Blockchain-Assisted Cybersecurity for the Internet of Medical Things

Subjects: Computer Science, Cybernetics

Contributor: Mohammed Saeed Alkatheiri , Ahmed S. Alghamdi

The Internet of Medical Things (IoMT) plays an important role in strengthening sustainable healthcare systems. IoMT significantly influences our healthcare because it facilitates monitoring and checking patient medical information before transferring the data to a cloud network for future use. The IoMT is a big-data platform which is growing rapidly, so it is critical to maintain all data safely and securely.

blockchain IoMT cybersecurity healthcare

1. Functional Architecture of Blockchain

Blockchain is a decentralized digital ledger that allows end-to-end communication and provides interaction between untrustworthy persons. Blockchain comprises *n* number of blocks, as illustrated in **Figure 1**.

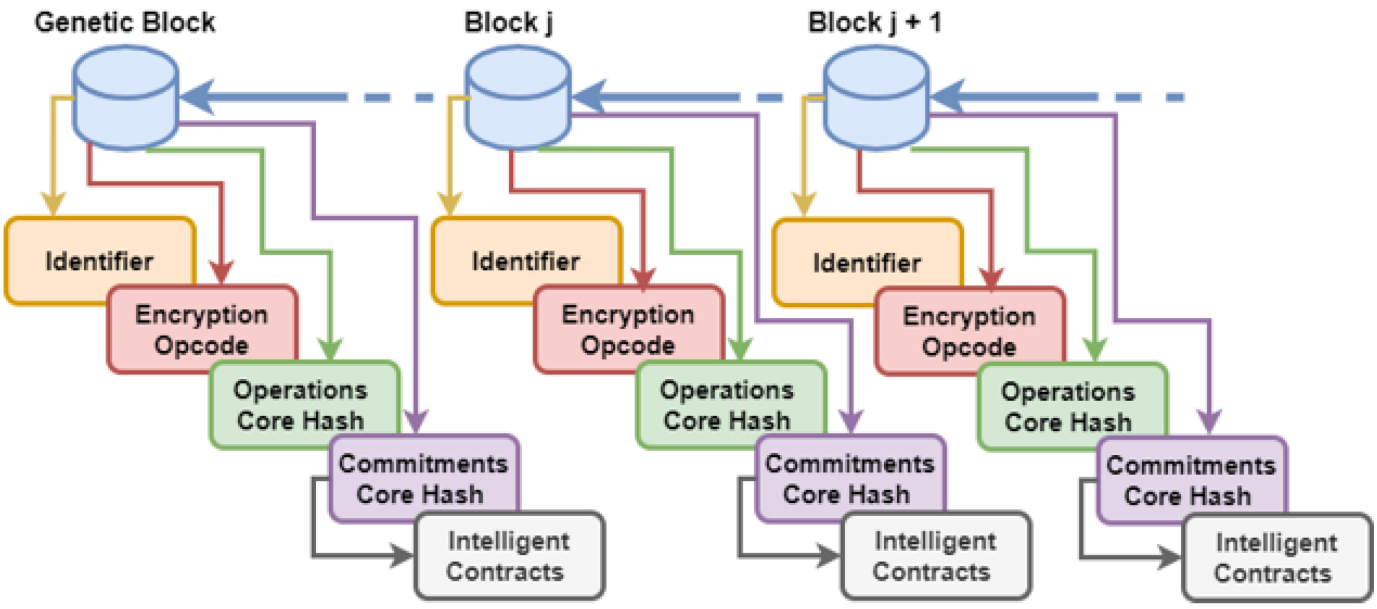

Figure 1. Functional architecture of blockchain.

In this functional architecture, apart from the initial block (genetic), each block is integrated into its preceding block through a reverse connection, the hash code of its earlier block. For example, block *j*+1 has the hash code of its earlier block *j*. Every block also includes additional data fields, such as an identifier, an encryption opcode, a core

hash of all operations, and a core hash of all commitments. Because even a single bit change might result in a unique hash code, the fixed-size core hash values of both operations and commitments are essentially irreversible.

Intelligent contracts are another disruptive invention in blockchain technology that the development of blockchain has propelled. When specific criteria are met, intelligent contracts operating on the upper end of the blockchain can streamline the implementation of contractual agreements and restrictions. Intelligent contracts are irreversible after being synthesized into executable code and recorded in blockchains related to the irreversibility of blockchain and the core hash of all intelligent contracts. Intelligent contracts can help streamline administration, increase the efficiency of business operations, and reduce potential threats. The following are the essential characteristics of blockchain architectures:

- Immutability indicates that falsifications of data kept in blockchain are exceedingly difficult since even little changes might result in incorrect data.
- Transactional non-repudiation can be enabled by digital signatures, non-symmetric encryption/decryption methods, and decentralized consensus procedures.
- Traceability denotes the ability to track data sources by examining currently accessible blockchain data with accompanying metadata.
- Diversity of blockchain enables transactions to be authenticated by the number of users spread across the network without the need for a central authority. In this manner, administrative costs may be reduced, while system dependability is improved.

Blockchain technologies are generally classified into three categories:

- Open blockchains;
- Personal blockchains;
- Collaborative blockchains.

Open blockchains, such as cryptocurrency, Bitcoin, and EOSIO, may be accessed by any user in the blockchain community, but personal blockchains feature intensive access control to restrict user functionality. Collaborative blockchains reside between private and open blockchains. Open blockchains often have less sustainability than personal blockchains due to the poorer capacity of cryptographic techniques, where capacity represents the number of operations confirmed per second. Collaboration blockchains yield less efficiency than personal blockchains but greater efficiency than open blockchains.

2. Overview of Internet of Medical Things (IoMT)

Recent advancements in sensing devices, healthcare instruments, and wireless communications have resulted in the emergence of the IoMT. It is employed in various healthcare situations, including e-medicine, remote rehabilitative services, and pandemic isolation. The IoMT, which connects various healthcare instruments and infrastructures with the healthcare industry, has resulted in huge amounts of diversified healthcare records. Healthcare providers can easily identify and diagnose a healthcare issue and treat patients using huge quantities of IoMT information. **Figure 2** illustrates the overview of the IoMT architecture. In the IoMT architecture, numerous IoMT sensors generate enormous amounts of IoMT information, captured, interpreted, and evaluated by healthcare providers.

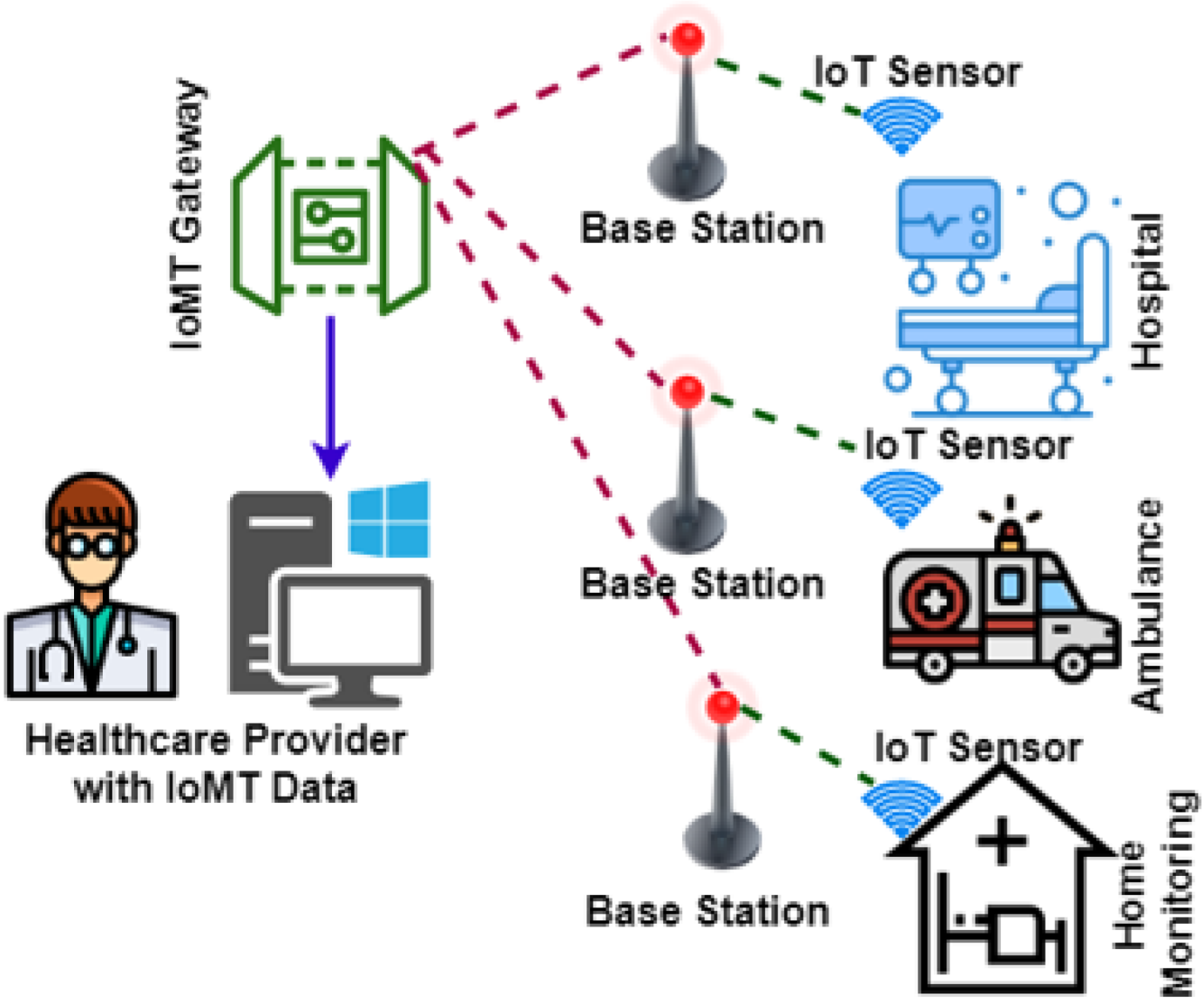

Figure 2. Overview of IoMT architecture. The figure shows the overall concept of the IoMT-based data acquisition, storage, processing, and distribution system. Base stations accumulate data from disparate sensors deployed in diverse situations. Data from the base station are received by the healthcare providers through the gateway.

The IoMT can provide dependable and effective healthcare services to both patients and healthcare providers. The emergence of the IoMT also brings with it the associated difficulties:

- A lack of compatibility across various IoMT domains;
- Confidentiality and cybersecurity flaws in the IoMT instruments and networks.

IoMT systems are heterogeneous because they are made up of various biosensors, healthcare systems, IoT interfaces, and wireless networks. Furthermore, the heterogeneity of the IoMT is evidenced in the variety of wireless systems, such as near-field transmission, Bluetooth technology, and wireless local area networks. The diversity of distributed IoMT systems leads to poor compatibility between systems, resulting in a variety of data barriers. As a result, it is difficult to transmit healthcare information between healthcare facilities and organizations. On the other hand, healthcare data transmission is critical for healthcare practitioners, particularly in preventing and managing pandemics. Furthermore, the IoMT is concerned with significant cybersecurity and confidentiality issues. Healthcare sensors and medical equipment, which are frequently resource-constrained, have inherent weaknesses to malicious assaults, such as eavesdropping, interference, malware, and worm threats. Secondarily, when compared to other forms of IoT information, IoMT information is highly confidential. The data confidentiality of patients may be purposefully or unintentionally leaked during the gathering, processing, and analysis of IoMT data.

3. Blockchain-Assisted Cybersecurity for the Internet of Medical Things

Blockchain interconnection with the IoMT can overcome cybersecurity and privacy problems. **Figure 3** illustrates the architecture of Blockchain-Assisted Cybersecurity for the IoMT. The proposed architecture comprises four states:

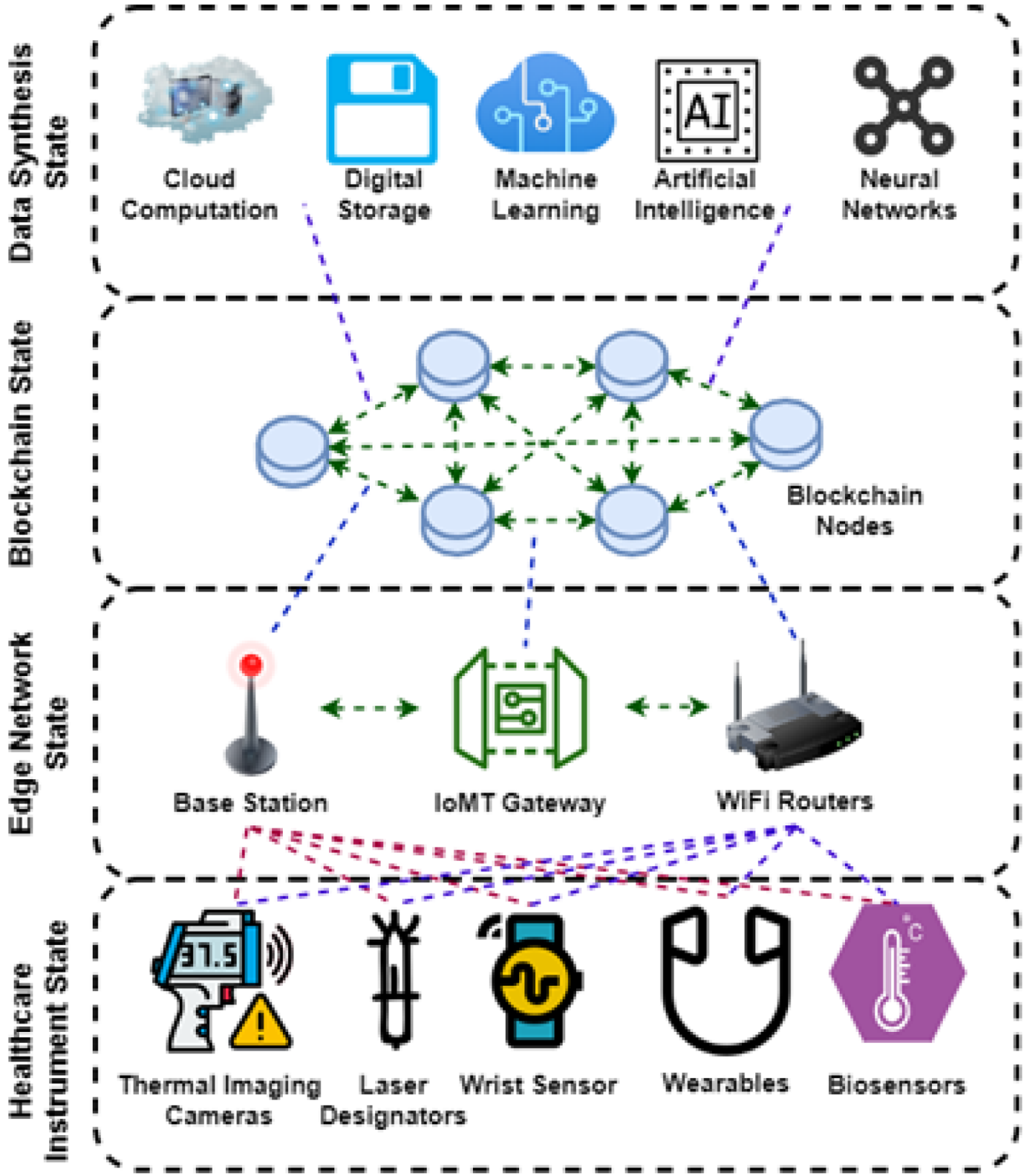

Figure 3. Architecture of Blockchain-Assisted Cybersecurity for IoMT systems. The overall architecture is organized into four states, i.e., healthcare instrument state, edge network state, blockchain state, and data synthesis state.

- Healthcare instrument state;

- Blockchain state;
- Edge network state;
- Data synthesis state.

The healthcare instrument state is equipped with numerous IoMT healthcare instruments, such as thermal imaging cameras, laser designators, wrist sensor systems, wearable devices, and biosensors. The edge network state is simply a combination of communications infrastructure and edge computational resources. IoMT data can be collected and pre-processed by edge computing nodes embedded with wireless networks, WiFi routers, and the IoMT gateway. Furthermore, the blockchain state serves as a critical gateway to provide reliable analysis of multiple resources across the preceding levels. The data synthesis state comprises cloud computation capabilities, digital storage platforms, machine learning, artificial intelligence, and neural networks algorithms. Edge computing capabilities in the edge network state or objects in the data synthesis state are connected to nodes in the blockchain state. As a result, blockchain-assisted IoMT can also provide excellent authenticity and authentication protocols at both the edge network state and the blockchain. The edge network state and the blockchain state minimize the complication of IoMT devices and the diversity of IoMT interactions. However, the blockchain state can deliver blockchain-assisted functions to other programs to ease the development process. The blockchain state uses the built-in augmented reality network of blockchain to interconnect various IoMT sub-networks across the complete IoMT network. The heterogeneous IoMT modules are therefore merged as a whole to provide complete satisfaction to other programs. As a consequence, IoMT system compatibility can be enhanced.
