PLAGIARISM SCAN REPORT

0%
Plagiarised

100%
Unique

463
Words

2983
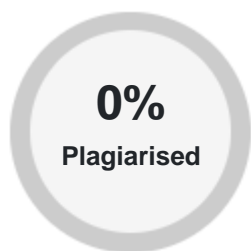**Characters**

Exclude Url : None

Content Checked For Plagiarism

The IOT, short term for Internet of Things, is a latest technology consisting of devices, mechanical and digital machines. The IOT has an ability to transfer data and capable for gathering and sharing electronic information. Several companies and industries are looking forward to invest for this latest trend technology when it comes to services, one of these is the health care industries. Wireless Body Area Network (WBAN), is one of the results of Internet of Things when it comes to advancements in technology. It provides communication that are implanted through sensors on human body with wireless network also called as Body Sensor Network (BSN). In today's generation, a lot of people are experiencing the wearable devices to help them monitor their own health information through sensors such as heartbeat, temperature, blood pressure, blood glucose levels, etc. A lot of instances that the collected data from the sensors is no use, the limited resources of on-body sensors are failed to analyze the data they sense. The issues in trust, privacy and data security of a user's have been concerning for them. The importance of security and the trust for the wearable devices is being concentrated by the manufacturer, they should ensure that the implanted devices on a user's body will provide a secure communication and produces the need to uniquely identify a communicating entity. The existing mechanisms like Unique Device Identifier (UDID), MAC Address, IP Addresses, Electronic Serial Number (ESN) and Digital Fingerprinting can act as unique identifiers. But, there are some tampering techniques and limitations of using these unique identifier mechanisms. These existing identification mechanisms are poses a serious risk for the users of Wireless Body Area Networks. The authentication of the user is a major concern of many industries that manufactures wearable sensor devices. So, there are some technique which is easy to embed in these devices. In today's era, most of the smartphones are embedded with the sensors like gyroscope, accelerometer, magnetometer, light sensor, etc. The accelerometer is an inexpensive sensor and easy deployable device which is used in tracking and classification of human daily activities. Recent study claimed that low cost accelerometers can be used in designing a wearable sensor networks, and motivate others to investigate the authentication methods on-body wearable sensors with the low cost accelerometers. These are some few aspects to be taken into consideration: Can accelerometer data provides reliable information to verify, whether the two sensors are carried by the same person? And what is the best active motion of an individual to track the similarities in the profile data? The unique property of acceleration can be replicated from walking motion of an individual. This paper aims at the authenticating sensors in Wireless Body Area Networks is finally posed a scheme using accelerometers.