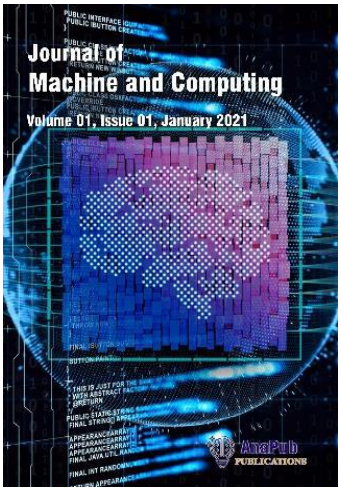
Journal Pre-proof

Design and Development of EHR Patterns in Local Blockchain Computing Layers for Privacy Enhancing Techniques



Namrata Bathli and Shantaladevi Patil

DOI: 10.53759/7669/jmc202505163

Reference: JMC202505163

Journal: Journal of Machine and Computing.

Received 21 January 2025

Revised from 12 April 2025

Accepted 18 July 2025

Please cite this article as: Namrata Bathli and Shantaladevi Patil, ‘‘Design and Development of EHR Patterns in Local Blockchain Computing Layers for Privacy Enhancing Techniques”, Journal of Machine and Computing. (2025). Doi: https:// doi.org/10.53759/7669/jmc202505163.

Design and Development of EHR Patterns in Local Blockchain Computing Layers for Privacy Enhancing Techniques

Namrata Bathli, Shantaladevi Patil
School of Computer Science and Engineering,
REVA University, Bengaluru,India
namratakottursheттar@gmail.com shantaladevi.patil@reva.edu

Abstract – The privacy of EHR is at most concern and challenging as the records are shared and validated across multiple users and databases. In this proposed system the databases at local servers (independent hospitals) are co-aligned to form a local database network, integrated via multiple hospitals from distributed geographical locations. The proposed framework is subjected with a local integration unit (LIU) for extracting and mapping local attributes at LIU. The process is further associated with attribute extraction and attribute occurrence mapping. The process of attribute weight and occurrence mapping is subjected with local integration block chain generation (LIBG). The LIBG blocks are framed with attribute mapping with respect to the attribute occurrence ratio. The objective is to generate a smarter and simplified privacy enhancer module at local server of blockchain to end-user security. The technique has secured an accuracy of 97.48% in attribute mapping with respect to occurrence.

Index Terms – IoMT, blockchain, privacy, local dataset distribution, attribute mapping, attribute occurrence ratio.

I. Introduction

Medical data and records processing is a challenging task and the demand for extensive medical record i.e. Electronic Medical Records (EMR) processing and analysis drives the industry of near future. According to [1] the rapidly evolving technology and advancements have driven a change in policy drafting standards of electronic medical records (EMRs). According to Stanford medicine, a white paper "Future of Electronic Health Records",[2] the integration of artificial intelligence and machine learning for personalized healthcare shall be the near future of medical research. For a supportive and sustainable medical ecosystem, a need for secure data-communication channel is required. In this paper, the research is focused on the process of defining and streamlining the EMR generation and integration process using a blockchain framework.

Technically, the blockchain framework is supported with the interoperability between the systems and servers for multiple purposes. Thus including to improve the security of the blocks and nodes connected under the defined channel. The purpose of calibration is to support and collaborate with multiple users across geographical locations to develop an inclusive framework. In this paper, the proposed blockchain

framework is developed on the principles of building a reliable ecosystem of data transferring via an enhanced privacy standard. The proposed standard's policies are defined and monitored by the distributed learning framework supported under the ages of federated learning (FL). The federated learning models are included on the local edge servers, which are distributive in nature.

The objective of the proposed system is as follows

- To develop a sustainable and supports interoperability blockchain framework for primary medical records/data transfer.
- The proposed system has enhanced the privacy element of the blockchain which internally influences the strengthening of interoperability policies
- The system has incorporated a distributive learning i.e. federated learning approach for edge based data computation and block-generation

The overall framework is supported on the principles of localization of data and hence preserving the data origin sources. The datasets included in this experimental setup is supported via the open source datasets such as Medical Information Mart for Intensive Care (MIMIC) and Observational Medical Outcomes Partnership (OMOP) common dataset model. These datasets each attribute is treated as a tuple of information, further customized for building and enhancing the block or nodes with a linkage of data origin and data dependencies. The blockchain framework is further supported and customized in the proposed framework is developed on light-weight processing i.e. edge-AI processing for effective data transfer via FL ecosystem. The manuscript is organized with an introduction to the scope and relevance of the proposed system in introduction section I, followed by a detailed and recent developments in section II. The proposed methodology is discussed in section III followed by a mathematical model in section IV. The outcome, observations and discussion on results is summarized in section V followed by a formal conclusion in section VI.

II. Literature Reviews

Electronic Health Records [3] are the details of Patients stored in digital format. The details includes all the tests they went through in terms of the Patients history, meditations underwent, diagnosis reports, Scans etc. One of the advantage of EHR is that it will be instantly available for the Doctor's/ any health Stakeholders to study the insights of the Patients, which is real-time and can be achieved seamlessly. This draws a line between a Stake holders and the Clients in terms of Privacy as it may be misused. On the other part of equation Block chain is the ground-breaking technology which allows decentralized and distributed Communication across the nodes of a network. It has the capability to overcome the problems associated with EHR by providing secure, safer and decentralized platform to exchange the health data. In this paper researchers have found 3 categories of Block chain based Potential Solutions to carry EHR: Conceptual, Prototype and implemented.

In [4] the authors are discussing on the interoperability policies for EHR such as HIPAA and HL7, these policies provide national and international standards of operations derived from latest literature reviews. This paper assures an ease in EHR sharing and data interoperability via mobilizing common attributes.

In [5] (IPFS) Inter Planetary File System which is temper proof model of Block Chain used in HER, which deals with the severe security issues when associated with (CSP) Cloud Service Provider. [6] These research Paper uses a Deep Learning based diagnosis model (HBESMD-DLD) which is a new hyper ledger Block Chain medical management approach to deal with the issue of the Owner/Admin whom to provide the access for the medical data.

[7] In this Paper, the authors have Proposed Patient Controlled EHR Scheme with the Collaboration of Cloud Computing and Block Chain Technology. (sc-PBFT) a node state checkable Practical Byzantine Fault Tolerance algorithm is used to check the fine grain access control. [8] General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA) are used to help minimize the health data breaches. In [9] they carry out a systematic survey on four questions, How to achieve Interoperability?, What are the different Privacy preserving Techniques in Storage of EHR?, How Block Chain is Secure for sharing the information?, What is the state of art of sharing the interoperability in EHR? A framework MyBlockEHR is proposed to address all of the research gaps. [10] This paper launches log creation with Modified Merkle tree structure for safe transmission of data between the providers, to update the information, and quick access to the medical records. [11] Along with IPFS, ABAC (Attribute-Based Access Control) Conceptual Model was designed based on Block Chain Technology, which helps in case of any emergency to access the whole history of patient as early as possible. In [12] an EHR Chain, a Block chain based approach using attribute-based and homo morphic cryptosystem is used to solve the issues of safe storage, reliable sharing and Privacy Protection by controlling the access.

III. Methodology and materials

The proposed system is developed with the objective of developing a secure local blockchain framework to support and compute inter-data privacy operations on standard block creations. The process of interdependency is further validated and processed in configuration multisource networking datasets. Primarily, the operation of multisource coordination is validated under local datacenters and administrators. The orientation of dataset is further recommended and monitored via centralized (local) datacenters such as hospitals and datacenters maintained by local authorities. The operating process is justified and processed with local firewall rules for data storage and data accessing in these servers (data centers) under the operational value paradigm, the customization of dataset values are archived in the patient centric approach.

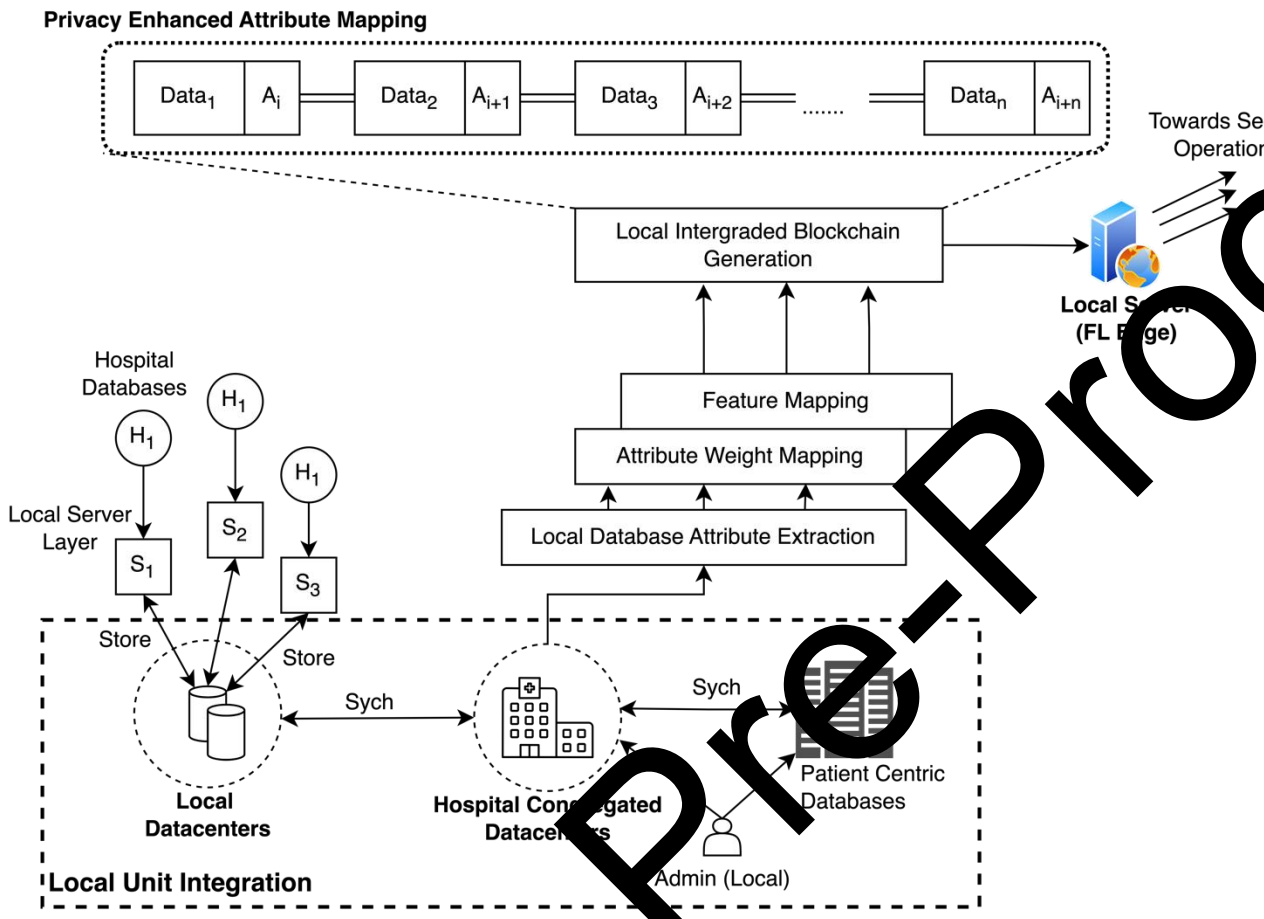


Fig. 1: Block diagram of local at ute enhanced blockchain creation of medical datasets

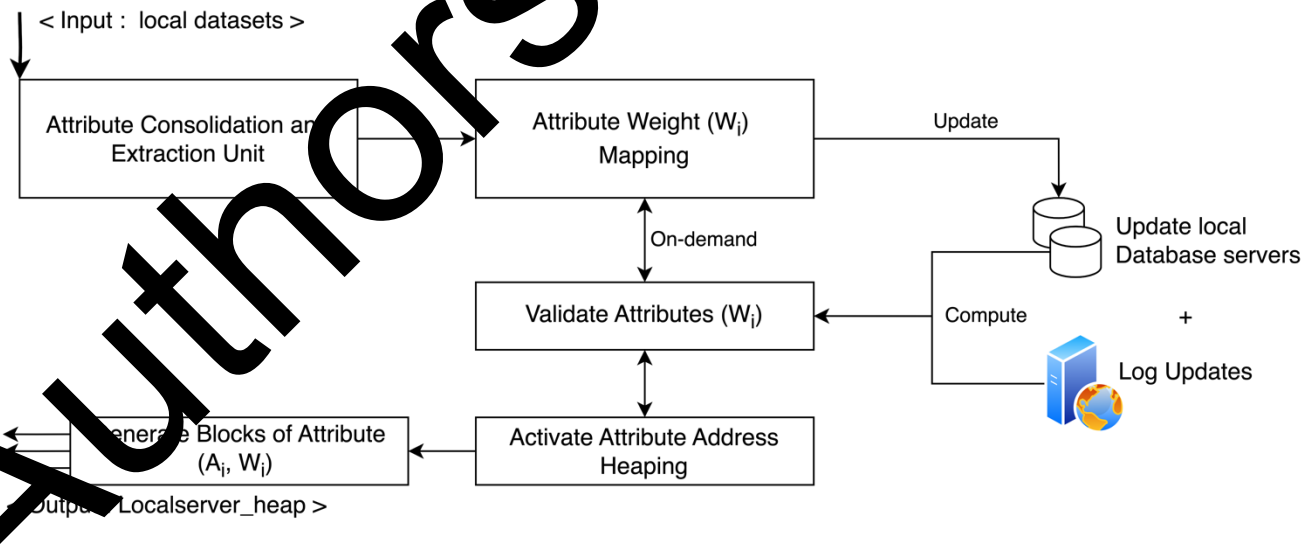


Fig. 2: Privacy enhanced chain operation of proposed system

At this stage, the processing of datasets (i.e.) incoming dataset values from multiple servers is stored and operated at centralized access authorizing particular authorities of hospital or datacenters. Primarily, the operations are further processed in local segmentation is supported by assigning dynamic range weights on the attributes such that, the most alike attribute heap indexing is achieved and processed to retrieve feature mapping. The feature mapping process further evaluates and extracts the interdependency matrixes of attributes and they aligned features for extractive validation of weight matrix. The features integrates a local generated blockchain framework for aligning blocks and its addresses are shown in Fig. 1. The extracted blockchain is represented as "data-blocks" aligned with attribute consolidation process is streamlined in Fig. 2 with stream of input data followed and aligned with extracted weights generated in the blocks as the output accordingly.

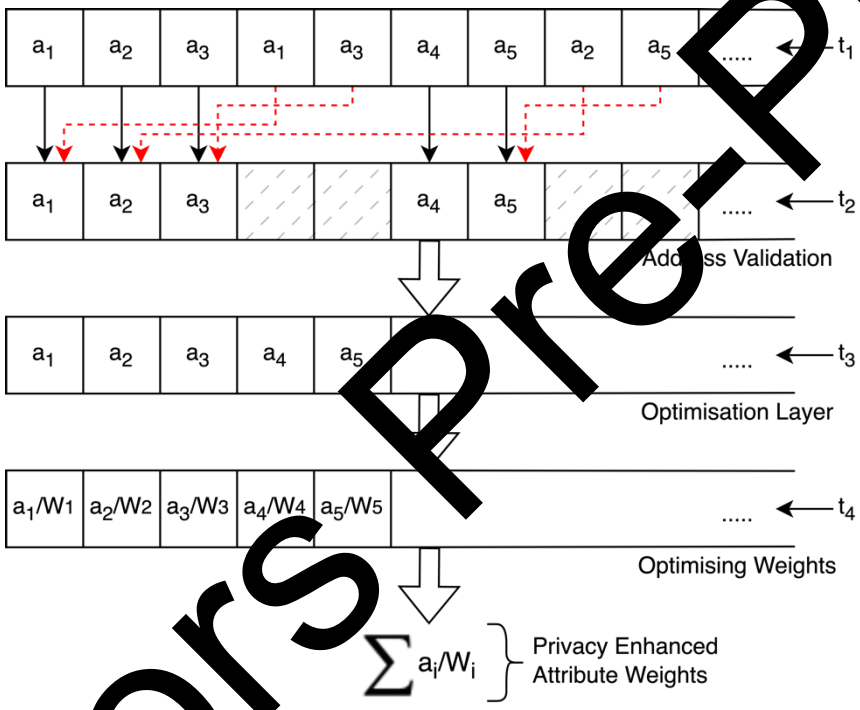


Fig. 3: Similar attributes mapping and heap-addressing for local blockchain generation

The attributes associated weight and optimization is reflected in Fig. 3. The process associates the matrix value of each inter-active attribute with address weight as "address validation and heaping process". The successive process is the further optimized with the address redundancy mapping. The end-result of the process is a stream of optimizing weights and associated attributes for effective blockchain creation. This summarizing the attributes and the origin priority of the same with interdependency mapping of attributes and weights are aligned. Further the blocks (local) can be streamlined in the creation of external blockchain for de-centralized processing.

IV. Mathematical Model

A. Multisource local attribute extracting and hashing

The proposed technique is aligned with creation of local blockchain models for effective privacy preservation and mapping. The process is initiated with multidimensional and multi-source datacenters coordination. Consider the common database unit as (D_U) such that supporting databases such as $(D_{U1}, D_{U2}, D_{U3}....D_{Un})$ are added. The databases are further supported and mapped with independent sources (S_i) such that $(\forall D_{Ui} \in S_j)$ where (i) is database and (j) is the sources such as hospitals, medical centers and datacenter archives etc. thus $(\forall D_{Ui} \in D_{Uj})$ if $(D_{Ui} \subseteq D_{Uj})$ and both $(D_{Ui}, D_{Uj} \in \ldots)$ the extent of database customization.

On the customization values of databases (D_{Ui}) there exist a hash function (f_i) aligned to represent the independent database instances as $(\forall f_i \in D_{Ui})$ such that if $(f_i \neq f_j)$ then function values of customization is reflected and blocked from further pairing. The independency database (D_{Ui}) and associated function (f_i) are reflected as $(\forall D_{Ui} \Rightarrow f_i)$ and refers to independent attributes (a_i) where each attribute is assigned and reflected with the instances of occurrences (θ) as $(\forall a_i \in \theta \in t_i)$ where (t_i) is the time interval for propagating attribute values, representing the association of occurrence as shown in Eq. 1.

$$\|\theta\| \Rightarrow \sum_{i=1}^{n} (D_{Ui}) \oplus \left(\frac{\delta(a_i)}{\delta t} \right)_{f_i} \tag{1}$$

$$\|\theta\| \Rightarrow \sum_{i=1}^{n} \left(\sum_{j=i+1}^{n} \left(D_{Ui} \bigcap D_{Uj} \right) \oplus \left\lfloor a_{i.} \right\rfloor \right)_{fi}^{fj} \tag{2}$$

From Eq. 2, the order of (D_{Ui}, D_{Uj}) is associated with attribute set $(a_{i.}, a_j)$ such that the occurrence ratio extracts repeated attribute values from each supporting database (D_U) and appending the minimal hash_function $(f_{i.,j})$ with a range of associated addresses. The address vectors are further generalized with each hash_function associated as shown in Eq. 3.

$$\left[f_{(a_{i.})} \| f_j(a_j) \right]_{(i,j)} \in D_{Ui} \tag{3}$$

The ratio of understanding is bounded within the occurrence scope of hashing function (Δf) and summarizing to the function at (t_i) interval. On consideration, the functional value of (f_i) and (f_j) are

interdependent at (Δt_i) such that $\left(f_i \oplus f_j \Rightarrow t_i\right)$ and $\left(\Delta f_i \oplus \Delta f_j \Rightarrow t_j\right)$ where (t_j) is initial time frame for database synchronization and (t_j) for collective instances of time accordingly. The hashing function (Δf) can be further represented as shown in Eq. 4.

$$\Delta f = \left[\int_0^n f_i \cup f_j\right] \oplus \left\{\sum_{i=1}^{\infty}\sum_{j=i+1}^{n} \overrightarrow{(D_{Ui})_{\Delta ti}} \oplus \|\theta\|_j\right\} \tag{4}$$

$$\therefore \|\Delta f\| = \|f_i - f_j\|_{(i,j)} \cup \left\{\sum_{i=1}^{\infty}\sum_{j=i+1}^{n} \overrightarrow{(D_{Ui})} \cap \|\theta\|_j\right\} \tag{5}$$

$$\therefore \|\Delta f\| = \|f_i - f_j\|_{(i,j)} \cup \left\{\sum_{i=1}^{\infty} \overrightarrow{(D_{Ui})} \oplus \frac{\delta\|\theta\|_j}{\delta t_i}\right\} \tag{6}$$

Thus according to the order of $\|f\|$, the hashing function can be re-assigned and calibrated with respect to the time (Δt) as shown in Eq. 5 and Eq. 6 respectively. Suppose the database (D_U) at (i^{th}) interval is aligned with multiple hashing function, the resultant requires the process to be minimized and associated with in the scope of (Δt) and ranging $(\Delta f_i), (\Delta f_j)$ such that $\left(\forall \Delta f \Rightarrow \|f_i - f_j\|\right)$ bounded at the time (Δt) .

B. Weight Matrix Distribution and Optimizing

The extracted paradigm of blocks (isolated units) are further reflected and supported via the weight matrix assignment and coordination. The proposed technique fetches the distributed weights (w_x) is aligned on the individual hashing function $\|f_i\|$ with connected dataset attributes are remapped and co-aligned accordingly. The resultant function values, result in a generic hashing function (Δf_{wx}) such that $\left(\forall w_{xi} \Rightarrow \|\Delta f\|\right)$ at given phase. The orientation of each $\|\Delta f_i\|$ is bound with attribute occurrences (θ_{ai}) as shown in Eq. 6. Thus expanding further towards the feature-attribute based hashing creation is shown as Eq. 7.

$$\Delta w_x = \|\Delta f\| \oplus \lim_{n\to\infty}\left[\frac{\left(\Delta a_{0x}\right) \oplus \left(\Delta a_{0(x+1)}\right)}{\Delta t}\right] \tag{7}$$

$$\therefore \Delta w_x = \|\Delta f\| \oplus \lim_{n\to\infty}\left[\sum_{i=1}^{n}\sum_{j=i+1}^{n-1}\left(\frac{\left(\Delta a_i\right) \oplus \left(\Delta a_j\right)}{\|f_i - f_j\|}\right)\right] \tag{8}$$

Thus according to Eq. 7, the resultant value of demonstrated attribute is reflected and aligned with the supporting matrix of weight and further associated with chain of heap addressing i.e. hashing addresses $\|\Delta f\|$ such that the association of weight (w_x) is resultant vector of each defined attribute resulting in series of blockchain creation as demonstrated in Fig. 3. The attribute alignments are represented within the ratio of weights as shown in Eq. 9.

$$(\Delta f_i)_t \Rightarrow \lim_{\delta x \to 0}\left(\sum_{i=1}^{n}\sum_{j=i+1}^{n}\left\{\frac{\delta(a_i)}{\delta(w_i)} \oplus \frac{\delta(a_j)}{\delta(w_j)}\right\}\|\Delta f\|\right) \tag{9}$$

$$\therefore (\Delta f_i)_t \Rightarrow \lim_{\delta x \to 0}\left(\sum_{i=1}^{n}\sum_{j=i+1}^{n}\left\{\frac{\delta(a_i) \Leftrightarrow \delta(a_j)}{\delta(w_i \oplus w_j)}\right\} \cap \|\Delta f\|\right) \tag{10}$$

Thus according to the hashing value, occurrence of attributes (a_i) and (a_j) should be aligned within the ratio of weight matrix assigned to it accordingly. The Eq. 9 represents the attribute sighting of weights in multiple orders of coordination and alignment. The explanation of Eq. 9 is demonstrated in Eq. 10 to support the correlative existence of (a_i) and (a_j) as similar entity of blocks and further associating it to the aligned weight (w_i) such that hash_function $\|\Delta f\|$ is constantly synchronized. The generalized representation of intermediate blocks is $(a_i w_i \oplus a_{i+1} w_{i+1} \oplus a_{i+2} w_{i+2} ....)$ with each block represents the supporting hashing value associated as $\|a_n w_n\| = \sum(\Delta f_n)$ where each associated value of (Δf_n) is customized and bound with the associated blocks. The further representation is aligned in Eq. 11.

$$\|\sum f_n\| \Rightarrow \|a_i w_i, a_i w_j ..... a_n w_{i+n} .... a_i w_n ..... a_n w_n\| \tag{11}$$

The Eq. 11 represents the multiple scenarios of attribute, weight alignment and order of justification before the blocks are assigned to external servers via blockchain address sourcing approach. The aligned order of information i.e. $\sum(\Delta f_n)$ are further aligned with $\|\Delta f\|$ and at (t_j) scenario the $\sum(a_n w_{i+n})$ is also assigned and reflected to $\|\Delta f\|$ and so on until the value of $\sum(a_i w_i)$ instances are occurring in the scenario.

C. Customizing blockchain privacy and enhanced indexing

In this phase, the customizing blockchain instances from multiple $\sum(a_i w_i)$ values are coordinated and congregated to form a relatively higher order of blockchain matrix. The privacy of proposed system is improved with respect to the attribute, corelationship mapping. The attributes matrixes are further associated and revalidated within a common value as the threshold value is within the range of incoming

attributes, i.e. $\left[\left\|a_i\right\| \le \left\|\Delta \mathrm{T}\right\| \le \left\|a_j\right\|\right]$ where $\left\|a_j\right\|$ is an independent attributes and $\left\|\Delta \mathrm{T}\right\|$ is the thersholding vector to align the weights as shown in Eq. 12.

$$w_x \Rightarrow \arg\max\left(\Delta \mathrm{T}\right) \oplus \left\{\left\|\Delta a_i\right\|_{t1} \oplus \left\|\Delta a_j\right\|_{t2} .....\right\} \tag{12}$$

$$\therefore \sum w_x \Rightarrow \arg\max\left(\Delta \mathrm{T}\right) \oplus \left\{\sum_{i=1}^{n} \sum_{j=i+1}^{n} \left(\left\|\Delta a_i\right\|_{\Delta t_j}\right)\right\} \tag{13}$$

Thus within the range of computation, the summarization values of $\left(w_x\right)$ is resultant in the series of $\left\|a_i\right\|$ occurrences and hence $\left(w_x = w_{x1}, w_{x2}, w_{x3} ... w_{xn}\right)$ is simulated and orchestrated accordingly. The weight $\left(w_{xi}\right)$ assures the associated matrixes such as $\left\|a_i .....a_n\right\|$ are secured and the original source is customized for the relative expansion of blockchain entity for external indexing. The external indexing of information from local servers is now available for global reach. In this manuscript the blockchain interdependency is retrieved by the order of privacy preservation of internal attributes. The resultant blockchain $\left(\mathrm{B}\right)$ is demonstrated as below.

$$\mathrm{B} = \left\|\Delta f\right\| \le \left[\lim_{\delta x \to 0}\left(\sum_{i=1}^{\infty} \sum_{j=i+1}^{n}\left(\frac{\delta\left(a_i\right) \to \delta\left(a_j\right)}{\delta\left(w_j\right)}\right) \Rightarrow a_i\right)\right] \tag{14}$$

The alignment matrix is resultant of information processing with hashing value selected within the scope of incoming attributes $\left(a_i, a_j, ..., a_n ...\right)$ provided if $\left(a_i\right)$ is pre-existing the values of $\left(a_j\right)$ at $\left(a_j \to \Delta \mathrm{T}_i\right)$ is remapped with $\left(a_i\right)$ in accordance to the supporting vector as $\left(a_i, a_j\right) \Rightarrow \left(\Delta \mathrm{T}_i\right)$ and $\left(\Delta \mathrm{T}_i \Rightarrow a_i\right)$. The interdependencies as further evaluated and resultant blockchain $\left(\mathrm{B}\right)$ is created as demonstrated in Eq. 14.

The scenario of development is reflected within the scope of $\left(\mathrm{B}\right)$ evaluation (i.e.) if $\left(\mathrm{B} \in \Delta f_x\right)$ and at $\left(\Delta t_j / \mathrm{B} \in \Delta f_x\right)$ then the correlated blockchain is interconnected at the junction of $\left(\mathrm{B}\right)$ with respect to $\left\|f_x, f_y\right\|$, the validation is further resultant of multiple order of $\left(\mathrm{B}\right)$ instance in external server (i.e.) interim via third party replication policies. Hence the $\left(\mathrm{B}\right)$ generated is co-aligned with similar blockchain in external sources, the order of expansion and alignment is detailed in results section with respect to implementation scope and validation process of proposed blockchain.

V. Results and Discussions

The proposed system has integrated the federated learning policies of the distributed server computing. These servers are treated as individual edge devices associated in the network of computation. The consent and coordination of data transfer and data immigration is channeled via a stream of computing devices of edge-servers via the integrated AI such as block-classification, log clustering and attribute dependency mapping. In the proposed system, the attribution of local attributes is extracted and mapped with the external ratios with a block 0^{th} instance as shown in Fig. . The representation is an initial phase of integrating blocks and its associations with reference to the blockchain formation. Similarly the progression of blocks is associated with the blockchains formation as represented in Fig. 5. The hash_table addressing is further associated to retain the stability of multiple-nodes/bocks originating from a given source.

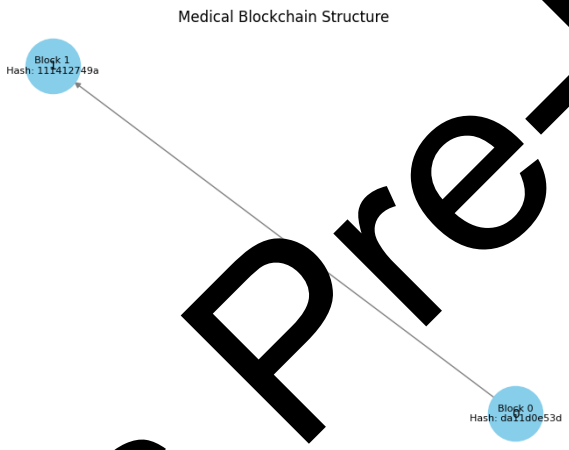


Fig. 4: Single Chain node-node model creation (initial phase)

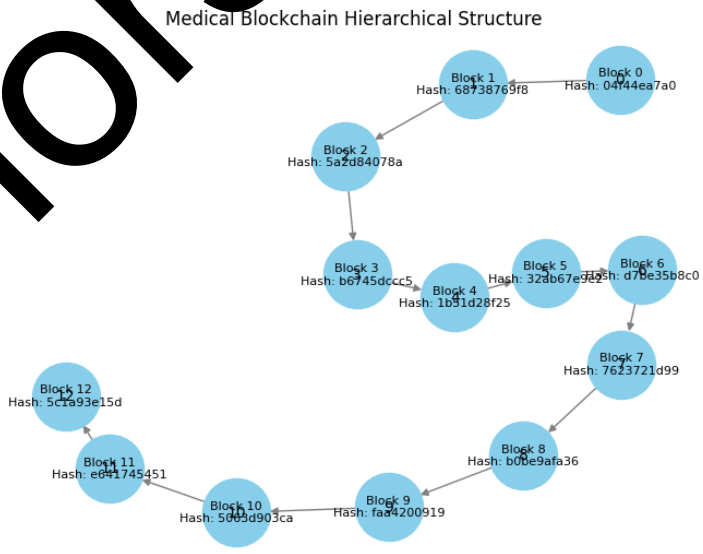


Fig. 5: Interconnected block-chain nodes (Connection phase)

The interdependencies of each block is associated with the attributes and the common dependency features as shown in Fig. 6. These interconnected blocks are further paradigm to retrieve a series of hashing addresses with reference to the attributes. The mapping further is aimed to classify the corresponding instances with relatively similar attribute weights and scoring as defined in the mathematical section, such that the thresholding weight vector of each instance is extracted and retrieved. The resultant vector of the blockchain is represented in Fig. 7. The 'red' blocks highlight the dependency attributes of each node, whereas the 'blue' blocks/nodes are independent from the source of origin. Thus, on the interdependency attributes (i.e. red nodes), the heap_addressing table initiates the assignment of dedicated addresses. Such that, the stream of attributes in blockchain (i.e. patient_id, disease, treatment type etc. are represented and thus improvising the privacy of interconnected attributes from the independent blocks/nodes resulting in security enhancement.

For ease in representation, the attributes such as 'Doctor_ID', 'Patient_ID', 'Treatment', and 'Diagnosis' is considered for the computational purposes. In Fig. 8, the heap matrix is represented with respect to the assignment and the probability of mapping with blocks and further generating the privacy enhanced models (via blockchain and FL policies). Each block is represented with a heap_address and the source of origin to provide a customized representation for ease in computation. The representation of the indivial block with respect to a given time (t), the instance is locked and framed in a given attributes (single). The single attribute value associated with the instance of blocks are further represented and streamlined to demonstrate the trailing link of "Source Origin".

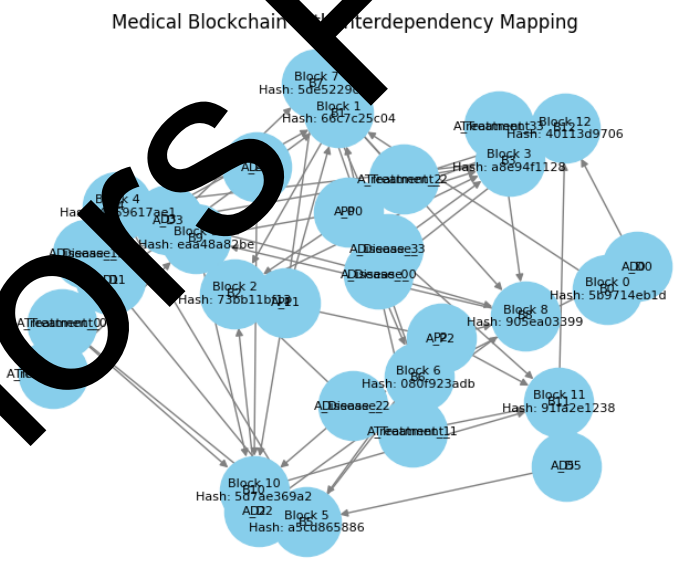


Fig. 6: Node-to-node cross-connecting in blockchain operation

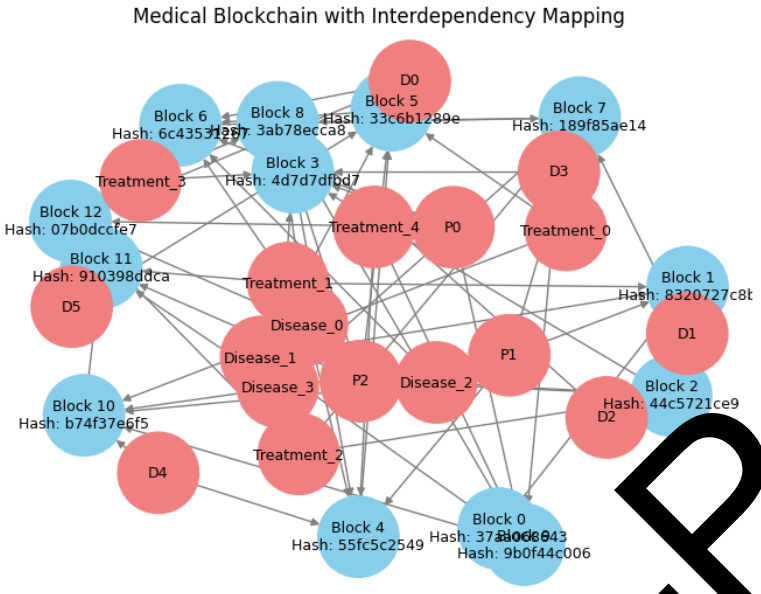


Fig. 7: Node-to-node cross-connecting in blockchain operation with priorities

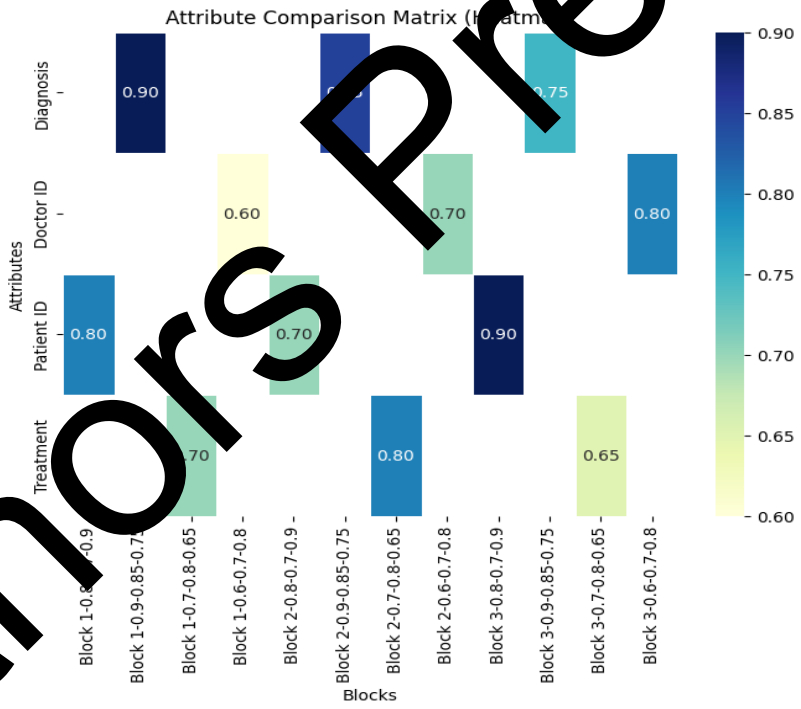


Fig. 8: Heap map validation of the nodes and blocks for probability validation

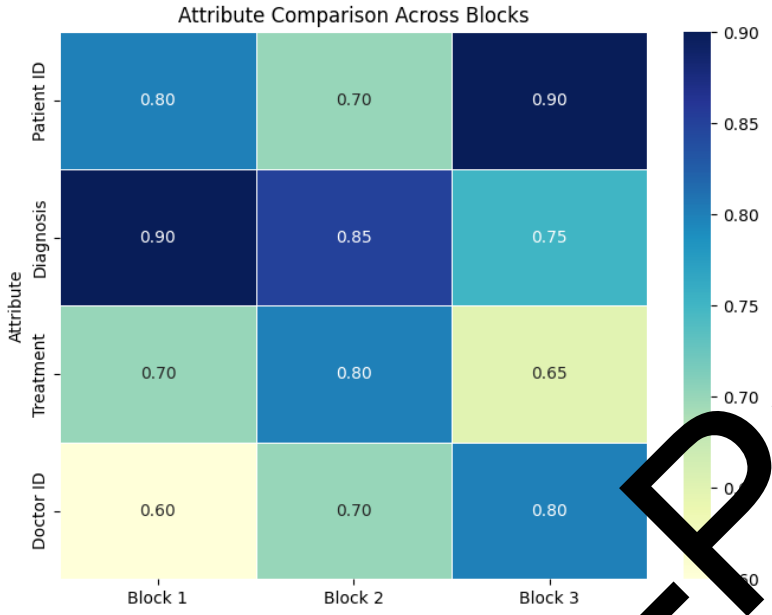


Fig. 9: Attribute comparison across blocks and validation

In Fig. 9, the comparison of attributes with respect to the individual blocks is demonstrated. The probability of relationship mapping and indexing is reflected within a block across all the associated attributes, for ease in representation we have considered three independent blocks and they association matrixes with the predefined attributes i.e. Doctor_ID, Patient_ID, Diagnosis, and Treatment. The ratio of independent probability is analysed and validated to assure the attributes (given) are completely associated with the blocks such that, the minimal diversion of attribute-missing is reported. Through this process of indexing, the second-order of mapping is extracted and customized in the overall block-chain framework.

VI. Conclusion

The proposed blockchain model has featured improved privacy optimization policies for secure EHR data transmission. The validation is resultant of multi-dimensional and multi-source EHR data configuration and indexing into a single indexed array via hashing address mapping. The technique has demonstrated a higher order of data processing with respect to blockchain via internal sources and collaborative attribute mapping. The supporting values of dependencies are bound with interconnected attribute occurrence ratios (i.e.) a correctness is performed on the incoming internal source attributes to correlate and map with most related and in-range threshold values. The outcome is subjected on internal privacy preservation policies development and further associated with blockchain generation. The proposed technique has demonstrated the accuracy of 97.48% in building and binding the primary internal attributes across global blockchain ratio. In near future the proposed technique can be expanded with dynamic attribute corelationship mapping and coordination for effective blockchain optimization.

References

1. Melton, G. B., McDonald, C. J., Tang, P. C., & Hripcsak, G. (2021). Electronic health records. In *Biomedical informatics: computer applications in health care and biomedicine* (pp. 467-509). Cham: Springer International Publishing.
2. Stanford Medicine. (2018). The future of electronic health records: A vision for 2028 [White paper]. https://med.stanford.edu/content/dam/sm/ehr/documents/SM-EHR-White-Papers_v12.pdf
3. Al Mamun, A., Azam, S., & Gritti, C. (2022). Blockchain-based electronic health records management: a comprehensive review and future research direction. *IEEE Access*, *10*, 5768-5789.
4. Reegu, F. A., Abas, H., Gulzar, Y., Xin, Q., Alwan, A. A., Jabbari, A., ... & Dziyauddin, R. A. (2023). Blockchain-based framework for interoperable electronic health records for an improved healthcare system. *Sustainability*, *15*(8), 6337.
5. Ramesh, D., Mishra, R., Atrey, P. K., Edla, D. R., Misra, S., & Qi, L. (2023). Blockchain based efficient tamper-proof EHR storage for decentralized cloud-assisted storage. *Alexandria Engineering Journal*, *68*, 205-226.
6. Pang, Z., Yao, Y., Li, Q., Zhang, X., & Zhang, J. (2022). Electronic health records sharing model based on blockchain with checkable state PBFT consensus algorithm. *IEEE Access*, *10*, 87803-87815.
7. Pang, Z., Yao, Y., Li, Q., Zhang, X., & Zhang, J. (2022). Electronic health records sharing model based on blockchain with checkable state PBFT consensus algorithm. *IEEE Access*, *10*, 87803-87815.
8. Ettaloui, N., Arezki, S., & Gadi, T. (2023, November). An overview of blockchain-based electronic health record and compliance with GDPR and HIPAA. In *The International Conference on Artificial Intelligence and Smart Environment* (pp. 405-412). Cham: Springer Nature Switzerland.
9. Sonkamble, R. G., Phansalkar, S. P., Potdar, V. M., & Hiwale, A. M. (2021). Survey of interoperability in electronic health records management and proposed blockchain based framework: MyBlockEHR. *IEEe Access*, *9*, 158367-158401.
10. Chelladurai, U., & Pandian, S. (2022). A novel blockchain based electronic health record automation system for healthcare. *Journal of Ambient Intelligence and Humanized Computing*, *13*(1), 693-703.
11. Saberi, M. A., Adda, M., & Mcheick, H. (2022). Break-Glass Conceptual Model for Distributed EHR management system based on Blockchain, IPFS and ABAC. *Procedia Computer Science*, *198*, 185-192.
12. Li, F., Liu, K., Zhang, L., Huang, S., & Wang, (2021). EHRChain: A blockchain-based EHR system using attribute-based and homomorphic cryptosystem. *IEEE Transactions on Services Computing*, *15*(5), 2755-2765.