Multi-factor Authentication layers in IOT of health care using Master-code bypassing Deepfakes

By

Omar Mohammed Rawdhan Rawdhan

Supervisor

Dr. *Ahmad* Abdallah Althunibat

Al-Zaytoonah University of Jordan, 2023

Abstract

The Internet of Things (IoT) has the potential to bring significant progress to various industries, including healthcare. It can improve efficiency and reduce costs by connecting devices and allowing for real-time communication and data analysis. However, it also poses potential security threats as sensitive patient data and transactions are handled by IoT devices. As long as we rely on central servers to store information, there will always be a risk of data breaches. To address these challenges, companies must be prepared to develop and update the security of their IoT systems. This includes implementing Multi-factor authentication to secure data stored on IoT devices and cloud services. This method involves using more than one layer of security to ensure that only authorized users can access the data and devices. In addition, this problem can also be solved by implementing a master-code strategy. This strategy can help to authenticate the device first before establishing any connection to the network. In this way, the devices can be protected from any kind of unauthorized access. In conclusion, the IoT presents both opportunities and challenges. While the benefits of this technology are undeniable, the potential for security breaches must be addressed to ensure the protection of sensitive data and transactions. By implementing Multi-factor authentication and master-code strategy, we can effectively address these concerns and fully realize the potential of the IOT in healthcare and other industries.