Privacy-Preserving Secured Data Distribution between Multiple Hospitals and Medical Institutes

Dr. D. R. Ingle [1], Ms. Bhagyashri B. Jadhav[2]

Bharati Vidyapeeth College of Engineering, Mumbai, Maharashtra, India[1]
Bharati Vidyapeeth College of Engineering, Mumbai, Maharashtra, India[2]

Abstract – Electronic healthcare information offers significant advantages over paper-based records in terms of storage capacity and recovery. However, current methods for sharing clinical information have security issues, such as the potential for fraud or data alteration, and they lack the ability to verify the authenticity of the source. To solve these issues, we propose a new approach for sharing clinical data using a trait-based cryptosystem. In this system, encrypted clinical data is stored in the cloud, along with access information and relevant medical data, ensuring secure storage and preventing any irreversible changes to the data. Our approach combines attribute-based encryption (ABE) with access control mechanisms, allowing for secure and privacy-preserving sharing of clinical data between multiple hospitals and medical institutions.

Keywords: **Secured Data Distribution, Electronic Healthcare Information, Attribute-Based Encryption (ABE)**

1. INTRODUCTION

In today's world, the healthcare sector is generating vast amounts of data, especially in the form of patient health records and medical details. This data is vital for medical organizations, as it helps in delivering quality healthcare services and making informed decisions regarding patient care. With the rapid advancement of technology, most healthcare institutions have adopted electronic systems for managing and storing patient data, utilizing cloud storage solutions to store large amounts of sensitive information. Cloud technology offers several advantages, including better data accessibility, flexibility, and scalability, which is crucial for the healthcare industry, where data needs to be stored and retrieved efficiently.However, the widespread adoption of cloud storage for medical data introduces significant risks, primarily around data security and privacy. One of the major concerns with the use of cloud-based systems is the potential for data breaches or hacking. If such data is accessed by unauthorized entities, it can lead to severe consequences, including identity theft, fraud, and manipulation of sensitive health records. The security of patient data must be a top priority to ensure that patient confidentiality is maintained, and that healthcare systems are not compromised in any way.

Given these risks, there is an increasing need to implement robust encryption techniques and data protection strategies to safeguard sensitive medical information. Data encryption and security measures are essential in preventing unauthorized access, data tampering, and theft. Medical fields have already integrated encryption and data mining techniques to help address these security concerns. However, it is still a challenge for hospitals and healthcare organizations to analyze large datasets effectively, especially when such data is coming from various institutions. The complexity of managing, sharing, and analyzing medical data from different sources can lead to difficulties in ensuring data consistency, privacy, and security.Furthermore, it is imperative that healthcare organizations have a reliable way to share this sensitive data securely across multiple medical institutes. Secure data sharing is necessary to facilitate collaboration between institutions for better patient care and research purposes, but it must be done in a way that ensures the integrity of the data and prevents any unauthorized access or alterations. Therefore, there is a growing need for a system that integrates various technological advancements to protect patient privacy and maintain the confidentiality of medical information.

To address these concerns, a new system must be developed that combines cloud technology with advanced encryption techniques. The system would store medical records in a centralized cloud server, where the data would be protected and accessible only to authorized healthcare providers. Access to the data would be granted through authentication mechanisms, ensuring that only the medical organizations with valid credentials can view or retrieve the data. Furthermore, the system should incorporate strong encryption protocols to prevent unauthorized access or tampering of the stored data. The use of encryption keys would ensure that even if the data is intercepted, it cannot be read without proper authorization.In addition to ensuring secure data access and storage, the system should be designed to handle large volumes of medical data generated by multiple hospitals. The vast amount of data can make it difficult for healthcare providers to extract useful insights or make timely decisions. Therefore, integrating smart data analysis techniques, such as clustering and machine learning, can help healthcare institutions analyze large datasets efficiently. This could be useful in various ways, such as developing personalized drug recommendation systems, optimizing treatment plans, and making informed decisions for healthcare policies.

By implementing such a system, healthcare organizations can ensure the security, integrity, and privacy of patient data while also enabling efficient data sharing and analysis across multiple institutions. The combination of secure cloud storage, advanced encryption techniques, and smart data processing can significantly improve the management of healthcare data, ultimately leading to better healthcare outcomes and improved patient care.

2. BACKGROUND AND RELATED LITERATURE

The healthcare sector has seen a dramatic shift with the adoption of digital technologies, particularly in managing and storing patient information. Over the years, electronic health records (EHRs) have largely replaced paper-based methods, enabling hospitals and healthcare facilities to store and organize patient data more efficiently. Cloud computing has become a central part of this digital transformation, offering solutions for scalable, flexible, and cost-effective data storage. The use of cloud technology in healthcare allows medical organizations to manage vast amounts of data, ensuring quick access and easier retrieval. However, this shift to cloud-based systems also brings concerns about the security and privacy of sensitive patient data. There are growing risks of data breaches, unauthorized access, and manipulation of health records, which can have severe consequences on both individual patients and healthcare systems as a whole. To address these issues, much research has focused on developing secure data-sharing protocols and improving the overall encryption of healthcare data. Techniques like attribute-based encryption (ABE) and trait-based cryptosystems are commonly explored to enhance security and ensure that only authorized individuals can access medical data. In parallel, various data analysis methods, such as clustering and data mining, have been studied to manage and interpret large healthcare datasets more effectively. These methods help healthcare organizations extract valuable insights from vast amounts of medical data, supporting better decision-making and fostering collaborations between different institutions. This section reviews key studies and advancements in these areas, shedding light on existing challenges and highlighting opportunities for further improvement in securing and sharing healthcare data.

Related Work and Background Literature

Fanyu Bu et al. [1] conducted a comparative study evaluating the performance of various clustering algorithms on two medical datasets, focusing on clustering accuracy and efficiency. Their results revealed that the High-request Possibilistic c-Implies Calculation (HoPCM) algorithm significantly outperformed other approaches in terms of accuracy and efficiency. However, the study noted a limitation: repetitive clustering was occasionally required for optimal results in HoPCM, a step that was not included in their implementation.Xiaodong Yang et al. [2] proposed a medical data sharing framework that integrated attribute-based cryptosystems with blockchain technology. This system utilized a cloud server to store encrypted medical data while the blockchain preserved the location of

the encrypted data and relevant medical information. While promising, the blockchain aspect introduced certain limitations that could be improved.

Ekblaw et al. [3] introduced MedRec, a decentralized record management system for handling Electronic Health Records (EHRs). This system offered patients an immutable log and easy access to their medical records across healthcare providers and facilities.Li et al. [4] presented a patient-centric framework that employed attribute-based encryption (ABE) for securing Personal Health Records (PHRs) on semi-trusted servers. The proposed mechanism enabled dynamic modification of access policies and attributes, supporting user revocation and emergency access scenarios.Wang and Song [5] developed a secure EHR system that combined attribute-based encryption (ABE) with identity-based encryption (IBE) and identity-based signatures (IBS). To achieve efficient cryptographic operations, the authors introduced a hybrid cryptographic primitive called Combined Attribute-Based/Identity-Based Encryption and Signature (C-AB/IB-ES).

Cheung and Newport [6] explored CP-ABE schemes that employed AND gates on positive and negative attributes. They demonstrated CPA (Chosen Plaintext Attack) security under the Decisional Bilinear Diffie-Hellman (DBDH) assumption and extended this to CCA (Chosen Ciphertext Attack) security using one-time signatures. The authors further optimized the scheme with hierarchical attributes to reduce ciphertext size and improve encryption and decryption efficiency.A detailed introduction to blockchain technology was provided by [7], covering blockchain architecture, consensus mechanisms, technical challenges, and emerging trends. The paper highlighted blockchain's potential for secure and scalable medical data exchange systems.

Mobile Fog, a programming model for latency-sensitive and geospatially distributed applications, was introduced by [8]. This framework demonstrated its effectiveness in real-world use cases such as connected vehicle systems and camera networks, showing improvements in application performance through simulation.The concept of fog computing was redefined and its objectives explored by [9]. The study proposed a modular fog platform architecture to integrate data from diverse sources securely. The implementation showcased fog computing's potential in healthcare systems, including its benefits for privacy and data security.A Health Fog framework [10] was introduced as an intermediary layer between the cloud and users to reduce communication costs. This architecture incorporated cryptographic primitives to secure data while ensuring modularity and flexibility.

Researchers [11] proposed a fog-based health monitoring system to improve efficiency in IoT-enabled healthcare. This system integrated event-based data transfer, temporal mining, and real-time decision-making, demonstrating superior accuracy in predicting health events compared to traditional methods.A fog-assisted e-health gateway [12] was developed for real-time data processing and local storage at the network edge. This system employed wavelet transform mechanisms for ECG analysis and feature extraction, highlighting its role in cardiac disorder diagnostics.The hierarchical computing architecture (HiCH) proposed in [13] addressed scalability, energy efficiency, and mobility challenges in IoT-based healthcare systems. The architecture utilized machine learning-based analytics and a closed-loop management system, demonstrating its effectiveness in arrhythmia detection for cardiovascular patients.

3. METHODOLOGY

The proposed system aims to implement a cloud-based solution for securely storing extensive medical records of patients. This platform will allow simultaneous access by multiple medical organizations, functioning as a client-server architecture where hospitals act as clients and the cloud infrastructure serves as the server. Authorized access to the system will be facilitated through verification by a trusted third-party authenticator and hospital authorities. The system will feature modules such as signature generation, access control

policy formulation, data encryption using ABS-OD, data clustering, and user authentication for secure data retrieval.

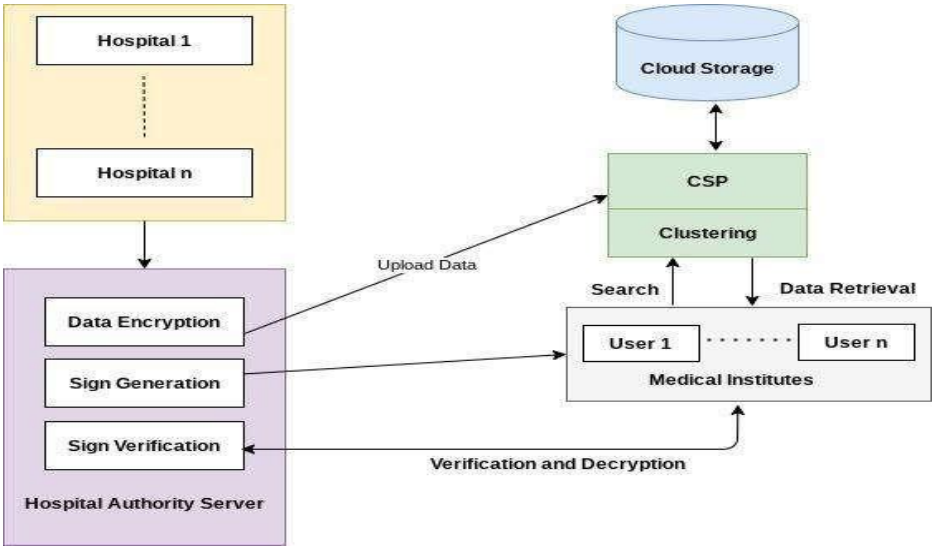

Figure 1. Proposed Architecture

Module 1: Signature Generation and Access Control Policy

In this module, the hospital defines access policies for users who require access to patient data. Hospitals and medical institutions first register with the hospital authority servers, after which they establish access control policies for patient data. These policies are then transmitted to the hospital authority server, which generates private and signature keys corresponding to these policies. The hospital authority server sends these keys to the respective hospitals and medical institutes.

The process is as follows:

1. Hospital send the attribute set SU = {SU1, · · · , SUw} ⊆ N
2. Hospital also send the globally verified identifier GID
3. Randomly select αi, γi ∈ Zp where i ∈ [1, n] for each attribute i
4. Calculate VK = {ˆe (g, g) αi, g γi} and SIK = {αi, γi} where i ∈ [1, n].
5. Calculate the signature key SIKi, GID = {g αi, H4 (GID) γi corresponding to each GID
6. Send SIKi, GID to the hospital authority, where i ∈ [1, n].

In the key-sharing schema, each share is managed by different participants, and no single participant can recover the secret alone. Only a collaboration between a few participants can reconstruct the secret. The first step involves secret generation, where the cloud authority selects a matrix M with x rows and j columns named the share-generation. Suppose that vector v = (s,r2, . . . ,rj) is the transpose of matrix, where s ∈ Zp is the secret value to be shared and r2, . . . ,rj ∈ Zp are random elements. Second step is secret distribution. The secret distributor assigns the shared secret value s to x members U1, . . . , Ux , where the secret share owned by the k-th member Uk is Mk ×v, and the k-th row of the matrix M is identified as the function ρ(k).

Module 2: Data Encryption with ABE-OD

Medical data from various hospitals are uploaded to the hospital authority server for secure storage. Given the sensitive nature of this data, it must be encrypted to prevent unauthorized access. After receiving the signature key, the hospital encrypts medical records using Attribute-Based Encryption for Outsourced Decryption (ABE-OD). The hospital authority server utilizes a cyclic group with bilinear maps for encryption. ABE-OD allows for key outsourcing, making it easier to manage encryption and decryption processes efficiently.

The process is as follows:

- Randomly choose $\zeta \in \{0, 1\}$ l and calculate ∂ = H1 (ζ ||m), C^{-} 1 = $\zeta \oplus$ H2 (φ ∂), C^{-} 2 = m $\oplus$ H3 (ζ), C^{-} 3 = g ∂.
- Calculate C^{-} 4 = H4 (3||C^{-} 1||C^{-} 2||C^{-} 3||C1|| . . . ||Cn) ∂ .
- Send cipher text CT = (3,C^{-} 1,C^{-} 2, C^{-} 3,C^{-} 4,{Ci}i$\in$N)

The hospital authority server generates the outsourced decryption key and stores it. The cloud authority then uploads the encrypted data, along with medical information and unique identifiers, to the cloud service provider.

Module 3: Data Clustering with HOPCM on CSP

Data from the hospitals is uploaded to the cloud as encrypted tensors. These tensors, representing hospital data, are then clustered using High-request Possibilistic C-Implied Calculation (HOPCM). This process is performed on the cloud platform to group the clinical data efficiently. After receiving the encrypted data from the hospital authority server, the cloud service provider applies HOPCM to categorize the data into clusters. The membership matrix is created, cluster centers are calculated, and the dataset is partitioned into subsets. Distances between data points are computed and stored. If the data volume increases, blockchain mechanisms can be employed for better management and transparency.

Algorithm HoPCM

Input: X = {x1, x2, ..., xn}, c, m, maxiter

Output: U = {uij}, V = {vi}

1 Initialize the membership matrix U;

2 for iter = 1, 2, ..., maxiter do

- Update the cluster center vi
- $\eta_i = \frac{\sum_{j=1}^{n} u^m d_{ij}}{\sum_{j=1} \quad j}$
- For each iii, update uij based on distance metrics.

Module 4: User Verification and Data Retrieval

In this module, the private key obtained from the cloud authority server is used to decrypt the downloaded data. A user, typically an authority figure from a medical institute, requests the

encrypted data from the cloud service provider. The CSP responds with the matching clustered data and an access key. The user then requests the decryption of the data from the hospital authority server. Before this, the user must verify their identity. This process of verification and data retrieval utilizes Attribute-Based Signature (ABS). Once the signature is verified, the hospital authority sends the decryption key to the user. The medical institute user can then access the clustered data in decrypted form for further analysis.

4. RESULT AND DISCUSSION

Computational Overhead

Computational overhead refers to the amount of time and resources required by the system to execute specific tasks. In this study, the computational overhead is assessed by evaluating the time taken for encryption and decryption processes. The evaluation focuses on how the computational time varies with the number of attributes, which are incrementally increased in each iteration.The proposed methodology involves calculating computational overhead as the combined cost of encryption and decryption operations. The time taken for these operations is measured against the increasing number of attributes. This analysis helps in determining the efficiency of the proposed system and its scalability when handling a growing number of attributes. By analyzing the correlation between the number of attributes and the time required for processing, the study provides insights into the performance impact of computational overhead in the system.

No.Of Attributes	Computational Overhead(ms)
2	6.8
4	11.0
6	15.8
8	22.0
10	28.6

Table 4.1 Computational overhead against attributes

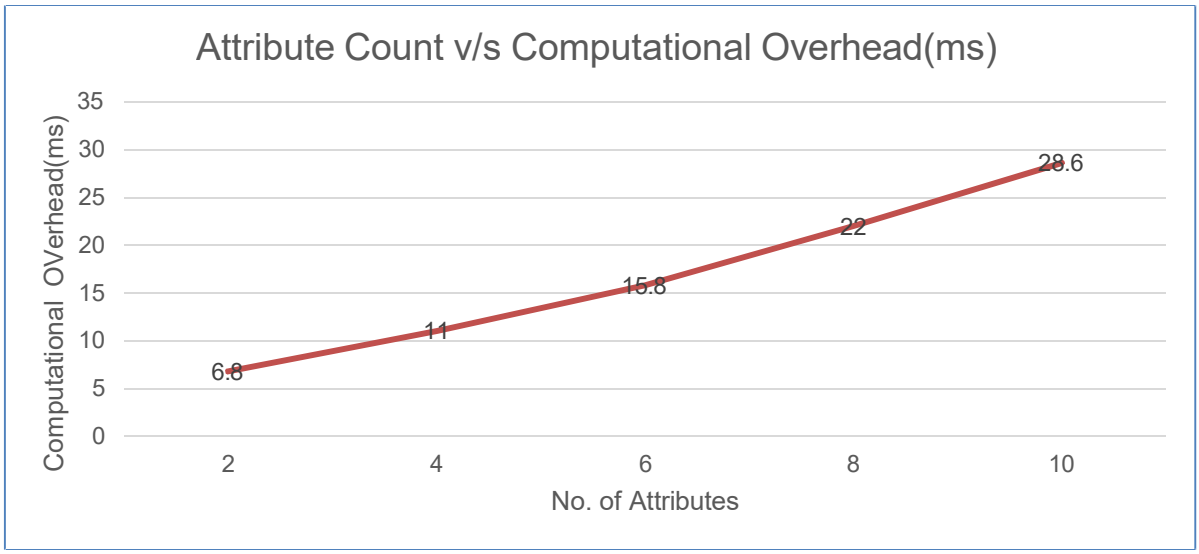

Figure 2. Computational overhead against attributes

The data presented in the table clearly illustrates a direct correlation between the number of attributes and the computational overhead measured in milliseconds. As the number of attributes increases, the computational overhead rises correspondingly. For instance, with just two attributes, the overhead is a minimal 1 millisecond. However, as the attributes increase to 3, 5, 8, and ultimately 10, the overhead progressively grows. This pattern highlights that systems with a higher number of attributes demand more computational resources and time for processing. These observations emphasize the significance of optimizing computational resources to maintain efficiency in systems with increasing complexity.

5. CONCLUSION

The description of this system outlines a robust framework aimed at securing and managing medical data across a network of entities, including hospitals, medical institutions, cloud service providers, and end-users. It addresses critical challenges such as access control, encryption, data clustering, and user verification, with each module playing a pivotal role in ensuring data privacy, integrity, and accessibility.A significant focus of the analysis is on computational overhead, which is highlighted as a key consideration. The data presented in Table 4.1 establishes a clear link between the number of attributes and the computational requirements, showing that as the number of attributes increases, so does the computational load. This observation underscores the importance of efficient resource management to sustain optimal performance in complex systems.In summary, the system effectively addresses the various stages of medical data management in a healthcare setting. The analysis underscores the necessity of accounting for computational overhead to ensure efficiency and scalability, offering valuable insights for enhancing the performance of complex systems.

6. REFERENCE

1. *Fanyu. Bu, C. Hu, Q. Zhang, C. Bai, L. T. Yang and T. Baker, "A Cloud-Edge-Aided Incremental High-Order Possibilistic c-Means Algorithm for Medical Data Clustering," IEEE Transactions on Fuzzy Systems, vol. 29, no. 1, pp. 148-155, Jan. 2021, doi: 10.1109/TFUZZ.2020.3022080.*
2. *Xiaodong. Yang, T. Li, X. Pei, L. Wen and C. Wang, "Medical Data Sharing Scheme Based on Attribute Cryptosystem and Block chain Technology," IEEE Access, vol. 8, pp. 45468-45476, 2020, doi: 10.1109/ACCESS.2020.2976894.*
3. *A. Ekblaw, ''A case study for blockchain in healthcare: MedRec prototype for electronic health records and medical research data,'' Proceeding of IEEE Open Big Data Conference, 2016, p. 13.*
4. *M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, ''Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,'' IEEE Transaction on Parallel Distribution System, vol. 24, no. 1, pp. 131–143, Jan. 2013.*
5. *H. Wang and Y. Song, ''Secure cloud-based EHR system using attribute-based cryptosystem and Blockchain,'' Journal of Medical System, vol. 42, no. 8, pp. 152–161, Jul. 2018.*
6. *L. Cheung and C. Newport, ''Provably secure ciphertext policy ABE,'' Proceeding of 14th ACM Computer and Communication Security Conference (CCS), 2007, pp. 456–465*
7. *P. Manjunath, M. Prakruthi and P. Gajkumar Shah, "IoT Driven with Big Data Analytics and Block Chain Application Scenarios," 2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT), Bangalore, India, 2018, pp. 569-572, doi: 10.1109/ICGCIoT.2018.8752973.*
8. *P. Verma and S. K. Sood, ''Fog assisted-IoT enabled patient health monitor ing in smart homes,'' IEEE Internet Things J., vol. 5, no. 3, pp. 1789–1796, Jun. 2018.*
9. *T. N. Gia, M. Jiang, A.-M. Rahmani, T. Westerlund, P. Liljeberg, and H. Tenhunen, ''Fog computing in healthcare Internet of Things: A case study on ECG feature extraction,'' in Proc. IEEE Int. Conf. Comput. Inf. Technol.; Ubiquitous Comput. Commun.; Dependable, Autonomic*

Secure Comput.; Pervas. Intell. Comput., Oct. 2015, pp. 1–8.

10. *B. Negash, A. Anzanpour, I. Azimi, M. Jiang, T. Westerland, A. M. Rahmani, P. Liljeberg, and H. Tenhunen, ''Leveraging fog computing for healthcare IoT,'' in Fog computing in the Internet of Things Intelligence at the edge. Cham, Switzerland: Springer, 2017, pp. 145–169.*
11. *A. M. Rahmani, T. N. Gia, B. Negash, A. Anzanpour, I. Azimi, M. Jiang, and P. Liljeberg, ''Exploiting smart e-health gateways at the edge of healthcare Internet-of-Things: A fog computing approach,'' Future Gener. Comput. Syst., vol. 78, pp. 641–658, Jan. 2018.*
12. *I. Azimi, A. Anzanpour, A. M. Rahmani, T. Pahikkala, M. Levorato, P. Liljeberg, and N. Dutt, ''HiCH: Hierarchical fog-assisted computing architecture for healthcare IoT,'' ACM Trans. Embedded Comput. Syst., vol. 16, no. 5s, pp. 1–20, Oct. 2017.*
13. *Y. Wang, Y. Kong and P. Fan, "Research on trusted traceability with Block Chain and Handle System Network," 2021 International Conference on Information Science, Parallel and Distributed Systems (ISPDS), Hangzhou, China, 2021, pp. 125-130, doi: 10.1109/ISPDS54097.2021.00032.*
14. *Y. Zhang, R. Wang, Q. Li, N. Xia, N. Zhang and J. Hu, "Research and Application of Block Chain Technology in Electricity Market Transactions," 2022 4th International Conference on Smart Power & Internet Energy Systems (SPIES), Beijing, China, 2022, pp. 2180-2183, doi: 10.1109/SPIES55999.2022.10082649.*
15. *Z. Xiaoming, L. Caiping, T. Dejin, S. Yuchen, H. Zhen and Z. Jisheng, "Design of Remote Sensing Image Sharing Service System Based on Block Chain Technology," 2019 IEEE International Conference on Signal, Information and Data Processing (ICSIDP), Chongqing, China, 2019, pp. 1-4, doi: 10.1109/ICSIDP47821.2019.9173237.*
16. *Pavan Manjunath, Pritam Gajkumar Shah, "IoT Based Food Wastage Management System", I-SMAC (IoT in Social Mobile Analytics and Cloud) (I-SMAC) 2019 Third International conference on, pp. 93-96, 2019.#*
17. *Z. Xiaoming, L. Caiping, T. Dejin, S. Yuchen, H. Zhen and Z. Jisheng, "Design of Remote Sensing Image Sharing Service System Based on Block Chain Technology," 2019 IEEE International Conference on Signal, Information and Data Processing (ICSIDP), Chongqing, China, 2019, pp. 1-4, doi: 10.1109/ICSIDP47821.2019.9173237.*
18. *Z. Ullah, G. Mokryani, B. Khan, I. Khan, C. A. Mehmood and S. M. Ali, "Smart Grid Block-Chain (BC) Conceptual Framework: Bi-Directional Models for Renewable Energy District and Utility," 2019 15th International Conference on Emerging Technologies (ICET), Peshawar, Pakistan, 2019, pp. 1-5, doi: 10.1109/ICET48972.2019.8994500.*
19. *W. Liu, S. S. Zhu, T. Mundie and U. Krieger, "Advanced block-chain architecture for e-health systems," 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), Dalian, 2017, pp. 1-6, doi: 10.1109/HealthCom.2017.8210847.*