Blockchain-Enabled IoT for Rural Healthcare

Subjects: Telecommunications
Contributor: Steve Kerrison, Jusak Jusak, Tao Huang

Internet of Things (IoT) and blockchains are enabling technologies for modern healthcare applications, offering the improved monitoring of patient health and higher data integrity guarantees. However, in rural settings, communication reliability can pose a challenge that constrains real-time data usage. Additionally, the limited computation and communication resources of IoT sensors also means that they may not participate directly in blockchain transactions, reducing trust.

Keywords: blockchain ; digital twin ; Internet of Things ; healthcare

1. Introduction

Internet of Things (IoT) technology has given rise to many new and innovative applications. In manufacturing, organisations from small to large scale use IoT to improve the monitoring of production processes, respond immediately when process deviation occurs, and to provide better services to their customers [1]. Implementation of IoT in the healthcare domain is a focus area for many researchers, academics, and industry as well. Healthcare IoT (HIoT) devices equipped with sensors, computation capability, and radio communications collect and process a patient’s health related data, such as body temperature, electrocardiograph (ECG), oxygen saturation, blood pressure, and others to be transmitted to a cloud storage system in the other parts of the world through the internet. The term Healthcare 4.0, analogous to Industry 4.0, has been used widely to mark the development of smart and connected healthcare offering a chance to shift from traditional patient treatment to technology-based solutions that allow remote monitoring and medication [2].

Healthcare IoT is expected to be widely adopted but primarily benefits those in city regions who are most likely enjoying more extensive communications capabilities compared to those living in remote areas. The deployment of HIoT-supporting infrastructure in rural areas may face several obstacles. Geographical features of remote areas may be dominated by mountains, forest, savanna, hills, and rivers. In such areas, due to impediments to signals and low population density, there is less incentive for telecommunication providers to invest in installing significant infrastructure. Therefore, in most rural environments, low-communication quality, such as low bandwidth and intermittent connections, is frequently experienced by IoT devices, which can pose a challenge for real-time data usage.

Several technologies have been introduced in an attempt to address these adverse impacts, such as low power wireless area network (LPWAN) solutions [3][4]. LPWAN networks were introduced to accommodate the need for long-range and energy-efficient communications IoT devices. An example of such a technology is the long range (LoRa) standard that has growing adoption and industry support [5][6].

In addition to rural communication issues, HIoT faces security and privacy challenges in managing massive amounts of collected data. Cloud-based electronic healthcare records (EHR) emerged as a widely adopted solution [7]. They have several advantages, including on-demand service, broad network access, resource sharing, rapid elasticity, and guaranteed quality of service from service providers. With these features, the implementation of the EHR contributes to reduced data storage and maintenance costs, improved speed and processing accuracy, and allows data exchange among parties within a particular EHR system [8][9]. However, the centralised nature of the EHR system creates a setback from the user’s point of view, in that users are more concerned about security and privacy due to the loss of control over clinical data in cloud storage.

2. Rural Healthcare Monitoring

Providing appropriate communication infrastructure for electronic rural healthcare monitoring has been one of the most challenging issues from both the technological and economics points of view [10]. The geographical structure and population of these areas are the main reasons for this. Rural areas are often dominated by hilly terrain for large
distances. Therefore, investing in the telecommunication infrastructure, such as 4th or 5th generation networks, in such areas has a low return on investment due to low population density and the complexity of installation for adequate coverage.

Alternatively, it has been suggested to exercise LPWAN technology, which lends itself to such settings due to low power transmission, while offering long-range communications among IoT devices. There are various standards bodies that are extensively working on developing LPWAN systems, such as the Institute of Electrical and Electronics Engineers (IEEE), the European Telecommunications Standards Institute (ETSI), the 3rd Generation Partnership Project (3GPP), the Internet Engineering Task Force (IETF), and the LoRa Alliance.\[11\]

For example, a study by Dimitrievski in \[3\] showed the use of LoRa to carry healthcare data from rural areas combined with fog computing and the low Earth orbit (LEO) satellite connectivity to provide real-time data transmission. This work also proposed techniques for energy conservation utilising the external ultra-low-power timers that allow the device to be powered down, and showed its advantage to extend battery life in the order of tens of times. The fog system is a computation machine that is usually located between the cloud and the end devices to enable computing, communications, storage, and data management within the close vicinity of IoT devices. Therefore, in this IoT setting, the fog computation gives advantages to any delay sensitive devices to accumulate and process their retrieved data quickly (i.e., to achieve its real-time mode operation) rather than pushing through all data into the cloud system. Furthermore, the edge computing can be used to alleviate computing, storage, and bandwidth burdens of the system by allowing data processing within the edge devices when the resources of the IoT devices can be exploited to support that purpose.\[12\]

Another study highlights a healthcare IoT architecture integrating blockchain and LoRa network to monitor patient health data securely.\[4\] To achieve real-time data transmission, the proposed model employs edge and fog devices to run the LoRa communication protocol whereby the edge devices with sensors attached on them collect data from healthcare data sources and subsequently send those relevant patient data to the upper fog layer using LoRa. To guarantee security, the data are stored in the interplanetary file system (IPFS) combined with blockchain technology. Finally, data monitoring and analytics for patients' health status were performed through mobile or web applications.

The delivery of healthcare and the associated monitoring can be considered a complex system, with many changing variables that could change patient outcomes and affect decision making. The digital twin concept was first envisaged to aid the management of complex manufacturing systems, and the definition by NASA has become widely accepted.\[13\] Therein, a digital twin is considered a virtualisation of a physical system, maintained via the supply of data, for example, via IoT. With adequate data and modelling, scenarios can be simulated with a digital twin in order to predict outcomes for the physical system, allowing optimisations or corrections to be made. Unsurprisingly, this has been also been applied to healthcare settings.\[14\]

### 3. LPWAN and LoRaWAN

The term LPWAN, or low-power wide area network, refers to technologies that have the capability to reach long-range communications but at the same time maintain the minimum use of energy.\[15\] This communications model is particularly important to accommodate the need for various small devices which inherit features such as low computational power, low memory, and low battery capacity. However, contrasting these advantages of LPWAN, the nature of wireless signals dictates that most LPWANs have a low bit rate. Although there are many LPWAN architecture available on the market, LoRa has found its acceptance in both wider communities and broad industry support compared to other similar technologies in this scope, such as narrow band IoT (NB-IoT), LTE machine-type communication (LTE-M), and Sigfox.\[16\]

Despite its long-range coverage and low-cost deployment, the most notable advantage of using LoRa is its reliance on a license-free operating frequency privilege operated on the industrial, scientific, and medical (ISM) frequency sub-band. The use of the chirp spread spectrum (CSS) modulation scheme on its bidirectional communications results in a signal transceiver with low noise levels yet high interference resilience. Utilising this modulation technique, the LoRa data rate varies from 250 bps to 50 kbps depending on the allocated spreading factor (SF) and channel bandwidth. For example, a lower spreading factor allows a higher data rate at the expense of a lower transmission range. The maximum payload length is 64–255 bytes, including its 13 bytes payload header, depending on the data rate chosen.

Alongside the growth of the LoRa adoption, LoRaWAN appeared as a protocol stack built on top of the LoRa physical layer. With its data link layer protocols support, this LoRaWAN shapes the LoRa network architecture into a typical gateway-nodes model that consists of a gateway that acts as a bridge between nodes, network servers and application servers over a backhaul interface.\[17\] In this structure, nodes can transmit messages to other LoRa devices or to a...
gateway. Hence, a gateway bears a task to gather data from all authorised sensor nodes (i.e., the end-devices) and pushes forward those data to the application server through the network servers.

The core of the LoRaWAN network resides in the network servers which maintain connectivity, routing, and security among devices. Therefore, gateways and network servers retain an important function in the LoRaWAN architecture to coordinate all nodes in its network, while at the same time synchronising data transmission to avoid collisions. This function was specifically defined in LoRaWAN as the medium access control (MAC) operation. Depending on how nodes should schedule their downlink traffic, users can alleviate the efficiency of LoRaWAN networks by properly selecting the class in which LoRaWAN networks are deployed. The LoRaWAN allows operation in one of three different classes: A, B and C. In Class A (ALOHA) communications, an end device has the capacity to start transmitting data at any moment, whereas in Class B (Beacon), an end device can only open a receive window and transmit data between a periodic beacon signal duration according to the network-defined schedule. In Class C (Continue), an end device constantly listens to the downlink signal from the network unless the end-device is transmitting data.

Additionally, LoRaWAN enforces the duty cycle to limit the transmission of large amounts of data that may consume the whole bandwidth of a channel, which would cause congestion in the networks. The duty cycle defines how much of the total time a device is allowed to transmit data per hour on a particular sub-band. For example, a 1% duty cycle restricts the total amount of time a device spends transmitting data to 36 s per hour. Realistically, the amount of the duty cycle applied to a LoRaWAN is governed by regional regulatory authorities [25]. Furthermore, the things network (TTN), a service providing a public LoRaWAN network, applies a more rigid rule to lessen congestion by employing a fair access policy. This policy, applied to each end device, restricts the device's uplink airtime to 30 s per day (24 h) and downlink messages to only 10 in number per day [26].

### 4. Blockchain Systems for Healthcare

A considerable number of works have proposed IoT-based healthcare systems to provide a more timely and cost-efficient remote patient-care system [16][19]. Among other advantages, the IoT system might be identified as a substitute for the common in-hospital health monitoring with the remote one, where patients might stay at home or live in a rural area. While the traditional client–server and cloud computing paradigm offers significant improvement to the way patient data are stored, it also raises security and privacy concerns. For example, it suffers from the issues of single point of failure, data privacy, centralised data administration, and system vulnerability. The major threats to this cloud model may include spoofing identity, tampering with clinical data, and the data leaks [18].

Recently, the blockchain system has presented itself as a novel technology that could have a role in preserving healthcare data security and maintaining patient privacy. In a blockchain system, multiple data transactions, such as a patient's treatment and medical history, are grouped together in a structure called a block [20]. Each block is uniquely identified by its hash and timestamp and is chained to the previous block by incorporating the hash value of the previous block, thus creating a chain of blocks. The hash algorithm that is used acts as a one-way function, meaning it is computationally infeasible to produce a different block that would result in the same hash, effectively making the contents of the chain immutable. As such, validation of each block before they are chained in a blockchain network is paramount, as they typically cannot be removed or edited. Validation of transactions and blocks is performed by a consensus mechanism, whereby a shared ledger of blocks in the blockchain network can only be altered by the agreement or consensus of a majority of members [21].

Blockchain technology has a promising future in the healthcare domain, as it can solve some inherent issues facing modern health-management systems. It has advantages as a tamper-resistant distributed ledger for recording healthcare data and transactions, and its high availability and resiliency that will deter system failures and other cyber attacks [22][23][24]. However, the integration of blockchain into the IoT system in the healthcare rural area use cases may encounter several challenges to solve.

IoT devices may have difficulty to process and store even the smallest elements in the blockchain. Secondly, the geographical structure of rural areas and decreased availability of reliable transmission due to a sporadic communications infrastructure being in place are the other two notable problems faced by researchers to initiate such a secure healthcare monitoring system. Besides focusing on its applications, there are also some blockchain-based frameworks proposed for managing secure healthcare systems, such as a framework for regulating mobile health apps and governing their safe use [25] and a framework for an asthma healthcare system that challenges its adoption during the COVID-19 pandemic [26]. All of these listed works use blockchain for medical data that have been collected in cloud storage, while the security of data transmission from IoT devices to the cloud is handled by encryption. However, the outlined works do not consider
that transmitting medical data in rural settings is problematic, and several steps are required for user authentication in order to commit valid transactions in the blockchain system.

References


Retrieved from https://encyclopedia.pub/entry/history/show/107321