**Hyperledger blockchain enabled secure medical record management with deep learning-based diagnosis model**

**Abstract**

Electronic medical records are being created in large amounts because of recent advances in the healthcare sector (EHRs). The data owner can manage his or her data and distribute it with certain individuals thanks to the EHR system. Data security and diagnostic procedures are challenging to maintain because of the enormous volume of data in the healthcare system. The HBESDM-DLD model, which combines secure medical data management with deep learning (DL)-based diagnosis to address these problems, is developed in this study. The provided architecture includes many phases of activities such encryption, the development of the best keys, secure data management using the Hyperledger blockchain, and diagnostics. The shown model enables the user to manage data access, allow hospital administrators to read and write data, and notify emergency contacts. It uses the SPECK block cypher algorithm for encryption. A Nutcracker Optimization algorithm (NOA) is used for the SPECK technique's best key generation at the same time to increase its effectiveness. Moreover, the exchange of medical data occurs via the multi-channel Hyperledger blockchain, which uses a blockchain to store information about patient visits as well as linkages to EHRs that are stored in other databases. Finally, a diagnostic model based on Supervised variational autoencoders (SVAE) is used to detect the presence of the illnesses once the data have been decrypted at the receiving end. Using a benchmark medical dataset, the HBESDM-DLD model's performance is validated, and the results are examined using a variety of performance metrics. The experimental data demonstrates the superiority of the HBESDM-DLD methodology over state-of-the-art approaches.

**Introduction**

To effectively handle patient information, the personal health record (PHR) system is an important healthcare industry resolution. The PHR system enables data exchange with healthcare professionals and aids in the predicting of health issues. It holds extremely sensitive data and stores health-related information []. A few inappropriate changes or revisions of certain PHR information might have serious outcomes. Hence, confidentiality becomes a key component of PHR systems. The PHR system needs a tamper-resistant element to function properly. When a person's lifetime health-related data can be gathered and kept in a way that makes it impossible for it to be tampered with, it significantly improves the quality of their personal protection healthcare. Blockchain's immutability, backup, and cryptographic verifiability features might make it a useful tamper-resistant storage option for the PHR system.

The crucial step in obtaining the greatest advantages from an innovative study is data sharing. It is crucial to understand the 3 Ws, or where, what, and when. Before beginning the process of data exchange, these inquiries should be precise. There aren't many operating scopes, and the owner of the data set must offer incentives and rewards. This study demonstrates safe data exchange while utilising blockchain's advantages. Blockchain, a distributed ledger, is a new development in the IT industry.

According to a Silicon Valley specialist, the consensus technique is regarded as an important and vital invention. The removal of unauthorised parties achieves trust, which is a key feature of blockchain technology. Blockchain is currently used in many industries, including health care, IoT, cloud computing, information security, data trade, etc []. The misunderstanding and abuse of information are the key difficulties in this data sharing.

In general, the cloud server is a centralised authority that stores a vast amount of data. A technology called decentralised storage enables data to be kept on several network nodes as a shared ledger. The difficulty is the network nodes' processing and storage limitations. With a storage system based on a decentralised structure and IPFS, data accessibility is ensured. The data owners do not have full access to the data in the architecture as it is now set up. The owner is often excluded from data sharing. For instance, when escrow is independently responsible for payment settlements and data delivery, the owner is a passive entity. Without blockchain, it is extremely difficult to guarantee fund transparency, without which it would be impossible to guarantee reasonable money distribution.

In this scenario, blockchain might offer network nodes transparency and trust for a fair distribution of the money received from the data requestor. If a customer is paying to get the content, on the other hand, integrity and quality of the information may not have partnered.

An exclusive remedy is offered to deal with these issues. In this circumstance, the owner (i.e., patient) manages the dissemination of the health record by keeping out other parties. Information would not be disclosed to other parties if the data owner fixed the access rules. With federated learning (FL), businesses pool their data to create an integrated, complex machine learning model that works as a closed-loop system. In the near future, companies will be able to accomplish amazing things like enhancing consumer data privacy, data security, data-access rights, and access to heterogeneous data thanks to their increased capacity to have deep customer insights. FL enables machine learning algorithms to gain real experience with a variety of distinct datasets that are all spread out across different locations. This method makes it easier to create models that different businesses may collaborate on without having to share sensitive information. The following are some of this article's significant contributions.

* With the use of deep learning (DL)-based diagnosis, the proposed model creates a novel Hyperledger blockchain-enabled secure medical data management (HBESDM-DLD) paradigm.
* It enables the user to manage data access, provide hospital administrators access to read and write data, and notify emergency contacts.
* The SPECK block cypher technology is used in the proposed HBESDM-DLD model to encrypt the medical records.
* By combining the best key generation process with the Nutcracker Optimization Algorithm (NOA), the efficacy of the SPECK approach may be improved.
* Additionally, the Hyperledger blockchain's multi-channel functionality is used for the exchange of medical records.
* The suggested methodology incorporates blockchain technology and the federated learning (FL) idea. A variational autoencoder (SVAE)-based diagnostic model is used in addition to the data decryption procedure for accurate illness diagnosis.
* The experimental findings of the HBESDM-DLD model are evaluated using a variety of performance indicators on benchmark medical datasets.

**Related Works**

This section examines the most cutting-edge blockchain-enabled healthcare systems that have recently been created, with a focus on secure medical data transfer. Nguyen et al. presented a new hybrid strategy using edge cloud and blockchain for data dumping and sharing in healthcare. An efficient data offloading system is first shown, with IoT healthcare data being transmitted to a nearby edge server for privacy-conscious data processing. The next step is leveraging blockchain to connect a data sharing system with data exchange between healthcare clients. In particular, an intelligent contract management offers a trustworthy access control method for obtaining authentication to complete protected EHR distribution. Al Mamun et al. proposed an IPFS-integrated blockchain solution architecture for EMR in the medical industry. It provides access guidelines to various customers and intends to develop a blockchain for EMR. The architecture that is being described safeguards individual privacy while allowing authorised parties, such as healthcare providers, appropriate access to medical data. Bisogni et al. a novel encryption technique that is specifically intended for signing and approving transactions in digital/intelligent contract systems. FaceNet and CNN have jointly developed a biometric key that uses face recognition. Yates [12] presented a brand-new hybrid approach to edge cloud and blockchain-based data offloading and sharing for the healthcare industry. When IoT healthcare data are offloaded in a nearby edge server for processing with privacy attention, an effective data offloading system is first envisioned. The next step is to create a data sharing system for leveraging blockchain to enable data exchange across healthcare facilities. An intelligent contract management primarily introduces a trustworthy access control system for accessing authentication to provide protected EHR distribution. By combining the strengths of blockchain and CC, Huang and Lee [13] were able to establish a privacy protection solution for medical data. This system presents CC and offers a service for blockchain nodes with CC servers where it collects, examines, processes, and preserves medical data in the identity authentication interface and addresses insufficient computing capabilities of a small number of blockchain nodes for verifying consistency and authenticity. Health Chain is a brand-new patient-centred blockchain architecture that was unveiled by Hylock and Zeng [14]. The goal is to improve data curation, controlled data transmission, and person appointment on an interoperable, secure platform. A person can also get a private and public key pair for a cryptographic identity. The blockchain stores the public keys, which are used to protect and validate transactions. The planned system also makes use of revocable intelligent contracts with proxy re-encryption (PRE) to share data while maintaining privacy and secrecy. Sun et al. [15] demonstrated a searchable distributed electronic medical record system that makes use of blockchain technology and intelligent contracting. To ensure the validity and integrity of the electronic medical data, they first perform hash calculations on it and deposit an equal value on then blockchain. The distributed storage technology, IPFS, is then used to encrypt it. Nonetheless, it is best in minimizing the load from data storage and more often accessing to blockchain. This process might resolve the central data storage of the server of numerous medical organizations. After that, a smart contract that uses the keyword search rather than a central third party is employed to understand the encrypted keyword index data stored on the Ethereum blockchain. In order to ensure that attributes can comply with the access rules for decrypting the encrypted data, they also used an attribute-based encryption system. Chen et al. [16] created a cloud-based and blockchain-based storage system for handling individual medical data. A service architecture for exchanging medical records is also shown. None of the parties involved in the shared storage and sharing systems are in a position to influence the process or rely on any third parties. An Identity Mixer and distributed ledger technology-based new EHR management system named PREHEALTH have been suggested (Idemix). a demonstration of a proof-of-concept that uses the permissioned blockchain architecture to mimic the interaction between apps and permissioned blockchains. It is conceivable to develop a system for preserving records while protecting patient privacy and unlikability. Results from the experiments demonstrate the system's viability for wide-scale application. Ekblaw et al. implemented [17] In addition to facilitating data exchange, MedRec makes use of blockchain technologies to provide secure authentication, confidentiality, and accountability. The system's modular design interfaces with the services providers' current local data storage options, enabling interoperability and enhancing the system's flexibility and use. We provide prizes in the form of bitcoin to encourage academics, public health professionals, and others to join the network as blockchain "miners." With this in place, miners may get rewards based on anonymized data while also using Proof of Work to support and maintain the network. In addition to providing vast data to researchers and involving patients and physicians in the decision of whether to make information publicly available, MedRec also empowers data economics. Hyperledger blockchain has an influence on the summary of suggested solutions, as seen in Table 1.

**Literature Survey**

Vora et al. [18] in this paper propose a blockchain-based method for effectively managing and preserving EHRs. This provides a safe and effective way to obtain medical data while also helping to maintain patient privacy.

for service suppliers, clients, and other stakeholders. Our study intends to assess how well the framework can satisfy the needs of patients, healthcare providers, and third parties. It also attempts to determine how well the framework manages to maintain privacy and security while incorporating the burgeoning healthcare 4.0.

This is significant since it addresses both the escrow issue and the blockchain's distributed data storage model [19]. By spreading the pseudorandom function seeds across the authorities and guaranteeing that no more than N - 1 of them are corrupt, the protocol prevents collusion attack by using the computational bilinear Diffie-Hellman assumption, this signature approach is formally demonstrated to be secure. This study provides a hybrid architecture for access management of EHR data that makes use of both blockchain and edge nodes [20]. A blockchain-based controller that simultaneously functions as a tamper-proof log of access events is used to enforce the identification and access control limitations. The second is that EHR data is stored on off-chain edge nodes, which work with access control logs based on blockchain technology to offer attribute-based access control on EHR data using ALFA, a predetermined set of characteristics. To make electronic health records (EHRs) safer and more private, Sharma et al. [21] are now creating a system that uses blockchain technology to deploy EHRs. This technology will control information access using decentralisation and cryptography. Also, it maintains a balance between data accessibility and privacy. The main goal of our study is to shed new light on the issues with data security and privacy in electronic healthcare. We develop a distributed system comprised of current EHRs that use consortium blockchain using Hyperledger fabric [22]. Peers maintain the blockchain that houses all patient data using the same ledger that peers use to record the address of a patient record in an EHR [23]. A local certificate authority, which collaborates with other certificate authorities to build a network channel, issues each patient's unique certificate. We use a proxy re-encryption method to protect patients' privacy when their data is sent. With the help of a centralised service provider, the Federated Learning setup uses machine learning with clients like mobile devices or large businesses to train a model collectively [24]. The participants in the learning process maintain the decentralised data. FL is committed to gathering the appropriate data while reducing the numerous privacy risks and expenses connected with the application of centralised standard machine learning and data science methodologies. The paper highlights recent developments and offers a comprehensive list of unresolved problems and difficulties, all spurred on by the sharp rise in FL research. Wang et al. [25] demonstrated it through the design and implementation of a novel privacy-preserving inference information flow. The computation time of inference and the payload size of activation signals are significantly impacted by the model's division farther down the computation chain. More model secrecy results from this, albeit at the expense of longer computation times. Rajadurai et al. [26] employ a technique to keep an SDF graph's optimal throughput while calculating the latency of a static schedule for a specific unfolding factor on a heterogeneous multiprocessor platform.

***TABLE 1***

The execution platform and synchronous data flow graph in the system model are both made up of timed automata. The result is defined using the UPPAAL model checker.

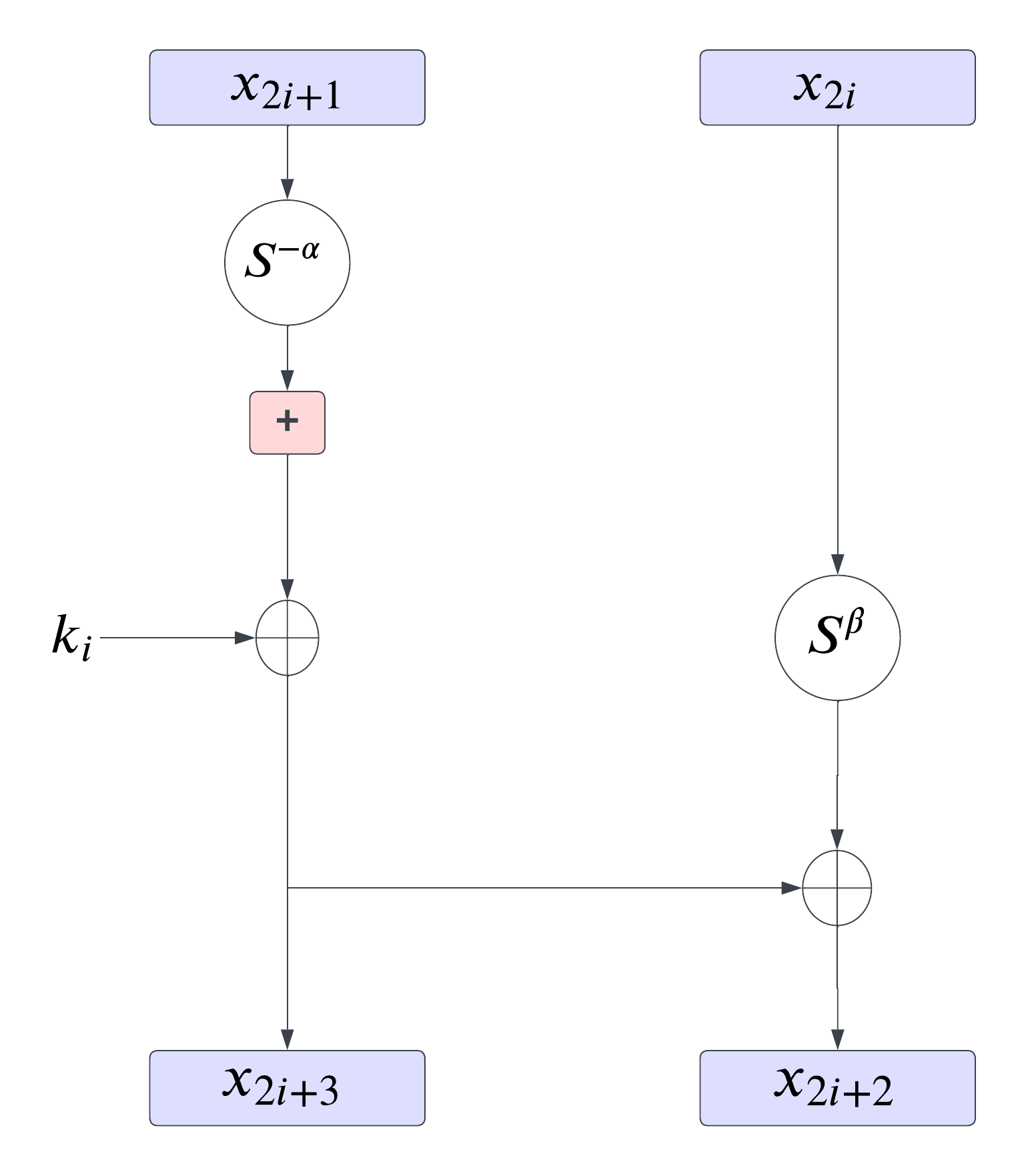
|  |  |  |  |
| --- | --- | --- | --- |
| **REFERENCES** | **OBJECTIVES** | **CONTRIBUTIONS** | **LIMITATION** |
| **[1]** K.N.G.L. Reshwanth, G. Rajyalakshmi, Yendeti Venkata Siva Prasanth, Chalicham Hanish, S. Aravind Raj, K. Jayakrishna, Chapter 7 - Blockchain technology approach for drug delivery in health care: A review, Editor(s): Kaliyan Mathiyazhagan, V. Raja Sreedharan, Deepak Mathivathanan, Vijaya Sunder M, Blockchain in a Volatile-Uncertain-Complex-Ambiguous World, Elsevier, 2023, Pages 89-99, ISBN 9780323899635,  <https://doi.org/10.1016/B978-0-323-89963-5.00004-6> | Blockchain; COVID-19; Digital Support; Drug Delivery; Health Care | Used the blockchain technology in healthcare with the potential to improve interoperability and patient-driven data sharing, which could better prepare the healthcare system to manage public health risks such as COVID-19. | Didn’t optimize the Model. |
| **[2]** Sharda Tiwari, Namrata Dhanda, Harsh Dev, A real time secured medical management system based on blockchain and internet of things, Measurement: Sensors, Volume 25, 2023, 100630, ISSN 2665-9174,  <https://doi.org/10.1016/j.measen.2022.100630> | IoT; Blockchain; Health; Medical; Sensor | Proposed an IoT-based prototype that uses Blockchain technology to get rid of this anonymous data access, in the common word patient's data are private through this system. | Didn’t applied the encryption process before using blockchain technology. |
| **[3]** Haddad, A.; Habaebi, M.H.; Suliman, F.E.M.; Elsheikh, E.A.A.; Islam, M.R.; Zabidi, S.A. Generic Patient-Centred Blockchain-Based EHR Management System. Appl. Sci. 2023, 13, 1761.  <https://doi.org/10.3390/app13031761> | Patient-Centred; IPFS; Blockchain; Privacy; Health Record | This research is developed a Patient-Centred Blockchain-Based EHR Management (PCEHRM) system that allows patients to manage their healthcare records across multiple stakeholders and to facilitate patient privacy and control without the need for a centralized infrastructure by means of granting or revoking access or viewing one’s records. | Not disclosed the key generation process. |
| **[4]** Abdelgalil, L.; Mejri, M. HealthBlock: A Framework for a Collaborative Sharing of Electronic Health Records Based on Blockchain. Future Internet 2023, 15, 87.  <https://doi.org/10.3390/fi15030087> | Electronic Health Records (EHRs); Blockchain; Hyperledger Fabric; Hyperledger Indy; Smart Contracts; Interplanetary File System (IPFS) | This paper proposes a framework called Health Block for collaboratively sharing EHRs and their privacy preservation. Different technologies have been combined to achieve this goal. The Interplanetary File System (IPFS) technology stores and shares patients’ EHRs in distributed off-chain storage and ensures the record’s immutability; Hyperledger Indy gives patients full control over their EHRs, and Hyperledger Fabric stores the patient-access control policy and delegations. | Didn’t applied the encryption with the key generation process. |
| **[5]** Ghassan Al-Sumaidaee, Rami Alkhudary, Zeljko Zilic, Andraws Swidan, Performance analysis of a private blockchain network built on Hyperledger Fabric for healthcare, Information Processing & Management, Volume 60, Issue 2, 2023, 103160, ISSN 0306-4573,  <https://doi.org/10.1016/j.ipm.2022.103160> | Blockchain; Healthcare; Hyperledger Fabric; Hyperledger Calliper | This paper contributes to the literature by presenting the use of Hyperledger Fabric in healthcare to improve information flow and solve the fragmentation problem between two medical institutions. In addition, two rate controllers on Hyperledger Calliper are used to evaluate the performance of our network: fixed and linear. | Not disclosed the key generation process. |
| **[6]** Stawicki, S.P., Firstenberg, M.S., Papadimos, T.J. (2023). The Use of Blockchain in Fighting Medical Misinformation: A Concept Paper. In: Stawicki, S. (eds) Blockchain in Healthcare. Integrated Science, vol 10. Springer, Cham.  <https://doi.org/10.1007/978-3-031-14591-9_15> | Blockchain; Censorship; Disinformation; Information Management; Misinformation; Oversight; Public Harm; social media; Source Credibility | Blockchain technology can help the medical community rapidly adapt to changes and prevent the spread of medical misinformation during pandemics. It promotes scientific consensus, transparency, and public access to scientific discourses, leading to better health outcomes and a more informed public. | Didn’t optimize the Model using meta-heuristic optimization algorithm. |
| **[7]** Pilares, I.C.A.; Azam, S.; Akbulut, S.; Jonkman, M.; Shanmugam, B. Addressing the Challenges of Electronic Health Records Using Blockchain and IPFS. Sensors 2022, 22, 4032.  <https://doi.org/10.3390/s22114032> | Blockchain; Cryptography; Electronic Health Record; Privacy; Security; Distributed File System | This research project is to aid the acceleration of EHR adoption. Another objective is to ensure the robustness of the system to resist malicious attacks. | Didn’t encrypt the EHR using Optimal Key |
| **[8]** Said, O. LBSS: A Lightweight Blockchain-Based Security Scheme for IoT-Enabled Healthcare Environment. Sensors 2022, 22, 7948.  <https://doi.org/10.3390/s22207948> | Blockchain; Healthcare; IoT; IoT-simulation; Security; IoT Security | This paper proposes LBSS, a security scheme for IoT-enabled healthcare that includes blockchain technology for transaction integrity, secure storage of data, and authorization tests for access. The scheme prioritizes data importance and outperforms traditional models in performance metrics, as shown by simulation results using the NS3 package. | Not done optimal key generation process and model optimization. |
| **[9]** Mohsan, S.A.H.; Razzaq, A.; Ghayyur, S.A.K.; Alkahtani, H.K.; Al-Kahtani, N.; Mostafa, S.M. Decentralized Patient-Centric Report and Medical Image Management System Based on Blockchain Technology and the Inter-Planetary File System. Int. J. Environ. Res. Public Health 2022, 19, 14641.  <https://doi.org/10.3390/ijerph192214641> | Digital Health; Blockchain; Smart Contract; Ethereum; Distributed Storage; IPFS; Medical Images Sharing; Health System | This research proposes a patient-centric test report and image management system using Ethereum blockchain and Inter-Planetary File System technology. The patient-centric access control protocol is designed for secure access control. The system enables distributed and secure data access for hospitals, patients, and image requestors. The proposed framework was tested using an Ethereum TESTNET blockchain and found to be efficient and practicable. | Not used the model optimization. |
| **[10]** Hiwale, M.; Varadarajan, V.; Walambe, R.; Kotecha, K. NikshayChain: A Blockchain-Based Proposal for Tuberculosis Data Management in India. Technologies 2023, 11, 5.  <https://doi.org/10.3390/technologies11010005> | Blockchain; Privacy; Healthcare; Data Management; Tuberculosis; Nikshay Poshan Yojana (NPY) | This work is identified the current implementation challenges of the NPY scheme from patient and healthcare stakeholder perspectives and proposes a blockchain-based architecture called Nikshay Chain for sharing patient medical reports and bank details among several healthcare stakeholders within or across Indian cities. The proposed architecture accelerates healthcare stakeholder productivity by reducing workload and overall costs while ensuring effective data management. | Didn’t optimize the Model using meta-heuristic optimization algorithm. |
| **[11]** Joao Cunha, Ricardo Duarte, Tiago Guimaraes, Manuel Filipe Santos, Permissioned Blockchain Approach using Open Data in Healthcare, Procedia Computer Science, Volume 210, 2022, Pages 242-247, ISSN 1877-0509,  <https://doi.org/10.1016/j.procs.2022.10.144> | OpenEHR; Blockchain; Healthcare; Hyperledger Fabric | The paper proposes the use of blockchain technology and the OpenEHR interoperability standard to address the problem of distributed and non-integrated digital health records. The combination of these technologies offers fine-grained access permissions and guarantees standardization of electronic records. The proposed architecture will be implemented in a Portuguese hospital's ICU to support clinical decision-making and ensure the interoperability, veracity, privacy, and security of the data used. | Didn’t applied the encryption process before using blockchain technology. |
| **[12]** Yuying Yang, Aixia Song, Qing Chang, Hongmei Zhao, Weidan Kong, Qian Xue, Qianlong Xue, "Improving the Use of Blockchain Technology in Stroke Care Information Management Systems", Computational and Mathematical Methods in Medicine, vol. 2022, Article ID 2642841, 9 pages, 2022. <https://doi.org/10.1155/2022/2642841> | Blockchain Technology, Distributed Digital Ledgers, Cryptographic Hashes, Data Security, Medicine Supply Chain, Patient Information | This study focused on evaluating the application of blockchain technology in Stroke Nursing Information Management Systems. This emerging technology is already in use in the healthcare industry. The patient’s data is kept decentralized, transparent, and mainly incorruptible, thus keeping it secured and sharing of data is quick. | Didn’t applied the encryption process before using blockchain technology. |

**The proposed HBESDM-DLD model**

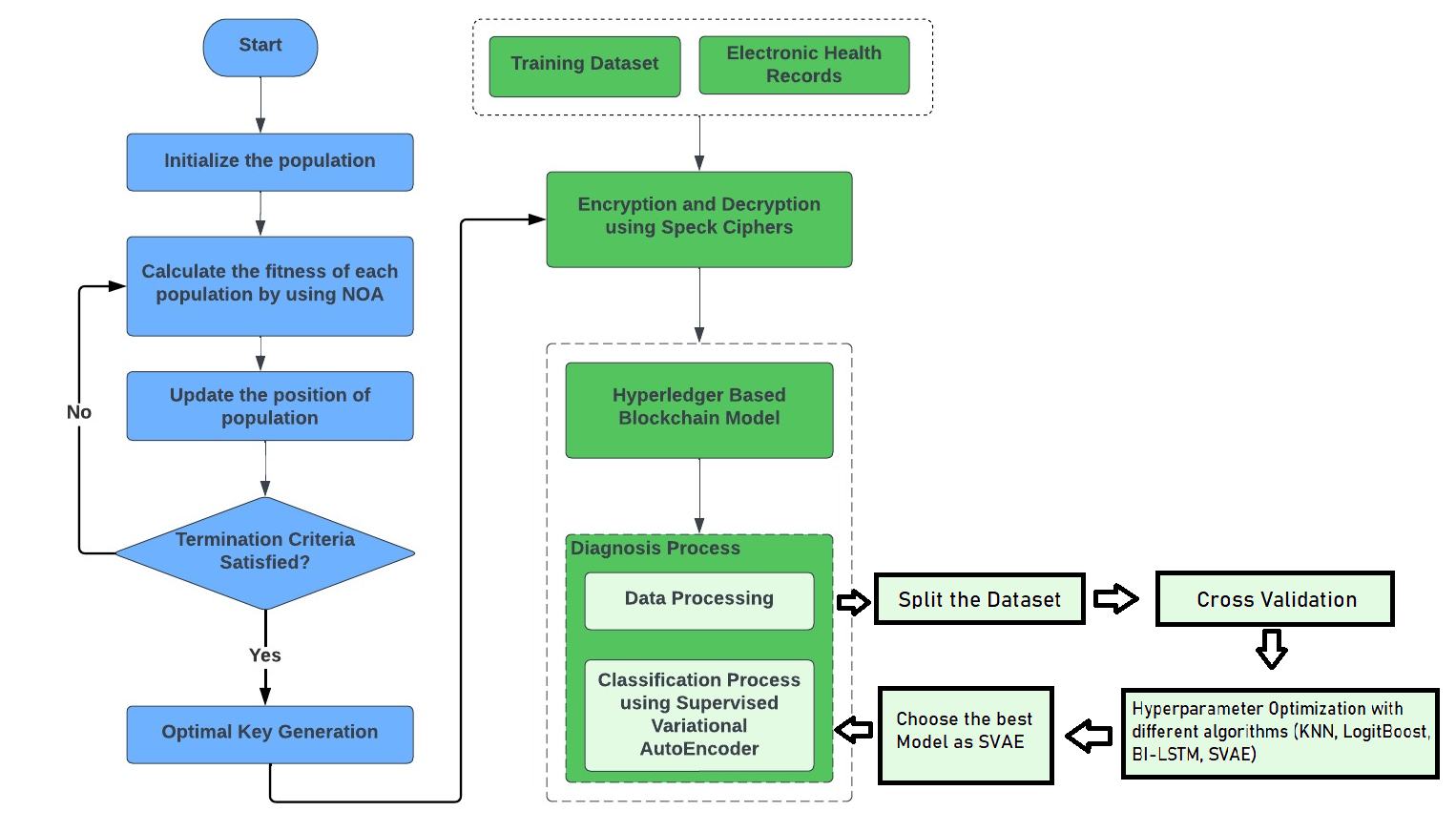
The HBESDM-DLD model is depicted in Fig. 1 as it goes through several stages of operation, including encryption, optimum key generation, Hyperledger blockchain-based secure data management, and diagnostics. The patient's health records are initially encrypted using the SPECK block cypher method and a NOA-based optimum key generation method. The Hyperledger blockchain, which has a global blockchain and several local blockchain for medical institutions, is also involved in the data encryption process. The patient grants or denies access to any doctor or medical facility. The authorised user can decode the encrypted data and obtain the genuine medical records. The SVAE-based diagnostic procedure is used to identify any illnesses at the very end of the process.

**Data encryption process**

Hash functions, block cyphers, validated decryption, and encryption modelling procedures are examples of low weight cryptographic techniques. For managing secure healthcare records, block cyphers are used in this study. Beginning with a more advanced encryption standard, lightweight cypher development occurs (AES). There are now several cyphers accessible, including the RECTANGLE, SPECK, TWINE, KATAN, SIMON, and KLEIN cyphers. The performance of SPECK, a compact block cypher, is based on hash function and effectiveness when connected to hardware. Ten functions in this cypher family, including key size and block, have different structures for the two variables. The key for each block is different depending on the picture pixels. The SPECK block cipher's construction is shown in Figure 2. The block quantifies the variance between 32 and 128 bits, which roughly equates to 16. It carries a block of encrypted material and performs an action on a set size block of plain text [27]. The SPECK cipher has direct and nonlinear characteristics for studying security in relation to block size and data. The person might think about a tree for each difference in all rounds while employing a set of input variances, creating some of the potential output variances.



**FIG – 2**



On the off chance that the key qualities are extended to further rounds, people might make use of the robust structure of round capabilities. The SPECK key calendar develops the number of pixels valued in a picture while utilising the round reliability for key schedule characteristics. With the 15-round SPECK48 on the light block cypher, there is just one single key difference signal. This block cipher's quality was not designed to be perfect. The chosen optimizer generates the optimal result, and this approach's quality is assured to have the fewest active S-boxes.

Today, encryption, rounding, biting, and decryption are some of the key elements used in cypher modules for safe data transport. Fig. 3 shows how the SPECK cypher round function divides an input plaintext block (2n) into two words of equal size as an illustration (each one is n-bit). Each round function performs three left shifts and bitwise AND logic operations on the left half block. The round key is employed, and the right half block is XORed with the XOR result, as illustrated in Fig. 2. At the end of each round, the created value is written back to the left block while the left half value is transferred to the right block. This round operation is continuously performed as long as the total number of rounds for the implemented configuration stays the same. Eq-1 can be used to represent F. The equivalents of the SPECK cypher with 2n-bit blocks are as follows:

**Table**: **Speck Parameters**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Block Size  *2n* | Key Size  *mn* | Key Words  *m* | Word Size  *n* | Rot  *α* | Rot  *β* | Rounds  *T* |
| 32 | 64 | 4 | 16 | 7 | 2 | 22 |
| 48 | 72  96 | 3  4 | 24 | 8 | 3 | 22  23 |
| 64 | 96  128 | 3  4 | 32 | 8 | 3 | 26  27 |
| 96 | 96  144 | 2  3 | 48 | 8 | 3 | 28  29 |
| 128 | 128  192  256 | 2  3  4 | 64 | 8 | 3 | 32  33  34 |

***EQ-1*** EncDI Cipheri ql,...Ciphern q1,i > 1.

This cypher is referred to as having round keys and round functions. Such function is referred to as an iterated block cypher. The SPECK round capability for encryption is provided by

***EQ-2***  (x, y) = ((x + y)k, y⊕(x +y)k)

The data is decrypted using the inverse function, as illustrated in Eq. (3)

***EQ-3*** (x, y) = (((xk) - x⊕y)), xy))

The terms used in Eq. (3) are for the left-most word in a block, for the right-most word, and for the right-round key.

**HBESDM-DLD algorithm**

HBESDM-DLD secure medical record management algorithm 1.

***algorithm-1***

**Optimal key generation process**

The SPECK cypher generates entire round keys from the master key to provide key expansion. The early 128-bit master key is converted by the selected SPECK64/128 formation into round keys that are 32 bits in size. By combining the saved previous round keys (key word variable) with trustworthy and 1 bit round, it secures the round. The main task of expansion makes use of related tasks.

* Indicated by bitwise XOR is .
* Left circular shift, , by j bits and right circular shift, , by j bits.
* Round counter with continuous sequence and and j = 0, 1, 2, 3, 4
* Constants, the number of cypher rounds, and the round key (sub-key).
* Right bitwise rotation ROR, where c stands for the number of rotations, is determined by .

Eq-(4) provides the crucial expansion procedure.

***Eq-4 4***

***4.4***

To decrypt the data, an ideal key can be chosen from among the many created keys. The NOA is used to optimise the value as minimum or maximum in order to choose the best key. A Nature Inspired meta-heurestic method is used to stimulate the NOA being delivered. The goal is to increase the class's collective knowledge. Given the wide range of differences among pupils, it is difficult to carry out in real time.

This section introduces a bio-inspired Nutcracker optimisation algorithm (NOA) based on the cunning actions of the nutcracker. The nutcracker's behaviour can be divided into two primary categories: the first involves collect and storing pine seeds (food), and the second involves searching for and retrieving storage locations. These two activities are distinguished by the fact that they occur during two different time periods. The initial activity takes place during the summer and fall seasons. The second habit, meanwhile, takes place during the winter and spring seasons. Based on the two primary behaviours, the proposed algorithm simulates nutcracker behaviour. Foraging and storage strategy and cache-search and recovery strategy are the two basic tactics.

**Foraging and storage strategy:**

This can be described as follows:

• **Foraging stage: Exploration phase 1**

At this phase, the nutcrackers start moving into the search space to occupy their beginning positions/food spots that were created by Eq. (19). (Collection area). Every nutcracker starts by inspecting the cone that houses the seeds in their initial placement. When it comes across quality seeds, the nutcracker will carry them to the storage area and bury them in a cache. The nutcracker will search for another cone in a different location within pine trees or other trees if it is unable to obtain good seeds. The position update approach can be used to model this behaviour analytically as follows:

Eqn1

where is described as new position of the ith nutcracker in the current generation t; is denoted as jth position of the ith nutcracker in the present generation; and are two vectors, including the upper and lower bound of the jth dimension in the optimization problem;is a random number generated according to the levy flight; is the jth dimension of the best solution obtained upto this; A,C, and B are three distinct indices that were arbitrarily chosen from the population to aid in the search for a high-quality food source; ,,r and are random real numbers in the range of [0,1]; is the mean of the jth dimensions of all solutions of the current population in iteration t; and µ is a number generated based on the normal distribution(levyflight( and randomly between one( and zero shown in the below equation:

where [0,1]-ranged random real values and are used. Eq. (1) was suggested to investigate high-quality food sources. The first state of Eq. (1) simulates the probability that the nutcrackers discover good seeds on the first try. This notion means that the nutcrackers will not change their original jth dimension in the solution() . The second state of Eq. (1) was proposed to allow the nutcrackers to globally explore random positions in the search space to enhance the search capability of NOA for exploring the search space as must as possible to avoid being stuck into local minima and reaching the promising regions that might include the near-optimal solution. In addition to moving globally in the search space with a probability δ to cover intractable regions by the second state of Eq. (1), the third state of Eq. (1) was introduced to allow the nutcrackers to investigate places surrounding a solution randomly chosen from the population (1). Later on, the sensitivity analysis for determining the ideal value for δ is shown. It was proposed that A and B inform the nutcrackers of the new food position. As scaling factors to control the exploration capacity in NOA, and were proposed. The suggested algorithm supports a variety of small and large values for and , and can switch between local and global searches.µ explains to the nutcracker the necessary direction and different step sizes to explore a new area.

**• Storage stage: Exploitation phase 1**

In the first step of investigation, phase 1, nutcrackers move the food they have collected to temporary storage areas (storage area). In this phase, referred to as "exploitation phase 1," the nutcrackers harvest and store pine seed crops. Mathematically, this behaviour can be described as follows:

Eqn3:

where () is a fresh location in the nutcrackers' storage region in iteration t,λ is a number produced using the levy flight, and is a random number between 0 and 1. To diversify NOA's exploitation behaviour, the component l was linearly reduced from 1 to 0. This variation in the NOA's exploitation operator will speed up convergence while also preventing the possibility of becoming caught in local minima when searching in one direction.

To maintain the balance between exploration and exploitation operators during the optimisation process, the exchange between the foraging phase and the cache is applied using the following formula:

Eqn(4)

where φ is a probability value that decreases linearly from one to zero based on the current generation and is a random number between zero and one. This step can drive the bulk of the solutions in one direction, covering the solutions there as much as possible while looking for the nearly ideal solution, according to Fig. 4(b), which illustrates the direction of the solutions generated using this stage. The first suggested strategy's exploration and exploitation procedures are flow-charted in Fig. 5 and listed in Algorithm 1.

**Reference memory**

The nutcrackers start the spatial memory after putting the seeds in the cache. In order to recall their cache, the nutcrackers create a mental image of it and use certain items as cues. To make it through the winter, these nutcrackers almost entirely rely on their recollection of where those caches are. Nutcrackers meticulously inspect and sketch the site of storage.

Their single chance of reproduction and survival is hidden food. Furthermore, because they are covered with snow during the winter, local characteristics are useless while nutcrackers appear to interpret towering trees or prominent topographical features as signs. The behaviour of nutcrackers retrieving their cache will then be simulated.

**Cache-search and recovery strategy**

There are two primary phases to this strategy: Stages of cache-search and recovery, which are covered in depth in the next two subsections:

**• Cache-search stage: Exploration phase 2**

When winter arrives, the trees become naked, signalling that it is time to leave hiding mode and transition to exploring and searching. The nutcrackers start looking for their stashes. This stage is known as the second exploration. To find their caches, the nutcrackers employ a spatial memory technique. Many objects are most likely used by nutcrackers as signals for a single cache. For the sake of simplicity, we'll assume that each cache contains just two objects. The markers or objects will be hidden at various angles from the concealing site. At this phase, the nutcrackers begin to assume their beginning positions/cache positions in the search space, which were generated by Eq. (19). (storage area). These things are what we refer to as Reference Points (RPs). Using the following matrix, two RPs for each cache/nutcracker in the population can be defined in NOA:

Eqn 5

Thus, for the ith nutcracker in the current generation t, () and () stand for RPs (objects) of the cache position (). We suppose that the three items represent the vertices of a triangle to demonstrate the relationship between the nutcracker, cache, and reference point. Nutcrackers can be seen from a variety of locales and perspectives. Three different 3D positions are shown for the nutcracker in Fig. 6, along with three different RP sites for a single cache.We presum that the cache is located at the origin point in 3D space. Nutcrackers are seen from different perspectives. The angles at which the first, second, and third locations are situated are acute, obtuse, and right, respectively. In 3D space, a nutcracker can be found on either the diagonal or coordinate axes. For RPs, the same is true.

Nutcrackers are highly accurate in finding hidden caches.However, pertinent research show that 20% of nutcracker attempts are unsuccessful on the first try [83]. The second RP will be used to identify the meal if the nutcracker is unable to find it using the first RP. The nutcracker will utilise the third reference if it is unable to get its cache a second time. To facilitate nutcracker exploration while looking for hidden caches, two different equations are created to generate the first and second RPs. In order to locate hidden caches near the nutcrackers, the current position is updated within the surrounding regions to create the first RP. The first RP is created using the following mathematical formula:

Eqn 6:

To assist the nutcrackers in investigating various areas in quest of the hidden caches, the second RP is created by modifying the present resolution within the search space of the problem. The following formula is used to calculate the second RP:

Eqn 7

Eqn8:

where k stands for the RP index, RPti,k for the cache position of the ith nutcracker in the current iteration t, and U and L for the higher and lower bounds of a D-dimensional problem, respectively. XtA is the cache position of the Ath nutcracker in the current iteration t; r2 is a vector with values randomly generated between zero and one; r3 is a random number of the second RP in the range [0, 1]; r is a random in the range [0, ]; and Prp is a probability used to calculate the proportion of globally investigating different areas within the search area.

To restore its cache, every nutcracker needs two RPs, which are produced using equations (6) and (7). The RP can quickly recover it when it is near the cache. In the first generation, it is assumed that the nutcrackers lack the expertise to choose the proper RPs (i.e., those that are close to the cache). However, with time, nutcrackers develop more expertise in the act of storage. To make it simple to retrieve items later, nutcrackers picture locations nearby their warehouses. It was suggested in these calculations that the nutcrackers be trained and given enough experience to pick an appropriate location for RPs. The early convergence of RPs towards the correct position is prevented in NOA by (cache site). The nutcracker's angle-of-view, which ranges from 0 to, is determined at random. The various nutcracker viewing angles are depicted in Fig. 7: (a) θ = 0; (b)0< θ < π/2; (c) θ = π/2; (d) 0< θ < π; (e) θ = π. () when (), showing that the RP position is on the same cache position. Eqs. (6) and (7) can be rewritten as follows to address this problem (RP):

Eqn 9

Eqn 10

where RPt i,1 denotes the ith row, first column, in the matrix given in Eq. (5); () denotes the ith row, second column, in Eq.(5). The cache/nutcracker index is represented by each row index in the matrix. In the meantime, the RP index is represented by each column index in the matrix. A random position is RP. To prevent the early convergence of RPs towards a potential solution, the third term of the initial state of Equations (9) and (10) (i.e.,() ) has been added, makes sure the NOA converges frequently, enabling the nutcracker to enhance RP selection in upcoming generations. α can be determined using the following formula:

Eqn 11:

where the current and maximum generations are denoted by t and Tmax, respectively. To speed up the proposed algorithm's convergence, the first state in Eq. (11) drops linearly with each iteration. In the meantime, the second state grows linearly to prevent falling into local minima that could happen as a result of the first state.

The optimisation method gives all nutcrackers sufficient practise in choosing the right RPs. According to the applicable RPs, these nutcrackers update the storage locations/solutions. All nutcrackers in NOA will use the exploration mechanism to look for the most promising regions that could have a nearly ideal answer. To prevent becoming stuck in local minima, the algorithm will search and utilise locations nearby caches with the proper RPs with each generation that passes. The following equation can be used to modify a nutcracker's position:

Eqn 12:

where Xt+1 i is the new location/new cache of the ith nutcracker at iteration (t+1), X i is the current position/current cache of the ith nutcracker in the present iteration t, and ()Ris the first RP of the current cache of the ith nutcracker at iteration t. Eq.(12) was proposed to guide NOA to explore and exploit the promising areas of the () . If NOA is unable to obtain the optimal locations around RPt i,1, it will investigate them in other regions, such as those near the reference () which are covered in more detail below.

**• Recovery stage: Exploitation phase 2**

Figure 8 shows potential obstacles a nutcracker can run into while looking for its stockpile. The first significant possibility is that a nutcracker can recall his cache's location using the first RP. The following are the two scenarios represented in Fig. 8: The initial scenario is that there is food, and the second is that there isn't any. The following equation can be used to mathematically model this behaviour.

Eqn 13.

where denotes the new position or cache of the ith nutcracker at iteration (t+1), Xtij denotes the present dimension or cache of the ith nutcracker in iteration t, Xtb denotes the best position or cache in iteration t, and RPti,1 denotes the first RP of the present location or cache of the ith nutcracker in iteration t.

Eq. (13)'s first state simulates the initial scenario (food exists). This idea implies that there is a potential that some dimensions in this cache/solution will persist until the future generation. The nutcracker will put more emphasis on food storage the following time because a cache that preserves pine seeds is actually beneficial. Eq. (13)'s second state simulates the second scenario. (Food does not exist). Since the solution region in this case does not look promising, the algorithm will use an escape strategy to prevent becoming caught in local minima. Food from the cache is lost for a variety of causes, including theft by another nutcracker or bird, natural disasters like rain and snow, or human error.

Eq. (13) state (1) enables a nutcracker to take advantage of potential search space areas and improve the local search capabilities of NOA. To improve the global search capabilities of NOA, eq. (13) state (2) enables a nutcracker to explore random areas in searching area.

Fig 7

Fig 8

The second main possibility is that the nutcracker will use the second RP to look for his hidden food because he cannot recall where it is using the first RP. A nutcracker memorises a lot of the RPs he will take during early storage. Nutcrackers restore caches on the first attempt (with the first reference), but the suggested technique takes the likelihood of failing on the first attempt into account. When the weather changes between autumn (storage time) and winter, the nutcrackers who can't discover their cache rely on nearby landmarks that may vanish. (Recovery time). The second RP is used for updating the nutcracker's spatial memory, Eq. (12):

Eqn 14:

where RPt i,2 is the second RP of the present cache of the ith nutcracker at iteration t and Xt i is the current position/current cache of the ith nutcracker in the current iteration t. The NOA has the chance to investigate uncharted territory around the second RP and take advantage of attractive places where a viable solution might be located thanks to Eq. (14). In NOA, it is expected that a nutcracker will use the second RP to locate its cache, hence Eq. (13) is revised utilizing the second RP:

Eqn 15:

where [0,1] is the range for the random values r1, r2, 5, and 6. The algorithm can increase the local search around the most suitable areas that contain the nearly optimal solution by entering the initial state of Eq. (15). The second condition of Equation (15) in the contract permits the algorithm to expand its ability to perform global searches by looking for new locations in the search space. In conclusion, the recovery behaviour simulation (Fig. 8) may be expressed as the following equation:

Eqn 16:

where [0,1] is a range of random numbers, and (tou7), (tou8) is one among them. A nutcracker who recalls the secret store is represented by the first instance in the equation above, whereas a nutcracker who forgets the hidden store is represented by the second case. Now, the subsequent equation describes how the exploring behaviours related to the initial and secondly RPs are balanced:

Eqn 17:

Finally, to maintain a balance between exploration and exploitation, the exchange between the cache-search stage and the recovery stage is applied using the following formula:

Eqn 18:

where is a chance number between 0 and 1, Pa2 is a probability value equal to 0.2, and this value was determined through additional trials. On the one hand, the exploration operator within this approach exhibits strong coverage, distributing the ability around broad areas that indicate the RPs followed by the nutcrackers to locate the hidden caches, according to simulation experiments carried out to demonstrate the characteristics of the cache-search and recovery strategy and reported in Fig. 9. The exploitation operator depicted in Fig. 9(b), on the other hand, focuses their search inside a constrained area to find the pine seeds buried in the covert stash. In Figure 10. the second suggested strategy's exploration and exploitation flowchart is shown and listed in Algorithm 2.

Eqn(1)

***Fig. 3 Flowchart of NOA***

They first take into account population, decision parameter, and fitness value relating to the students in order to alter this approach to be suited for optimization procedure [28]. Subsequently, a straightforward group teaching module is developed without losing generalizability. The approach achieves consensus via transaction witness and pseudorandom sortition. Throughput, latency, and latency three dimensions have been added to the formula to boost the algorithm's scalability. Using a consensus technique with strong scalability, low latency, high throughput, and decentralised properties is recommended.

The NOA algorithm is used in this work to offer an enhanced hybrid consensus algorithm. Verifiable cryptographic sortition chooses the consensus node in a dynamic manner, allowing a large number of nodes to fairly participate in the consensus while assuring low latency and high throughput.

**HYPERLEDGER BLOCKCHAIN:**

In this study, federated learning(FL) method is utilised in the blockchain with ML(Machine Learning)based disease diagnostic model. Blockchain is a shared ledger implementation method. It provides decentralisation, appropriateness, security, accessibility, and all of the above. Data stored in the Blockchain can now be replicated across a number of machines, eliminating the single point of failure associated with a centralized server. While the data is accessible when needed, very few computers really malfunction. Integrity with data upkeep, preserving it from unwanted changes.

The capacity to track all stored data in blockchains is possible.

Finally, privacy allows the members to remain anonymous. Technically speaking, the blockchain is made up of a collection of well-ordered and trustworthy blocks of chain, each of which includes a header and stores data. The header is made up of several elements, including the previous block, the identification, and the signature. The identification represents an internationally distinctive value with a mathematical function that encloses each block of data. Chaining blocks is managed by the preceding block. A logical chain of connections would be created since each novel block in the chain would include the identifier value of the block before it. One of the open-source blockchains provided by the Hyperledger management is called Hyperledger Fabric. It seeks to create a decentralised setting. It involves committed peer, client, certificate authority, order, and endorser peer. Additionally, the components communicate through channels that have been set up to enable transactions in a private and hidden manner, dividing various application domains. There are two methods that the fabric certificate authority is in charge of. First, it ensures that different components (users or smart contracts) can use the specified system. Then, it verifies the component and grants permission to use it for a certain function (such as carrying out a transaction) or access another part as a result of the authorization. The chain sent by the system-generated channel must be continued by the committing peer. As a result, they maintain different blockchains for every channel that an individual has formed. Scalability and anonymity are provided by this ‘individual chain per channel’ method.

When compared to privacy, a component that lacks easy access to a network cannot access a chain from a committed peer connected to the channel. Scalability states that individual for each channel permits the exchange of various transactions and data stored with in various committed nodes, increasing the demanded amount where a node gets fulfilled and to raise quantity of data, thus enhancing the system's sustainability. Peers who are approving are in charge of two processes. The first step is to collect the transaction from the client. After that, it is examined using a smart contract system because the transaction contains a number of linked rules that must be adhered to. Two processes are carried out by gathering peers, such as obtaining consumer transactions and organising transactions for assessing the blockchain's dependability. As a result, every ordering peer on a given chain needs to attest that the transaction was added to the committing peers. It is claimed that even though a person may frequently visit identical medical facilities, this blockchain only records one visit. The EHR pertinent to the individual is stored on the blockchain for each medical facility (also known as the local blockchain). It is assumed that the medical facility maintains the minimal structure needed to operate the Hyperledger network in order to put the blockchain.

A smart contract is a chain code application in Hyperledger fabric. It is typical practise to construct network-agreed business logic using chain codes. The state that results from the generation of a chain code belongs to that chaincode alone and is unavailable to other chaincodes. If you have the required authorization, you can call another chaincode. It is useful to think about the following two sorts of chaincode while discussing them: a chain of application-specific code for the entire system In general, chaincode is in charge of processing system-related transactions, including lifecycle management and policy configuration. Nonetheless, users have access to the system's chaincode API and are free to modify it as needed. Application states, such as digital assets or arbitrary data input, must be maintained on the ledger by the application chaincode. A chaincode begins with a package that contains metadata, which is used to ensure the consistency of the code and metadata, such as the name, version, and counterparty signatures. The software is installed automatically on the counterparties' local computers when the chaincode package has been loaded on the counterparties' network nodes. A registration function is carried out within the smart contracts (chaincode) for the private health authority designated by the fabric network administrator to administer and manage the fabric network in order to register the members. For enrolled parties, the healthcare authorities establish a private, permissioned network to which only they have accessibility. A virtual private network connection will be used by everyone to access the registration system with added security (VPN). The patient will just provide enrollment data at the time of registration, including name, social security number, address, and contact details. Also, the principal physician, hospital, laboratory, pharmacy, researcher, and insurance will all register with the body that regulates the healthcare industry. The public health authority checks the record when they have finished the enrollment process and issues a chaincode address. The registration procedure has been finished by all parties, and all transactions on the network have been finished.

The hyperledger blockchain procedure in the healthcare industry is shown in Figure 4. The modular nature of the Hyperledger Fabric model offers security, resilience, flexibility, and scalability. It provides plug-in implementation of a variety of components and adapts to the economic ecosystem's complexity and subtleties. The main components of the block diagram's fundamental fabric technology concepts are as following.

**Chain codes:**

It is a self-executing software that is currently developed in Go (identical to smart contracts).

**Channels:**

It is a confidential "subnet" of communication between specific network users (or hospitals), with the intention of facilitating private transactions.

**Ordering service:**

It guarantees the regularity and planning of transactions

**Endorsement policy:**

It consists of the set of guidelines that a node can use to determine whether or not a transaction is accepted.

**Application SDK**:

Based on the endorsement policy outlined in the chain codes, it approves transactions prior to commitment

**Endorsing peers:**

To validate the blocks, it obtains them from the ordering service.

**Committing peers:**

It also updates the state of the data in the State DB and the ledger.

**Disease diagnosis process:**

The SVAE model, which correctly detects the presence of disease, is used to diagnose the condition from the medical records. Min—Max data normalisation is used to normalise the data before using the SVAE model. The appropriate class labels for the applied health records are then determined using the SVAE model. In the latent parameter space, the SVAE network offers a probabilistic perception. Using the latent parameter z to define the sharing of the novel dataset is one of the SVAE's key goals. They believe that the Gaussian distribution is necessary for the qualified sharing of the latent parameter z. Figure 5 depicts the SVAE structure. This idea shows how the hidden parameter z satisfies the Gaussian distribution, which might be used by NN to produce information that satisfies some distribution. The latent parameter z provides a dataset that is comparable to the actual data by boosting the produced variable. It follows that it would take use of the marginal probability

Equation:14

The SVAE presents an identifying component q(z|x) to estimate the uncertain true posterior p(z|x), as the true posterior density p(z|x) is intractable. By using Kullback-Leibler (K L) divergence, the SVAE compares the identification module q(z|x) with the genuine posterior distribution p(z|x).

Equation:15

Since the KL divergence is generally greater than zero

This equation named (i.e., variational) low bound on peripheral probability of data point i, is stated as follows:

Equation:16

The variational lower bound on the marginal probability sets the entire optimization goal of SVAE in order to improve logp(x). The initial term on the right side of Eq. (16) corresponds to the regularisation term and a negative autoencoder reconstruction error. As a result, p (x(i) | z) is referred to as a probabilistic decoder with generation variable, and q(z|x(i)) is referred to as a probabilistic encoder with variational variable and (). The Bernoulli/Gaussian distribution is frequently provided under the conditional distribution p (x(i) | z). Instead of binary data, patient medical records are used as the network's inputs in this study, and the distribution p (x(i) | z) is thought to be Gaussian. In a later step, they calculate the stochastic gradient variational Bayes estimator of the variational lower limit (,, x(i)). They use the reparameterization method to present the identification module q(z|x(i)), where z is a continuous arbitrary parameter and q(z|x(i)) is a conditional distribution with a summary of an auxiliary noise variable p(). In this case, the marginal probability distribution for p() is known. The result of applying a distribution conversion on the data in q(z|x(i)) is z g(, x(i)). They consider qφ(z|x(i) ) that fulfills a Gaussian distribution where (z) N(z; 0, I). The calculation qφ(z|x(i) ) N(z; u, σ2 I), regularization term is given by Equation:17

Figure 6

where j represents dimension of z. While resolving the reconstruction term, by Monte Carlo evaluation, we attain the succeeding equation

Equation18

**Performance validation:**

Table 2:

and Fig. 6

The data reconstruction is predicated on the SVAE principle, and the exception's fundamental cause is looked at. The entire module is learned throughout the module's training phase using standard medical records. As a result, the decoder and encoder of the module would show on the rebuilt data of the hidden parameter z if the modules achieved superior illness diagnostic results on the tested data. This section uses the Heart Statlog, Pima Indian Diabetes, and EEG Eye-state datasets to evaluate the performance of the proposed HBESDMDLD approach. 270 instances with 13 attributes make up the initial Heart Statlog dataset. There are 768 cases with 8 attributes in the second PIMA Indians diabetes dataset. Eventually, there are 14,980 cases with 15 attributes in the EEG Eyestate dataset. provides the detailed dataset.

Table 3

provide a thorough security study of the NOA-SPECK approach on three different datasets. It is evident from the table values that the NOA-SPECK technique has For example, the NOA-SPECK technique obtains an encryption time of 6.82 s, a decryption time of 6.70 s, and a security level of 93.28% on the cardiac statlog dataset with 20% data size. The NOA-SPECK technique therefore achieves an encryption time of 31.88 s, a decryption time of 24.87 s, and a security level of 93.52% with 100% of the data size. Likewise, the NOA-SPECK technique produced decryption and encryption times of 9.63 and 8.35 seconds, respectively, and a security level of 92.78% on the PIMA Indian diabetes dataset with 20% data size. The NOA-SPECK technique therefore achieves an encryption time of 47.08 s, a decryption time of 44.01 s, and a security level of 95.87% with 100% of the data security in terms of encryption time, decryption time, and security level. Similarly, the NOA-SPECK technique produced encryption and decryption times of 21.73 and 19.82 seconds, respectively, and a security level of 93.70% on the EEG EyeState dataset with 20% data size. The NOA-SPECK technique thus achieves an encryption time of 95.38 s, a decryption time of 93.03 s, and a security level of 96.84% with 100% of the data amount.

A brief comparative analysis is presented in Table 4 and Fig. 7 to ensure the NOA-SPECK technique's increased security efficiency. According to the results, the Blowfish approach has the lowest security rating (90.81%). The security levels for the ECC and RSA models, respectively, have increased somewhat and are now 91.03% and 91.67%. Concurrently, 94.29% and 93.71%, respectively, of reasonable security levels have been reached using the SPECK and SC techniques. Nonetheless, with a maximum-security level of 94.46%, the NOA-SPECK approach has achieved notable efficiency.

Table 5 and Fig. 8 provide a thorough comparison of the HBESDMDLD's results with those obtained using the Heart Statlog dataset [37, 38]. It is clear from the findings that the RT model has the least outcome and the lowest accuracy (0.76). Likewise, the J48 model has marginally improved performance, with an accuracy of 0.77.

Table4

Figure 7

Figure 8

Table 5

Next, the RBF Network model, with an accuracy of 0.84, predicted a mild outcome. The EEPSOC-ANN and GBT models both concurrently displayed respectable accuracy of 0.95 and 0.95, correspondingly. The provided HBESDMDLD strategy surpassed all other methods with a maximum accuracy of 0.98, despite the DOD-GBT model trying to achieve an optimal efficiency of 0.96.

Table 6 and Fig. 9 [39] provide a thorough comparison of the results obtained using the HBESDMDLD and currently used methods on the Pima Indian Diabetes dataset. It is clear from the data that the Voted Perceptron technique yields the least accurate results, with a minimal accuracy of 0.67. The DT model's performance has also been marginally improved, with an accuracy of 0.74. Next, the LogitBoost model, with an accuracy of 0.74, showed a moderate outcome. The LR model has simultaneously demonstrated a respectable accuracy of 0.77. The reported HBESDM-DLD technique surpassed all other strategies with a better accuracy of 0.95, despite the MR-OGBT model's attempts to achieve the ideal correctness of 0.89.

Table 7 and Fig. 10 show a thorough comparison of the HBESDMDLD's results with those of other methods on the EEG EyeState dataset [40, 41]. Findings indicate that the least productive RT model has the lowest accuracy of 0.76.

Table 6

Figure 9

Table 7

Figure 10

Meanwhile, SA-LSTM has greater performance with 0.86 of accuracy. Both the RS-LSTM and DE-LSTM approaches have simultaneously demonstrated a respectable and comparable accuracy of 0.90 each. With a maximum accuracy of 0.93, the reported HBESDM-DLD approach surpassed all other models.

The study of the results described above makes it clear that the HBESDM-DLD technique has achieved the maximum level of secrecy while having a considerable detection accuracy. As a result, it can be used in a real-time setting for the secure transmission of medical records and the associated diagnostic procedure.

**Conclusion**

A novel HBESDM-DLD model for secure data transfer and diagnostic procedures has been created in this research. The concept that is being described consists of many stages of activities, including SPECK block cipher-based encryption, NOA-based optimum key generation, secure data management using the Hyperledger blockchain, and SVAE-based diagnosis. The health record transmission procedure has increased security due to the inclusion of NOA in the key generation process. The Hyperledger blockchain, meanwhile, offers secure health record management, allowing patients to grant or revoke access to any doctor or healthcare facility. Finally, the SVAE-based diagnostic procedure is used to identify any disorders that may occur. Using a benchmark medical dataset, the HBESDMDLD research's data are evaluated, and the findings are assessed using a variety of performance metrics. The experimental findings show that the HBESDM-DLD methodology outperforms cutting-edge techniques. Future versions of the HBESDM-DLD approach could incorporate training speed schedules for the SVAE model and a hyperparameter optimizer based on metaheuristic optimization.

**References:**

[1] Naz M, Al-zahrani F, Khalid R, Javaid N, Qamar A, Afzal M, Shafiq M (2019) A secure data sharing platform using blockchain and interplanetary file system. Sustainability 11(24):7054. https:// doi.org/10.3390/su11247054

[2] Hasselgren A, Kralevska K, Gligoroski D, Pedersen S, Faxvaag A (2020) Blockchain in healthcare and health sciences—a scoping review. Int J Med Informatics 134:104040. https://doi.org/10.101 6/j.ijmedinf.2019.104040

3. Zhang X, Poslad S (eds) (2018) Blockchain support for flexible queries with granular access control to electronic medical records (EMR). Institute of Electrical and Electronics Engineers Inc 4. Sun Y, Zhang R, Wang X, Gao K, Liu L (eds) A decentralizing attribute-based signature for healthcare blockchain. In: 27th International conference on computer communication and networks (ICCCN), 30 July 2018–2 Aug. 2018 5. Abu-elezz I, Hassan A, Nazeemudeen A, Househ M, Abd-alrazaq A (2020) The benefits and threats of blockchain technology in healthcare: a scoping review. Int J Med Informatics 142:104246. https://doi.org/10.1016/j.ijmedinf.2020.104246 6. Li H, Zhu L, Shen M, Gao F, Tao X, Liu S (2018) Blockchain-based data preservation system for medical data. J Med Syst. https://doi. org/10.1007/s10916-018-0997-3 7. Zhang P, White J, Schmidt D, Lenz G (2017) Applying Software Patterns to Address—Interoperability in Blockchain-based Healthcare Apps. arXiv preprint at arXiv:170603700 8. Passerat-Palmbach J, Farnan T, Miller R, Gross MS, Flannery HL, Gleim B (2019) A blockchain-orchestrated federated learning architecture for healthcare consortia. arXiv preprint at arXiv:1 910.12603. 9. Nguyen DC, Pathirana PN, Ding M, Seneviratne A (2021) A cooperative architecture of data offloading and sharing for smart healthcare with blockchain. arXiv preprint at arXiv:2103.10186 10. Al Mamun A, Jahangir MUF, Azam S, Kaiser MS, Karim A (2021) A combined framework of interplanetary file system and blockchain to securely manage electronic medical records. In: Proceedings of international conference on trends in computational and cognitive engineering. Springer, Singapore, pp 501–511 11. Bisogni C, Iovane G, Landi R, Nappi M (2021) ECB2: a novel encryption scheme using face biometrics for signing blockchain transactions. J Inf Secur Appl 59:102814. https://doi.org/10.1016/ j.jisa.2021.102814 12. Yates T (2020) Enhancing healthcare information sharing with blockchain technology. Open Sci J. https://doi.org/10.23954/osj. v5i2.2400 13. Fan K, Wang S, Ren Y, Li H, Yang Y (2018) MedBlock: efficient and secure medical data sharing via blockchain. J Med Syst. https:// doi.org/10.1007/s10916-018-0993-7 14. Hylock R, Zeng X (2019) A blockchain framework for patientcentered health records and exchange (HealthChain): evaluation and proof-of-concept study. J Med Internet Res 21(8):e13592. https://doi.org/10.2196/13592 15. Sun J, Ren L, Wang S, Yao X (2020) A blockchain-based framework for electronic medical records sharing with fine-grained access control. PLoS ONE 15(10):e0239946. https://doi.org/10.13 71/journal.pone.0239946 16. Chen Y, Ding S, Xu Z, Zheng H, Yang S (2018) Blockchain-based medical records secure storage and medical service framework. J Med Syst. https://doi.org/10.1007/s10916-018-1121-4 17. Ekblaw, Ariel et al (2016) A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data