Título: **Preservação da privacidade de dados em mobile health: uma abordagem baseada em blockchain**

Data: **18/10/2019**

Horário: **10:00h**

Local: **ala de Seminários - Bloco 942-A (GREat)**

Resumo:

A privacidade e a segurança em sistemas de registros de saúde, como os sistemas *mobile health* , estão entre os problemas mais relevantes de um ecossistema de *Internet of Things* (IoT). Devido ao fator de restrição de recursos dos dispositivos médicos implantáveis e dispositivos IoT vestíveis, as soluções de segurança tradicionais não podem ser empregadas. À vista disso, nós apresentamos um modelo de sistema mobile health descentralizado que combina blockchain, IPFS, prova de conhecimento zero não-interativa (NIZKP) e criptografia baseada em atributos (ABE) para garantir a privacidade e a segurança dos dados do paciente. No modelo proposto aqui, a blockchain, por meio de contratos inteligentes, assume o papel de um autenticador descentralizado que garante acesso apenas aos usuários legítimos do sistema. Esse mecanismo de autenticação usa uma abordagem baseada na ideia de NIZKP, que substitui a troca de mensagens interativas, própria das provas de conhecimento zero (ZKP), por uma única mensagem. Isso leva à otimização do processo, tornando a NIZKP adequada para dispositivos com recursos restritos. Para obter um controle de acesso flexível e completamente centrado no paciente, nós empregamos um esquema de criptografia baseada em atributos (ABE). Em tal esquema, o proprietário dos dados tem a capacidade de distribuir chaves secretas de decifração para os usuários legítimos do sistema e compartilhar os dados cifrados especificando uma política de acesso. Deste modo, somente os usuários cujos atributos especificados atendem à política de acesso podem decifrar os dados. Neste trabalho, o principal objetivos é fornecer um *framework* que especifica como armazenar e compartilhar dados de saúde em sistemas de monitoramento remoto da saúde do paciente. Como esses dados são extremamente sensíveis, focamos em um refinado controle de acesso para preservar a privacidade do paciente.

Banca:

- Prof. Dr. José Neuman de Souza (MDCC/UFC - Orientador)
- Prof. Dr. José Cláudio do Nascimento (UFC-SOBRAL - Coorientador)
- Prof. Dr. Emanuel Bezerra Rodrigues (MDCC/UFC)