PUC Minas

**Pontifícia Universidade Católica de Minas Gerais**
***Campus* Poços de Caldas**

**Departamento de Ciência da Computação**
**Curso de Ciência da Computação**

# A SEGURANÇA DE DADOS E PRIVACIDADE PARA IMPLANTES DE BIOCHIP RFID E NFC

Tuanne Assenço Pessoa

Poços de Caldas – MG
Outubro de 2020

# A SEGURANÇA DE DADOS E PRIVACIDADE PARA IMPLANTES DE BIOCHIP RFID E NFC

PROJETO DE PESQUISA

Projeto de pesquisa apresentado ao Curso de Ciência da Computação da PUC – Minas.

Poços de Caldas – MG
Outubro de 2020

**Sumário**

## 1. APRESENTAÇÃO

Este documento tem como objetivo apresentar uma proposta de projeto de pesquisa, notadamente no campo das Tecnologias da Informação e Comunicação (TIC), pela Pontifícia Universidade Católica de Minas Gerais, *campus* Poços de Caldas. O projeto aqui reportado está inserido no contexto das pesquisas bibliográficas realizadas sobre o assunto, integrando ações de pesquisa, desenvolvimento e inovação no curso de Ciência da Computação.

Lidando com o cenário onde a integração da tecnologia é exponencial e inevitável, vê-se necessário o alinhamento e a preparação da sociedade para adotar e confiar nos benefícios inclusos nesta. A premissa dos avanços das TIC, tem a comodidade e praticidade como aliadas, entretanto, nota-se receio por parte das pessoas em acolhê-las. Isto se deve ao medo gerado pela exposição de dados pessoais e da privacidade; e a falta de conhecimento sobre como estas tecnologias funcionam, causando a falta de apoio e dificultando o desenvolvimento destas.

A proposta relaciona-se a problemática de segurança e privacidade de dados gerada pela inserção de *biochips* em humanos, estes que utilizam RFID (*Radio-Frequency IDentification*), e NFC (*Near Field Communication*). Aplicando o conhecimento tecnológico de computação com o intuito de diminuir a exposição e vazamento de dados pessoais; e também de proteger a privacidade dos usuários.

## 2. ESTADO DA ARTE

O desenvolvimento da tecnologia de *biochips* para implantes em humanos, se deve na integração de um circuito eletrônico envolto em uma cápsula de vidro, onde este é inserido em alguma parte do corpo, geralmente na parte posterior da mão, de forma subcutânea. Esta tecnologia é dividida em duas partes: uma memória, que funciona como uma memória secundária, armazenando informações e dados (como arquivos e informações de saúde); e outra criptografada, onde se encontram os registros de senhas e códigos de acesso [1].

Os *biochips* utilizam sensores de RFID ou NFC, ambos permitem a troca de dados sem fio e por aproximação. Estes sensores se comunicam com outros sensores instalados em cartões,

portas, catracas, chaves de carros, etc. Os usos ainda estão sendo explorados e são diversos, ampliando a aplicação para a praticidade de transações realizadas cotidianamente pelas pessoas, desencadeando cenários inovadores e personalizados para cada tipo de necessidade [1].

O receio em torno dos implantes RFID e NFC pouco tem relação com a tecnologia em si, pois estes já são amplamente utilizados em animais de estimação e na agropecuária. A empresa Verichip, que vem desenvolvendo os próprios implantes de microchips voltados para a área da saúde, realizou uma pesquisa que indicou que 90% dos estadunidenses se sentiam desconfortáveis com a tecnologia voltada para si. Esta empresa obteve a aprovação do FDA (*Food and Drug Administration*), para seus dispositivos em 2004, mas desistiu em apenas três anos. Grande parte devido a estudos que sugeriam uma ligação potencial entre a tecnologia RFID e o câncer em animais de laboratório, com tudo, em 2006 relatou-se que o risco de câncer em humanos foi praticamente inexistente e também insignificante para animais [1].

A problemática acerca da ampliação dos estudos e desenvolvimento de *biochips* para humanos, é pautada principalmente na possibilidade de os dados armazenados dos usuários serem hackeados. Levando em conta a exposição de informações sigilosas que ocasiona no prejuízo dos usuários, que por sua vez se distanciam do foco atrativo dos benefícios que o desenvolvimento desta tecnologia tem o potencial de oferecer [2].

Além da preocupação do hackeamento dos dispositivos, outro ponto importante se deve ao acesso da localização geográfica do usuário, que, por um lado se tornaria um importante aliado para a resolução de crimes, como por exemplo sequestros, assassinatos e etc; por outro lado teria um impacto direto ao direito de privacidade do cidadão, como descrito na Constituição Federal, em seu artigo 5°, inciso X, que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”. Apesar desta vertente já possuir grande debate de opinião pelo uso de GPS (*Global Positioning System*), dos dispositivos móveis que já estão amplamente inseridos na sociedade [2].

O intuito dos resultados advindos deste projeto de pesquisa é de auxiliar e contribuir para que o desenvolvimento de *biochips* para humanos seja efetuado com maior aceitação e

confiabilidade da sociedade; e também de forma mais segura para o usuário, preenchendo parte das lacunas que impedem o progresso efetivo destes estudos.

## 3. JUSTIFICATIVAS

Apesar dos evidentes avanços que o desenvolvimento da tecnologia de *biochips* acarretariam para a sociedade (como o arquivamento do histórico médico de indivíduos, auxiliando profissionais da área da saúde em uma situação de emergência por exemplo; o acesso aos bens materiais de forma personificada, como a abertura de portas, acionamento de alarme, acesso a um automóvel ou também autorização de entrada em uma área restrita; o auxílio na resolução de crimes por intermédio do registro de localização do GPS; além da gama de evolução que acarretaria se tivesse maior possibilidade de pesquisas sobre novas funções), um dos barramentos para amplificação das propostas de estudos desta área, é devido a possível fragilidade da segurança de dados e de privacidade para o usuário.

Identificado um dos causadores que impedem o avanço desta tecnologia, torna-se essencial o desenvolvimento da segurança destes dispositivos, com o foco voltado às suas falhas de implementação, de forma que assegure de maneira ética o auxílio para amplificar a utilização destes.

## 4. OBJETIVOS E METAS

Conforme já expresso, este trabalho tem como objetivo auxiliar e contribuir no desenvolvimento da tecnologia de implantes de *biochips* para humanos, através da criação de um sistema de segurança de dados e privacidade do usuário. Difundindo de maneira que preencha parte das lacunas da problemática acerca desta tecnologia. Colaborando com o desempenho dos protótipos já criados, com a finalidade de proporcionar a confiabilidade e diminuir o receio da sociedade, através de um projeto de segurança com criptografia de dados pessoais e assegurando a privacidade dos usuários.

Abrangendo o conhecimento do potencial que está atrelado ao uso dos implantes de *biochips* para o desenvolvimento da sociedade, tornando-a mais segura, otimizada e integrada.

## 5. HIPÓTESES QUE ESTE PROJETO PRETENDE VALIDAR

No contexto em que este projeto se insere, pretende-se obter respostas aos seguintes questionamentos: 1) *De que maneira a proposta de criptografia para segurança e*

*privacidade de dados pode auxiliar no desenvolvimento das tecnologias acerca dos implantes biochips para humanos?* 2) *De que forma o desenvolvimento de um sistema de segurança para biochips acarretaria em uma maior confiabilidade da sociedade?* 3) *O quão importante é o desenvolvimento de segurança de dados e privacidade de usuário dos implantes de biochip para a sociedade?*

## 6. METODOLOGIA E ESTRATÉGIAS DE PESQUISA

A metodologia de pesquisa está direcionada no desenvolvimento de um sistema de segurança e privacidade de dados para implantes de *biochips* para humanos, já que os esquemas criptográficos convencionais não asseguram de maneira efetiva os dados e a privacidade do usuário. A atividade de desenvolvimento deste sistema requer um estudo aprofundado de criptografia de sigilo OTP (O*ne-Time Pad*), em conjunto de algoritmos QKD (*Quantum Key Distribution*), que propõem a impossibilidade de clonagem de um único fóton [3].

No decorrer do desenvolvimento do projeto será realizado atividades contínuas de pesquisas e testes de segurança para a validação e funcionalidade dos resultados, utilizando o método do ciclo *Sprint* de planejamento; desenvolvimento; testagem; *deploy* e revisão [4].

## 7. REFERÊNCIAS

[1] WEISS, Hayley: Why You´re Probably Getting a Microchip Implant Someday: Microchip implants are going from tech-geek novelty to genuine health tool-and you might be running out of good reasons to say no. The Atlantic, 2018.

[2] CONSTITUIÇÃO FEDERATIVA DO BRASIL. Título II: Dos Direitos e Garantias Fundamentais. Capítulo I: DOS DIREITOS E DEVERES INDIVIDUAIS E COLETIVOS. Artigo 5°, Inciso X, 1988.

[3] DI FALCO, Andrea Et. Al.: Perfect secrecy cryptography via mixing of chaotic waves in irreversible time-varyng silicon chips. Nature Communications, 2019.

[4] KNAPP, Jake; ZERATSKY, John; KOWITZ, Braden. Sprint: How to Solve Big Problems and Test New Ideas in Just Five Days. 1ª Edição. Simon & Schuster, 2016.