou adulteração dos dados transmitidos no meio sem fio poderia originar erros como administração equivocada de medicamentos ou prestação de cuidados inadequados ao diagnóstico do paciente. Além disso, a privacidade de pacientes também pode estar em risco. Portanto, deve-se evitar o acesso indevido a identidades e registros de pacientes por pessoas não autorizadas, por exemplo, um visitante.

A transmissão de dados entre dispositivos pode estar sendo escutada por atacantes, ou ainda, impostores podem tentar se passar por dispositivos legítimos para ter acesso às informações pessoais de terceiros. Assim, a fim de limitar o acesso a tais informações somente para pessoal autorizado, se faz necessário o uso de um mecanismo de autenticação para verificar a identidade das partes envolvidas na conversação.

No contexto da presente proposta, uma *tag* NFC tem papel fundamental na identificação dos pacientes e medicamentos. Para tal, as *tags* devem ser acopladas aos leitos dos pacientes, como ilustrado na Figura 3. O protocolo NDEF não estabelece nenhum mecanismo de proteção aos dados transmitidos e gravados em *tags* NFC (SETHIA et al.,

Figura 8 – Modelo Entidade Relacionamento - ER



2014). Dessa forma, um ponto altamente vulnerável a ataques é a comunicação entre os *smartphones* e *tags*.

Dado que muitas *tags* não têm a capacidade de processar informações, o mecanismo proposto foi projetado para funcionar nesses dispositivos, que possuem menor custo. Essas *tags* se limitam a oferecer as funcionalidades de leitura e escrita para seus leitores quando energizadas pela própria onda de rádio emitida pelo leitor. Portanto, esse tipo de *tag* não suporta qualquer mecanismo que necessite fazer processamentos. Na Figura 9, é possível visualizar as mensagens trocadas entre *tags*, *smartphones* e o servidor durante o processo de autenticação e recuperação de identificação de pacientes. Esse processo antecede e restringe o acesso e modificação de qualquer tipo de informação armazenada no servidor por parte dos *smartphones*, ou seja, apenas dispositivos legítimos serão capazes de acessar ou alterar informações da base de dados do Servidor.

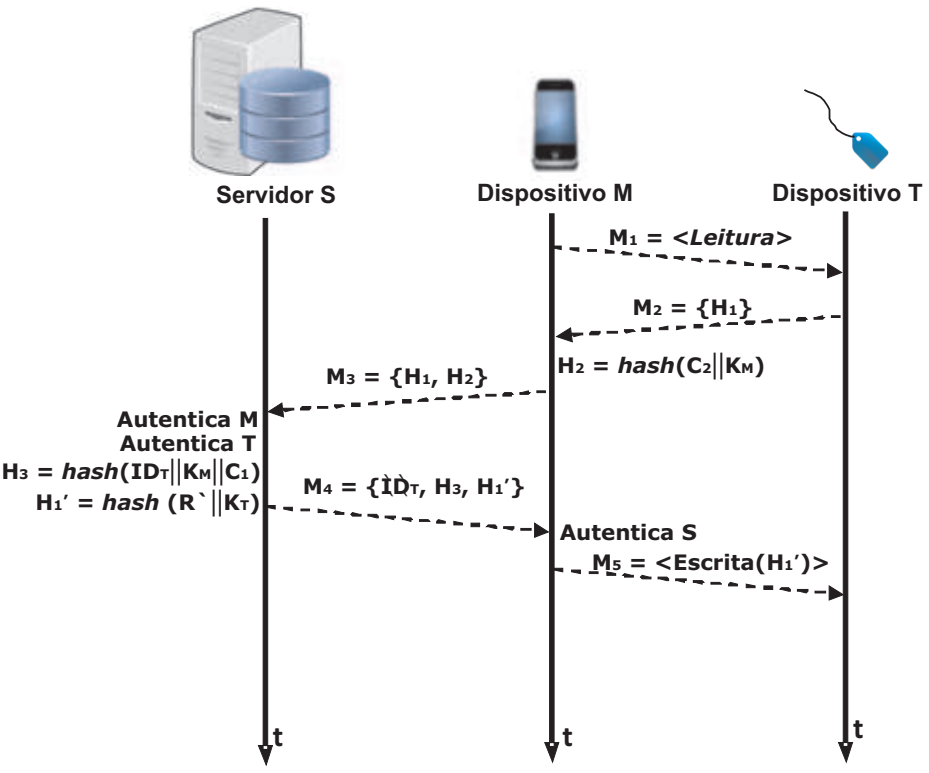
Suponha que cada um dos Dispositivos T representa uma *tag*, acoplada ao leito do paciente. Um Dispositivo T possui um resumo *hash* H_1 pré carregado. Esse resumo consiste do resultado da função *hash* que tem como entrada um número aleatório R, gerado pelo servidor S, concatenado com a chave K_T que corresponde a respectiva *tag*. Dessa forma, T armazena $H_1 = hash(R||K_T)$.

O Dispositivo M representa o dispositivo móvel, que consiste em um (*smartphone*) de um profissional da saúde. Tal dispositivo, possui uma chave K_M que compartilha com o servidor e também um contador de transações C_2 que é incrementado a cada conversação realizada. Além disso, no momento da autenticação, M gera H_2, que consiste no hash dessas informações.

O servidor S possui uma base de dados, onde são armazenadas informações que apóiam o funcionamento do mecanismo de autenticação. Para cada registro correspondente a uma *tag* T cadastrada no sistema, são armazenados os seguintes atributos: a identificação ID_T, a chave K_T, o número aleatório R utilizado na geração de tal chave e o resumo *hash* da concatenação de R com K_T - denominado H_1'. Além disso, para cada *smartphone* cadastrado no servidor, é armazenada uma chave compartilhada K_M, um contador de transações C_1 e o hash de K_M concatenado com C_1, denominado H_2'.

Dado que qualquer dispositivo com capacidade de leitura NFC é capaz de obter H_1

Figura 9 – Processo de Identificação segura de *tags* pelo *smartphone*



sem nenhum tipo de verificação de identidade, o servidor trata esse problema através do mecanismo de autenticação apresentado nesta Seção. Assim, antes de retornar quaisquer informações sobre um paciente para um dispositivo que fez uma requisição, o servidor verifica sua autenticidade. Dessa forma, a informação H_1 consiste em uma pista para que um dispositivo legítimo obtenha ID_T, ou seja, o ID da respectiva *tag* T que foi lida.

Na prática, o processo de obtenção de *ID* do paciente, a fim de se ter acesso aos dados do mesmo é precedido pela autenticação dos dipositivos T e M pelo servidor, e também a autenticação de T e S pelo dispositivo M. Para se dar início a tal processo, o Dispositivo M deve ser aproximado do Dispositivo T, a fim de recuperar H_1. A primeira mensagem M_1 do mecanismo consiste em uma requisição de leitura de T por M. Na próxima mensagem, denominada M_2, o Dispositivo T responde ao Dispositivo M com o hash H_1 que foi previamente gravado nessa tag.

Então, após a leitura de H_1 obtido de T, no passo anterior, o *Smartphone* deve computar o resumo *hash* H_2, que é gerado a partir da concatenação do contador de transações C_2 com K_M. Ou seja, $H2 = hash(C_2||K_M)$. O Dispositivo M envia então uma mensagem M_3, contendo H_1 e H_2 para o Servidor S.

O Servidor S é capaz de verificar a validade de H_2 através da comparação desse *hash* com cada H_2' armazenado em sua base de dados. Uma vez que essa comparação for bem sucedida, o Dispositivo M é considerado autêntico. O processamento anterior é descrito no Algoritmo 1. Quando M é considerado autêntico, S inicia o processo de autenticação de T, onde T corresponde a *tag* lida anteriormente pelo *Smartphone* M. Esse procedimento consiste na comparação de *hash* H_1 recebido de M com cada H_1' armazenado. Quando a igualdade for satisfeita, T é considerado autêntico e C_1 é incrementado.

A partir desse momento, o Servidor S assume que está conversando com um dispositivo M confiável e que o mesmo fez a leitura de uma tag T legítima. Assim, M está apto a receber ID_T. Portanto, visto que um atacante pode escutar essa conversa, a solução empregada pelo mecanismo consiste na utilização da chave K_M para cifrar as informações sensíveis antes da transmissão das mesmas. No caso da mensagem M_4, a informação relevante é o ID_T.

Então, S computa o *hash* H_3 a partir da concatenação de $E_{K_M}(ID_T)$, K_M e C_1. A fim de refrescar a pista gravada em T, para que a cada autenticação essa pista deja diferente, S calcula H_1' a partir da geração de um número aleatório R' concatenado à chave K_T. O *hash* H_1' de uma autenticação conssite no *hash* H_1 da próxima autenticação. Após gerar os resumos H_3 e H_1', o Servidor S envia para o Dispositivo M a mensagem M_4, contendo H_3, H_1' e $E_{K_M}(ID_T)$. É importante notar que ID_T é cifrado com K_M, essa cifragem é denotada com as listras sobre o ID_T na Figura 4.3.1.

O Dispositivo M computa o *hash* H_3' da concatenação de ID_T, K_M e C_2. Ao

comparar H_3 com H'_3, S é considerado um servidor legítimo quando essa comparação resultar em sucesso. Assim, o contador C_2 é incrementado e H'_1 é gravado em T. O Algoritmo 2 ilustra tal processo de autenticação. Ao término desse processo, o usuário do smartphone tem permissão de acesso aos registros do paciente. Toda informação confidencial a partir desse momento é cifrada com K_M antes de ser transmitida.

4.4 Implementação

Nesta Seção serão descritos os algoritmos mais relevantes, que consistem no mecanismo de autenticação. Esses algoritmos utilizam basicamente resumos *hashes*, listas de *Strings* e alguns métodos de recebimento e envio de mensagens via NFC e TCP. Para fins didáticos, pseudo-códigos que representam os algoritmos implementados são apresentados a seguir.

O Algoritmo 1 consiste no processo de autenticação do dispositivo móvel M e da *tag* T, que é feito pelo servidor S. Esse pseudo-algoritmo foi traduzido para a linguagem de programação *Java*, para *desktop*.

Por outro lado, o Algoritmo 2 representa o processo onde o dispositivo móvel M autentica o servidor S. Esse pseudo-algoritmo foi traduzido para a linguagem de programação *Java*, para Android a fim de rodar no sistema operacional do *Smartphone* utilizado.

4.5 Telas do Sistema

Nesta seção serão apresentadas algumas das telas - interfaces gráficas - do sistema. Primeiramente, na Figura 11, é possivel visualizar a interface onde o recepcionista é capaz de fazer o cadastro e manutenção de pacientes. Em seguida, na Figura 12, é possivel visualizar a interface onde o recepcionista cadastra e faz a manutenção de medicamentos.

Na Figura 13, é apresentada a interface onde o recepcionista faz a internação de pacientes e digita o diagnóstico prévio, informado pelo médico no momento da internação. Em seguida, na Figura 14 é exibida a interface onde o médico faz a prescrição de medicamentos a um paciente.

A Figura 15 apresenta a interface onde enfermeiros e técnicos em enfermagem são capazes de visualizar o pré diagnóstico de um paciente. Além dessa informação, nessa mesma interface são exibidas as datas de internação e nascimento do paciente além do médico responsável pelo conteúdo registrado. Essa interface é exibida e a informação recuperada assim que houver uma aproximação de um *smartphone* autêntico da tag que está no leito de um paciente. No momento em que esse profissional toca no menu de administrações de medicamentos, destacado na Figura 16, é exibida nessa mesma interface, da Figura 16, a lista de medicamentos prescritos àquele paciente.

Algoritmo 1 Verifica M

```
1: Mobile M = new Mobile(C_1, K_M, H'_2)
2: Tag T = new Tag(ID, K_T, H'_1)
3: Lista Mobiles L_M[ ] = {M_1, M_2, ..., M_n}
4: Lista Tags L_T[ ] = {T_1, T_2, ..., T_n}
5: String H_1, H_2, H_3, H'_1
6: H_1 = RecebeH_1()
7: H_2 = RecebeH_2()
8: for i = 0 até |L_M| do
9:    if H_2 = H'_2 then
10:      Autenticação de M bem Sucedida
11:      M = M_[i]
12:      for i = 0 até |L_T| do
13:         if H_1 = H'_1 then
14:            T = T_[i]
15:            Autenticação de T bem Sucedida
16:            M.C_1 = C_1 + 1
17:            H_3 = hash (T.ID||M.K_M||C_1)
18:            H'_1 = hash (R'||T.K_T)
19:            Envia(T.ID, H_3, H'_1)
20:         end if
21:      end for
22:   end if
23: end for
24: if M = null then
25:   Envia "Falha na Autenticação do Dispositivo Móvel."
26: end if
27: if T = null then
28:   Envia "Falha na Autenticação da Tag."
29: end if
```

Algoritmo 2 Verifica S

```
1: String C_2, K_M, ID_T, H_1, H_2, H_3
2: ID_T = RecebeID_T();
3: H_3 = RecebeH_3();
4: H'_1 = RecebeH'_1();
5: if H_3 = H'_3 then
6:    Autenticação bem Sucedida
7:    C_2 = C_2 + 1
8:    EscritaTag(H'_1)
9: end if
10: if H_3 ≠ H'_3 then
11:   Falha de Autenticação
12: end if
```

Figura 10 – Diagrama de Classes do Sistema

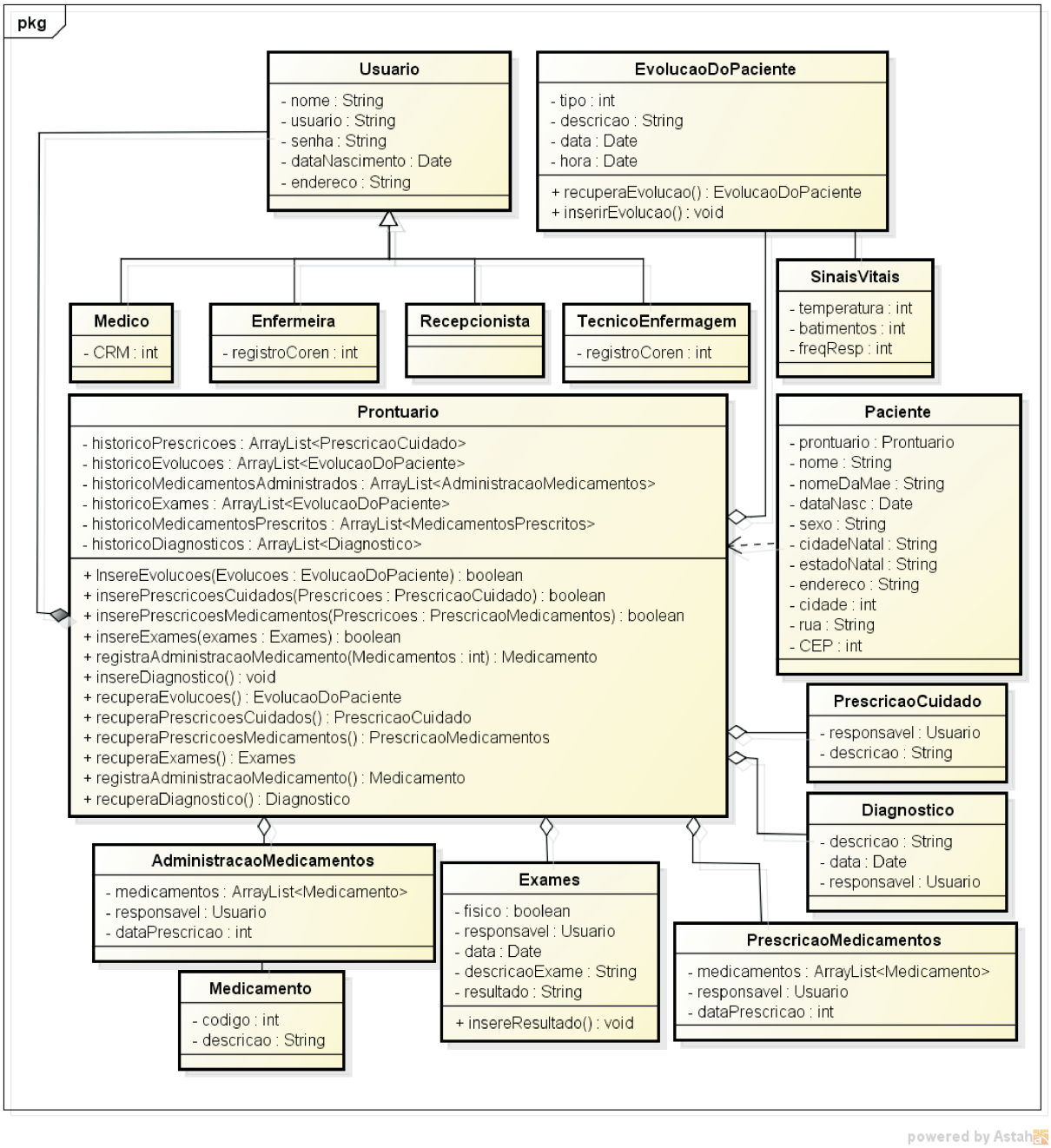


Figura 11 – Interface de Cadastro de Pacientes

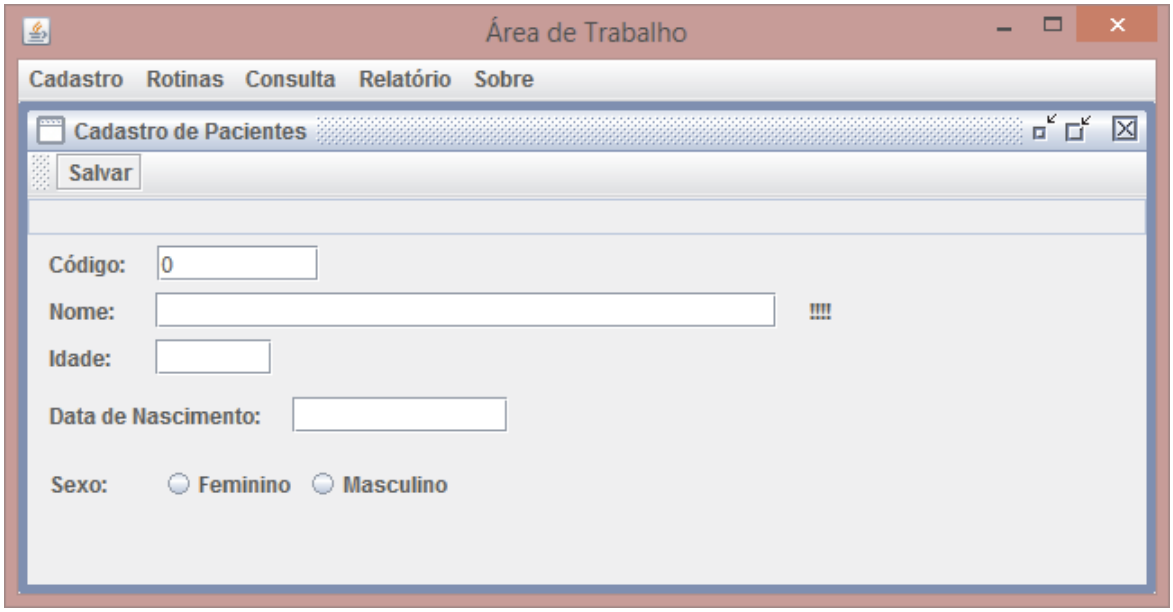


Figura 12 – Interface de Cadastro de Medicamentos

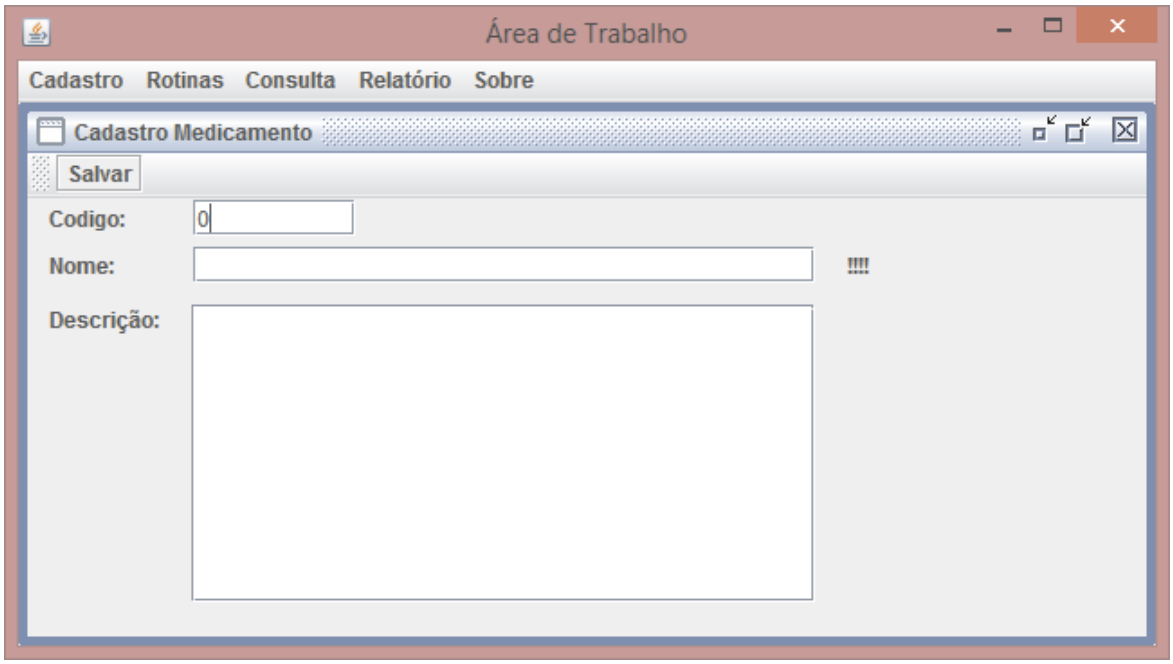


Figura 13 – Interface de Internações de Pacientes

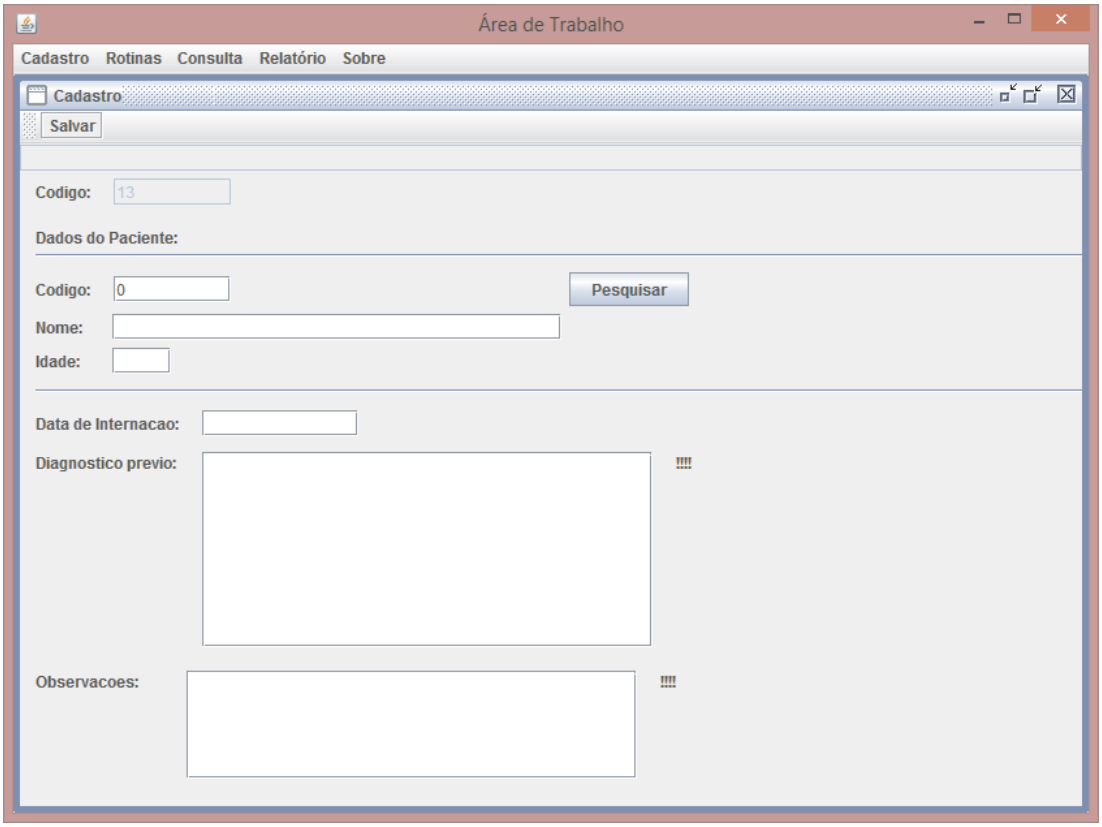


Figura 14 – Interface de Prescrição de Medicamentos

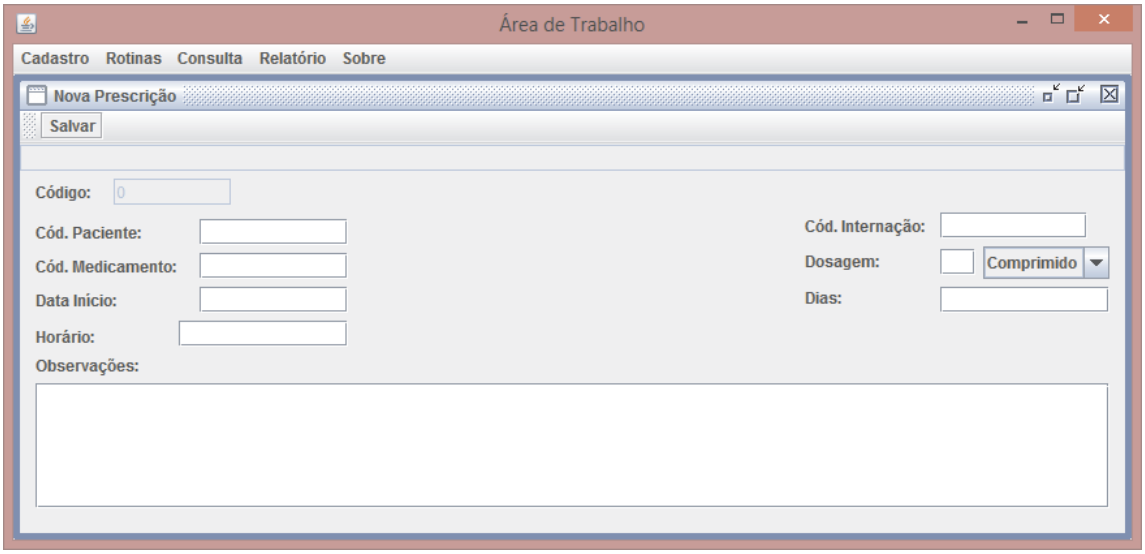


Figura 15 – Interface de Identificação de Pacientes

Figura 16 – Interface de Administração de Medicamentos

5 Avaliação

Neste capítulo é apresentada a análise, avaliação prática e validação da arquitetura proposta. Primeiramente, na Seção 5.2, a análise da segurança dessa arquitetura é discutida. Em seguida, são detalhados na Seção 5.3 os experimentos práticos baseados em um protótipo. Tal protótipo foi avaliado no HCJ, onde foram envolvidos profissionais da saúde com diferentes cargos. Adicionalmente, a fim de provar a eficiência do mecanismo de segurança, foi executada uma validação através da lógica BAN (BURROWS; NEEDHAM, 1990), na Seção 5.1.

5.1 Validação do Mecanismo de Segurança

Um dos componentes da arquitetura proposta, que é essencial para a segurança da mesma, consiste em um Mecanismo de Autenticação. A fim de validar tal mecanismo, o mesmo foi submetido à prova de segurança imposta pela metodologia BAN. Tal metodologia utiliza um conjunto de expressões lógicas. As expressões utilizadas nesse trabalho estão descritas na Tabela 17.

Tabela 17 – Notação da Lógica BAN.

Representação	Significado
A $\mid\equiv$ B	A acredita em B: Para A, B é verdadeiro
A $\triangleleft$ X	A recebe X: A recebeu uma mensagem contendo M.
P $\mid\sim$ X	P disse X: P enviou uma mensagem contendo X.
P $\mid\Rightarrow$ X	P tem jurisdição sobre X: P é responsável por X.
#(X)	*Novo* X: X é novo e não foi utilizado antes em nenhuma sessão.
$\{X\}_K$	Fórmula X cifrada com a chave k
$A \overset{K}{\leftrightarrow} B$	K é uma chave de conhecimento exclusivo de A e B.
$\frac{F}{F'}$	Se a fórmula F for considerada verdadeira, isso infere que F' é verdadeira.

Os objetos distinguidos pela notação básica da lógica BAN nesse trabalho são os participantes T, M e S. Além desses, são distinguidas as chaves simétricas K_M e K_T, e os contadores C_1 e C_2. As mensagens envolvidas no protocolo, conforme discutido na Seção 4.3.1, podem ser descritas da seguinte forma:

M1. $M \rightarrow T : Leitura$

M2. $T \rightarrow M : hash(R||K_T)$

M3. $M \rightarrow S : hash(R||K_T), hash(C_2||K_M)$

M4. $S \rightarrow M : K_M(ID_T), hash(ID_T||K_E||C_1), hash(R||K_T)$

M5. $M \rightarrow T : hash(R||K_T)$

A representação de uma mensagem enviada consiste no símbolo: $\rightarrow$. Para representar uma mensagem M enviada de A para B, usa-se A $\rightarrow$ B: M, por exemplo.

5.1.0.0.1 Idealização

O processo de Idealização busca padronizar - ou formalizar - a escrita do protocolo a ser validade, de acordo com a notação BAN.

M2. $T \rightarrow M : H(\#(R)||K_T)$

M3. $M \rightarrow S : H(\#(R)||K_T), H(\#(C_2)||K_M)$

M4. $S \rightarrow M : K_M\{ID_T\}, H(ID_T||K_M||\#(C_1)), H(\#(R)||K_T)$

5.1.0.0.2 Suposições

A partir do protocolo idealizado, é possível de se fazer algumas suposições para mais adiante por as mesmas à prova.

1. $S \mid\Rightarrow K_T$
2. $S \mid\equiv S \overset{K}{\leftrightarrow} B$ M
3. $S \mid\equiv ID_T$
4. $S \mid\Rightarrow C_1$
5. $S \mid\Rightarrow R$
6. $S \mid\equiv T$
7. $S \mid\equiv M$
8. $S \mid\equiv M \mid\equiv K_M$
9. $S \mid\equiv M \mid\equiv T \mid\equiv H(R||K_T)$

10. $T \mid \equiv H(R||K_T)$
11. $T \mid \sim M\ H(R||K_T)$
12. $M \triangleleft S\ \{ID_T\}K_M$
13. $M \mid \equiv S\ A \overset{K}{\leftrightarrow} B\ M$
14. $M \mid \Rightarrow C_2$
15. $M \triangleleft ID_T$
16. $M \mid \equiv S$
17. $M \mid \equiv T$
18. $M \mid \equiv T \mid \equiv H(R||K_T)$
19. $M \mid \equiv S \mid \equiv ID_T$
20. $M \mid \equiv S \mid \equiv K_T$
21. $M \mid \equiv S \mid \equiv K_M$
22. $M \mid \equiv S \mid \equiv C_1$
23. $M \mid \sim S\ H(R||K_T)$
24. $M \mid \sim S\ H(\#\{C_2\}||K_M)$

5.1.0.0.3 Avaliação de Segurança

Esta Seção faz a análise sobre os postulados - fórmulas - apresentados na Seção anterior. Assim, pode-se provar se os objetivos do protocolo estão sendo alcançados.

M2:

25. Como M desconhece K_T, a informação dessa mensagem não é suficiente para afirmar que M acredita T como verdade. Em outras palavras, essa mensagem ainda não autentica T perante M, mas prova que T acredita na informação que foi transmitida. Além disso, apesar de M desconhecer R, a presença de $\#(R)$ torna $\#(H(R||K_T))$. Ou seja, o *hash* recebido de T é fresco para M. Assim a propriedade de anti-rastreio é alcançada, impossibilitando que essa informação seja associada com T.

$$\frac{T|\sim H(\#(R)||K_T)M}{M|\equiv T|\equiv H(R||K_T)}\ ,\ \frac{\#(R)}{\#(H(R||K_T))}\ \text{Logo,}\ \frac{T|\sim H(\#(R)||K_T)M}{M|\equiv \#(H(R||K_T))}$$

M3:

26. Com base na premissa de que S tem jurisdição sobre C_1 - que deve ser idêntico a C_2 - e na premissa que S compartilha K_M com M, ao receber o resumo *hash* de C_2 concatenado a K_M, o Servidor S consegue computar o *hash* dessas informações e comparar com $H(\#C_2||K_M)$. Assim, S acredita que M é autêntico. Dado que o contador C_1 deve estar igual ao contador C_2, que é um valor fresco, S tem a segurança contra ataques de repetição de mensagem, o que reforça essa crença.

$$\frac{S|\Rightarrow C_1, S \overset{K_M}{\leftrightarrow} M, S \triangleleft H(\#(C_2)||K_M)}{S|\equiv M}$$

27. O resumo consiste em um resumo fresco devido a presença de $\#(R)$. Dessa forma, o dispositivo S, que conhece o *hash* de R concatenado a K_T acredita que a mesma é oriunda de uma tag T autêntica, com a garantia de que não se trata de um ataque de repetição.

$$\frac{T|\sim M\#(H(R||K_T))M, M|\sim\#(H(R||K_T))S, S|\Rightarrow H(R||K_T)}{S|\equiv T}$$

M4.

28. Dado que o S enviou ID_T cifrado com a chave K_M para M, além do resumo *hash* da identificação da *tag*, concatenado ao contador atualizado e também concatenado a essa chave que somente S e M conhecem, infere-se que S é acreditado como autêntico por M.

$$\frac{M \overset{K_M}{\leftrightarrow} S, M\Rightarrow C_2, S|\sim\{ID\}K_M M, S|\sim MH(ID_T||\#C_1||K_M)}{M|\equiv S}$$

Uma vez que S acredita em T e M acredita em S, pode-se inferir que M acredita em T.

$$\frac{M|\equiv S, S|\equiv T}{M|\equiv T}$$

Assim, está provado que o protocolo atinge a autenticação mútua e que as mensagens contendo chaves secretas são dinâmicas, evitando o rastreio ou associação de mensagens estáticas. Adicionalmente, é constatado que os contadores são refrescados, logo ataques de repetição podem ser facilmente detectados e a propriedade de Anti-rastreio é alcançada. Ao analisar-se as mensagens envolvidas no protocolo, tendo como metodologia a lógica BAN, conclui-se que o protocolo é fiel ao seu propósito.

5.2 Análise de Segurança

Nesta seção, são discutidas as características da segurança do mecanismo proposto.

1) Autenticação Mútua: O mecanismo de autenticação fornece a verificação de autenticidade do dispositivo M e do Servidor S. Essa propriedade é alcançada devido ao segredo compartilhado K_M entre ambos. Adicionalmente, a identidade da *tag* é verificada pelo servidor S. Ou seja, O servidor verifica se a *tag* faz parte do sistema recuperando sua *ID* a partir de H_1, na Mensagem M_3.

2) Confidencialidade: Após a execução do mecanismo de autenticação, todas as informações trocadas entre S e M podem ser criptografados com K_M.

3) Anti-Rastreio: A informação armazenada em uma *tag* é atualizada toda vez em que o mecanismo de autenticação é terminado com sucesso, isto é, quando não há falha na autenticação. Esta característica evita o rastreio de um dispositivo.

4) Anti-Repetição: Contadores são utilizados, a fim de evitar a repetição de mensagens. Os valores de C_1 e C_2 são aumentados de acordo com as autenticações efetuadas. Assim, M e S podem detectar eventuais mensagens repetidas.

5) Anti-Clonagem: Em nosso trabalho, o servidor autentica a *tag*. Em outras palavras, ele identifica as *tags* que não pertencentes ao sistema. No entanto, mantém-se a possibilidade do ataque de clonagem de *tags* (COSKUN; OZDENIZCI; OK, 2013) (SETHIA et al., 2014). Esse desafio carece de soluções eficientes, e está prevista para ser abordada em um trabalho futuro.

5.3 Experimento Prático

A fim de avaliar a arquitetura proposta de forma prática, foi definido um cenário composto de duas rotinas dependentes entre si nas quais os profissionais da saúde submetem a arquitetura a um teste de aceitação. Na Figura 17 está representado o processo de recuperação das prescrições de medicamentos por um técnico em enfermagem. Aqui assume-se que os medicamentos foram previamente prescritos por um médico. Nesta figura, os traços sobre as informações representam que as mesmas estão cifradas. Para a cifragem, foi utilizado a operação *Exclusive Or* (XOR) bit a bit. O algoritmo de resumo criptográfico utilziado neste TCC é o MD5.

5.3.1 Descrição do Cenário

Para que os profissionais da saúde sejam capazes de acessar, alterar ou inserir registros no prontuário de algum paciente, os mesmos devem obter a identificação vinculada à *Tag* NFC que está acoplada no leito desse paciente. Independente se a *tag* possui ou não

a capacidade de fazer o processamento de informações, ela deve ser lida pelo *smartphone* a fim de que o processo de obtenção de ID inicie. Este experimento será feito com o uso de *tags* que não tem capacidade de processamento devido ao fato de que as mesmas são mais populares no mercado por ter um baixo custo comparadas às *tags* mais sofisticadas que são capazes de executar alguns algoritmos.

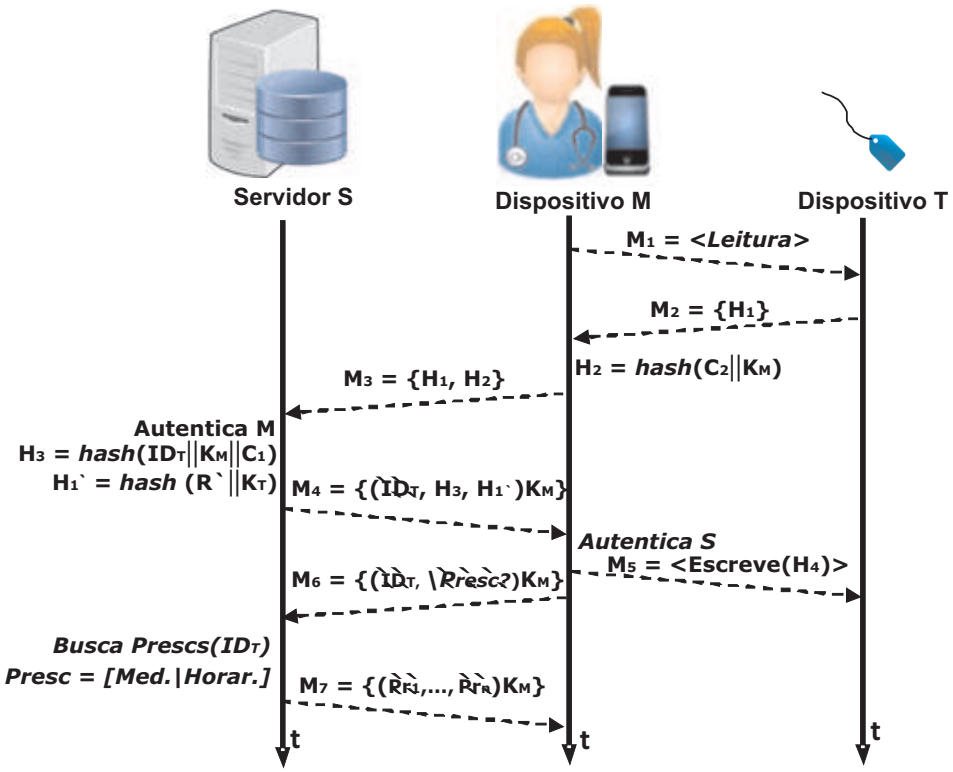
Para se fazer a prescrição de medicamentos o médico deve aproximar seu *smartphone* M da *tag* T que está acoplada ao leito do paciente para a obtenção de sua identificação ID_T. O processo de recuperação de ID_T ocorre conforme o mecanismo especificado na Seção 4.3.1, portanto somente dispositivos legítimos são capazes de obter essa informação.

A partir do momento em que um dispositivo é conhecedor de ID_T o mesmo é capaz de solicitar as informações competentes ao perfil do profissional de saúde que está utilizando o *smartphone*. O processo de prescrição de medicamentos se dá através do envio da mensagem M_4 para o servidor S. Essa mensagem consiste em ID_T acompanhado do comando $presc < Pr_x >$, onde Pr_x representa uma nova prescrição composta por um medicamento Med e o horário Hor para sua administração. A mensagem M_5 serve como confirmação de sucesso ou alerta de fracasso da operação por S para M. No caso de novas prescrições para esse mesmo paciente, somente as mensagens M_4 e M_5 precisam ser transmitidas. A obtenção dessa mesma ID_T não é necessária até que outra *tag* seja lida ou até que o médico faça *logoff* do sistema.

Com base nas informações inseridas no sistema, os demais usuários podem executar algumas rotinas como acompanhamento diário de pacientes ou registro de administração medicamentos, por exemplo. A Figura 17 ilustra o procedimento de registro dos medicamentos administrados por um técnico em enfermagem a partir de seu *smartphone* E a um paciente que está no leito com a *tag* de identificação ID_T.

O registro de administração de um medicamento é baseado na identificação de um paciente. Portanto, o dispositivo E deve ser aproximado de T para que se inicie o processo de obtenção de sua ID_T através do mecanismo de segurança. A mensagem M_4 é semelhante à mensagem M_4, mas se difere pelo fato de que possui um ponto de interrogação ao invés de argumentos. Isso significa que essa mensagem é uma requisição de busca ao invés de uma inserção de novos registros. Ao receber o comando *presc*? acompanhado de ID_T, o servidor faz uma busca por todas as prescrições pendentes para o paciente que está no leito ID_T. Entende-se por administração pendente aquela que ainda não foi administrada por nenhum técnico. A mensagem M_5, consiste em uma lista contendo todas as prescrições encontradas nessa busca.

Figura 17 – Processo de recuperação de prescrições de medicamentos sendo executado por um técnico em enfermagem.



5.3.2 Questionário

Com o intuito de coletar informações pertinentes a experiência dos usuários em contato com a arquitetura proposta, foi aplicado um questionário aos funcionários do HCJ. Participaram das experimentações um total de 5 funcionários, sendo 1 Médico, 2 Enfermeiros e 2 Técnicos em Enfermagem, conforme a Figura 21. O questionário completo pode ser visualizado no Anexo A.

A primeira pergunta do questionário consiste em uma pergunta objetiva, que visa coletar a opinião dos funcionários em relação ao quão útil seria a adoção da arquitetura validada caso viesse a ser implantada no HCJ. Segue a baixo a mesma:

- Pergunta 1: O aplicativo seria útil?

Para essa pergunta, os funcionários poderiam escolher somente uma das seguintes opções: Pouco, Médio e Muito.

A segunda pergunta tem por objetivo verificar se, na visão dos profissionais, o processo seria ou não agilizado com o uso da arquitetura proposta.

- Pergunta 2: Com o uso do aplicativo você acha que o processo de registro e recupe-

ração de informações será acelerado?

Para essa pergunta, os funcionários poderiam marcar apenas uma das opções "Sim"ou "Não".

A terceira pergunta questiona o quanto o processo foi agilizado, considerando a adoção da arquitetura proposta.

- Pergunta 3: Na sua opinião, em uma escala de 1 à 5, quanto o processo foi agilizado?

Para essa pergunta, os funcionários poderiam avaliar a agilização do processo ao selecionar uma das opções "1", "2", "3", "4"ou "5", onde 1 representa uma agilização mínima e 5 apresenta um grande ganho em termos de agilidade.

A quarta pergunta questiona o cargo do profissional entrevistado.

- Pergunta 4: Qual seu cargo?

Para essa pergunta, os funcionários poderiam informar seu cargo através da seleção de uma das seguintes opções: "Recepcionista", "Médico", "Enfermeiro"ou "Técnico".

A quinta pergunta tem por objetivo definir se, na visão dos profissionais, a arquitetura proposta contribui na redução de erros na administração de medicamentos.

- Pergunta 5: Na sua opinião, o aplicativo auxilia na redução de erros na administração de medicamentos?

Para essa pergunta, os funcionários poderiam marcar apenas uma das opções "Sim"ou "Não".

A sexta pergunta questiona a usabilidade do aplicativo da perspectiva do usuário.

- Pergunta 6: Na sua opinião, o aplicativo tem sido de fácil manuseio?

Para essa pergunta, os funcionários poderiam marcar apenas uma das opções "Sim"ou "Não".

A sétima pergunta busca coletar a opinião do usuário em relação ao uso de dispositivos como aparelhos celulares em ambiente de trabalho como forma de aproximação de usuário e sistema.

- Pergunta 7: Na sua opinião, aplicativos para celulares aproximam o usuário do sistema?

Para essa pergunta, os funcionários poderiam marcar apenas uma das opções "Sim"ou "Não".

A oitava pergunta busca coletar a opinião do usuário em relação a apresentação da interface gráfica do sistema. Assim os funcionários poderiam julgar o *layout* dos sistemas para *desktop* e *android*.

- Pergunta 8: Sobre a interface do sistema, você achou ela amigável?

Para essa pergunta, os funcionários poderiam marcar apenas uma das opções "Sim"ou "Não".

A nona pergunta é relacionada a satisfação do usuário com o sistema. Assim, a mesma questiona se o usuário recomendaria o uso dessa arquitetura para outros usuários ou hospitais.

- Pergunta 9: Você recomendaria o uso do aplicativo?

Para essa pergunta, os funcionários poderiam marcar apenas uma das opções "Sim"ou "Não".

A décima pergunta questiona o tempo de aprendizado do sistema por parte do usuário entrevistado.

- Pergunta 10: Você demorou quanto tempo para aprender a operar o sistema?

Para essa pergunta, os funcionários poderiam marcar apenas uma das opções "Menos de Um Dia", "Até dois dias"ou "Mais de dois dias".

A última pergunta questiona o desejo da utilização da aplicação em outros dispositivos móveis, como *tablets*.

- Pergunta 11: Você gostaria de usar a aplicação em *tablets*?

Para essa pergunta, os funcionários poderiam marcar apenas uma das opções "Sim"ou "Não".

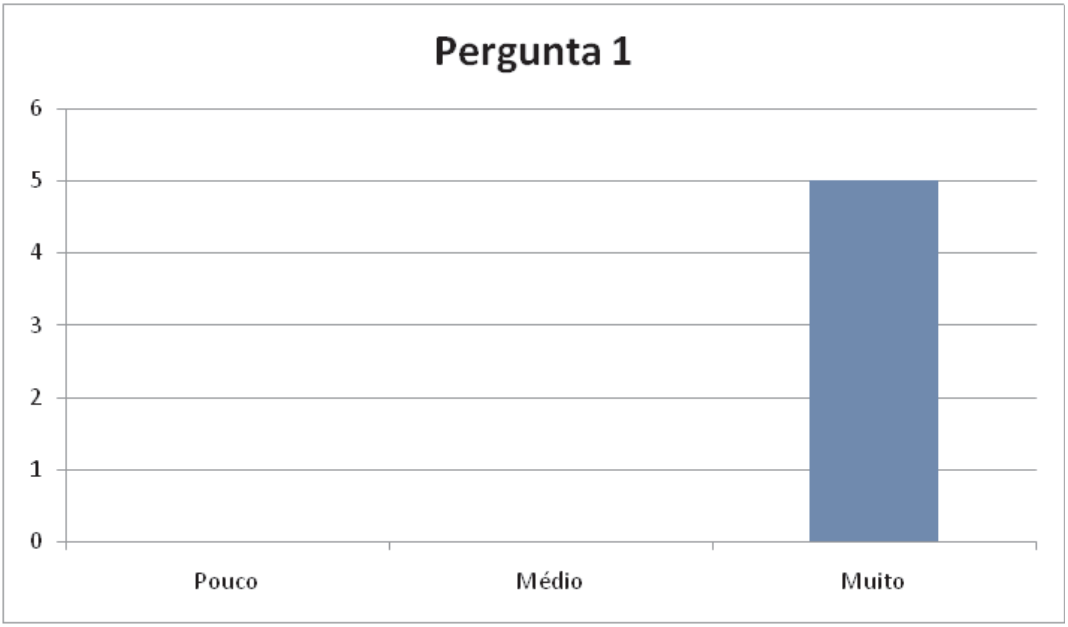
Adicionalmente, para finalizar o questionário, os usuários foram convidados a preencher um espaço reservado para sugestões.

5.3.3 Resultados e Discussão

Inicialmente, os Enfermeiros e Técnicos se mostraram empolgados com a praticidade e agilidade que seria adicionada ao processo caso a Administração do HCJ viesse a adotar o uso contínuo dessa arquitetura para apoiar os procedimentos hospitalares

de verificação e registro medicamentos administrados. O médico demonstrou expectativas positivas principalmente pelo fato da capacidade da verificação de administrações de medicamentos e capacidade de se efetuar novas prescrições remotamente, do próprio consultório médico.

Figura 18 – Gráfico dos resultados da Pergunta 1.



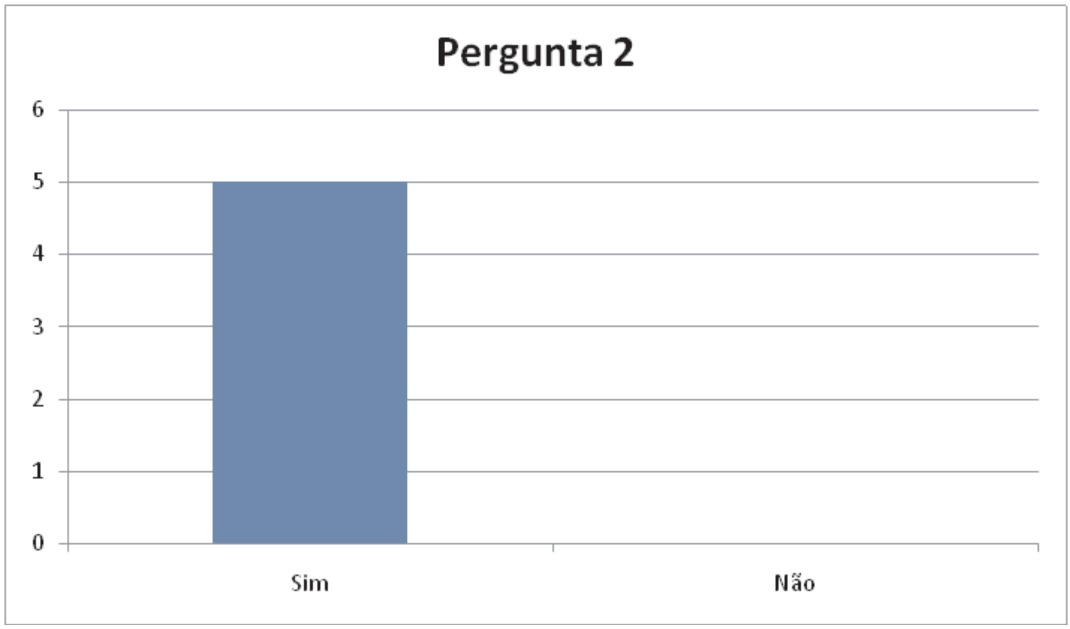
Pergunta 1: O aplicativo seria útil?

Segundo os funcionários, o aplicativo seria muito útil devido à praticidade que traria aos procedimentos que são executados no hospital. Dado que hoje tais procedimentos são executados manualmente, ou seja, através do preenchimento de fichas. Esse processo é oneroso e pode ser melhorado com a implantação da arquitetura proposta nesse TCC. Além da agregação em eficiência e segurança que esse processo poderia ganhar, o tempo de execução desses procedimentos seria reduzido conforme os testes qualitativos.

Os resultados do questionário aplicado a esses funcionários apontam que todos os usuários envolvidos nos testes julgaram a utilização desse sistema como "Muito Útil", conforme o gráfico da Figura 18. Além disso, houve a constatação de expectativas de aceleração e ganhos de agilidade nos processos, conforme o gráfico das Figuras 19 e 20, além disso, os usuários avaliaram positivamente a arquitetura proposta em relação a expectativa de redução nos erros de administração de medicamentos, como mostra o gráfico da Figura 22. Todos os usuários também classificaram o sistema como sendo de fácil operação e demoraram menos de um dia para aprender as rotinas de apresentadas, conforme as Figuras 23 e 27, respectivamente.

A interface gráfica foi classificada como amigável por todos os usuários, como

Figura 19 – Gráfico dos resultados da Pergunta 2.

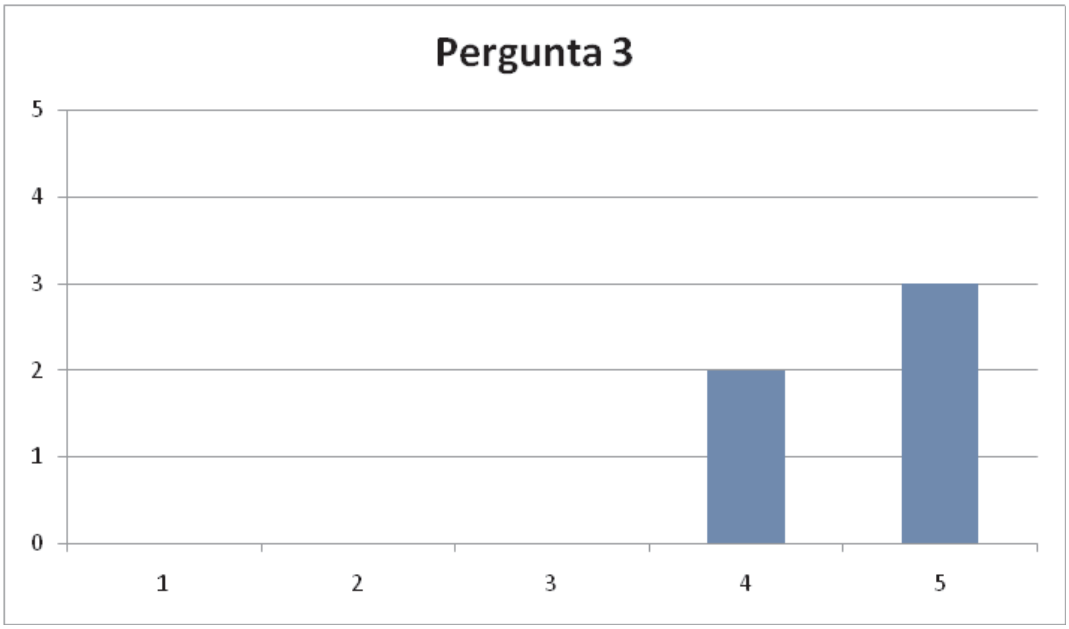


Pergunta 2: Com o uso do aplicativo você acha que o processo de registro e recuperação de informações será acelerado?

exibido o gráfico da Figura 25. Essa característica foi alcançada devido a utilização da identificação de pacientes automatizada, com apoio da tecnologia NFC. Além disso, todos participantes dos testes recomendariam a utilização desse sistema, conforme o gráfico da Figura 26. A opinião geral dos funcionários é que aplicações para celulares aproximam o usuário do sistema e que a ideia de envolver *tablets* na arquitetura seria interessante 24.

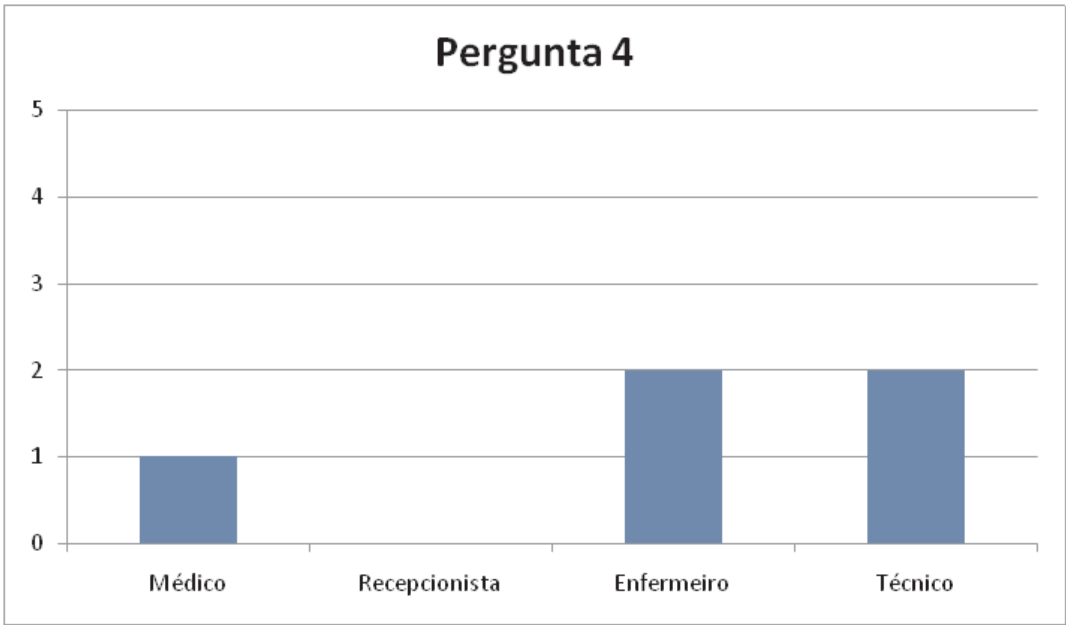
A segurança dos pacientes e de suas informações foi um dos pontos observados pelos funcionários. Nesse aspecto, a arquitetura também foi considerada satisfatória, entretanto o médico ressaltou a importância de uma utilização mais prolongada do sistema para a constatação mais precisa de seus benefícios.

Figura 20 – Gráfico dos resultados da Pergunta 3.



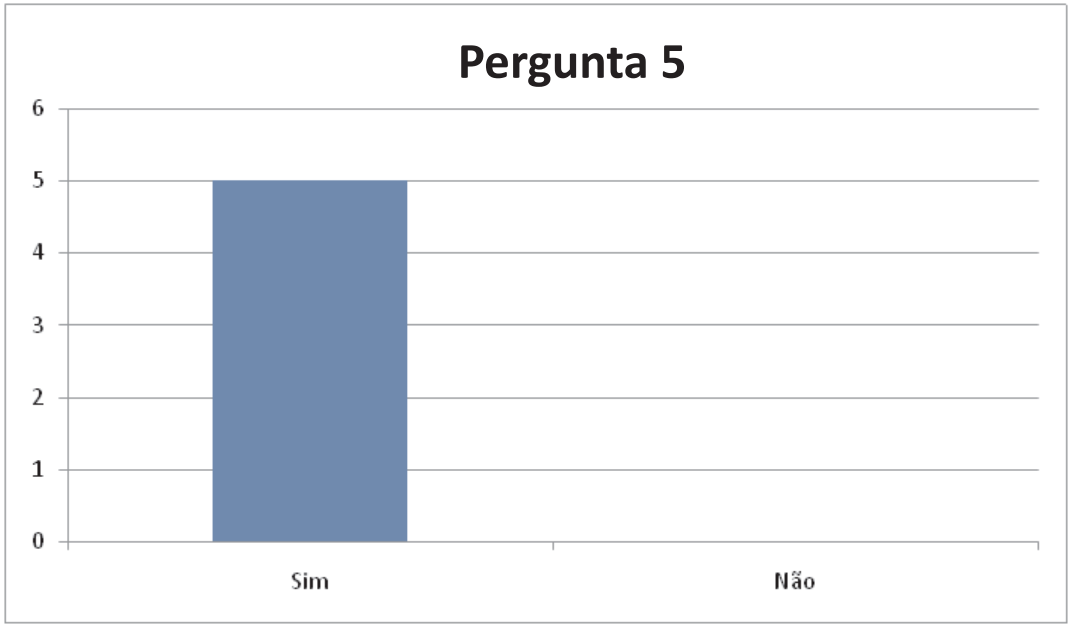
Pergunta 3: Na sua opinião, em uma escala de 1 à 5, quanto o processo foi agilizado?

Figura 21 – Gráfico dos resultados da Pergunta 4.



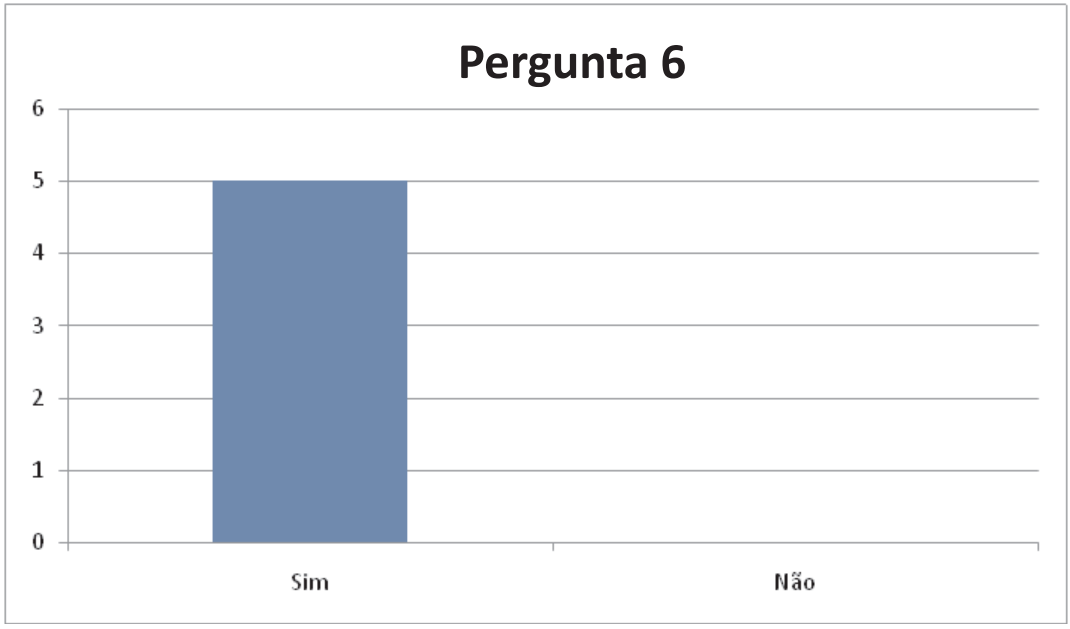
Pergunta 4: Qual seu cargo?

Figura 22 – Gráfico dos resultados da Pergunta 5.



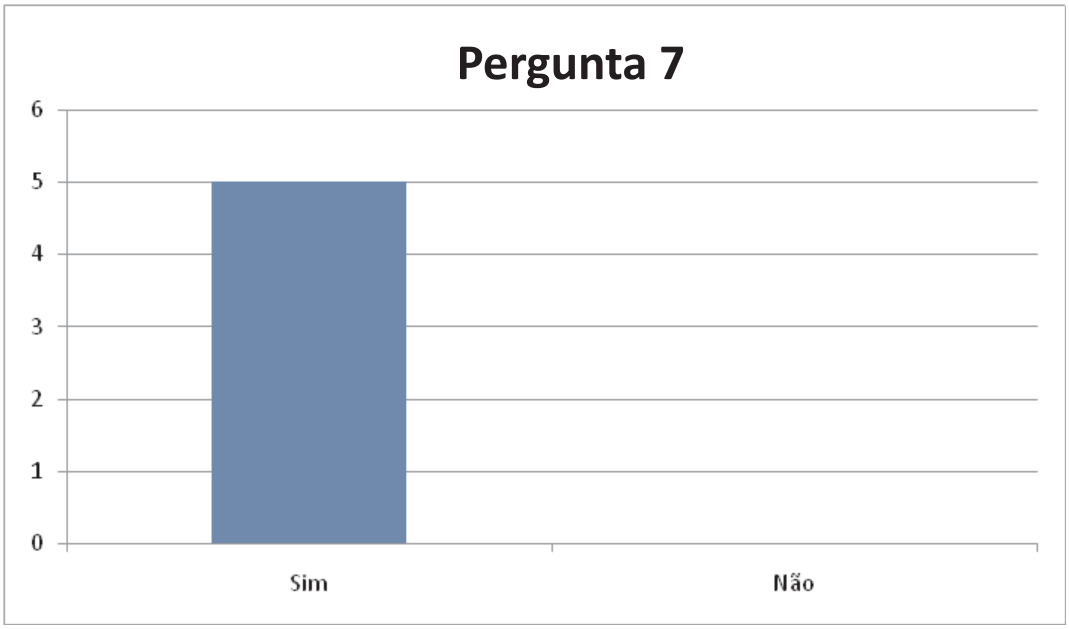
Pergunta 5: Na sua opinião, o aplicativo auxilia na redução de erros na administração de medicamentos?

Figura 23 – Gráfico dos resultados da Pergunta 6.



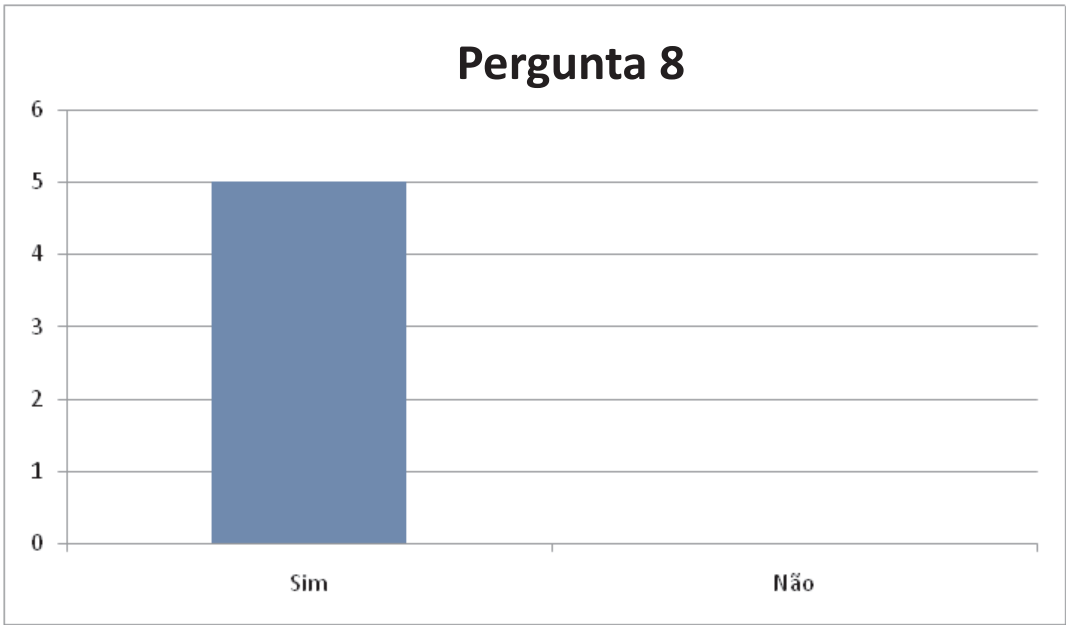
Pergunta 6: Na sua opinião, o aplicativo tem sido de fácil manuseio?

Figura 24 – Gráfico dos resultados da Pergunta 7.



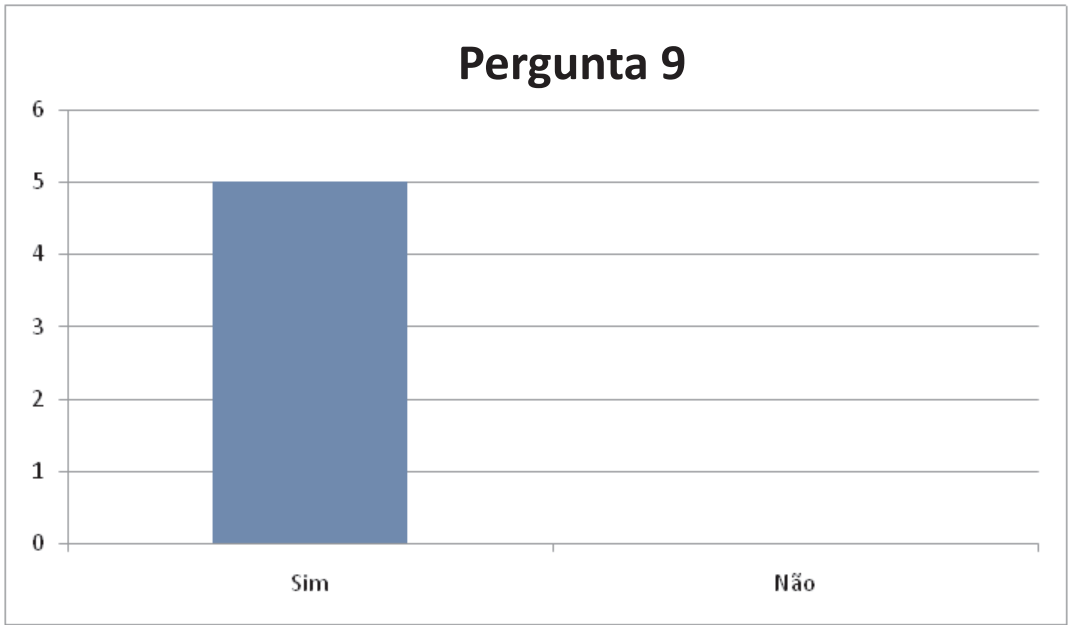
Pergunta 7: Na sua opinião, aplicativos para celulares aproximam o usuário do sistema?

Figura 25 – Gráfico dos resultados da Pergunta 8.



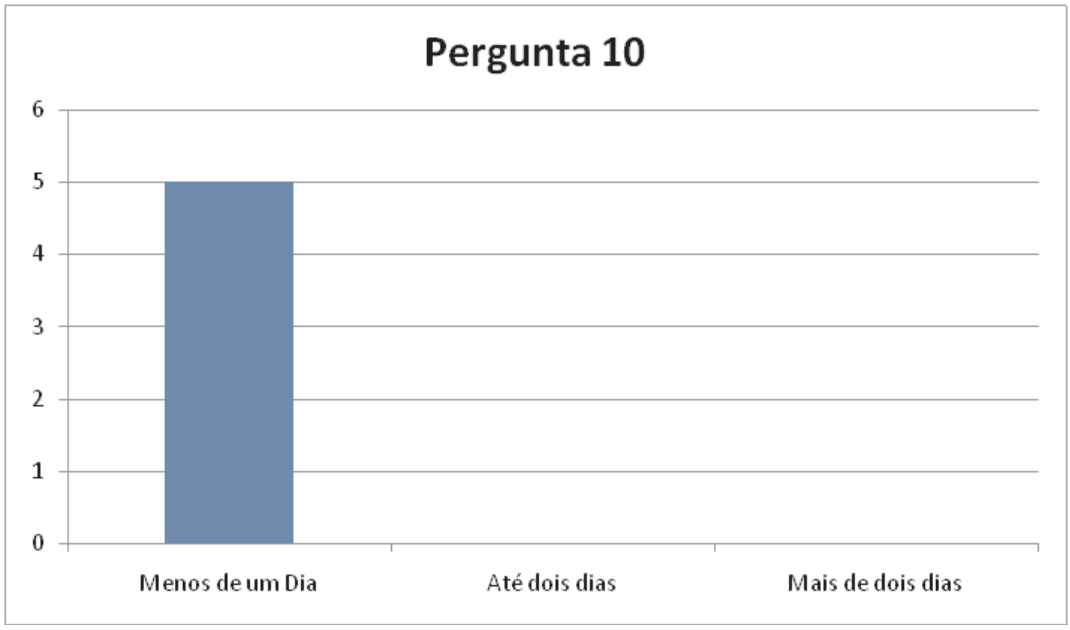
Pergunta 8: Sobre a interface do sistema, você achou ela amigável?

Figura 26 – Gráfico dos resultados da Pergunta 9.



Pergunta 9: Você recomendaria o uso do aplicativo?

Figura 27 – Gráfico dos resultados da Pergunta 10.



Pergunta 10: Você demorou quanto tempo para aprender a operar o sistema?

6 Conclusão

Com o avanço da tecnologia da informação e comunicação, novos sistemas são introduzidos trazendo novas formas de interação com os mesmos, onde o NFC tem ganho papel essencial na identificação de entidades.

Dado que o protocolo NDEF utilizado na comunicação de mensagens NFC não possui a devida proteção necessária, os dados trocados entre dispositivos estão vulneráveis à ataques como interceptação e retransmissão. Além disso, a modificação de mensagens também é possível por dispositivos maliciosos. Para aumentar a segurança nas comunicações sem fio é necessário então a presença de mecanismos apoiadores.

Neste trabalho é feita uma revisão da literatura e proposto um sistema de acesso e recuperação segura de prontuários eletrônicos em uma rede interna hospitalar, com apoio da tecnologia Wi-Fi para comunicação de *smartphones* com o servidor. A identificação de medicamentos e pacientes se dá através da tecnologia NFC, onde um mecanismo de segurança é introduzido a fim de prover a segurança necessária para a arquitetura.

A arquitetura proposta foi avaliada por todos os profissionais da saúde em ambiente hospitalar, onde sua eficiência e segurança revelaram que a mesma é promissora. A arquitetura é considerada segura porque o mecanismo inserido na arquitetura previne contra ataques de personificação de dispositivos além de fornecer proteção anti-rastreio, anti-reprodução e garantindo a confidencialidade dos dados. A eficiência da arquitetura se justifica devido ao uso da computação ubíqua e pervasiva, inserindo inclusive os próprios *smartphones* dos profissionais de saúde em seu ambiente de trabalho, aproximando-os do sistema.

Em trabalhos futuros serão feitos logados registros como tempo de execução, atraso na comunicação e outros dados quantitativos. Deseja-se também aplicar a padronização estabelecida pelo HL7 e expandir a utilização desse sistema para o próprio paciente e familiares, a fim de prover um ambiente no qual seja possível ter um auto-controle de seus registros médicos. Para tal, uma interface de acesso à registros (do tipo PHR) será implementada e oferecida para instalação nos *smartphones* dos usuários. Com isso o sistema teria um módulo PHR e outro EHR, sendo um para uso de quaisquer pessoas e outro para uso instituição de saúde, respectivamente. O tratamento ambulatorial também deve ser tratado futuramente, isto é, quando pacientes não são internados os mesmos possuiriam uma tag nfc como *healthcard* (SETHIA et al., 2014). Adicionalmente, a expansão do aplicativo para *tablets* é uma das intenções para trabalhos futuros.

Referências

802.11, I. *IEEE 802.11TM WIRELESS LOCAL AREA NETWORKS*. 2014. Disponível em: <http://www.ieee802.org/11/>. Citado 2 vezes nas páginas 27 e 38.

ABOELFOTOH, P. M. M. H.; HASSANEIN, H. S. A mobile-based architecture for integrating personal health record data. In: *2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom)*. [S.l.: s.n.], 2014. p. 216–221. Citado 4 vezes nas páginas 17, 18, 22 e 33.

ANDRADE, E. D. O.; SILVA, R. D. S. *RESOLUÇÃO CFM nº 1.638/2002*. Publicada no D.O.U. de 9 de agosto de 2002, Seção I, p.184-5, 2002. Disponível em: <http://www.portalmedico.org.br/resolucoes/cfm/2002/1638_2002.htm>. Citado 2 vezes nas páginas 21 e 22.

ATKINS, W. *The Smart Card Report*. [S.l.]: Elsevier, 2003. Citado na página 35.

BENHARREF MOHAMED ADEL SERHANI, R. M. A. Smart data synchronization in m-health monitoring applications. In: *2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom)*. [S.l.: s.n.], 2014. p. 78–83. Citado na página 33.

BURROWS, M. A. M.; NEEDHAM, R. M. A logic of authentication. In: CITESEER. *ACM Transactions on Computer Systems*. [S.l.], 1990. v. 8, p. 18–39. Citado 2 vezes nas páginas 26 e 63.

CEIPIDOR, U. B. et al. Kernees: A protocol for mutual authentication between nfc phones and pos terminals for secure payment transactions. In: *9th International ISC Conference on Information Security and Cryptology (ISCISC)*. [S.l.: s.n.], 2012. p. 115–120. Citado na página 36.

CHEN, W. et al. NFC mobile transactions and authentication based on GSM network. In: *Second IEEE International Workshop on Near Field Communication (NFC)*. [S.l.: s.n.], 2010. p. 83–89. Citado 2 vezes nas páginas 35 e 36.

COMMISSION, I. O. for S. E. et al. Iso/iec 18092 information technology—telecommunications and information exchange between systems—near field communication—interface and protocol (nfcip-1). *ISO/IEC*, v. 18092, 2013. Citado na página 28.

COSKUN, V.; OZDENIZCI, B.; OK, K. A Survey on Near Field Communication NFC Technology. *Wireless Personal Communications*, Springer, v. 71, p. 2259–2294, dez. 2013. Citado 3 vezes nas páginas 28, 29 e 67.

COULOURIS, G. et al. *Sistemas Distribuídos - 5ed: Conceitos e Projeto*. [s.n.], 2013. ISBN 9788582600542. Disponível em: <https://books.google.com.au/books?id=6WU3AgAAQBAJ>. Citado na página 26.

EDIDIN, H.; BHARDWAJ, V. *HL7 for BizTalk*. [S.l.]: Apress, 2014. Citado na página 22.

EMV Contactless Specifications for Payment Systems. [S.l.], 2014. Version 2.4. Disponível em: <http://www.emvco.com/downloadagreement.aspx?id=653>. Citado 2 vezes nas páginas 35 e 36.

EUN, H.; LEE, H.; OH, H. Conditional privacy preserving security protocol for NFC applications. *IEEE Transactions on Consumer Electronics*, IEEE, v. 59, n. 1, p. 153–160, 2013. Citado 3 vezes nas páginas 28, 35 e 36.

HANSMANN, U. *Pervasive computing: The mobile world*. [S.l.]: Springer Science & Business Media, 2003. Citado na página 18.

HASELSTEINER, E.; BREITFUSS, K. Security in near field communication (nfc). In: *Workshop on RFID security*. [S.l.: s.n.], 2006. p. 12–14. Citado na página 29.

IGLESIAS, R. et al. Experiencing nfc-based touch for home healthcare. In: ACM. *Proceedings of the 2nd international conference on pervasive technologies related to assistive environments*. [S.l.], 2009. p. 27. Citado 4 vezes nas páginas 18, 22, 27 e 34.

INFOMONEY. *iPhone 6 é lançado a oficialmente à meia noite*. 2014. <http://www.infomoney.com.br/minhas-financas/gadgets/noticia/3691789/iphone-lancado-oficialmente-meia-noite-veja-onde-comprar>. Acessado em: 01-12-2014. Citado na página 27.

ISO/IEC. *ISO/IEC 14443*. 2011. Disponível em: <http://www.iso.org/iso/catalogue_detail.htm?csnumber=50942>. Citado na página 27.

JEPSON, B.; COLEMAN, D.; IGOE, T. *Beginning NFC Near-Field Communication with Arduino, Android, and PhoneGap Jepson*. [S.l.]: Tom O'Reillg Media, Inc, 2012. Citado 2 vezes nas páginas 28 e 30.

JUELS, A. Rfid security and privacy: A research survey. *Selected Areas in Communications, IEEE Journal on*, IEEE, v. 24, n. 2, p. 381–394, 2006. Citado na página 27.

KUROSE, J. F.; ROSS, K. W. *Redes de Computadores e a internet: uma abordagem top-down*. [S.l.]: Pearson, 2010. Citado na página 25.

LAHTELA, A.; HASSINEN, M.; JYLHA, V. Rfid and nfc in healthcare: Safety of hospitals medication care. In: IEEE. *Pervasive Computing Technologies for Healthcare, 2008. PervasiveHealth 2008. Second International Conference on*. [S.l.], 2008. p. 241–244. Citado na página 17.

LOPEZ, J.; SETOLA, R.; WOLTHUSEN, S. *Critical Infrastructure Protection: Advances in Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense*. [S.l.]: Springer, 2012. Citado 2 vezes nas páginas 22 e 23.

MAGNUSON, J.; FU, P. C. *Public Health Informatics and Information Systems*. [S.l.]: Springer, 2014. Citado na página 23.

MENEZES, A. J.; OORSCHOT, P. C. V.; VANSTONE, S. A. *Handbook of applied cryptography*. [S.l.]: CRC press, 2010. Citado 2 vezes nas páginas 17 e 25.

MIORANDI, D. et al. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, Elsevier, v. 10, n. 7, p. 1497–1516, 2012. Citado na página 17.

MULLINER, C. Vulnerability analysis and attacks on nfc-enabled mobile phones. In: *Availability, Reliability and Security, 2009. ARES'09. International Conference on*. [S.l.: s.n.], 2009. p. 695–700. Citado 2 vezes nas páginas 27 e 29.

MUTCHUKOTA, T. R.; PANIGRAHY, S. K.; JENA, S. K. Man-in-the-middle attack and its countermeasure in bluetooth secure simple pairing. In: *Computer Networks and Intelligent Computing*. [S.l.]: Springer, 2011. p. 367–376. Citado na página 34.

NFC-FORUM. *NFC Data Exchange Format (NDEF) Technical Specifications*. 2006. <http://members.nfc-forum.org/specs/spec_license/survey_form/process>. Acessado em: 02-12-2014. Citado na página 28.

NFC-FORUM. *NFC Data Exchange Format (NDEF) Technical Specifications*. 2014. <http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/record-type-definition-technical-specifications/>. Acessado em: 02-12-2014. Citado na página 28.

PATEL, D. R. *Information Security: Theory and Practice*. [S.l.]: PHI Learning Pvt. Ltd., 2008. Citado na página 25.

PERSPECTIVAS Da Tecnologia Da Informação: As Tecnologias Da Comunicação E Da Informação E a Economia Da Informação. OECD, 2003. ISBN 9788573593877. Disponível em: <https://books.google.com.br/books?id=xpH6nChXu-AC>. Citado na página 26.

QUINCOZES, S. E.; KAZIENKO, J. F. Um mecanismo simples e eficiente para a autenticação de dispositivos na comunicação por campo de proximidade. In: *XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg 14)*. [S.l.: s.n.], 2014. p. 318–321. Citado 2 vezes nas páginas 27 e 36.

RODRIGUES EDGAR T. HORTA, B. M. C. S. F. D. M. G. D. F. M.; RODRIGUES, J. J. P. C. A mobile healthcare solution for ambient assisted living environments. In: *16th International Conference on E-health Networking, Application and Services*. [S.l.: s.n.], 2014. p. 115–120. Citado 3 vezes nas páginas 18, 22 e 33.

ROLAND, M.; LANGER, J. Digital signature records for the nfc data exchange format. In: *Near Field Communication (NFC), 2010 Second International Workshop on*. [S.l.: s.n.], 2010. p. 71–76. Citado na página 18.

SCHNEIER, B. *Why Technology Won't Prevent Identity Theft*. 2009. Disponível em: <http://www.wsj.com/articles/SB123125633551557469>. Citado na página 23.

SETHIA, D. et al. Nfc based secure mobile healthcare system. In: *COMSNETS*. [S.l.: s.n.], 2014. p. 1–6. Citado 6 vezes nas páginas 17, 18, 34, 53, 67 e 79.

SISTEMAS Colaborativos. Elsevier, 2011. ISBN 9788535250862. Disponível em: <https://books.google.com.br/books?id=YTJ8bahZFLoC>. Citado na página 26.

SLEE, D. A.; SLEE, V. N.; SCHMIDT, H. J. *Slee's health care terms*. [S.l.]: Jones & Bartlett Publishers, 2009. Citado na página 23.

STALLINGS, W. *Criptografia e segurança de redes 4ª ed.* [S.l.]: São Paulo: Pearson Prentice Hall, 2008. Citado 3 vezes nas páginas 17, 23 e 25.

STEELE, R.; MIN, K.; LO, A. Personal health record architectures: technology infrastructure implications and dependencies. *Journal of the American Society for Information Science and Technology*, Wiley Online Library, v. 63, n. 6, p. 1079–1091, 2012. Citado na página 38.

TAN, J.; PAYTON, F. *Adaptive health management information systems: Concepts, cases, & practical applications*. [S.l.]: Jones & Bartlett Learning, 2009. Citado na página 22.

THORSTEINSON, P.; GANESH, A. . *Net Security and Cryptography*. [S.l.]: Prentice Hall Professional Technical Reference, 2003. Citado na página 25.

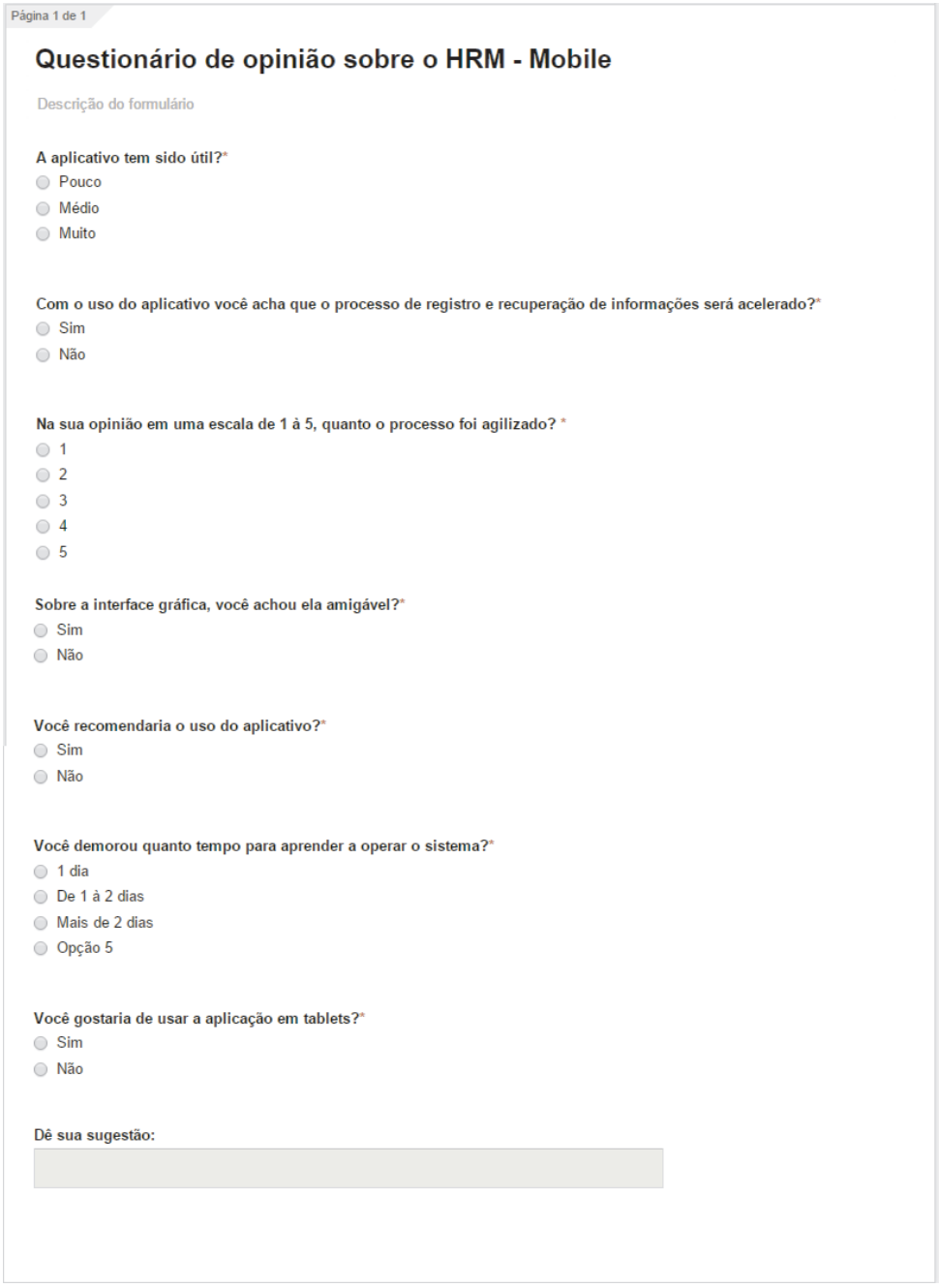
TIPTON, H. F.; KRAUSE, M. *Information security management handbook*. [S.l.]: CRC Press, 2012. Citado 2 vezes nas páginas 24 e 25.

WEISER, M. The computer for the 21st century. *Scientific american*, Nature Publishing Group, v. 265, n. 3, p. 94–104, 1991. Citado na página 18.

Anexos

ANEXO A – Questionário

[1]



Página 1 de 1

Questionário de opinião sobre o HRM - Mobile

Descrição do formulário

A aplicativo tem sido útil?*
- Pouco
- Médio
- Muito

Com o uso do aplicativo você acha que o processo de registro e recuperação de informações será acelerado?*
- Sim
- Não

Na sua opinião em uma escala de 1 à 5, quanto o processo foi agilizado? *
- 1
- 2
- 3
- 4
- 5

Sobre a interface gráfica, você achou ela amigável?*
- Sim
- Não

Você recomendaria o uso do aplicativo?*
- Sim
- Não

Você demorou quanto tempo para aprender a operar o sistema?*
- 1 dia
- De 1 à 2 dias
- Mais de 2 dias
- Opção 5

Você gostaria de usar a aplicação em tablets?*
- Sim
- Não

Dê sua sugestão:

[1] Questionário aplicado.