International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6309
***Article Received**: 20 December 2022 **Revised**: 28 January 2023 **Accepted**: 04 February 2023*

Secure Blockchain Transactions for Electronic Health Records based on an Improved Attribute-Based Signature Scheme (IASS)

Prathipa Ravanappan[1], P. Ilanchezhian[2], N. Chandrasekaran[3], S. Prabu[4], N. Naga Saranya[5]

[1]Associate Professor,
Department of ECE,
Panimalar Engineering College,
Email: prathipa.srini@gmail.com

[2]Associate Professor,
Department of Information Technology,
Sona College of technology,
Email: ilanchezhianp@sonatech.ac.in

[3]Professor,
Department of EEE,
PSNA College of Engineering and Technology,
Dindigul, Tamil Nadu,
Email: chandrasekaran283@gmail.com

[4]Professor,
Department Of ECE,
Mahendra Institute of Technology,
Namakkal,
Email: vsprabu4u@gmail.com.

[5]Associate Professor,
Department of MCA
Meenakshi College of Engineering,
Email: drnagasaranya@gmail.com

Abstract- Electronic Health Records (EHRs) are entirely controlled by hospitals, not patients, making it difficult to obtain medical advice from individual hospitals. Patients need to keep tabs on their health details and take back control of their medical data. The rapid development of blockchain technology has facilitated large-scale healthcare, including medical records and patient-related data. The technology provides comprehensive and immutable patient records and free access to electronic medical records for providers and treatment portals. To ensure the validity of the blockchain-connected EHR, the Improved Attribute-Based Signature Scheme (IASS) has considerable powers, allowing patients to approve messages based on attributes but not validated. In addition, it avoids the problem of having multiple authorities without a single or central source of trust for generating and distributing patient public/private keys and fits into the blockchain model for distributed data storage. By sharing a secret, pseudo-random activity seed between authorities, the protocol resists collusive attacks by corrupt officials. The technology provides patients with a comprehensive, immutable record and free access to their EHR from providers and treatment portals. To ensure the validity of blockchain-connected EHRs, propose an attribute-based multi-authority signature scheme that authorizes messages based on their attributes without revealing any information.

Keywords: Electronic Health Records (EHRs), Blockchain, Improved Attribute-Based Signature Scheme (IASS), records, public/private keys.

I. INTRODUCTION

An Electronic Health Record (EHR) provides features that effectively support health records. It moves away from the traditional paper patient clinical records and makes them available electronically online. In the current scenario, a patient could spread her EHR across the region in a life-changing situation, starting her EHR with one expert collaborative dataset and moving on to the next. Afterwards, patients may need help keeping up to date with medical information, and specialist co-ops often keep up with primarily administrative duties. Patient consent to access the EHR is minimal, and patients often require more time to access this information from scientists and healthcare providers easily.

The framework is intended to give patients command over EHR creation, the executives and imparting to family, companions, medical care suppliers and other approved information customers. Also, admittance to these EHRs abroad by clinical specialists and suppliers of such administrations is supposed to empower movement programs for clinical arrangements. Be that as it may, in the ongoing circumstance, patients disperse their EHRs across various regions during life-altering situations, making the EHRs move to start with one specialist organization data set and then on to the next. Accordingly, the patient might need help to grasp current medical care information, while the specialist co-op usually keeps up with the essentials.

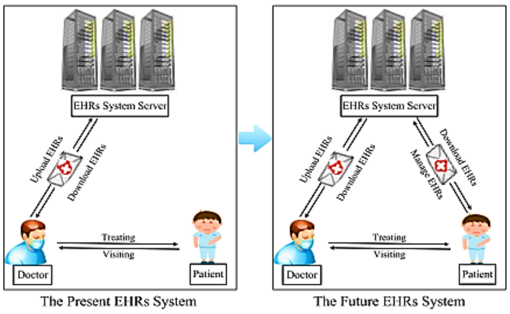

Figure 1: Electronic Health Care System

Patients have negligible admittance to their EHRs, and can only, with significant effort, share this information with specialists and medical care suppliers. They are expanding boundaries to superior execution information sharing. Clinical records can become disrupted and divided without critical information between the board and trade. Patients can safely and extensively oversee and share their electronic clinical records, as shown in Figure 1.

Blockchain innovation is first evolved and presented for the cryptographic money Bitcoin. Since the coming of blockchain innovation, it has been a mechanical insurgency for its effect on society, like the creation and the internet. A blockchain is a decentralized data set in which information blocks are connected sequentially. In the medical care industry, dealing with a person's EHR blockchain (a model for unified blockchains) requires the cooperation of different gatherings, for example, experts, clinics and insurance companies.

Get-togethers can bring asset verification and costly data handling for every applicable partner. Because of Ethereum blockchain innovation, the Pearl Health Organization means working with admittance to patient information by clinical experts and divisions, decreasing the wastage of clinical assets, and treating severe ailments quicker. For this situation, the patient's electronic clinical record (a type of blockchain) should be confirmed because of proprietorship to avoid misdiagnosis before a precise determination is composed to the blockchain. Moreover, electronic clinical records put away in the modules contain names, personalities, sensitivities, and other fundamental information. Health Insurance Portability and Accountability Act (HIPPA) rules require patient security to be safeguarded during EHR sharing. In character confirmation, quality-based multi-substance marks are a successful answer for demonstrating an individual's personality while preserving the protection of an electronic clinical record framework for taking care of various clinical field attributes.

A. Contribution of this work

It uses an Improved Attribute-Based Signature Scheme (IASS) with multiple authorities to meet blockchain requirements in decentralized EHR systems. This proposal uses ABS with blockchain technology to protect patient privacy and maintain EHR immutability. Contributions to this work are as follows:

- First, Blockchain technology conjunction with construction proposes a multi-authority ABS scheme for monotonic predicates in EHR systems, where the number of bilinear pairs involved in signatures increases with the number of authorizations. Proportionately increase.
- Second, a significant challenge for many officers is to collude in attacks. To address this risk, random functional seeds are shared by both organizations and stored confidentially. KeyGen embeds each company's private key into the patient's private key. According to this framework, protocol N-1 is resistant to combinatorial attacks.
- Finally, under the computational dichotomous Diffie-Hellman assumption, prove that propositions are inexcusable under selective prediction attacks in a random oracle model and enjoy perfect privacy from signatories, preventing patient data leakage. Standard works on cost and properties. This shows that this scheme usually gives better performance.

II. RELATED WORK

A medical services stage because of a seamless Electronic Clinical Record (sEMR) approach. Our main goal is to assist crisis patients requiring critical consideration and follow-up care after release or case reference, utilizing present-day innovation to serve the underserved populace

***Article Received**: 20 December 2022 **Revised**: 28 January 2023 **Accepted**: 04 February 2023*

better [1]. Electronic Health Record Information and Machine learning Procedures to Distinguish Chance Variables Foreseeing Maternal Effects in a Pandemic [2].

The general objective of to give data connected with music treatment, chiropractic and swimming in the EHR framework. Three hundred clinical notes were arbitrarily examined and physically commented on. It depicts every strategy's condition, side effects and recurrence [3]. Blockchain innovation can be utilized to supplant EHR frameworks to resolve these issues [4].

It designs a blockchain-empowered unique access control engineering with neighbourhood differential security systems to give trait-based security insurance in exchange for work processes. It will foster four sorts of shrewd agreements into the system to address the issues of unknown discussions, dynamic access control, good matching choices, and public information assessment in open organizations [5]. Patients and doctors frequently request the information they need while getting electronic clinical records. Recovering data is sometimes right, and access can be limited [6]. Current frameworks present a few obstructions to patient-focused, including security and protection concerns, information irregularities, and convenient admittance to the correct records from different clinical substances [7].

Specialists have proposed possible blockchain-based answers for EHRs: ideas, models, and executions. Centres around a Systematic Literature Review (SLR) to distinguish and look at good or execution articles submitted for overseeing EHRs utilizing blockchain [8]. A protection saving plan in light of blockchain and distributed innovation that works with the consistent and secure trade of client information, for example, electronic Health record (EHR) related data. A node-State-checkable Practical Byzantine Fault Tolerance consensus algorithm (sc-PBFT) with Hub Status Confirmation to Keep Byzantine Hubs from Hacking Consortium Chains.

Electronic well-being record (EHR) interoperability is essential for consistent data division between medical care experts [11]. EHRs are frequently divided among medical care experts, making them helpless against blackouts, information abuse, and the absence of protection, security, and review trials. Then a blockchain chain is a spearheading innovation that gives an endlessly decentralized climate where hubs in an organization can interface with one another without a focal authority [12]. One of the issues is the capacity to be a reliable method for putting away and sharing electronic clinical records in new and imaginative ways. Current clinical record stockpiling and transmission techniques are exclusive and have interoperability and security issues [13]. Cloud electronic clinical records tackle the data-sharing issue of customary electronic clinical records. Nonetheless, there are centralization issues in cloud-based EHRs: cloud administration focuses and key age places [14]. In light of the cybertext guideline characteristic encryption framework and the IPFS stockpiling climate, in the mix with blockchain innovation, foster an Attribute-Based Encryption (ABE) plan to safeguard electronic clinical records in Inter-Planetary Document Framework (IPFS) stockpiling and proficient sharing of the stockpiling climate [15].

III. PROPOSED METHOD

This section includes an EHR system model and a detailed IASS framework. The proposal is a multi-organizational IASS project that can be applied to healthcare using blockchain technology.

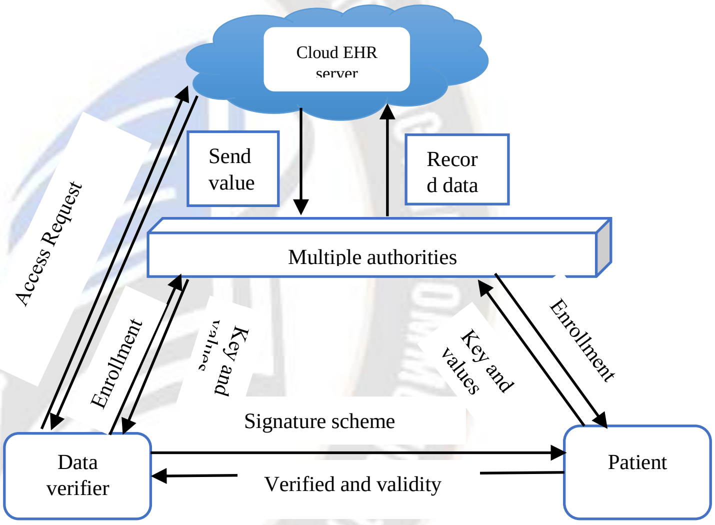

Figure 2: Proposed diagram for IAAS

The EHR framework model comprises four sections: As displayed in Figure 2, the EMR server is like a distributed storage server, answerable for putting away and moving EMRs. Complex associations incorporate emergency clinics, health care coverage organizations, clinical examination foundations, and associations that record and trade patient data. Patients can make, make due, control, sign their own EHRs and characterize predicates. It permits information validators to get to the mark and check its accuracy.

A. Cloud EHRs

Patients, physicians, nurses, and medical assistants can access EHR systems through a private network portal using various devices, including smartphones, laptops, and desktop computers. Patient information and data security are provided through public key cryptography and steganography. Recorded patient data is periodically stored

***Article Received**: 20 December 2022 **Revised**: 28 January 2023 **Accepted**: 04 February 2023*

and transferred to a web server via a secure file transfer protocol (FTPS) for later reference. Doctors can use the patient's medical data accessed by doctors along with the patient's medical history, response to medications, progress and sometimes the correct evidence to send medical advice to patients. Additionally, doctors can interact with patients through the portal, and patients can access their medical records.

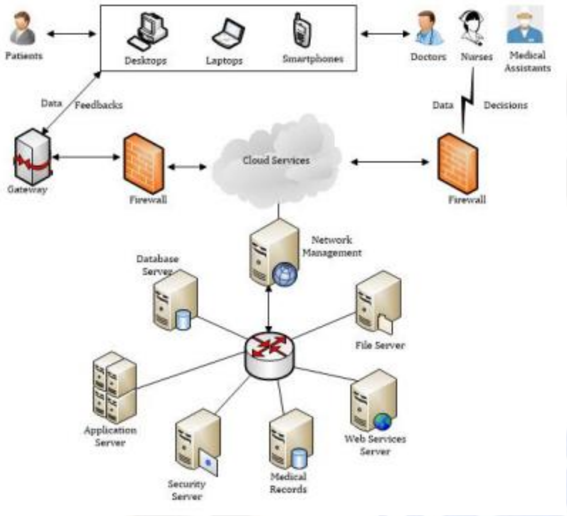

Figure 3: Proposed architecture for Cloud EHRs

Figure 3 describes the proposed framework's architecture, the cloud-based EHR system. On the user side, the framework allows two types of users (including patients and practitioners/assistants) to access the system using different devices (e.g. smartphones, laptops and desktops). The patient requests remote access to the system through the gateway while the physician/assistant accesses the system over the communication network. A cloud is a collection of servers, such as applications that handle all application functions between users and computer back-end databases and database servers that provide database services to other infrastructure components. File servers that act as shared disks. The web service server provides the business logic to meet user requirements. The security server ensures the security and access control of the stored data.

B. *Setup and attribute scheme for Attribute-Based Signature*

With Lagrange coefficients defined as$R(x) = Qj \in c, j6 = ix - ji - j$, for any $x \in Zc$ whose elements Zc belong to the characteristic set S. For each quality, this plan partners components in Z*c with positions comparing to that property. The specific programs are as follows:

Setup: The EHR server selects two suitable additional cycle groups, G and GT, as prime order q and bilinear graphs. $e\hat{}: F \times F \rightarrow FT$.

Allow P to be an irregular number generator in N and M: {0, 1} ∗ → Z ∗ c be areas of strength for a safe hash capability, for example, SHA-256. Compute (C) = H (GID) for GID, the global identifier of the patient. Assume that this system has N transformations, x1 and x2.

Each control Ck tracks the attribute set eAk = ck, 1, CK, 2 . .ck, nk. Choose randomly ω ∈ Z ∗ q and let Q = ωP. The public parameters for this system are params = e^, q, P, Q, G, GT, H.

a. Attribute Based setup

Each authority CK chooses $ck \in S_x^*$ at the chance and calculates $x_n = \alpha_k Q$. For each element $CK, x \in \check{a}_k$,

$xki \in S\_x^\wedge *$ Choose any value you want between Ax and Ay as the secret cryptographic function.

Randomize and share the key exchange, then set $x\_ij \in S\_x^\wedge * q$ to randomly share the chosen value as the Secret Random Function (SRF) seed for the two-party key exchange.

// A CA implements an agreement to allocate permissions and limitations to an attribute.

If Assignment (ω, as, t) = true, then

$N\omega$ ← fixed of number of authorities;

$T\omega$ ← the Threshold values;

End if

$SRF = \left(\frac{x_k y_j}{x_{j+u}}\right)$ The ability C_k outputs the public keys as

$$PKk = yk, Tk, i\ i \in \{1,2,\ldots,nk\}$$

E and the private (secret) keys as $SKk = D\ \alpha k, xk,$

$$skj\ j \in \{1,2,\ldots,N\}\{k\},$$

$$tk, i\ i \in \{1,2,\ldots,nk\}\ E.$$

Which then sets $sk_j = s_{jk}$. C_k and Cj choose xi, xj ∈ Z ∗ q, respectively. , Each Attribute has two parameters: a count of As nω and ω, an entry to manage the feature. A data consumer needs to obtain tω authorization from nω attribute authority to access attributes.

b. Key Generation

Collected with the Shamir secret sharing plan to produce a public property key for each quality and transfer it to the blockchain. Since each trait is mutually overseen by various A's, the framework needs an agreement to gather the public quality key cut created by the A's. As displayed in the calculation, after the framework statement stage, collect the tω general property key split pki, ω from AA and call Lagrangian addition to process the general trait key PAKω for information encryption increases.

```
//As invoke SSS to generate the segmentation of public
attribute key

              If segPAKGen (AAi

                 PKI,ω) = true then

                  AAi send PKI,ω to contract;

                 Count[ω] ++;

   If Count[ω] = tω then

   // this agreement conjures the Lagrangian addition
   technique to produce PAKω

      PAKω ← Lagrangian (tω, pki,ω);

   End if

    End if
```

PAKGen PKI) → PAK: After receiving tω public attribute key splits PKI,ω, the PAKGC calculates,

$$e(g,g)^{\alpha_\omega} = \prod_{i=1}^{t_\omega} e(g,g)^{sk_{\alpha_\omega,i} \prod_{j=1,j\neq i}^{t_\omega} \frac{aid_j}{aid_j - aid_i}}$$

$$g^{\beta_\omega} = g^{sk_{\beta_\omega,i} \prod_{j=1,j\neq i}^{t_\omega} \frac{aid_j}{aid_j - aid_i}}$$

The Public Attribute Key (PAKω) = (e (g, g) αω, g βω), and the secret attribute key SAKω = (αω, βω)

```
 If segUAKGen(AAi

      UK, ω, uid) = true, then

      AAi send UAKi, ω, uid to contract;

      Count[ω] ++;

If C thenount[ω] = tω

//This contract invokes the Lagrangian interpolation method
to generate UAKω

      UAKω ← Lagrangian (tω, UAKi,ω);

 End if

End if
```

When joining a DU system, the AAs collaborate to create user attribute key sections UAKi, ω, and uid in their respective administrative domains using Shamir's secret sharing plan. As displayed in the calculation, after KAG gathers tωAK, ω, uid segments from AA, it naturally executes the Lagrange addition technique to work out the client characteristic key UAKω, uid, and afterwards sends the information to the client for encryption.

C. Multi authority Signature Attribute key Access scheme

With a highly efficient searchable asset as the key access point, this scheme remains secure even in selective data loss. Cyphers have been recently implemented and evaluated based on key policy attributes. Searchable asset key access points have also been introduced to improve the transaction verification process and increase security.

a. Steps for Signature Attribute key Access scheme

```
Input: data file Blockchain (D)

Output: Search results based on the user ID

While (Read the file (D))

            {

            While (Read the id (W) in D)

                  {

            If (Find the user id, W)== False)

                  Insert (user Id, W);

                  Get W's List

            Insert a node to W's position list;

                  }

            }

End

Step 1: Procedure: Hashcode and get permission

Check to verify (IASS←Attribute Searching)

            Compute the joining chain to the relative
      block to access the data

Step 2: Provide access character to the chain block

Step 3: Return access
```

The proposed access method enhances security at the block level. Use the user role to set the personal value for attribute searches for object purposes. Create user identity cognitive blocks for each other.

IV. RESULT AND DISCUSSION

This section presents the results of recommended experiments performed with the C#.net language and the Visual Studio tools. The proposed algorithm, the Improved Attribute-Based Signature Scheme (IASS), compared with existing algorithms, is a state-checkable Practical Byzantine Fault Tolerance consensus algorithm (sc-PBFT), Attribute-Based Encryption (ABE) approach.

TABLE 1: SIMULATION PARAMETERS

Parameters	**Values**
Tool	Visual Studio 2019
Language	C#
Technology	Blockchain
Number of users	1000
File Size	500MB

Table 1 presents Simulation parameter measurements used to assess the proposed algorithm. Comparative parameter measurements for the proposed algorithms are Transaction accuracy (TA) performance, Encryption/Decryption Performance, Access Control Analysis, and time complexity.

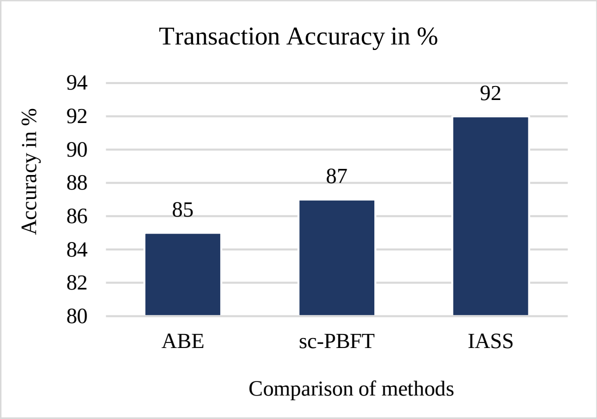

Figure 4: Performance Transaction Accuracy

Figure 4 defines the analysis of Transaction Accuracy performance based on proposed and existing results. The proposed Improved Attribute-Based Signature Scheme (IASS) algorithm security performance is 92%. The proposed algorithm enhances the security performance compared with the existing algorithm.

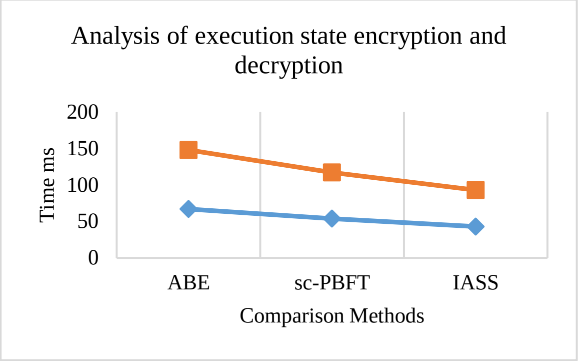

Figure 5: Analysis of execution state encryption and decryption

Figure 5 defines the analysis of execution state encryption and decryption performance comparison results. The proposed IASS algorithm produces a low time performance than existing algorithms. The proposed IASS algorithm encryption and decryption execution time are 50ms and 43ms.

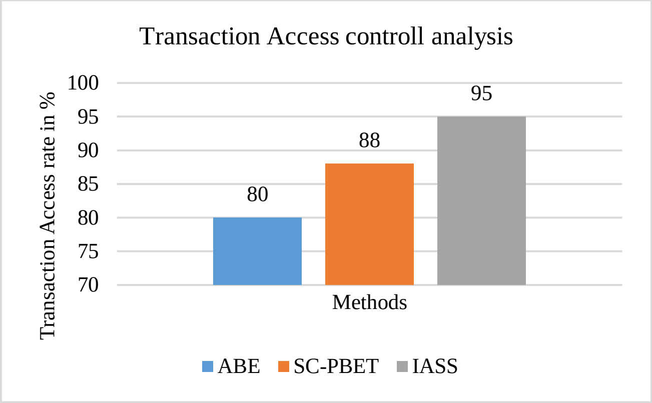

Figure 6: Transaction Access control analysis performance

Transaction Access control analysis performance comparison results are shown in figure 6. The proposed IASS algorithm performance is 95%,

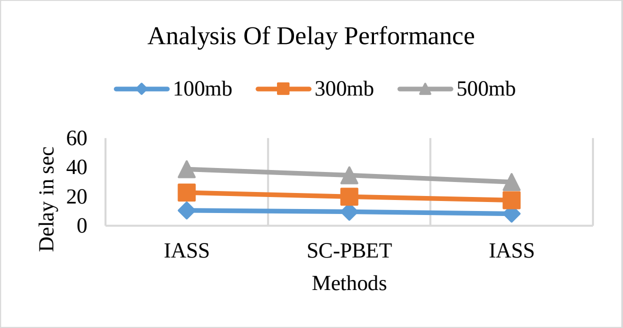

Figure 7: Delay performance

Figure 7 defines the analysis of delay performance comparison results. The proposed IASS algorithm has 12.1 sec for a 500 MB file size. Similarly, the previous algorithm is better than the previous methods.

***Article Received**: 20 December 2022 **Revised**: 28 January 2023 **Accepted**: 04 February 2023*

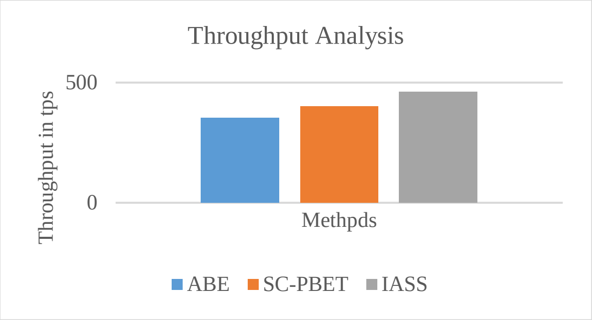

Figure 8 Throughput Analysis

The comparison of the throughput analysis is presented in figure 8. In this analysis of the proposed method, the IASS method has a 460tps higher transaction throughput rate than other existing methods.

V. CONCLUSION

To conclude patient privacy in the EHR system on the blockchain, IASS introduces multiple agents whose signatures meet the blockchain architecture's requirements and guarantee the information's anonymity and immutability. It is required between authorities, and the patient's private key must be constructed. Dishonest officials cannot scheme in the attacks. Finally, further down the signature standard, the protocol's security is proven in terms of ability and perfect confidentiality. Comparative analysis shows that the effectiveness and cost of this protocol increase proportionally with the number of admissions and patient attributes. Predictors can improve the predictor expressions in many distributed computing applications. A direction for future work is to support assertions common to blockchain technology.

REFERENCE

[1] K. Intawong, P. Ong-artborirak and W. Boonchieng, "Seamless Electronic Medical Record for Health Management System in Emergency Patients," 2021 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunication Engineering, 2021, pp. 189-192.

[2] T. Lyu and C. Liang, "Predict Pregnancy Outcomes in the COVID-19 Pandemic Using Electronic Health Records and Machine Learning Approach," 2022 IEEE 10th International Conference on Healthcare Informatics (ICHI), 2022, pp. 483-483, doi: 10.1109/ICHI54592.2022.00079.

[3] H. Zhou et al., "Annotating Music Therapy, Chiropractic and Aquatic Exercise Using Electronic Health Record," 2022 IEEE 10th International Conference on Healthcare Informatics (ICHI), 2022, pp. 610-611, doi: 10.1109/ICHI54592.2022.00121.

[4] Shahnaz, U. Qamar and A. Khalid, "Using Blockchain for Electronic Health Records," in IEEE Access, vol. 7, pp. 147782-147795, 2019, doi: 10.1109/ACCESS.2019.2946373.

[5] G. Wu, S. Wang, Z. Ning and B. Zhu, "Privacy-Preserved Electronic Medical Record Exchanging and Sharing: A Blockchain-Based Smart Healthcare System," in IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 5, pp. 1917-1927, May 2022, doi: 10.1109/JBHI.2021.3123643.

[6] S. Niu, L. Chen, J. Wang and F. Yu, "Electronic Health Record Sharing Scheme With Searchable Attribute-Based Encryption on Blockchain," in IEEE Access, vol. 8, pp. 7195-7204, 2020, doi: 10.1109/ACCESS.2019.2959044.

[7] Y. Zhuang, L. R. Sheets, Y. -W. Chen, Z. -Y. Shae, J. J. P. Tsai and C. -R. Shyu, "A Patient-Centric Health Information Exchange Framework Using Blockchain Technology," in IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 8, pp. 2169-2176, Aug. 2020, doi: 10.1109/JBHI.2020.2993072.

[8] A. Mamun, S. Azam and C. Gritti, "Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction," in IEEE Access, vol. 10, pp. 5768-5789, 2022, doi: 10.1109/ACCESS.2022.3141079.

[9] P. P. Ray, B. Chowhan, N. Kumar and A. Almogren, "BIoTHR: Electronic Health Record Servicing Scheme in IoT-Blockchain Ecosystem," in IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10857-10872, 1 July1, 2021, doi: 10.1109/JIOT.2021.3050703.

[10] Z. Pang, Y. Yao, Q. Li, X. Zhang and J. Zhang, "Electronic Health Records Sharing Model Based on Blockchain With Checkable State PBFT Consensus Algorithm," in IEEE Access, vol. 10, pp. 87803-87815, 2022, doi: 10.1109/ACCESS.2022.3186682.

[11] R. G. Sonkamble, S. P. Phansalkar, V. M. Potdar and A. M. Bongale, "Survey of Interoperability in Electronic Health Records Management and Proposed Blockchain Based Framework: MyBlockEHR," in IEEE Access, vol. 9, pp. 158367-158401, 2021, doi: 10.1109/ACCESS.2021.3129284.

[12] Haddad, M. H. Habaebi, M. R. Islam, N. F. Hasbullah and S. A. Zabidi, "Systematic Review on AI-Blockchain Based E-Healthcare Records Management Systems," in IEEE Access, vol. 10, pp. 94583-94615, 2022, doi: 10.1109/ACCESS.2022.3201878.

[13] T. F. Stafford and H. Treiblmaier, "Characteristics of a Blockchain Ecosystem for Secure and Sharable Electronic Medical Records," in IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1340-1362, Nov. 2020, doi: 10.1109/TEM.2020.2973095.

[14] F. Tang, S. Ma, Y. Xiang and C. Lin, "An Efficient Authentication Scheme for Blockchain-Based Electronic Health Records," in IEEE Access, vol. 7, pp. 41678-41689, 2019, doi: 10.1109/ACCESS.2019.2904300.

[15] J. Sun, X. Yao, S. Wang and Y. Wu, "Blockchain-Based Secure Storage and Access Scheme For Electronic Medical Records in IPFS," in IEEE Access, vol. 8, pp. 59389-59401, 2020, doi: 10.1109/ACCESS.2020.2982964.