Blockchain-Assisted Secure Fine-Grained Searchable Encryption for a Cloud-Based Healthcare Cyber-Physical System

Mamta, Brij B. Gupta, *Senior Member, IEEE*, Kuan-Ching Li, *Senior Member, IEEE*, Victor C. M. Leung, *Fellow, IEEE*, Kostas E. Psannis, and Shingo Yamaguchi, *Senior Member, IEEE*

***Abstract*—The concept of sharing of personal health data over cloud storage in a healthcare-cyber physical system has become popular in recent times as it improves access quality. The privacy of health data can only be preserved by keeping it in an encrypted form, but it affects usability and flexibility in terms of effective search. Attribute-based searchable encryption (ABSE) has proven its worth by providing fine-grained searching capabilities in the shared cloud storage. However, it is not practical to apply this scheme to the devices with limited resources and storage capacity because a typical ABSE involves serious computations. In a healthcare cloud-based cyber-physical system (CCPS), the data is often collected by resource-constraint devices; therefore, here also, we cannot directly apply ABSE schemes. In the proposed work, the inherent computational cost of the ABSE scheme is managed by executing the computationally intensive tasks of a typical ABSE scheme on the blockchain network. Thus, it makes the proposed scheme suitable for online storage and retrieval of personal health data in a typical CCPS. With the assistance of blockchain technology, the proposed scheme offers two main benefits. First, it is free from a trusted authority, which makes it genuinely decentralized and free from a single point of failure. Second, it is computationally efficient because the computational load is now distributed among the consensus nodes in the blockchain network. Specifically, the task of initializing the system, which is considered the most computationally intensive, and the task of partial search token generation, which is considered as the most frequent operation, is now the responsibility of the consensus nodes. This eliminates the need of the trusted authority and reduces the burden of data users, respectively. Further, in comparison to existing decentralized fine-grained searchable encryption schemes, the proposed scheme has achieved a significant reduction in storage and computational cost for the secret key associated with users. It has been verified both theoretically and practically in the performance analysis section.**

***Index Terms*—Cloud-based cyber-physical systems (CCPS), data encryption, healthcare information search and retrieval, keyword search, public-key cryptosystems, searchable encryption.**

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication.

Recommended by Associate Editor Laurence T. Yang. *(Corresponding author: Brij B. Gupta.)*

Citation: Mamta, B. B. Gupta, K.-C. Li, V. C. M. Leung, K. E. Psannis, and S. Yamaguchi, "Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system," *IEEE/CAA J. Autom. Sinica*, 2021, DOI: 10.1109/JAS.2021.1004003

Mamta is with the Department of Computer Engineering, National Institute Technology, Haryana 136119, India (e-mail: er.mamta.dabra@gmail.com).

B. B. Gupta is with the Department of Computer Engineering, National Institute Technology, Haryana 136119, India, and also with the Asia University, Taiwan, China (e-mail: gupta.brij@gmail.com).

K.-C. Li is with the Department of Computer Science and Information Engineering, Providence University, Taichung 43301, China (e-mail: kuancli@pu.edu.tw).

V. C. M. Leung is with the Computer Science and Software Engineering, Shenzhen University, Shenzhen 518000, China, and also with the University of British Columbia, Vancouver, Canada (e-mail: vleung@ece.ubc.ca).

K. E. Psannis is with the Department of Applied Informatics, University of Macedonia, Thessaloniki 54636, Greece (e-mail: kpsannis@uom.gr).

S. Yamaguchi is with the Department of Information Science and Engineering, Graduate School of Sciences and Technology for Innovation Yamaguchi University, Yamaguchi 753-8511, Japan (e-mail: shingo@yamaguchi-u.ac.jp).

I. Introduction

CYBER-PHYSICAL systems (CPS) tightly intertwine software and physical components that can have applications in nearly any field we can think of, including healthcare, energy conservation, environment protection, defense, agriculture and many more. CPS tirelessly produce huge silos of data, and to ensure scalability and efficient storage, large companies like Microsoft and Honeywell, etc., are moving towards cloud-based solutions. Cloud-based CPS (CCPS) improves existing CPS functionalities, but at the same time, presents security challenges.

The data related to healthcare and defense may contain sensitive information. Therefore, in CCPS, in addition to applying security policies at the physical level, there is a need to ensure security at the cyber level, i.e., the cloud component. The cloud-based CPS for healthcare offers many benefits like monitoring and controlling patient's health by deploying sensors and actuators in the form of wearable devices. These devices keep track of the essential vitals and may even alert associated medical practitioners in case of critical situations. The data involved in the entire process of monitoring and alerting is highly sensitive, whether it is the location of the patient or the vitals stored by these devices. Therefore, a need for a security mechanism is as essential as providing healthcare services to the patients. Further, the data involved in the continuous monitoring may be massive, and the devices which gather this data are resource constrained. Hence the data is generally stored at a third party cloud server. For this purpose, an obvious solution is to encrypt sensitive data first and then store it to an untrustworthy cloud platform. Encryption indeed ensures security but severely debilitates the accessibility of data. It makes even the most basic operation of searching, a highly challenging task. The searchable

encryption (SE) technique is the answer to this problem.

SE enables the cloud server to search confidential data without revealing any information about the data being searched. Further, in the cloud environment, users from multiple domains interact; therefore, access control must be embedded to enable fine-grained searching functionalities. All the stated features in the encryption scheme including search capability and access control fulfills our requirement for cloud-based CPS for healthcare. However, these features come with an inherent cost, and cannot be directly applied for the resource-constraint devices. There is a need of a mechanism to reduce this cost, and this is the key goal of this paper. To enable fine-grained searching capabilities, we have used attribute-based encryption (ABE) and specifically its ciphertext-policy (CP) variant as it makes it possible for the data owners to implement access rule over the encrypted data. Also, the data owner has full control over his shared data which is the essential requirement in any healthcare system. To reduce the associated cost with the ciphertext-policy ABSE scheme, we have leveraged the blockchain technology, where most of the computational load of the ABSE scheme is delegated to the blockchain network.

A. Research Methodology

This section describes the approach followed for the reduction in computational complexity, starting with the problem formulation of the proposed scheme.

1) Problem Formulation

The ABSE scheme provides fine-grained search capabilities to its users but it comes with an inherent computational overhead. In a typical ABSE scheme the associated storage and the computational cost varies linearly with the number of attributes possessed by a user. In a healthcare CCPS, the devices participating in the network are resource constraint. Thus it is not feasible to directly apply the ABSE schemes to access the encrypted information.

Given the above problem, we aim to construct a keyword search scheme with fine-grained search capabilities that can handle a large number of diverse attributes. Furthermore, it should be lightweight enough to be able to be deployed at devices with resource constraints.

2) Proposed Hypotheses

The proposed hypotheses state that the computational complexity of the existing state-of-the art fine-grained searchable encryption schemes is high and also varies with the number of attributes involved in the system. To use such security solutions for devices with limited resources, there is a need to develop a delegation mechanism which can reduce the computational burden from the entities involved in the system. The proposed scheme aims to reduce the associated cost of a fine-grained searchable encryption scheme with the assistance of blockchain technology.

3) Proposed Solution

To address the above-stated problem, in our view, there can be two possible solutions. First, is to make the associated cost independent of the number of attributes. It has already been the focus of many works, like [1]–[4]. Second, resource-constraint devices should not execute computationally intensive tasks involved in a typical ABSE scheme by themselves and leverage other technology like blockchain technology, which can improve both flexibility and reduce system overhead.

With blockchain technology, the proposed scheme can attain the following characteristic features:

Decentralization: It is the key property of blockchain technology, which means that there is no central control, i.e., there exists no single authority responsible for governing the system. The searchable encryption system developed using the blockchain technology inherits this fundamental property and hence results in a fully decentralized system.

Reduction in computation overhead: In the blockchain-assisted searchable encryption system, the task of system initialization is not the responsibility of a single entity. However, it is handled together by blockchain consensus nodes. Furthermore, the task of search token generation is assisted by consensus nodes to reduce the burden from end-users.

Improves system reliability and free from a single point of failure: In the blockchain-assisted searchable encryption system, there is no need for a central authority, and no master secret key is needed to generate user credentials. Hence, this makes the system more reliable in case one or more nodes fails or becomes malicious.

The remaining of this article is organized as follows: Section II discusses related works. In Section III, the reader is enlightened with the essential background required to understand the construction of the proposed scheme. Further, it presents an introduction to the blockchain and other retrospective techniques which forms the basis of the paper. Section IV gives the system and security definitions and explains the system and security model of the proposed scheme. Section V provides detailed construction of the proposed scheme along with its correctness and security analysis. Section VI finally concludes the paper with possible directions for future work.

II. Related Work

ABSE enables fine-grained searching capabilities in a multi-user environment. Several attribute-based searchable schemes have been developed using either of the two design frameworks (ciphertext-policy or key-policy) [1]–[3]. Moreover, in the area of healthcare, there exist some attribute-based keyword search schemes [5]–[8]. However, most of them need a central authority for management and distribution of secret keys to the cloud users. Consider a scenario where a data owner wants to share his data with a large number of users who possess attributes from different domains. Then the single authority cannot efficiently manage such a large and diverse set of attributes alone. Such a scenario is prevalent in the healthcare system, e.g., in healthcare networks, a data owner, i.e., a patient may want to share his data with users like a researcher, or a doctor or some insurance agent. All of these users belong to an entirely different domain; hence, there is a need for a multi-authority system where each authority is responsible for the management of a disjoint set of attributes from different domains.

One such multi-authority searchable encryption scheme was recently proposed by Miao *et al.* [9]. They achieved decentralization by eliminating the central authority. However, the schemes mentioned above, including the one in [9] comes with tremendous computational complexity inherited from the underlying ABE scheme. To reduce this computational overhead and to achieve decentralization at the same time, the authors leveraged the blockchain technology. They delegated most of the computationally intensive tasks either to the blockchain network or to the cloud server. In the proposed scheme, the system initialization and partial search token generation tasks are handled by the blockchain network, while the cloud server handles the search task. Thus, the users can stay relaxed and get their task completed by the smart blockchain technology. There exist several scenarios in literature where blockchain technology has been used [10]–[13]. In [16], the searchable encryption scheme has been developed by leveraging blockchain technology, but it focuses on the searchable encryption in the symmetric setting. In [12], a searchable encryption scheme has been proposed with the assistance of blockchain technology in the public-key setting, but they did not consider the fine-grained searching capabilities into account.

III. Background

This section gives the necessary information about the bilinear map, hardness assumptions on which the proposed scheme relies, and the structure of the access policy used in the proposed scheme.

A. Bilinear Map and Hardness Assumption

Let G be a source cyclic group of prime order, p, and G_T be a target cyclic group of same order p and g be the generator of the source group, G. Let e be a map between G and G_T, $e: G\times G \rightarrow G_T$, it is called a bilinear map if it satisfies the following conditions:

1) $\forall X = g^u \in G_1$ and $Y = g^v \in G_2 : e(g^u, g^v) = e(g,g)^{uv}$ where $u, v \in Z_p$. This is called the bilinearity property.

2) $e(g,g)$ is the generator of the target group, G_T, if g is the generator of G. This property is called non-degeneracy.

3) $\forall X, Y \in G$; $e(X,Y)$ is efficiently computable.

Assumption (q-decisional parallel bilinear diffie-hellman exponent (DPBDHE)): Let $e: G\times G \rightarrow G_T$ be a bilinear map defined above. Consider another cyclic group Z_p of integers of order again p. Choose $s, a, b_1, b_2, \ldots, b_q \in Z_p$, $U \in G_T$ and compute the tuple D, which consists of the following elements: $g, g^s, \left(g^{a^i}\right)_{i\in[2q],i\neq q+1}, \left(g^{b_j a^i}\right)_{(i,j)\in[2q,q],i\neq q+1}$,

$$\left(g^{\frac{s}{b_j}}\right)_{j\in[q]}, \left\{g^{\frac{sa^i b_j}{b_k}}\right\}_{(i,jk)\in[q+1,q,q],j\neq k}.$$

The distinguishing probability of the distributions $\left(D, V = e(g,g)^{sa^{q+1}}\right)$ and (D,U) is negligible [14].

B. Access Structure

To construct the proposed searchable encryption scheme, we have used the monotonic access structure, which is defined as: Let the attribute universe be represented by $\mathcal{U}$. A monotonic access structure, $\mathbb{A}$, on $\mathcal{U}$ consists of non-empty subsets of $\mathcal{U}$ such that if a subset belongs to $\mathbb{A}$ then its superset must also be there in $\mathbb{A}$, i.e., $\forall B, C \in \mathbb{A}$, if $B \in \mathbb{A}$ and $B \subseteq C$, then $C \in \mathbb{A}$ [15]. To distribute the secret over the access structure we use a linear secret sharing scheme (LSSS), π, over Z_p, which is defined as follows [15]:

1) The shares of a secret $s \in Z_p$ forms a vector over Z_p.

2) For each access structure defined on the attribute universe, there exists a share generating matrix, $\mathbb{A}$, of order $l\times n$ whose elements are taken from Z_p. Let $\rho: [l] \rightarrow \mathcal{U}$ be a function that maps each row of the matrix to the attributes from set $\mathcal{U}$, i.e., $\rho(i)|_{i=1}^{l} \in \mathcal{U}$. To generate the secret shares of s, consider a vector $\overrightarrow{v} = (s, v_2, \ldots, v_m)$ where $v_2, \ldots, v_m \in Z_p$ and compute $\overrightarrow{\lambda} = \mathbb{A}\overrightarrow{v}^T$ where $\lambda_i = \mathbb{A}_i \overrightarrow{v}^T|_{i=1}^{l}$ represents a secret share of s.

LSSS should satisfy the linear reconstruction property which states that if $\exists S \in \mathbb{A}$ such that I represents the set of rows (l) such that $\rho(l) \in S$ then $\exists [c_i]_{i\in I} \in Z_p : \sum_{i\in I} c_i \lambda_i = s$, given λ_i represents the valid shares of secret, s.

C. Shamir's Secret Sharing Scheme

It is used to divide a secret into n shares such that the secret can only be constructed if a minimum of k shares is available among them. Therefore, k represents the threshold because after collecting k shares, the secret can be revealed. It is based on polynomial interpolation, given k points, (x_i, y_i), such that no two different points have the same x-axis component, and in a two-dimensional space, there exists a single unique polynomial, q, of degree $k-1$ such that $q(x_i) = y_i \forall i$. Thus, the idea is to construct a polynomial of degree $k-1$, where the data to be shared is placed at the position of a constant term and rest of the coefficients are selected randomly, i.e., $q(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{k-1}x^{k-1} : c_0 = s, c_i|_{i=1}^{k-1} \xleftarrow{\$} Z_p$, where Z_p is the group of integers over which the polynomial is constructed. Now, generate the n points from this polynomial by putting different values of $x_i|_{i=1}^{n}$, i.e., generate (x_i, y_i). The secret can be reconstructed by using any of the k points among the available n points using the Lagrange interpolation method. To find the coefficients of $q(x)$, first, find the Lagrange identities by using these k points as follows:

$$l_j = \prod_{\substack{m=1 \\ m\neq j}}^{k} \frac{(x - x_m)}{(x_j - x_m)}. \tag{1}$$

Now, find the polynomial, $q(x) = \sum_{j=1}^{k} y_j l_j$. Among the coefficients computed using this formula, the coefficient of the term, x^0 (constant term), is the secret that we have shared.

D. Consortium Blockchain Platform and its Role in the Proposed Scheme

The consortium blockchain (CB) platform extends the concept of private blockchain where the entire network is managed by a group of organizations instead of a single organization like in a private blockchain platform [16]–[18]. A CB platform represents the fine line between public and private blockchain platforms. It adds flexibility in rules to be more like public blockchain. The visibility of the blockchain

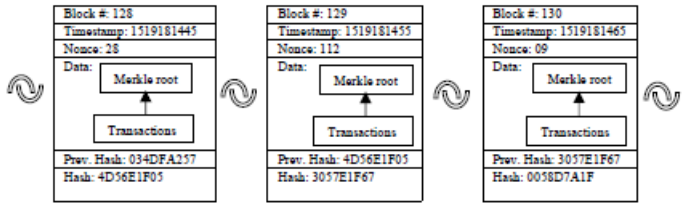

Fig. 1. General structure of a blockchain.

may be limited only to validators, authorized users or is visible to everyone, thereby combining the features of both the public and private blockchain platforms. The most noticeable difference between both public and private blockchain platforms is observed during the consensus. Unlike the open system in public blockchain or a completely closed system in a private blockchain, in consortium blockchain, a group of equally powered nodes participate in consensus. The typical structure of the blocks and how these blocks are connected in any blockchain platform is shown below in Fig. 1.

Blockchain, as the name suggests itself that it is a chain of blocks, and this chain is formed and secured with the application of cryptography. Blockchain can also be defined as a sequence of records which is analogous to traditional ledgers with an additional property of immutability. Hence, it is often called an immutable ledger. Now, depending upon the requirement and application area, the responsibility of managing and updating this ledger is given either to everyone in the blockchain network (public blockchain platform, e.g., the Bitcoin network [19]), or to one particular organization (private blockchain platform, e.g., Hyperledger), or to a selected set of users from different organizations with equal power (consortium blockchain platform, e.g., Quorum).

In cloud-based healthcare CPS, the public blockchain platform does not seem suitable because the public blockchain allows access to everyone on the system and the data involved in the healthcare CPS may contain sensitive information which is not for the public use. The private blockchain platform also does not fit in the considered scenario because it is too restrictive, and there is still control by one single authority who can manipulate the data for their benefit. Therefore, the option that is suited well for the present scenario is the consortium blockchain where different entities associated with the healthcare CPS makes a consortium and pre-decides the nodes that will participate in the consensus. By leveraging the benefits of consortium blockchain in healthcare-CCPS, one can impose control as well as can enjoy the decided degree of freedom. The architecture of the consortium blockchain used in the proposed scheme is shown in Fig. 2.

The consortium blockchain for healthcare CPS may involve entities like hospitals, research institutions, various state and central health departments managed by the health ministry, and the insurance and pharmaceutical industries, etc. These organizations pre-select some of the nodes as the consensus nodes as per their governance policy. These designated nodes

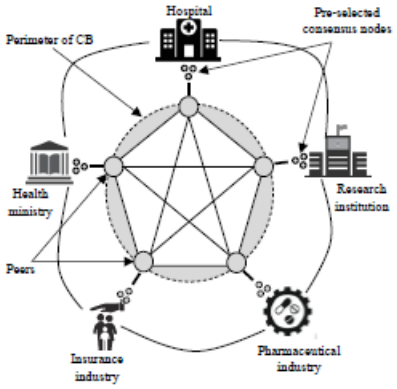

Fig. 2. Architecture of consortium blockchain for healthcare CPS.

are the one which participate in managing and updating the distributed ledger. In contrast, the other nodes can generate or contribute data. If the number of the consensus nodes is increased, then it results in a more secure and fault-tolerant system. Because now more nodes must agree to reach consensus. Further, the system becomes more scalable in terms of the number of transactions processed. Because in the consortium blockchain consensus nodes are the ones who can contribute a new block in the blockchain. the consensus protocol also requires less computational power because the consensus nodes are chosen by the organizations with a high trust level.

Thus, as the number of consensus node increases, there will be an increase in the number of new blocks, and as a result, more transactions will be included for processing. Lastly, as we increase the number of consensus nodes, the degree of decentralization also increases, which results in a more robust system.

Role of CB in the proposed scheme:

1) System Setup: The consensus nodes initialize the system and generate the global public parameters by using Shamir's secret sharing scheme.

2) User Registration and Generation of Partial Search Token: Any user can register themselves to CB by storing their public key corresponding to their unique global identity.

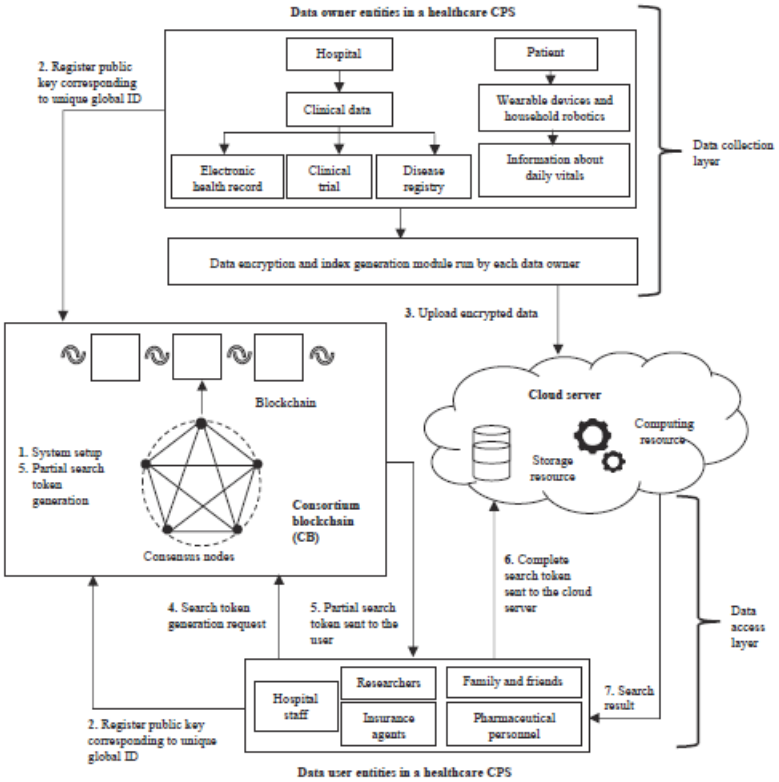

Fig. 3. Architecture of the proposed scheme for CCPS.

It is also responsible for managing and generating the search token when some user wants to retrieve encrypted information from the cloud, he/she can reach the CB to generate the partial search token corresponding to the attributes possessed by the user.

3) Free From Keeping the Master Secret: In the CB assisted proposed scheme, there is no single entity that manages the system. Hence, it is free from keeping master secret unlike the existing schemes [11]–[14].

IV. Scheme Preliminaries

This section explains the architecture that provides the general algorithm for the proposed scheme. Further, it gives the security definition along with the game-based security model for the proposed scheme.

A. Architecture of the System

The system is composed of the following four entities, as shown in Fig. 3:

1) Consortium Blockchain (CB): This entity will initialize the system and generate global parameters. Further, it registers the public key of the user corresponding to their unique global ID (GID). When a user wants to perform a search, then he/she can reach the CB along with the attributes possessed by him/her and the CB will generate the partial search token for the user.

2) Data Owner (DO): As the name suggests, DO is the one who owns some data (health data in the considered scenario) and wants to share his/her health data to a third-party cloud server. Before outsourcing both the health data file and the associated data, the keywords are first encrypted. In a healthcare system, the data owner is a patient who encrypts his health data using any standard encryption algorithm and probably the symmetric key algorithm (fast computation). The associated symmetric key used for encrypting data and the keywords contained in that data are encrypted using the *GenIndex* algorithm of the proposed scheme.

proposed scheme, the attributes are not embedded while generating the secret key for the user. At the same time, it is done directly during the search token generation by the consensus nodes. Here, the user will generate a public and private key pair for himself/herself corresponding to his/her unique global identity and sends the public key to blockchain network to register himself/herself to the blockchain network. Therefore, the proposed scheme eliminates the need of a central authority for the management of users attributes. It is done by the consensus nodes when a search token generation request is received from the user.

Fig. 5(b) shows the time taken by the index generation algorithm. As it can be observed from the Fig. 5(b), the index generation time of the schemes under consideration is almost the same and varies linearly with the number of attributes. Fig. 5(c) presents the time taken by the search token generation algorithm at the user's end. It also increases linearly with the number of attributes for all the three schemes. Fig. 5(d) shows the time taken by the search algorithm executed by the cloud server. It also varies linearly with the number of attributes, and the proposed scheme has higher time complexity as compared to [9] and [22]. The time complexity of [9] is least among the three since it only has two pairing operations, and thus the time taken by the search algorithm is almost constant. However, this algorithm is executed by the cloud server, which is assumed to have plenty of resources, and will not affect the performance of the scheme. Hence, the experimental results validate the theoretical claims made in the asymptotic complexity analysis section.

VI. Conclusion and Future Directions

In this paper, we have proposed a truly decentralized, robust and computationally efficient ABSE scheme for healthcare CCPS with the assistance of consortium blockchain. The devices involved in a typical healthcare CCPS are resource constrained. Further, the users in a healthcare CCPS may belong from a variety of domains, and to manage such a large number of diverse users, a single authority is not sufficient.

Keeping that in mind, we have proposed a scheme where computationally intensive tasks are delegated to the consensus nodes in the blockchain network to increase efficiency and to avoid single point failure. The consensus nodes are responsible for initializing the system and generating partial search tokens for users. This helps in reducing the computational burden from data users and also eliminates the need for a global central authority which sets up the system. Further, consensus nodes in the blockchain network handle the user's attributes, unlike the central trusted authority in similar ABSE schemes. Therefore, a large number of attributes from diverse domains can efficiently be handled by the proposed scheme. The proposed scheme addresses both of the aforementioned constraints in a healthcare CCPS, and thus works well in this scenario.

As a part of future work, one can work in two directions. First, one can impart efforts to incorporate a proper reward mechanism like the bitcoin network. In the proposed scheme, if we add a proper mechanism to reward users financially by means of a token, which can be spent by the users either in availing healthcare services or can be converted to other cryptocurrencies in return for sharing their data with government and healthcare agencies. By doing this, we can inspire users to utilize the system for the benefit of both the healthcare agencies and themselves. Second, one can work on adding scheme-specific features like verifiability of the search results and handle the event of user revocation with the assistance of the blockchain network to increase the correctness, robustness and dynamicity of the system.

References

[1] Q. Zheng, S. Xu, and G. Ateniese, "VABKS: Verifiable attribute-based keyword search over outsourced encrypted data, " in *Proc. IEEE Infocom*, 2014, pp. 522–530.

[2] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, "Protecting your right: Attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud, " in *Proc. IEEE Infocom Conf. Computer Communications*, 2014, pp. 226–234.

[3] Mamta and B. B. Gupta, "An efficient KP design framework of attribute-based searchable encryption for user level revocation in cloud," *Concurr. Comput. Pract. Exp.*, p. e5291.

[4] Mamta and B. B. Gupta, "Secure fine-grained keyword search with efficient user revocation and traitor tracing in the cloud," *J. Organ. End User Comput.*, vol. 32, no. 4, pp. 112–137, 2020.

[5] Y. Miao, J. Ma, X. Liu, F. Wei, Z. Liu, and X. A. Wang, "m2-ABKS: Attribute-based multi-keyword search over encrypted personal health records in multi-owner setting," *J. Med. Syst.*, vol. 40, no. 11, Article No. 246, 2016.

[6] C. Guo, R. Zhuang, Y. Jie, Y. Ren, T. Wu, and K.-K. R. Choo, "Fine-grained database field search using attribute-based encryption for e-healthcare clouds," *J. Med. Syst.*, vol. 40, no. 11, Article No. 235, 2016.

[7] Z. Chen *et al.*, "Verifiable keyword search for secure big data-based mobile healthcare networks with fine-grained authorization control," *Futur. Gener. Comput.* Syst., vol. 87, pp. 712–724, 2018. DOI: 10.1016/j.future.2017.10.022.

[8] Mamta and B. B. Gupta, "An attribute-based keyword search for m-Health networks," *J. Comput. Virol. Hacking Tech.*, pp. 1–16, 2020.

[9] Y. Miao, R. Deng, X. Liu, K.-K. R. Choo, H. Wu, and H. Li, "Multi-authority attribute-based keyword search over encrypted cloud data," *IEEE Trans. Dependable Secur. Comput.*, Article No. 2019. DOI: 10.1109/TDSC.2019.2935044

[10] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Futur. Gener. Comput. Syst.*, vol. 95, pp. 420–429, 2019.

[11] S. Cao, G. Zhang, P. Liu, X. Zhang, and F. Neri, "Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain," *Inf. Sci. (Ny).*, vol. 485, pp. 427–440, 2019.

[12] Y. Wang, A. Zhang, P. Zhang, and H. Wang, "Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain," *IEEE Access*, vol. 7, pp. 136704–136719, 2019.

[13] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE access*, vol. 6, pp. 11676–11686, 2018.