International Journal of Internet, Broadcasting and Communication Vol.15 No.4 261-269 (2023)
http://dx.doi.org/10.7236/IJIBC.2023.15.4.261

IJIBC 23-4-31

A Secure Healthcare System Using Holochain in a Distributed Environment

Jong-Sub Lee*, Seok-Jae Moon**

**Professor, College of General Education, SeMyung University, Jecheon, Korea*
***Professor, Department of Artificial Intelligence Institute of Information Technology,*
KwangWoon University, Korea
E-mail: 99jslee@semyung.ac.kr, msj8086@kw.ac.kr

Abstract

We propose to design a Holochain-based security and privacy protection system for resource-constrained IoT healthcare systems. Through analysis and performance evaluation, the proposed system confirmed that these characteristics operate effectively in the IoT healthcare environment. The system proposed in this paper consists of four main layers aimed at secure collection, transmission, storage, and processing of important medical data in IoT healthcare environments. The first PERCEPTION layer consists of various IoT devices, such as wearable devices, sensors, and other medical devices. These devices collect patient health data and pass it on to the network layer. The second network connectivity layer assigns an IP address to the collected data and ensures that the data is transmitted reliably over the network. Transmission takes place via standardized protocols, which ensures data reliability and availability. The third distributed cloud layer is a distributed data storage based on Holochain that stores important medical information collected from resource-limited IoT devices. This layer manages data integrity and access control, and allows users to share data securely. Finally, the fourth application layer provides useful information and services to end users, patients and healthcare professionals. The structuring and presentation of data and interaction between applications are managed at this layer. This structure aims to provide security, privacy, and resource efficiency suitable for IoT healthcare systems, in contrast to traditional centralized or blockchain-based systems. We design and propose a Holochain-based security and privacy protection system through a better IoT healthcare system.

Keywords: *IoT, Sensitive Personal Data, Blockchain, Holochain, Healthcare System, Privacy Security, Distributed Cloud*

1. INTRODUCTION

Due to the large scale and physical dispersion of many applications, such as smart healthcare, IoT is increasingly being implemented in a distributed environment [1]. Because of the distributed implementation characteristics of entities connected in IoT networks, they can be exposed to personal information security and security threats [2]. However, IoT healthcare systems contain a large amount of sensitive and personal data,

Manuscript Received: october. 2, 2023 / Revised: october. 20, 2023 / Accepted: october. 25, 2023
Corresponding Author: msj80386@kw.ac.kr
Tel:*** - **** - **** Fax: +82-10-916-4751
Author's affiliation: Professor, Department of Artificial Intelligence Institute of Information Technology, KwangWoon University, Korea

which is emerging as a serious problem. Blockchain [3] has been proposed as a solution in this situation because it has distributed ledger technology, but it has the disadvantage of being impossible to implement because storage and calculation requirements increase rapidly as the network size increases. This paper introduces a security and privacy protection mechanism based on Holochain [4], considering the resource constraints of IoT healthcare systems. The proposed architecture is composed of four parts: the PERCEPTION layer, the network connectivity layer, the distributed storage layer, and the application process layer. The PERCEPTION part detects and collects essential data such as patient data and medical information. The network connectivity layer assigns IP to the data from PERCEPTION to various hApps and ensures stable data transmission through standard transmission methods. In the distributed storage layer, important medical information is securely stored for resource-limited IoT devices, and it supports users to easily share the information. The application process layer manages the structuring and representation of data in the IoT network. As a result of this research, it was confirmed that the IoT healthcare methodology centered on Holochain provides effective privacy protection and stability while using fewer resources than blockchain-based methods. Chapter 2 discusses related research. Chapter 3 describes the proposed system. Chapter 4 provides an explanation of the comparative analysis. Finally, Chapter 5 concludes the paper.

2. RELATED WORK

Holochain is an example of the latest DLT(Distributed Ledger Technology) [5], aiming to build the next-generation internet. This technology operates on a P2P network foundation, handling agent-centric commitments and consensus among users. One of the unique advantages of Holochain is its ability to maintain an independent secure ledger even during interactions with other network participants. Holochain fuel refers to the mutual trust system required by Holochain users when processing hundreds of millions of transactions. In Figure 1, the individual hashchain structure of users is described [6]. For instance, in a smart healthcare environment, patients, doctors, medical staff, and other professionals connect through the same DHT to a specific hApp to exchange and store information while ensuring data integrity.

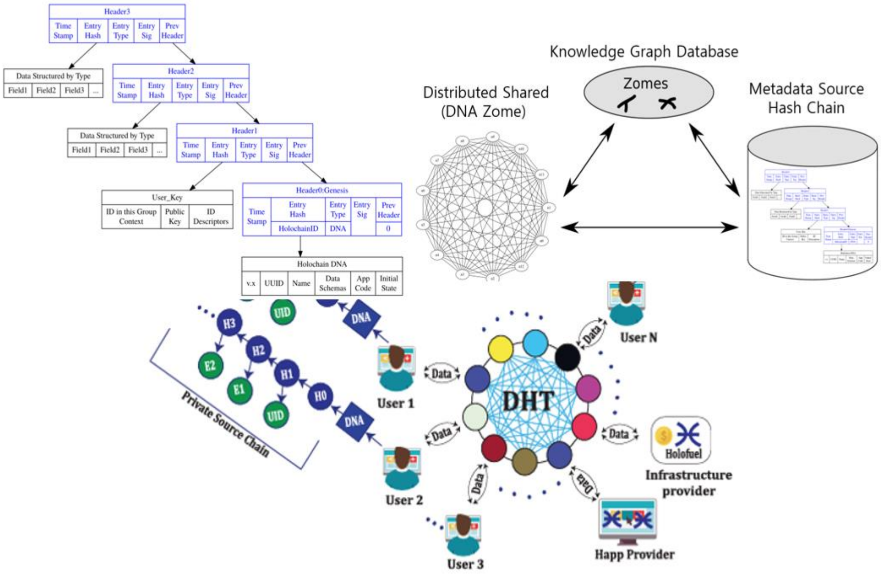


Figure 1. The Chain Structure of a Holochain on Knowledge Graph DB

3. PROPOSED SYSTEM

3.1 System Component

In this section, we introduce an IoT healthcare system based on Holochain, emphasizing high data integrity and rigorous network security. This IoT healthcare architecture consists of four core layers. Figure 2 presents the PERCEPTION layer, the network connectivity layer, the distributed storage layer, and the application processing layer, explaining the role and protocols used in each layer.

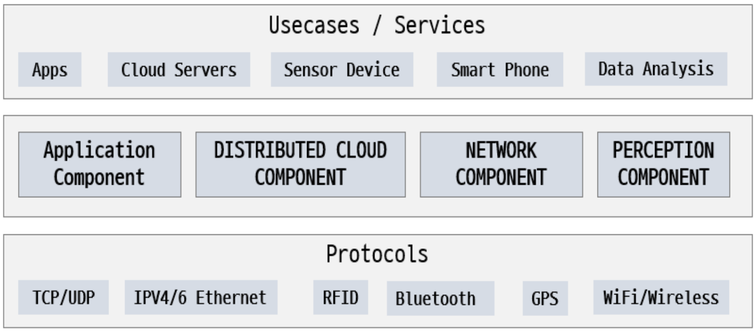


Figure 2. The Propose Structure

■ **PERCEPTION COMP.**

This layer is responsible for detecting and aggregating key patient information and health-related data. IoT devices detect and aggregate information, utilizing various communication methods such as Ethernet, IEEE 802 series, wireless sensor networks, GPS, Bluetooth, etc., for transmission. A reliable evaluation system securely collects data from authenticated users. Figure 2 depicts the connections of various medical participants such as patients, doctors, medical staff, experts, pharmacists, and medical equipment in an IoT medical structure centered around Holochain. Each medical entity can include multiple hApps, and each hApp follows its unique logic rules for specific service provision.

■ **NETWORK COMP.**

This layer delivers the data processing results from the PERCEPTION layer to IPs through various hApps. It ensures stable data transmission using standard protocols. In this process, various devices and technologies, such as routers, gateways, base stations, master communication stations, central hubs, switches, Bluetooth, and WiFi, are used for transaction processing and service provision. Once data packets are processed, this layer transmits reliable information to a higher level called the cloud layer. The cloud layer is responsible for the distributed storage and sharing of the received data. This information must be securely exchanged and stored among IoT devices.

■ **DISTRIBUTED CLOUD COMP.**

In this layer, considering the resource constraints of IoT devices, essential medical information is securely stored and preserved in the distributed cloud. Users can easily exchange and share this information. Not only patients but also other participants can back up their information in the cloud, and by sharing this information with authenticated colleagues, they can enhance service quality. In this layer, protocols related to TCP, UDP, and data analysis and machine learning are mainly used for data transmission and processing. To maintain the security of the cloud layer and the integrity of the data, Holochain technology is utilized in cloud devices.

- **APPLICATION COMP.**

This layer, being the top tier of the IoT network, is responsible for data formatting and representation. It defines a set of rules for message transmission, applying them to various medical services. Moreover, it directly communicates with users to provide app-based services.

3.2 IoT Healthcare System Overview

Medical institutions operate app services that allow users of various types to participate for health monitoring and continuous support. In this healthcare environment, Holochain-based medical applications are structured in a manner similar to a marketplace to provide services. Medical service providers introduce various smart features that apply special rules and protocols to deliver value to users. Users can search for and select the desired service offerings through this marketplace and can approve the relevant agreement. The selected service establishes a direct connection between the medical service provider and the user through a new health service app. In this paper, as described in Figure 3, the implementation of a fully distributed IoT healthcare system based on Holochain was made easy for information storage, network security, and privacy protection. Holochain can be applied at the edge of the network and on cloud servers. In this paper, Figure 3 represents the overall chain structure of the proposed healthcare system, where various stakeholders appear as individual agents.

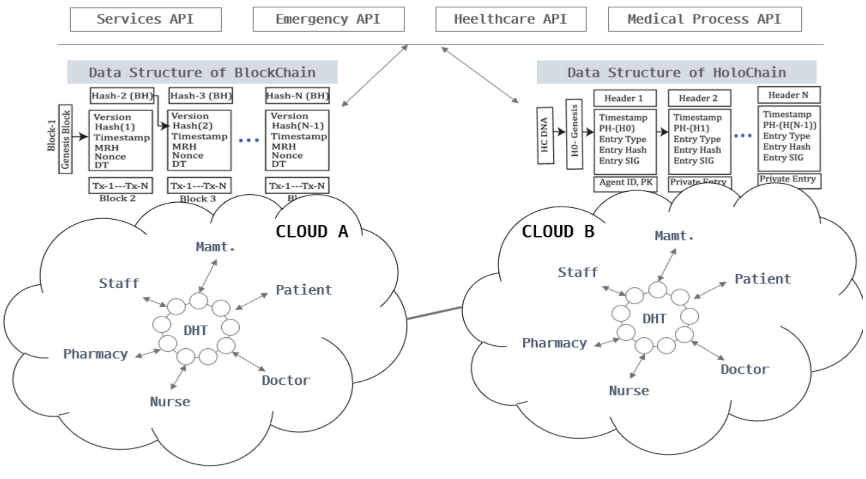


Figure 3. The Holochain & Blockchain-based IoT Healthcare System Overview

Each maintains its unique source chain that stores transactions locally with the assistance of cloud servers. An agent can decide whether to use one or more healthcare applications based on their needs. Each hApp is identified through its unique personal digital signature, the DNA, which includes initial item types, executable code, and parameters for a specific application. Therefore, even if two different healthcare hApps write code using the same attributes, they will have two different names and generate different DNAs. When an agent of the medical system joins the hApp network, it creates its identifier by generating a key pair consisting of a private key and a public key. Through this key pair, the agent acquires a unique identification within the network, ensuring data authorization, accessing data, and assisting in analyzing and detecting various types of threats and attacks. The private key is secretly stored within the agent's node, serving a role similar to a password, and is used to generate a digital signature with DNA. This digital signature, along with the agent's public key, is published as a public resource and used as the agent's address (identifier) in the Holochain network. However, other participants with the public key can verify the integrity of the agent's digital signature and process encrypted data to transmit it only to specific users. Every Holochain agent does not have a global shared consensus; instead, each maintains its own local source chain where all transactions are stored and verified. Communications between multiple users are signed by each participating agent and restricted to their individual source chains. They have the ability to transmit health data through the same public DHT. Each medical agent maintains a secure personal peer group that shares new transaction details, the validity of the transaction, the origin of information, and the sender's chain header (including historical order, peer creation, and network status). When a doctor wishes to monitor a patient remotely through the IoT network, they request a set of health reports from the patient. The patient then generates an authorization or token for specific reports or medical data they wish to share and stores a new transaction or narrative as a new entity in Holochain. Additionally, the patient shares the hash of the authorization item, which will be used as an ability token, with the authorized doctor.

3.3 Proposal Algorithm

The method of applying Holochain to the platform proposed in this paper is as follows: Algorithm 1. hApp bundle verification protocol configuration. We first initialize the DNA into the legacy system (LS) LhAppi by designing it into a local source chain, LSlocal. Here i means i = 1, 2, 3, ... N. The process of creating DNA in the LSlocal function sets the entity type as a validation rule. After setup, we set the executable function efx for the specific hAppi. We then set another parameter x that we expect to specify a unique hAppi. Initialize the second entity of the local source chain LSlocal to create a DNA Zome for hAppi. Calculate the timestamp time of Zome creation in the LSlocal function. Then we initialize the private and public key set IDs (P mrk, P mbk). And calculate the hash value of Zome. The metadata Holochain creation function creates a new Holochain metadata entity based on the hash chain. Functions that require a new transaction entity calculate the timestamp for the new metadata entity. We then specify a new item type and calculate the digital signature in step 25. Afterwards, a hash of the current data is generated and a hash of the previous header hash metadata is calculated. Store signed metadata entities in LSlocal before broadcasting. The new Holochain metadata entity creation function cryptographically signs each hashchain metadata entity. Afterwards, a digital signature of the transaction is calculated and stored for each new metadata entity in the Holochain using the agent's private key.

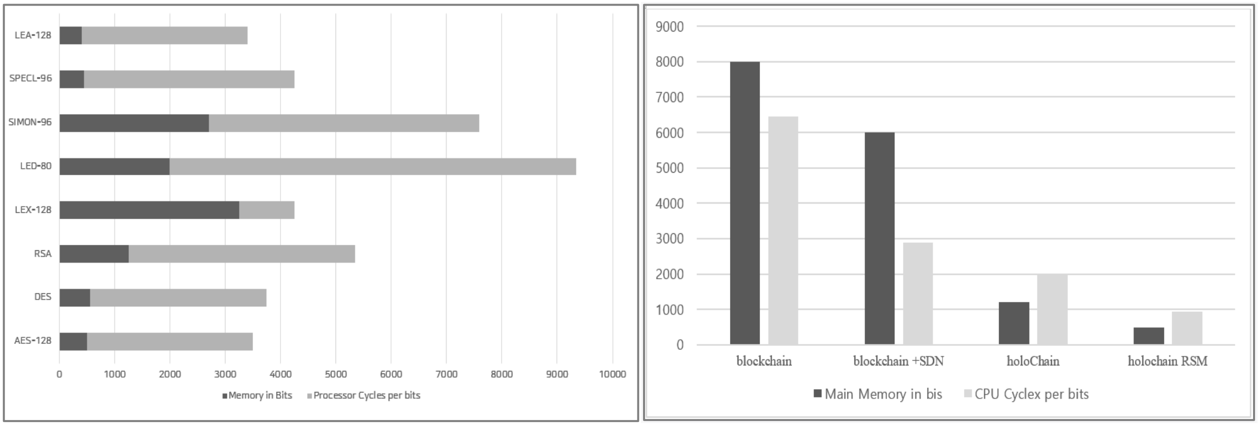
Algorithm 1. A Step-by-Step Implementation Holochain Framework

```
import hashlib, import datetime, import random
from Crypto.PublicKey import RSA
from Crypto.Signature import pkcs1_15
from Crypto.Hash import SHA256

# Setting up and verifying the hApp
def setup_and_verify_hApp():
    # This function will setup and verify hApp. Actual implementation will depend on the hApp details.
    pass
```

```
# Initializing the DNA as the first entity in the legacy system (LS) LhAppi
def initialize_DNA(i):
    # Create the DNA for each LhAppi
    LSlocal = {}    # The local source chain for each LhAppi
    LSlocal[i] = "DNA_{}".format(i)    # Example representation of DNA in LSlocal
    return LSlocal

# Create DNA in LSlocal
def create_DNA_in_LSlocal():
    # Set the metadata entity type as a validation rule
    metadata_entity_type = "validation_rule"

    # Set executable function for metadata of specific hAppi
    executable_function = "function_for_hAppi"

    # Set other expected parameter metadata to be unique hAppi
    for m in range(1, n+1):
        metadata["hAppi_{}".format(m)] = "metadata_value_{}".format(m)

# DNA Zome generation capability for hAppi
def generate_DNA_Zome_for_hAppi():
    # This function will generate a DNA Zome for hAppi. Actual implementation will depend on the hApp details.
    pass

# Initialize the second entity in the local source chain LSlocal
def initialize_generate_second_entity(LSlocal):
    LSlocal["second_entity"] = "Second_Entity_Value"
    return LSlocal

# Create Zome in LSlocal
def create_Zome_in_LSlocal():
    # Calculate the timestamp time of Zome creation
    timestamp = datetime.datetime.now()

    # Initialize private and public key set IDs
    private_key = RSA.generate(2048)
    public_key = private_key.publickey()
    P_mrk = private_key.export_key()
    P_mbk = public_key.export_key()

    # Calculate the hash value of Zome
    zome_content = "Example_Zome_Content"
    zome_hash = hashlib.sha256(zome_content.encode()).hexdigest()

    return zome_hash

# Create a new holochain metadata entity based on hash chain
def create_holochain_metadata():
    # This function creates a new holochain metadata entity. Actual implementation will depend on the details.
    pass

# Demands for a new transaction entity
def demands_for_new_transaction_entity():
    # Calculate the timestamp of the new metadata entity
    timestamp = datetime.datetime.now()

    # Specifies a new item type
    item_type = "new_item_type"

    # Calculate electronic signature using another function
    electronic_signature = creating_new_holochain_metadata_entity()

    # Generate current data hash
    current_data = "Example_Current_Data"
    current_data_hash = hashlib.sha256(current_data.encode()).hexdigest()

    # Calculate the hash of the previous header hashmetadata
    previous_header = "Example_Previous_Header"
    previous_header_hash = hashlib.sha256(previous_header.encode()).hexdigest()

    # Storing signed metadata entities in LSlocal before broadcasting
    LSlocal = {}
    LSlocal["signed_metadata"] = electronic_signature

    return LSlocal

# Creating a new holochain metadata entity
def creating_new_holochain_metadata_entity():
    # Cryptographically sign each hashchain metadata entity
    message = "metadata message"
    hash_obj = SHA256.new(message.encode())
    private_key = RSA.generate(2048)
    signature = pkcs1_15.new(private_key).sign(hash_obj)

    # For each new metadata entity in Holochain
    # Calculate the electronic signature of the transaction using the agent's private key
    electronic_signature = signature.hexdigest()

    # Store signed metadata entities in hashchain based LSlocal before broadcast
    LSlocal = {}
    LSlocal["signed_metadata_entity"] = electronic_signature

    return electronic_signature
```

4. COMPERATIVE ANALYSIS

Figure 4-(a) shows a performance comparison analysis of traditional IoT security mechanisms. Figure 4-(a) indicates that, when compared to other considered cryptosystems, LEX has the fastest speed in terms of CPU performance. While AES and DES [8] are slightly faster than SPECK, SPECK outperforms AES and DES in terms of memory usage. Considering the performance of various security mechanisms, it is suggested that SIMON and SPECK would provide better performance in resource-constrained IoT networks.



(a) **(b)**

Figure 4. Comparative Analysis of Existing Encryption Mechanisms in IoT Network.

Figure 4-(a) presents a performance comparison analysis of the proposed traditional IoT security mechanisms. Figure 4-(b) compares the performance of popular DLT technologies from the perspective of IoT security. On the other hand, Figure 4-(b) includes a comparison of the performance of popular DLT (Distributed Ledger Technology) technologies from the perspective of IoT security. The functionality of DLT differs from traditional encryption mechanisms, making memory requirements more critical than CPU cycles. A hybrid technology of Software-Defined Network (SDN) and blockchain offers superior performance compared to traditional blockchain. While the blockchain encompasses all user requests, SDN ensures secure connections and avoids unnecessary requests, thereby reducing memory usage and bits per CPU cycle. This technology brings groundbreaking advancements to the blockchain field, but memory requirements and processing techniques remain as challenges. However, Holochain and its newer version, Holochain RSM, can significantly reduce data processing and storage loads in dynamic and real-time implementations like IoT networks.

5. CONCLUSION

This paper introduced a novel architecture using Holochain, which proved more efficient and resource-saving than traditional blockchain methods. Holochain's unique agent-centric approach, combined with its Distributed Ledger Technology (DLT) nature, provides a secure environment for individual users to maintain their data integrity. The four-layered structure ensures a streamlined process from data collection to application processing. Comparative analysis with traditional security mechanisms highlighted LEX's superior CPU performance and SPECK's impressive memory management. The emergence of hybrid technologies merging SDN and blockchain offers promising solutions, setting a new standard in the field. In conclusion, the future of secure, distributed IoT healthcare seems bright with advancements like Holochain leading the way.

ACKNOWLEDGEMENT

This paper was supported by the SeMyung University Research Grant of 2023.’

REFERENCES

[1] D. El Majdoubi, H. El Bakkali, and S. Sadki, "SmartMedChain: A Blockchain-Based Privacy-Preserving Smart Healthcare Framework," Journal of Healthcare Engineering, vol. 2021. Hindawi Limited, pp. 1–19, 05 Nov 2021. DOI: https://doi.org/10.1155/2021/4145512

[2] A. Barua, M. A. Al Alamin, Md. S. Hossain, and E. Hossain, "Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey," IEEE Open Journal of the Communications Society, vol. 3. Institute of Electrical and Electronics Engineers (IEEE), pp. 251–281, 2022. DOI: https://doi.org/10.1109/OJCOMS.2022.3149732

[3] J. K. Parmar and K. G. Vaghani, "A Conceptual Study on Holochain and Blockchain Technology," Artificial Intelligence and Communication Technologies. Soft Computing Research Society, pp. 331–341, 2022. DOI: https://doi.org/10.52458/978-81-955020-5-9-33

[4] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," arXiv, 2019. DOI: https://doi.org/10.48550/arXiv.1906.11078

[5] S. Mthethwa and M. Pretorius, "Academic and Skills Credentialing Using Distributed Ledger Technology (DLT) and W3C Standards: Technology Assessment," International Conference on Intelligent and Innovative Computing Applications, vol. 2022. Society of Information Technologists and Engineers Ltd, pp. 170–182, 31 Dec 2022. DOI: https://doi.org/10.59200/ICONIC.2022.019

[6] S.-J. Moon, S.-B. Kang, and B.-J. Park, "A Study on a Distributed Data Fabric-based Platform in a Multi-Cloud Environment," International Journal of Advanced Culture Technology, vol. 9, no. 3, pp. 321–326, Sep 2021. DOI: https://doi.org/10.17703/IJACT.2021.9.3.321

[7] S. D. Putra, M. Yudhiprawira, S. Sutikno, Y. Kurniawan, and A. S. Ahmad, "Power analysis attack against encryption devices: a comprehensive analysis of AES, DES, and BC3," TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 17, no. 3. Universitas Ahmad Dahlan, p. 1282, 01 Jun 2019. DOI: http://doi.org/10.12928/telkomnika.v17i3.9384