ABSTRACT

The development of the medical world has been very rapid, wearable medical warfare has got an important role in the medical world. Unlike cable-connected devices, wearables are devices with wireless connections, which are devices that canbe worn remotely. In the manufacture of this system, it will be used on ahealth vest,where the purpose of this vest will be implanted some sensors such as, heart rate readings in real time and others. In terms of efficiency, this device is very useful and very easy to use. But given that it stores data and uses a Wi-Fi or Bluetooth Low Energy (BLE) connection to transmit data to health authorities, it will be particularlyvulnerable to attacks from cyber criminals and get data from users.

Therefore, this medical system requires several steps that can be used to secure the user's data.The device will complete the key with an embedded key symmetric method where authentication and firmware verification use symmetric keys sent to the device.However, these wearable devices usually have computing power that is not as good as desktop computers, making it difficult to adopt a complete security algorithm.So in the creation of this system, the author will use efficient authentication and encryption (OTP), using AES and SHA standards that can provide two-way authentication between devices and servers remotely and protect patient privacy from various network threats..

Keywords : OTP, Wearable, Authentication, AES and SHA