Decentralized Identifiers (DIDs)-Based Authentication Scheme for Smart Health Care System

Alnazif Mohammed Alnour
dept. Computer Engineering
Ajou University, Suwon, South Korea
e-mail: alnour@ajou.ac.kr

Ki Hyung Kim (Member, IEEE)
Department of Cyber Security,
College of Information Technology
Ajou University, Suwon, South Korea.
e-mail: kkim86@ajou.ac.kr

***Abstract*—** The smart health care system collects users' health data, stores and shares it with other associated users in the platform. The ability to remotely access and manage smart medical equipment is handy, but it's also perilous, because vulnerable devices may be used to spy on people or execute other criminal actions. This emphasizes the need of developing a reliable and secure authentication system. Recently, there has been a lot of interest in employing blockchain in the smart environment (e.g., Distributed Internet of Things (IoT)) for both maintaining trust and privacy-preserving. Although several proposals have been handled with blockchain-based IoT issues, there are still numerous challenges such as authentication, revocation, delays, anonymity, and impersonation. Motivated by these facts, in this work, we construct an efficient Decentralized Identifiers (DIDs)-Based Authentication Scheme for Smart Health Care. The model integrates DIDs in the Smart Health care system to provide a secure and efficient authentication service. We also demonstrate that the suggested system meets the security and privacy criteria, such as anonymity, traceability, and confidentiality, through implementation and assessment.

Keywords—Blockchain (BC), Internet of Things (IoT), Decentralized Identifier (DID)

I. INTRODUCTION

A. IoT, Blockchain, and DIDs fundamentals

The Internet of things (IoT) consists of interconnected objects that, through unique address schemes, can interact, generate, process, and exchange a bunch of data. (3). Consequently, its systems have numerous prospective applications, such as smart home, smart healthcare, and intelligent manufacturing, to name a few areas (5). Today, more and more industries are beginning to adopt IoT technology to automate management processes, using data supplied by sensors and remote monitoring and control devices. IoT's vital functional elements include detection, computation, communication, and control or actuation. These features are made possible by combining embedded devices, wireless communication technologies, sensors, and actuators. Careful configuration and distribution of hardware, software, and network components are critical to achieving the desired application objectives.

Blockchain (BC) technology these days is becoming more familiar. In the BC network, the concept of centralization is eliminated, where it stores peer-to-peer digital ledger transactions into a form of structured data commonly known as a block (9). Recent research has revealed that blockchain has gone beyond the basic structure such as store blocks of transactions. Furthermore, the newly introduced form can contain smart contracts which could be executed on the blockchain. Thus, existing BC models can provide a distributed storage and computational framework for a program's execution (10). The integration of blockchain and the Internet of things has recently received more attention. Blockchain is considered the missing puzzle for IoT to fulfill privacy and security objectives. The current solutions adopted to integrate BC and IoT differ considerably from the structure of the crypto blockchain. Conceptually, the basic concepts are the same, but component integration and algorithms vary widely, such as consensus building, ordering, etc. (11).

The decentralized identifier (DIDs) is a new and open standard form of a globally unique identifier that allows for a decentralized and verified digital identity. DIDs allow the controller of a DID to prove control over it using cryptographic proofs such as digital signatures. DID has achieved four core properties, it is a persistent identifier (never needs to change), a resolvable identifier (we can look it up to discover metadata), a cryptographically verifiable identifier (we can prove control over it using cryptography), and a decentralized identifier (no centralized registration authority is required). (13) (14).

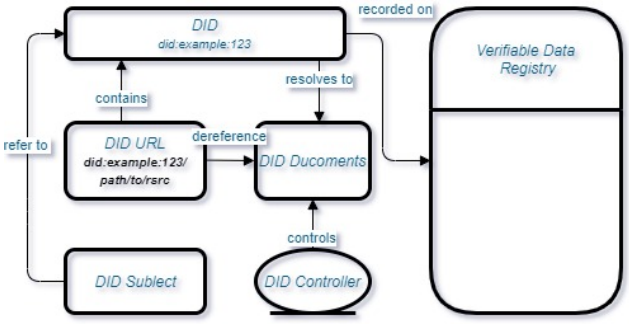

Figure. (1) DID Architecture

The main basic components of DID architecture and the relationship among them are shown in figure (1). e.g., DID are recorded on verifiable data registries, such as blockchains rather than centralized trusted third parties. A DID resolves to a DID document, which is consist of a bunch of information about the entity such as public keys that can be used for authentication, or service endpoints used to interact with the

entity. the DID subject is the entity identified by the DID, in many cases, the DID subject will also be its controller. The DID controller is the entity that has the capability to modify the DID document associated with the DID. (13) (14). A DID document is a set of instructions that describe how to use the DID, Figure (2) below shows an example of simple DID document.

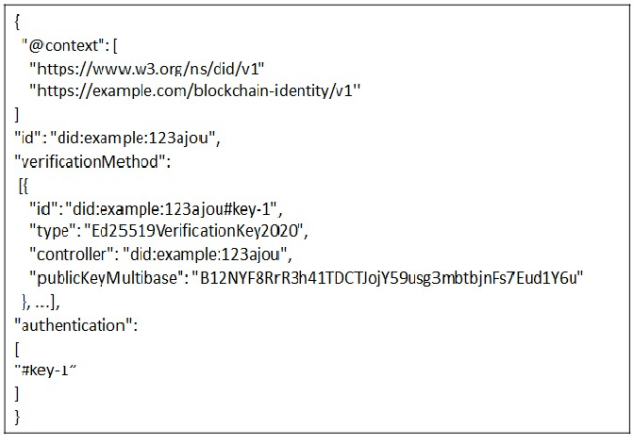

Figure. (2) Example of DID Document

B. *Motivation*

Most of the existing IoT security authentication methods are based on third-party system architecture, which has limitations regarding privacy and anonymity. As well as single-server systems suffer from common problems a single point of failure. (15) (16). For instance, the most common method for two-factor authentication is the s/key one-time password system, which appears to resist various attacks. (18). Another method is the smartcard-based remote user authentication techniques. Because of its efficiency, ease, and cheap computational cost has been widely employed in applications requiring remote user login, Web access, and other online services. However, once an attacker obtains the smart card from a legitimate user, he can pass himself off to access the remote system. (19). Therefore, a reliable system to mitigate these issues above has attracted more research attention. Meanwhile, blockchain appeared to provide a promise solution. Even though few works considered the blockchain-based IoT authentication issues, they still face some critical challenges (e.g., Assurance User's Anonymity, Lack of Completeness and Confidentiality).

C. *Research Contributions*

The main research contributions of this paper are summarized as follows:

1. We present a novel blockchain-based IoT authentication system, that eliminates the need for a trusted third party and offers an efficient, verifiable, and trustworthy authentication process for the end-user (u), IoT Smart Device (IDs), and a relying party (Rp). In addition, the proposed method enables the end-user to anonymously authenticate a collection of IoT devices while also giving him additional control over these devices throughout the authentication process (e.g., revoke the authentication at any time).

2. The scheme has been deployed on the Hyperledger Indy platform, and an in-depth assessment of the scheme demonstrates its ability to secure a Smart Health Care use case.).

3. The suggested authentication technique is being compared to other current schemes for further security research, demonstrating the proposed scheme's robustness. The method is very efficient and secure, according to the performance study.

The rest of the paper is structured as follows. Next, in Section II we present an overview of the related background. Next, the Decentralized Identifiers-Based Authentication System is proposed in Sections III, in section IV we discuss the performance evaluation, and we present the security and performance comparison in section V. finally, we conclude the paper in Section VI.

Table 1 summarizes the definitions and symbols used throughout the paper.

Symbol	Description
$DIDu$	Decentralized Identifier of User
PKu	Public Key of User
PKs	Private Key of User
VC	Verifiable Credential
Cm	Challenge Message of m
$auth$	Authentication Request
Ts	Timestamps
$E(m)$	Encryption Message of m
$ECCk$	Elliptic Curve Cryptography Key Pair
$H()$	One-way Hash function
IDs	Smart Device Identification Number
s	Web Server
$Enck(.)/Deck(.)$	Encryption Decryption Using Key K
$\|$	Concatenation Operation

Table I. Notations

II. RELATED WORK

Until now, several studies have looked into IoT authentication using blockchain technology. The authors discuss some of the existing studies in this section. Zhaofeng et al. [20] proposed a blockchain-based authentication scheme. They supposed all registered nodes in the blockchain system to participate in the authentication process and store the authentication logs. Such a system will avoid the single side fault. (e.g., if one node fails, other nodes will replace it). In [21], three levels of the Blockchain paradigm were presented. It uses a one-way hash chain approach to give IoT devices a key generation and management mechanism that enables self-verification at any moment. The model provides a transparent key management scheme. And also cover Mutual Authentication, Message Integrity, and Resistance to different types of attacks. Xiaoding et al. [22] created a transfer learning and blockchain-based authentication technique. The authors used blockchains to keep their data private. Also, they implemented a deep learning algorithm to train and improve the model to enhance authentication accuracy. Guo et al. [23] presented a distributed authentication system combining edge computing and blockchain. A physical network, blockchain

edge, and blockchain network layers were employed in a hierarchical authentication design. Their objectives are to achieve authentication and data exchange across various IoT systems. The system can prevent Denial of Service using a False Signature. It can also do mutual authentication and protect against forgery.

In summary, most existing research is still in the early stages. Even though some accomplished a range of features, including anonymity, decentralization, and system transparency, however proper execution, analysis, and achieving effective authentication across various IoT systems have received less attention. As a result, this article suggests an efficient Decentralized Identifiers (DIDs)-Based Authentication Scheme for Smart Health Care.

III. OUR SCHEME

A. System Architecture

In this article, a Decentralized Identifiers -Based Authentication Scheme is proposed to handle trust, privacy-preserving, and efficiency problems. As shown in Fig. 3, the architecture consists of four major entities defined as follows.

1. Medical IoT Devices Layer: this layer contains wearable devices and other smart medical sensors that collect daily health information to monitor some vital body parameters (e.g., blood pressure, body temperature, and daily physical activity or weight).

2. Smart Hospital Service Layer: in this layer, we are assuming the hospital is acting as Relying Party for the system. The medical devices send a request to upload data in the hospital web server, which allows medical professionals to track real-time health status and rapid response to actions when needed.

3. DIDs Services Layer: maintain the DID architecture (e.g., verifiable data registries, DID RUL, DID controller, DID document, and DID authentication service). In this scheme, we assume the user and relying party are interacting with the same Decentralized Identifiers Platform Architectures. thus, no discrepancy in terms of authentication service and DID method, etc.

4. User Interface Layer: The main role of the UI layer is a point of user interaction with the system, also it shows the application data on the mobile screen. Whenever the data changes, either due to user interaction or smart devices input, the UI layer is updated to reflect those changes.

B. System Authentication Phase

In this phase to register any IoT smart device, the user generates DIDs, Verifiable Credentials (VC), and Identification Number (IDs) for each device and securely store this metadata in the targeted device. the user can interact with IoT devices through Smart-health App installed in his smartphone, also this credential can be stored in his wallet.

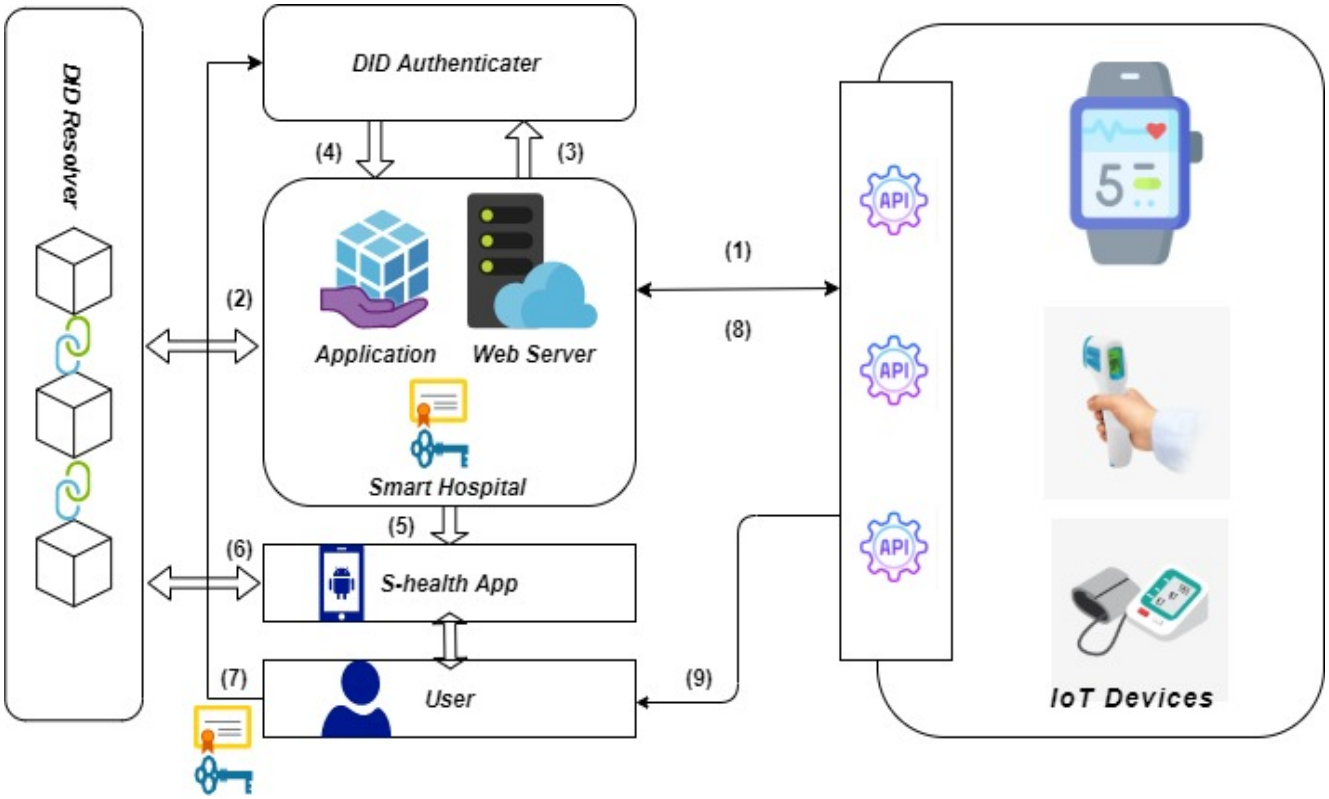

Figure. (3) System Architecture.

Authentication Process Algorithm

Generate $[DIDs, VC, IDs]$
/verify metadata/
if $[DIDs, VC, auth, IDs]$ = erro **then**
  return Compute cm = [DIDs‖ VC‖ auth‖ IDs‖ Ts]
else
  devices is already registered
end if
/verifymetadata/
if [cm ‖ Ts] = true **then**
  compute cms = [DIDs ‖ cm ‖ Is]
end if
print verify the validity of cms
if cms = cm **then**
  return $[DIDs, VC, auth, IDs] = true$
  print node authenticated
end if

C. *Proposed system Workflow*

In Fig. 4, we present the workflow of the proposed architecture. First, when a targeted IoT device requests to communicate with Relying Party (RP) (e.g., hospital webserver), it generates an encrypted message by computing the following equation: E(m) = [DIDs‖ VC‖ auth‖ IDs‖ Ts] and send authentication request to RP containing this metadata. When RP receives a message, it resolves and verifies the message's information. If the machine has never been authenticated, the challenge message will be computed by the RP using DID authenticates service and forwarded to the user. When the user receives a message, he will resolve and validate the continent, then react to the challenge statement using a DID authenticator. When RP gets a response from the user, it sends a message to the device, indicating that authentication has been authorized. As a result, the user's instrument will alert him that it has been authenticated. fig.5. shows the message sequences in the proposed model.

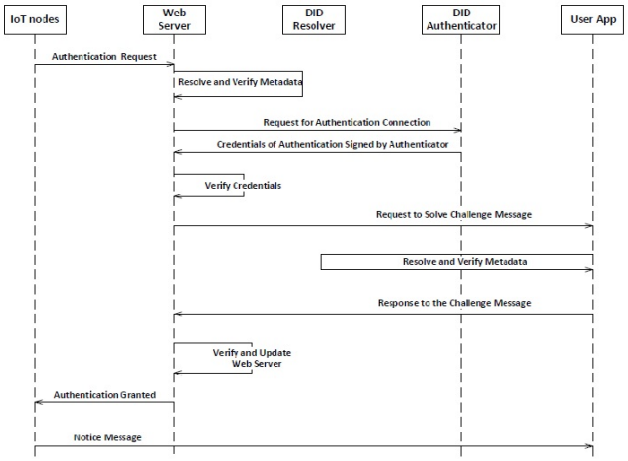

Figure. (4) System Workflow

IV. PERFORMANCE EVALUATION

A. *Simulation Setup*

We conduct the simulation with the computer of i5 2.5GHZ CPU, 8-G memory, and 64-b win10 system. We simulated the proposed DIDs-Based Authentication system on the Hyperledger Indy using VMware Virtual box of one processor, 4-G memory, and 20 GB of Ubuntu system. The Hyperledger Indy contained the functionality of DID creation, registration, and secure message communications. Fig.6. shows the list of DIDs created for three devices in the platform. After the Decentralized Identifiers Networks system was created, transactions, initiated by users will be written into the Verifiable Distributed Ledgers.

B. *Security Verification Using SPAN+AVISPA Tool*

The security validation of the authentication system is evaluated with SPAN+AVISPA tool [25]. It is a simulation tool that determines whether a security protocol is safe, unsafe or inconclusive using "high level protocol specification language (HLPSL). The simulation results clearly demonstrate that DIDs-Based Authentication scheme is secure against various attacks. The parameters of this simulation are given in fig.8.

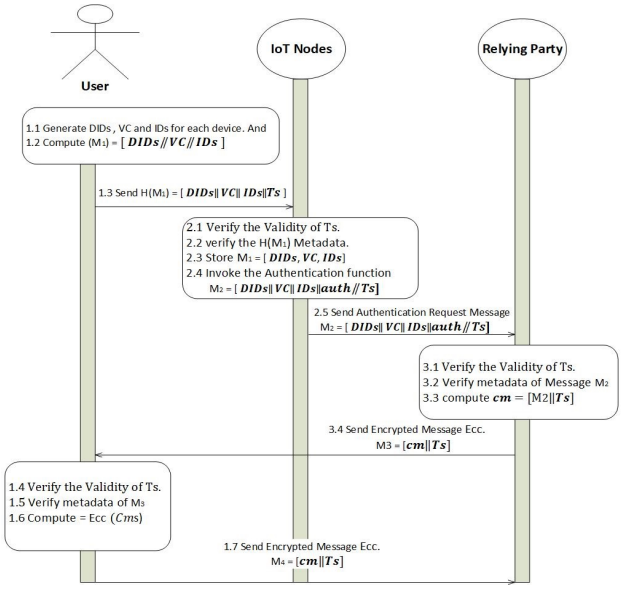

Figure. (5) Message Sequence

V. SECURITY AND PERFORMANCE COMPARISON

A solid blockchain-based IoT authentication solution should fulfill several fundamental security criteria, as mentioned in section 2. As a result, in this part, we will examine the security of the suggested design and illustrate how it can resist several known attacks.

Based on the vital security features defined above, we first demonstrate user anonymity in our design. All communications sent between a user (u), an IoT Smart Device (IDs), and a relying party (Rp) during the authentication process are not

dependent on the genuine identities of the (u), IDs, and Rp. It does, however, only work with demonstrating capabilities that DID holders could prove. Furthermore, due to unique and random components, each message is individual. As a result, an attacker cannot identify or track the entities participating in communication over time.

Second, the design assures privacy-preserving because the data of an entity is not visible in the system, and the method doesn't utilize any verification list. Therefore, when a device is verified, it might connect to Rp regularly whenever it validates its identity. Furthermore, each entity has its unique DID that cannot be reverse engineered to get a real identity without the encryption keys.

Third, the model offers Mutual authentication and Authentication revocations. For instance, the Rp can authenticate U by verifying Cm. The calculation of Cm needs the correct measure of Enck(.) [DIDs‖ VC‖ IDs], which involves the private key of U. Moreover, U can also authenticate Rp by verifying Enck(.)[cm‖Pks‖Ts]. Thus, the mutual authentication between Rp and U is offered by our scheme. In addition, using DID allows the user to have more control over the authentication process. For example, when U generate (DIDs ‖ VC ‖ IDs), he can set specific conditions or time limiting, thus when the situation is met, the entity can revoke the authentication process. table No. 2 shows the security criteria of our scheme compare to other related work.

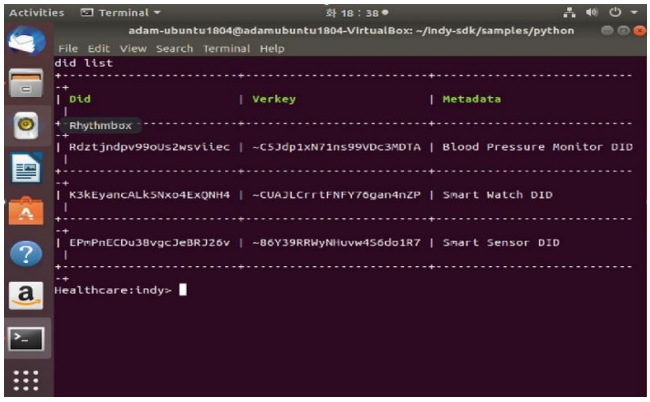

Figure. (6) DID List

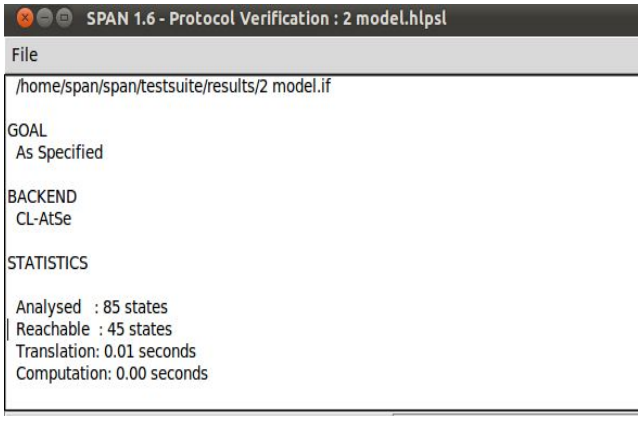

Figure. (7) Simulation Result

A. COMPARISON TO PRIOR WORK

The performance of the proposed system is examined in this part to ensure that it is effective. Nevertheless, it is hard to compare the efficacy of this scheme to other schemes since research on blockchain-based identity authentication systems for IoT is still in its early stages, and there are few related models. We will compare our scheme to four exiting authentication schemes [20], [21],[22], [23]. We will consider the signing, verification, computation cost, and communication time. The results are listed in Table 3.

	[20]	[21]	[22]	Our scheme
UserImpersonation	×	✓	✓	✓
TamperingResistance	×	✓	×	✓
MessageReplay	✓	×	✓	✓
ManIntheMiddle	✓	✓	✓	✓
MasqueradeResistance	✓	✓	✓	✓
Scalability	×	×	✓	✓
MutualAuthentication	✓	✓	×	✓
Decentralization	✓	✓	✓	✓

Table II. Security Comparison

Signing and verification cost: We implemented our scheme in the Hyperledger Indy environment. The consensus in Hyperledger Indy is based on Redundant Byzantine Fault Tolerance (RBFT), which is a protocol inspired by Plenum Byzantine Fault Tolerance (Plenum). The consensus is achieved through the use of voting-based procedures. This algorithm has the benefit of providing low-latency finality. Thus, the agreement is reached when most nodes validate a transaction or block.

Computing cost: The scheme's execution shows that ordinary nodes with limited computing power don't need to perform computational operations like encryption and signature; instead, these operations are delegated to the user's node U. This node has a lot of processing and computational capacity to handle complicated tasks and operates as a blockchain mining node.

Communication costs: We evaluate the proposed scheme based on the communication time it takes to send an authentication message from start to finish in the Decentralized Identifiers Network system. In most cases, the time required depends on the network speed of the test environment. In other words, for longer periods of time, the network will be slower. In this study, fore systems' device identifiers are examined for response time. Various outcomes from identity authentication, either successful or unsuccessful, are taken into account while measuring the effectiveness of the method.

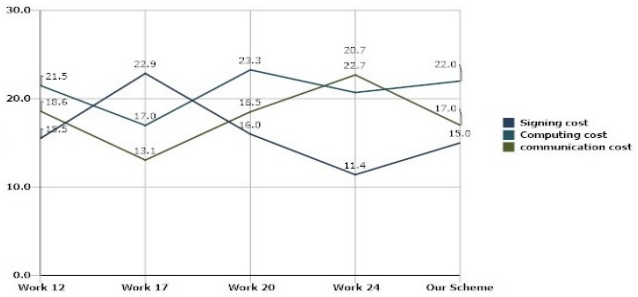

Figure. (8) Cost Comparison

CONCLUSION

IoT and blockchain are two trending topics at the moment, and in this paper, we showed how blockchain may be used in conjunction with other techniques to ensure secure authentication between smart devices and reliant parties in a smart health care system. The suggested system, in particular, uses Decentralized Identifiers (DIDs) technology to authenticate a requestor without exposing the end user's information. Furthermore, the suggested scheme incorporates anonymity and traceability as security elements. It's also been proved to be resistant to a variety of possible attacks through informal security research. When compared to other current competing authentication techniques, a detailed comparison reveals that the model provides greater security with comparable computing costs and low communication costs. Towards achieving the privacy of access policy, we will consider access control approaches in the future. Furthermore, we plan to implement and evaluate a prototype of the extended system in order to achieve higher utility in real-world applications.

ACKNOWLEDGMENT

This research was partially supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP2021-2021-0-01835) and the research grant (No.2021-0-00590 Decentralized High-Performance Consensus for Large-Scale Blockchain) supervised by the IITP (Institute of Information and Communications Technology Planning and Evaluation). This research was also partially supported by KIAT (Korea Institute for Advancement of Technology) grant funded by the Korea Government (MOTIE) (P0008703, The Competency Development Program for Industry Specialist) and the Basic Science Research Program through the NRF (National Research Foundation of Korea) funded by the Ministry of Education (2021R1F1A1045861).

REFERENCES

[1] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram. 2017. "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home.". doi:10.1109/PERCOMW.2017.7917634.

[2] Biswas, Sujit, Kashif Sharif, Fan Li, Sabita Maharjan, Saraju P. Mohanty, and Yu Wang. 2019. "PoBT: A Lightweight Consensus Algorithm for Scalable IoT Business Blockchain." IEEE Internet of Things Journal 7 (3): 2343-2355.

[3] Cui, Zhihua, XUE Fei, Shiqiang Zhang, Xingjuan Cai, Yang Cao, Wensheng Zhang, and Jinjun Chen. 2020. "A Hybrid Blockchain-Based Identity Authentication Scheme for Multi-WSN." IEEE Transactions on Services Computing 13 (2): 241-251.

[4] Guo, Shaoyong, Xing Hu, Song Guo, Xuesong Qiu, and Feng Qi. 2019. "Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System." IEEE Transactions on Industrial Informatics 16 (3): 1972-1983.

[5] Haller, Neil. 1995. "RFC1760: The S/KEY One-Time Password System." .

[6] Lin, Chao, Debiao He, Neeraj Kumar, Xinyi Huang, Pandi Vijayakumar, and Kim-Kwang Raymond Choo. 2019. "Homechain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes." IEEE Internet of Things Journal 7 (2): 818-829.

[7] Liu, Jia-Yong, An-Min Zhou, and Min-Xu Gao. 2008. "A New Mutual Authentication Scheme Based on Nonce and Smart Cards." Computer Communications 31 (10): 2205-2209.

[8] Mohanty, Sachi Nandan, K. C. Ramya, S. Sheeba Rani, Deepak Gupta, K. Shankar, S. K. Lakshmanaprabu, and Ashish Khanna. 2020. "An Efficient Lightweight Integrated Blockchain (ELIB) Model for IoT Security and Privacy." Future Generation Computer Systems 102: 1027-1037.

[9] O. Novo. 2018. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. Vol. 5. doi:10.1109/JIOT.2018.2812239.

[10] Pal, Shantanu, Tahiry Rabehaja, Ambrose Hill, Michael Hitchens, and Vijay Varadharajan. 2019. "On the Integration of Blockchain to the Internet of Things for Enabling Access Right Delegation." IEEE Internet of Things Journal 7 (4): 2630-2639.

[11] Pal, Shantanu, Tahiry Rabehaja, Michael Hitchens, Vijay Varadharajan, and Ambrose Hill. 2019. "On the Design of a Flexible Delegation Model for the Internet of Things using Blockchain." IEEE Transactions on Industrial Informatics 16 (5): 3521-3530.

[12] Panda, Soumyashree S., Debasish Jena, Bhabendu Kumar Mohanta, Somula Ramasubbareddy, Mahmoud Daneshmand, and Amir H. Gandomi. 2021. "Authentication and Key Management in Distributed IoT using Blockchain Technology." IEEE Internet of Things Journal.

[13] Preukschat, Alex and Drummond Reed. 2021. Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials Simon and Schuster.

[14] Qu, Chao, Ming Tao, and Ruifen Yuan. 2018. "A Hypergraph-Based Blockchain Model and Application in Internet of Things-Enabled Smart Homes." Sensors 18 (9): 2784.

[15] Qu, Chao, Ming Tao, Jie Zhang, Xiaoyu Hong, and Ruifen Yuan. 2018. "Blockchain Based Credibility Verification Method for IoT Entities." Security and Communication Networks 2018.

[16] R. A. Memon, J. P. Li, M. I. Nazeer, A. N. Khan, and J. Ahmed. 2019. DualFog-IoT: Additional Fog Layer for Solving Blockchain Integration Problem in Internet of Things. Vol. 7. doi:10.1109/ACCESS.2019.2952472.

[17] Reed, Drummond, Manu Sporny, Dave Longley, Christopher Allen, Ryan Grant, Markus Sabadello, and Jonathan Holt. 2020. "Decentralized Identifiers (DIDs) V1. 0: Core Architecture, Data Model, and Representations." W3C Working Draft 8.

[18] Umar, Mubarak, Zhenqiang Wu, and Xuening Liao. 2020. "Mutual Authentication in Body Area Networks using Signal Propagation Characteristics." IEEE Access 8: 66411-66422.

[19] Vangala, Anusha, Anil Kumar Sutrala, Ashok Kumar Das, and Minho Jo. 2021. "Smart Contract-Based Blockchain-Envisioned Authentication Scheme for Smart Farming." IEEE Internet of Things Journal.

[20] Wu, Fan, Xiong Li, Arun Kumar Sangaiah, Lili Xu, Saru Kumari, Liuxi Wu, and Jian Shen. 2018. "A Lightweight and Robust Two-Factor Authentication Scheme for Personalized Healthcare Systems using Wireless Medical Sensor Networks." Future Generation Computer Systems 82: 727-737.

[21] \Xiaoding, Wang, Sahil Garg, Hui Lin, Md Jalilpiran, Jia Hu, and M. Shamim Hossain. 2021. "Enabling Secure Authentication in Industrial Iot with Transfer Learning Empowered Blockchain." IEEE Transactions on Industrial Informatics.

[22] Zhaofeng, Ma, Meng Jialin, Wang Jihui, and Shan Zhiguang. 2020. "Blockchain-Based Decentralized Authentication Modeling Scheme in Edge and IoT Environment." IEEE Internet of Things Journal 8 (4): 2116-2123.

[23] Guo, Shaoyong, Xing Hu, Song Guo, Xuesong Qiu, and Feng Qi. 2019. "Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System." IEEE Transactions on Industrial Informatics 16 (3): 1972-1983.

[24] Vangala, Anusha, Anil Kumar Sutrala, Ashok Kumar Das, and Minho Jo. 2021. "Smart Contract-Based Blockchain-Envisioned Authentication Scheme for Smart Farming." IEEE Internet of Things Journal.

[25] Automated Validation of Internet Security Protocols and Applications, AVISPA, 2020. Accessed: Oct. 2020. [Online]. Available: http://www.avispa-project.org/.