Título: **SECURITY AND PRIVACY-PRESERVING OF DATA IN MOBILE HEALTH SYSTEMS: AN APPROACH BASED ON NON-INTERACTIVE ZERO-KNOWLEDGE PROOF AND BLOCKCHAIN**

Data: **07/04/2021**

Horário: 9:00

Local: **Videoconferência**

Resumo:

People of different ages have used miniaturized mobile devices with wireless communication capabilities and integrated with biosensors as wearable accessories to collect health data regularly. This type of medical assistance, which uses mobile devices to monitor patients and offer healthcare services remotely, is known as mHealth. The mHealth devices are typically wearable and have resource-limited — so that many mHealth resources are managed through a smartphone. In this scenario, one of the most worrying issues involves communication between the monitoring devices and the smartphone. When the communication uses Bluetooth, it is standard for the device to be paired with the smartphone; but generally, it is not exclusively

associated with a specific mHealth application. This feature can allow for a data theft attack. Thus, to address this problem, the present work proposes an authentication scheme based on Non-Interactive Zero-Knowledge Proof (NIZKP) — a cryptographic primitive lightweight enough to run on mHealth devices with resource-limited. In order to ensure the patient's privacy-preserving throughout the system, this work also addresses the issues of storing, managing, and sharing data using blockchain. Through smart contracts, the blockchain assumes the role of a decentralized authenticator that guarantees access to data only to legitimate users. As there is no privacy in the standard public blockchain, this work presents a scheme in which the data transmitted, stored, or shared is protected by Attribute-Based Encryption (ABE). Here, the data owner can share the encrypted data along with an access policy, and he/she himself/herself has the ability to distribute the secret keys to legitimate users to decrypt the data. Preserving privacy and data security in electronic health record systems, including mHealth systems, are currently among the biggest concerns for patients. Given this scenario of concerns, the proposal presented in this work holistically addresses all these issues, proposing a model for constructing a mHealth system that guarantees the security and privacy of data from end to end, with robust access control and fully managed by the patient.

Banca examinadora:

- José Neuman de Souza (Orientador) (UFC)
- José Cláudio do Nascimento (Coorientador) (UFC)
- Emanuel Bezerra Rodrigues (UFC)
- Atslands Rego da Rocha (UFC)
- Joaquim Celestino Júnior (UECE)
- José Augusto Miranda Nacif (UFV)