Books > Industrial Internet of Things... > An Efficient Elderly Disease Prediction...

An Efficient Elderly Disease Prediction and Privacy Preservation Using Internet of Things

Publisher: Wiley AI

Cite This | PDF

is part of: Industrial Internet of Things (IIoT): Intelligent Analytics for Predictive Maintenance

Resmi G. Nair ; N. Kumar **All Authors**

Editor(s): R. Anandan ; Suseendran Gopalakrishnan ; Souvik Pal ; Noor Zaman

10
Downloads

Abstract

Chapters & Sections

Show Full Outline ▾

Authors

Keywords

Metrics

More Like This

Chapter Abstract:

Summary IoT (Internet of Things) is the physical object network that connects many inbuilt devices to the Internet for data collection and exchange. The ability to link such systems to vast pools of data, such as the cloud, is an essential improvement. IoT is widely applicable in many aspects of our life by integrating integrated appliances and cloud servers. Embedding devices with a cloud server will give aged people a more versatile facility without going to hospitals with the ageing population. While the sensor-cloud paradigm has benefits, there are still many security challenges. Therefore, it is important to understand the architecture and integration of security problems such as authentication and data protection to protect elderly people's privacy. An intelligent and safe health control system is proposed in this article with an IoT sensor focused on cloud storage and encryption. Here, initially, using the IoT devices, a smart wearable device can be designed using ESP 32. Then, the obtained data can be normalized, and pointed features can be extracted by using the semantic component analysis method. Then, by implementing the iterative multistate uplift, ANN can classify and identify the diseased data precisely. Then, the data is stored on a cloud server or maintained and monitored. The PHR must be protected from the attack in the cloud. To comply with this privacy preservation system, techniques of cryptography are used. The polynomial HMAC encryption algorithm is initially used for the PHR service. The cloud server produces the key for authentication purposes as the data owner queries the file and checks it out with the user. The user will access the decrypted file when the key is given using a polynomial HMAC algorithm. Then, the emergency message and the generated key can be sent to the patient and doctor for earlier treatment. Finally, the performance analysis is performed, and the proposed and the existing techniques are analyzed to demonstrate the schem...

Show More

Page(s): 369 - 392

DOI: 10.1002/9781119769026.ch15

Copyright Year: 2022

Publisher: Wiley AI

Edition: 1

▸ **ISBN Information:**

Authors

Keywords

Metrics

IEEE Personal Account

CHANGE USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS

VIEW PURCHASED DOCUMENTS

Profile Information

COMMUNICATIONS PREFERENCES

PROFESSION AND EDUCATION

TECHNICAL INTERESTS

Need Help?

US & CANADA: +1 800 678 4333

WORLDWIDE: +1 732 981 0060

CONTACT & SUPPORT

Follow

About IEEE *Xplore* | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | IEEE Ethics Reporting | Sitemap | IEEE Privacy Policy