IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

BLOCK CHAIN- BASED SECURE HEALTHCARE SYSTEM (BSHS) USING KNN ALGORITHM FOR PREDICT THE DISEASES

Dr.G.IndraNavaroj [1], P.BalaMurugan [2], K.Esakkimuthu [3], S.Gokul [4], I.Johnprakash[5]

Computer Science and Engineering
Jayaraj Annapackiam CSI College of Engineering, Nazareth, India.

Abstract: *The Blockchain-Based Secure Healthcare System for Diabetic-Cardio Disease Prediction is a novel healthcare solution that combines Blockchain technology and machine learning to predict the likelihood of developing diabetic-cardiovascular diseases. The application provides patients and healthcare providers with a secure platform to store and share medical data while maintaining privacy and security. The BSHS uses KNN algorithms to analyse patient data and predict the likelihood of developing diabetic cardio vascular diseases. The predictions are stored on the Blockchain, ensuring the security and immutability of the data. Patients can access their predictions and health status at any time through the application. Healthcare providers can also use the application to monitor patient health, provide timely interventions, and improve patient outcomes. The Blockchain-Based Secure Healthcare System for Diabetic-Cardio Disease Prediction provides an innovative solution to the growing healthcare challenges of chronic diseases and the need for secure, decentralized, and personalized healthcare services.*

Key words: Block chain, KNN, BSHS

I. INTRODUCTION

Health care refers to the maintenance or improvement of one's physical, mental, and social well-being through various medical, surgical, and preventive interventions. It involves the diagnosis, treatment, and prevention of diseases, injuries, and other medical conditions. Health care services are provided by a variety of healthcare professionals, including physicians, nurses, pharmacists, and allied health professionals. Health care systems may be operated by governments, private organizations, or a combination of both, and can vary widely in their organization, financing, and delivery. The goal of health care is to help people live longer, healthier lives, and to improve their overall quality of life. A blockchain-based framework for data sharing with fine-grained access control in decentralized healthcare systems. Blockchain-based framework for data sharing with fine-grained access control in decentralized healthcare systems. The system uses encryption to protect patient data and ensure confidentiality. The authors demonstrate that their system can effectively protect patient privacy while also providing efficient and secure data sharing among healthcare providers

II. LITERATUREREVIEW

"Blockchain for Secure Sharing of Medical Imaging Data via Untrusted Cloud Storage Providers" (by Nguyen et al. in IEEE Access): This paper proposes a Blockchain-based system for secure sharing of medical imaging data. The system uses encryption to ensure that patient data remains confidential and secure, even when stored on untrusted cloud storage providers. The authors demonstrate that their system can effectively protect patient privacy while also providing efficient and reliable access to medical imaging data [1].

"Secure sharing of medical data through Blockchain" (by Panchal et al. in Journal of Medical Systems): This paper explores the use of Blockchain for secure sharing of medical data. The authors propose a system that uses encryption to protect patient data and ensure confidentiality. They demonstrate that their system can effectively protect patient privacy while also providing efficient and secure sharing of medical data among healthcare providers [2].

"A review of Blockchain in healthcare: framework, applications, and future research directions" (by Al Omar et al. in Journal of Medical Systems): This paper provides a comprehensive review of the use of Blockchain in healthcare. The authors discuss how encryption can be used to protect patient data in Blockchain-based systems. They also highlight the potential benefits of using Blockchain in healthcare, including improved security, interoperability, and patient empowerment [3].

"Privacy-preserving Blockchain-based electronic health records system with automatic access control" (by Li et al. in Future Generation Computer Systems): This paper proposes a privacy-preserving Blockchain-based system for electronic health records (EHRs) with automatic access control. The system uses encryption to protect patient data and ensure confidentiality. The authors demonstrate that their system can effectively protect patient privacy while also providing efficient and secure access to EHRs [4].

"Blockchain-Based Decentralized Patient-Controlled EHR System" (by Yin et al. in Journal of Medical Systems): This paper proposes a Blockchain-based decentralized system for patient-controlled electronic health records (EHRs). The system uses smart contracts to enable patients to control access to their own health data, while also ensuring data security and privacy. The authors demonstrate that their system can effectively address the challenges of data privacy and security in traditional EHR systems [7].

III. IMPLEMENTATION

In the medical domain, control of access, validity, data confidentiality and integration are essential to protecting the identity of the patient and sharing data within the healthcare environment with other organizations. The traditional way to achieve control of access usually implies confidence among the data owner and the entities that store them. Such agencies are also entirely assigned servers for identifying and implementing policies on access management. Interoperability is the capability of dissimilar information systems, software or frameworks to link data between stakeholders in a synchronized way, within and across organizational borders, to improve individual safety [8,9].

1. BLOCK CHAIN

A Blockchain is a decentralized, distributed ledger technology that allows for secure, transparent, and immutable recording of transactions across a network of computers. It was originally created to serve as the underlying technology for crypto currencies such as Bitcoin, but it has since expanded to be used in various applications beyond just finance.

A Blockchain consists of a series of blocks, each containing a set of transactions, and each block is linked to the previous block in the chain. Once a block is added to the chain, it cannot be modified or deleted without also modifying all subsequent blocks in the chain, making the data stored on the Blockchain immutable [10].

2.SHA – 512

SHA-512 is a hashing algorithm that is used to generate a fixed-size message digest from input data. It belongs to the SHA-2 family of cryptographic hash functions and is widely used in various security applications such as digital signatures, message authentication codes, and password storage. The SHA-512 algorithm takes an input message of arbitrary length and produces a fixed-size 512-bit output called the message digest. The message digest is unique for each input message, and even a small change in the input message will result in a completely different message digest [11].

3 . ADVANCED ENCRYPTION STANDARD

Key Expansion: In this step, the original key is expanded into a key schedule that contains a number of additional round keys that will be used in the encryption process.

Initial Round: The input plaintext is divided into blocks, each of which is then subjected to an initial round of transformations. This involves XORing the plaintext block with a round key, and then applying a substitution-permutation network (SPN) to the result.

Rounds: The plaintext block is then subjected to a series of rounds, each of which consists of four steps:

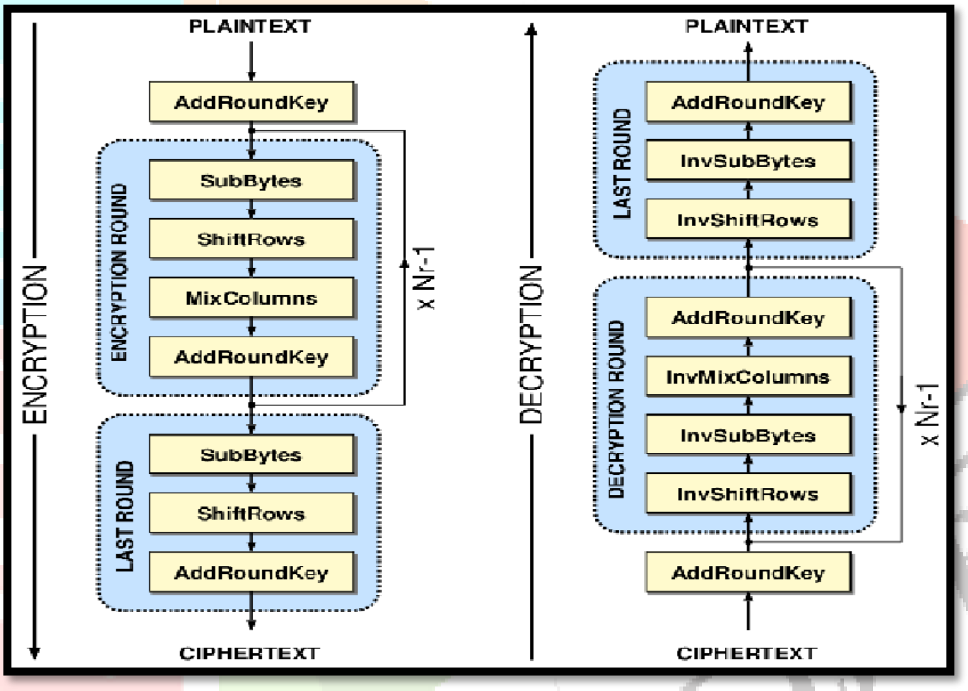
Sub Bytes: In this step, the values in the block are replaced with values from a lookup table, known as the S-box.

Shift Rows: In this step, the rows of the block are shifted by a certain number of bytes.

Mix Columns: In this step, the columns of the block are mixed together using a mathematical operation known as a matrix multiplication.

Add Round Key: In this step, the block is XORed with a round key.

Final Round: After the final round, the resulting cipher text block is output.



4. KNN Algorithm

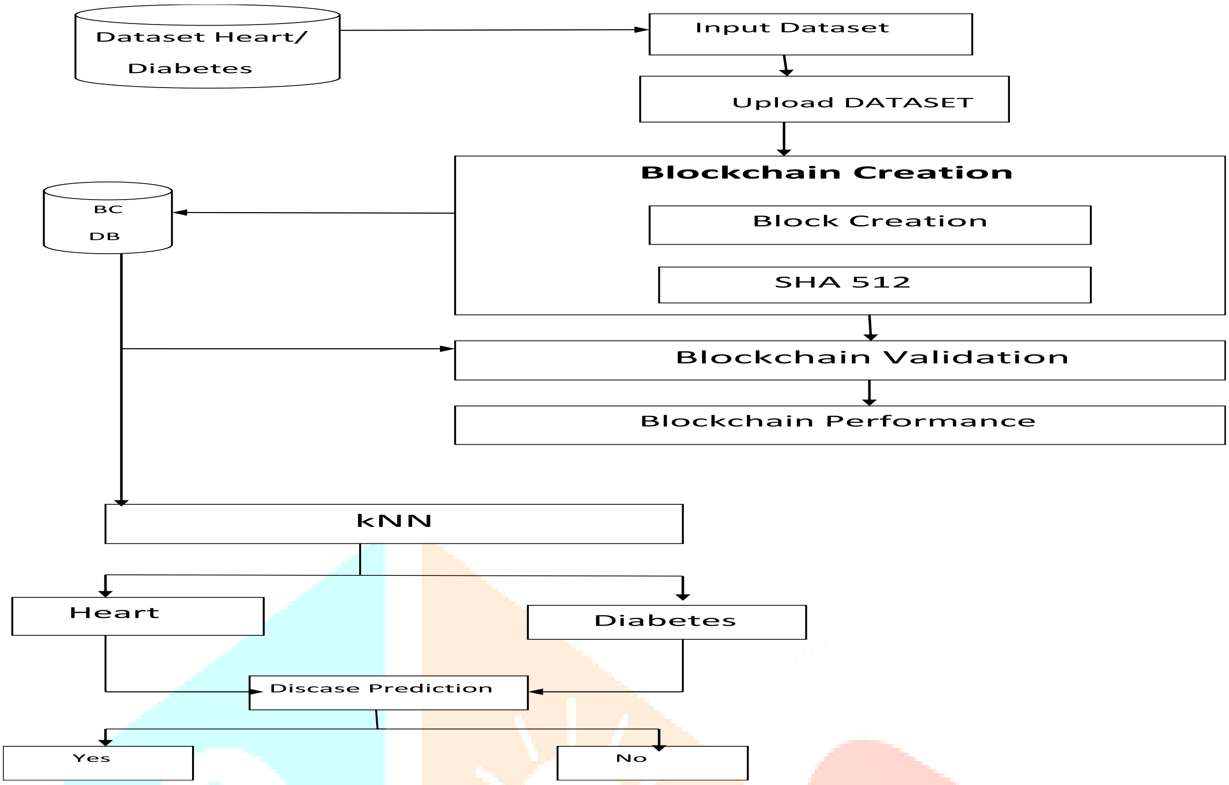
Determine the value of K: The first step is to determine the value of K (the number of nearest neighbours to consider). This value can be determined empirically or using cross-validation.

Calculate distance: Once the value of K is determined, the next step is to calculate the distance between the new data point and all the other data points in the dataset. Euclidean distance is the most commonly used distance metric.

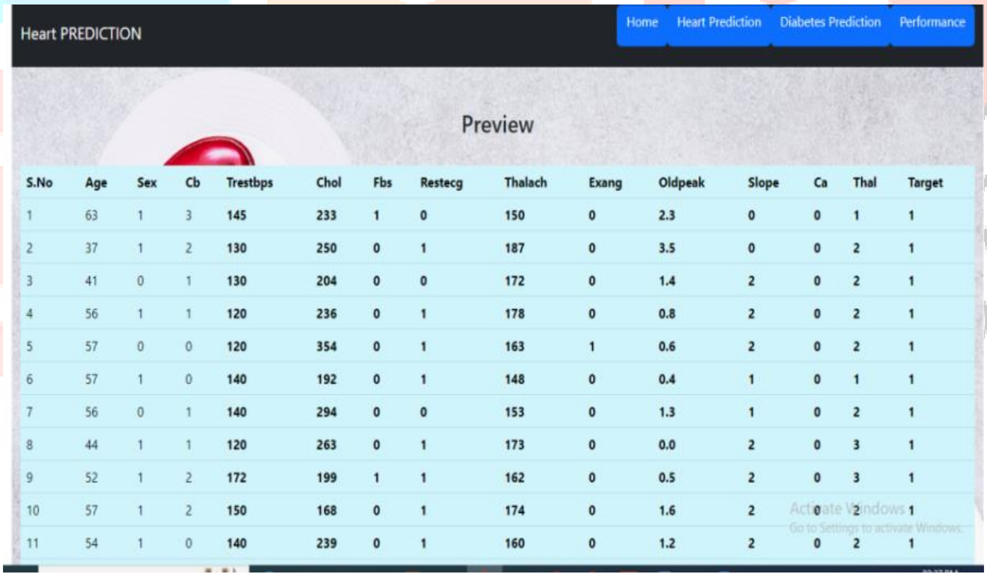
Find K nearest neighbours: After calculating the distance, the algorithm selects the K nearest neighbours to the new data point based on the calculated distance.

Predict the class or value: Once the K nearest neighbours are identified, the algorithm predicts the class of the new data point by taking the majority class among the K neighbours (for classification) [12].

IV.SYSTEM ARCHITECTURE

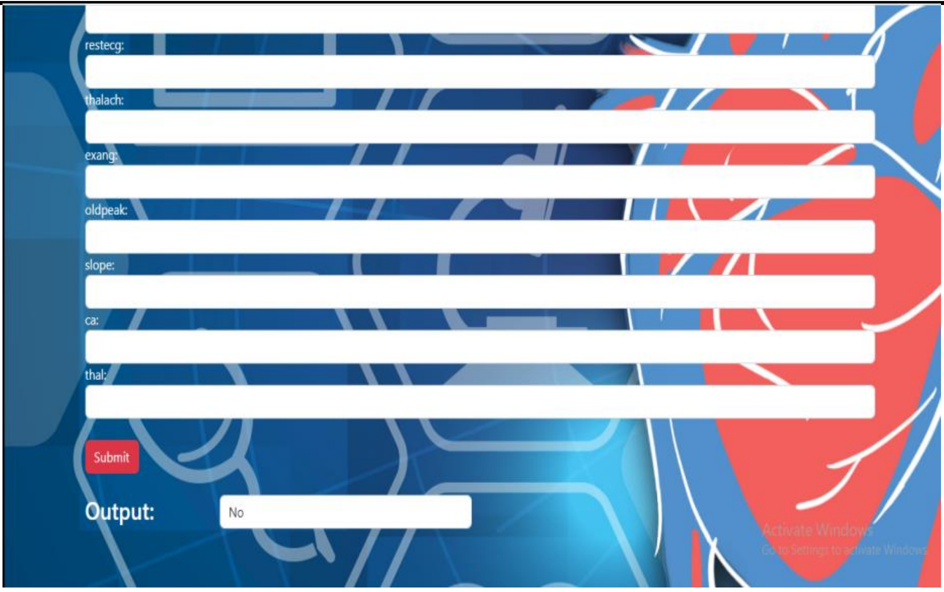


V. SCREENSHOTS



S.No	Age	Sex	Cb	Trestbps	Chol	Fbs	Restecg	Thalach	Exang	Oldpeak	Slope	Ca	Thal	Target
1	63	1	3	145	233	1	0	150	0	2.3	0	0	1	1
2	37	1	2	130	250	0	1	187	0	3.5	0	0	2	1
3	41	0	1	130	204	0	0	172	0	1.4	2	0	2	1
4	56	1	1	120	236	0	1	178	0	0.8	2	0	2	1
5	57	0	0	120	354	0	1	163	1	0.6	2	0	2	1
6	57	1	0	140	192	0	1	148	0	0.4	1	0	1	1
7	56	0	1	140	294	0	0	153	0	1.3	1	0	2	1
8	44	1	1	120	263	0	1	173	0	0.0	2	0	3	1
9	52	1	2	172	199	1	1	162	0	0.5	2	0	3	1
10	57	1	2	150	168	0	1	174	0	1.6	2	0	2	1
11	54	1	0	140	239	0	1	160	0	1.2	2	0	2	1

Heart prediction(screen shot)



restecg:

thalach:

exang:

oldpeak:

slope:

ca:

thal:

Output: No

Prediction Result(screen shot)

VI. FUTURE ENHANCEMENT

In the current healthcare system, the use of Blockchain plays a crucial role. It can result in automated processes for collecting and verifying data, correcting and aggregating information from different resources that are indisputable, defiant to manipulation and providing protected data, with condensed cybercrime chances and which also supports disseminated information, with system redundancy. This work proposes efficient Blockchain-based secure healthcare services for disease prediction in fog computing. Diabetes and cardio diseases are considered for prediction. The proposed work efficiently clusters and predicts the disease compared to other methods. In the future, the security and privacy for accessing patient medical data and some hybrid clustering and classification model can be added to enhance the performance of the prediction results.

VII.REFERANCES

1. Patel, Vishal. “A Framework for Secure and Decentralized Sharing of Medical Imaging Data via Blockchain Consensus.” *Health Informatics Journal*, vol. 25, no. 4, Dec. 2019, pp. 1398–411. *DOI.org (Crossref)*, https://doi.org/10.1177/1460458218769699.
2. Huang, Haiping, et al. “A Blockchain-Based Scheme for Privacy-Preserving and Secure Sharing of Medical Data.” *Computers & Security*, vol. 99, Dec. 2020, p. 102010. *DOI.org (Crossref)*, https://doi.org/10.1016/j.cose.2020.102010.
3. Chukwu, Emeka, and Lalit Garg. “A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations.” *IEEE Access*, vol. 8, 2020, pp. 21196–214. *DOI.org (Crossref)*, https://doi.org/10.1109/ACCESS.2020.2969881.
4. Al’Aref, Subhi J., editor. *Machine Learning in Cardiovascular Medicine*. Academic Press, 2021.
5. Chen, Liang, et al. “The Emerging Roles of Machine Learning in Cardiovascular Diseases: A Narrative Review.” *Annals of Translational Medicine*, vol. 10, no. 10, May 2022, pp. 611–611. *DOI.org (Crossref)*, https://doi.org/10.21037/atm-22-1853.
6. The State Budget Institution «The Research Institute of Health Care Organization and Medical Management of the Moscow Health Care Department», 115184, Moscow, Russia, et al. “The Methodological Approaches to Formation of Rating Evaluation of Activities of Medical Organizations and Health Care Systems in Russia and Abroad.” *Problems of Social Hygiene Public Health and History of Medicine*, vol. 27, no. 4, July 2019. *DOI.org (Crossref)*, https://doi.org/10.32687/0869-866X-2019-27-4-459-463.
7. Gordon, William J., and Christian Catalini. “Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability.” *Computational and Structural Biotechnology Journal*, vol. 16, 2018, pp. 224–30. *DOI.org (Crossref)*, https://doi.org/10.1016/j.csbj.2018.06.003.