International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Protecting Patients' Health Records using Block chain Technology

Niti Dey[1], Shivnath Ghosh[2], Souvik Pal[3,4], Sudipto Bhattacharyya[5]

Submitted: 05/05/2024 **Revised**: 17/06/2024 **Accepted**: 24/06/2024

Abstract: The world is advancing, and the progress necessitates a robust community for sustainable development. Healthcare data represents forecasts of an individual's well-being over time. Breaches in information occur due to the centralized approach to storing hospital records. According to the 2017 Phenomenon Cost of Data Breach Research, the cost of a security breach for healthcare entities is estimated to be $380 per record. Personal client information, such as names, addresses, and medical conditions, is frequently compromised in the era of smart homes and cities, which is inversely correlated with the security of Electronic Health Records (EHRs). Users often encounter difficulty accessing data due to the sophisticated privacy measures already implemented for EHRs. These systems must strike a delicate balance between the need for regular data interaction among users and healthcare providers, and safeguarding data. Blockchain technology addresses these challenges by distributing data in a decentralized and secure manner. It is utilized in healthcare to maintain the equilibrium between the availability and security of EHRs. This article introduces a Blockchain-based e-Health Report Management Model (BC-EHRMM) to effectively manage and preserve EHRs. Moreover, it provides patients, clinicians, and third parties with convenient and secure access to healthcare records while ensuring patient confidentiality. The research discussed in this article examines how it meets the needs of patients, clinicians, and other stakeholders, while addressing privacy and security concerns in healthcare 4.0.

Keywords: *Electronic Health Records, Data Protection, Block chain, Management Model, Secure Access*

1. An Overview:

It defines interoperability in the field of healthcare as the ability of disparate software programs and IT infrastructures to exchange and utilize data in a dependable, precise, and consistent manner [1]. Access to medical professionals or practitioners has worsened as the healthcare needs of people in many countries have increased dramatically in recent years [2]. In light of the proliferation of the term "block chain," it is becoming clear that this type of technological innovation is not important yet essential in the modern Internet era [3]. Patients can access healthcare through a wide range of providers, including community clinics, schools, medical practices, walk-in clinics, emergency rooms, pharmacies, diagnostic labs, and hospitals [4]. Providers are chosen based on factors such as cultural fit, care quality, comfort with patients, and accessibility [5]. Patients may sustain unnecessary injuries, excessive use of resources, and even death when their records are spread out across multiple providers [6]. If a healthcare provider tries to combine data from several distinct sources, the likelihood of making a mistake increases dramatically due to data fragmentation [7]. Medical errors leading to an adverse drug event account for 18% of all medical errors that occur in hospitals [8]. Manual errors are less likely to occur with interoperable systems. Reducing paperwork and eliminating unnecessary processes are two ways in which an integrated healthcare system can boost healthcare quality [9].

Inadequate information interchange leads to unnecessary repetition of diagnostic and laboratory testing, which accounts for a sizable portion of healthcare costs [10]. An interoperable health system's data accessibility is a key factor in reducing unnecessary duplication of effort [11]. When two or more systems can exchange data while keeping the meaning intact, they are said to be "semantically interoperable [12]." One of the most common targets of cybercriminals is the healthcare industry. One-third of all security breaches in 2014 were in the healthcare sector, according to a survey conducted that year [13]. In 2016, healthcare networks were the target of 88% of ransomware attacks. A block chain can be thought of as a distributed ledger that records and verifies all electronic transactions and communications that have taken place between participants. Each and every one of block chain's transactions is recorded and may be verified at any time [14].

[1] *Department of Computer Science and Engineering, Brainware University, Barasat, Kolkata, India*
dey.niti@gmail.com
[2] *Department of Computer Science and Engineering, Brainware University, Barasat, Kolkata, India*
dsg.cs@brainwareuniversity.ac.in
[3] *Department of Management Information Systems,*
Saveetha College of Liberal Arts and Sciences, Saveetha Institute of Medical and Technical Sciences,
Chennai, India
[4] *Department of Computer Science and Engineering*
Sister Nivedita University (Techno India Group)
Kolkata, India
Souvikpal22@gmail.com
[4]*Department of Computer Science & Engineering, Global Institute of Management and Technology, Krishnagar, India*
sdipto@gmail.com
Corresponding: Souvik Pal

Block chain technology allows for decentralized processing of transactions. As a result, Block chain has the potential to dramatically cut costs while boosting efficiency. Almost every industry, from energy to e-commerce to banking to government to administration to healthcare and education, has been affected by the revolutionary new technologies based on block chain technology [15]. Prominent businesses have quickly come to understand block chain technology's revolutionary potential, seeing it as a watershed moment in a variety of commercial use cases, including the healthcare industry. There has been a lot of work done in this area because block chain technology has been used by enterprises on such a wide scale. Many healthcare records were compromised as a result of these security lapses, which led to their loss, theft, disclosure, or unauthorized release [16]. There was an average of healthcare data breaches per day. The potential applications of block chain technology in the healthcare industry have recently received more attention. The healthcare industry is showing early signs of widespread interest in block chain technology. Block chain technology has the potential to consolidate a patient's medical and pharmaceutical records from several websites and data sources into a single, up-to-date database that doctors may use to better care for their patients. Significant technical obstacles prevent widespread use of block chain in the healthcare industry. As a result, it is both an urgent and difficult task to assess the effectiveness of various models of block chain technology for protecting online medical records system.

Block chain technology is distributed, transparent, and secure against manipulation. Block chain technology is predicated on distributed ledger technology, in which all nodes in a network keep their own copy of the ledger. Block chain technology has come a long way since then, and its many benefits have led to its widespread adoption across a wide range of industries. With block chain technology, many businesses are reaping the benefits of increased security and anonymity. When data is kept in a block chain, it is protected from tampering and can never be altered from its original state, guaranteeing its integrity and redundancy. Data from patient lab tests, X-rays, MRIs, CT-scans, financial documents, past medications, medical histories, and notes from last appointments are some examples of the massive amounts of information generated by the healthcare business every minute of every day [17].

The paper's main contributions are as shown below:

I. By introducing a model named Block Chain based e-Health Report Management Model (BC-EHRMM) that is built on the block chain which will allow for more efficient data distribution and maintenance, and many other problems that can be addressed by the distributed ledger technology.
II. In addition to safeguarding patients' confidentiality, this facilitates easy, protected access to medical records for patients, doctors, and other interested parties.
III. The paper explores into the ways in which healthcare 4.0 addresses concerns about patient privacy and safety without sacrificing the needs of clinicians and other stakeholders.

The rest of the paper is broken out as follows: In the first part, explain Block chain technology and discuss its potential uses in healthcare to enhance data exchange, interoperability, and integrity. In Section II, provide context for the techniques by which various approaches have attempted to address these issues. Section III details the computational experiments run to verify the solution's efficacy and dependability and describe the block chain's core procedures and components. In Section IV, briefly summarize our findings and offer suggestions for additional research. Section V offers the conclusion of the content described using the block chain.

2. Literature Review:

The healthcare sector's transition to new technology raises a number of pressing concerns that must be addressed. Priority should be given to addressing issues of data privacy, accessibility, and interoperability. Numerous studies have highlighted the security difficulty and conceded to little progress. The primary goals of medical data security are authentication, secrecy, and non-repudiation.

Jabbar, R et al [18] developed Improving Electronic Health Record Sharing through Block chain-Based Data Interoperability and Integrity Framework (BiiMED). One proposed solution is a decentralized Trusted Third Party Auditor (TTPA), while another is an access management system that allows doctors to more easily share electronic health records (EHRs). This work lays the groundwork for future studies on ensuring the integrity and compatibility of dynamic data in a decentralized setting. Main industry players place a premium on care continuum data integrity and interoperability. Despite being a top goal, this objective remains difficult to realize due to the vast quantities of EHR data, security concerns, and the variety of healthcare IT platforms. The proposed system, thus, addresses these concerns.

Zarour, M et al. [19] incorporated in the present research which employs a tried-and-true method for assessing block chain technology's effects, and it offers fresh inspiration and a promising new direction for academics of the future. For this purpose, we utilized the Fuzzy-Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) and the Fuzzy-Technique for

Analytical Network Process (F-ANP) to assign relative importance to the criteria and evaluate the results of various solutions. Furthermore, the findings of the empirical research will be a useful guide in selecting the best Block chain model for keeping EHRs secure. In this regard, a precise mechanism for analysing the impact of several existing block chain models for its features is necessary for choosing the best block chain model for reliable and protected electronic health records in the medical field.

Sharma, Y et al [20]. elaborated the use of Block Chain Technology [BCT] which can help keep these records confidential. Patients with serious conditions, such as heart disease or cancer, should have their electronic health records (known as an electronic medical record or patient health record) reviewed regularly after they are released from the hospital. Both the patient and the treating physician benefit greatly from the use of the electronic medical record. More precautions must be taken to prevent the disclosure or misuse of these medical files. In rare cases, it has been seen that the security of a patient's electronic medical records has been compromised. In this paper, we will present a thorough overview of the various approaches to protecting the confidentiality of EMR by means of block chain technology. Block chain is an implementation of distributed ledger technology, is one sort of decentralized technology. The immutability and security of block chain technology make it an ideal solution for storing sensitive information. While the technology's benefits have been demonstrated in various fields, some detractors have raised questions about it due to technical problems such as block chain storage capacity and some security issues.

Han, Y et al [21]. proposed by providing a definition of Electronic Health Records (HER -BT) and of block chain technology, and then propose some traditional schemes built on block chain to improve EHR interoperability and privacy. Then, we take a look at the problems that still need fixing in data management efficiency, access equity, and user confidence. This article argues that if block chain-based EHRs are to be implemented, further research in health informatics, data sciences, and ethics is required. Concerns about healthcare inequities, a large carbon footprint from computing needs, and patient mistrust must be factored into block chain-based EHR systems.

Ghazal, T. M et al [22]. introduced with the goal to supply secure solutions, this research developed a Block Chain-based Encryption Framework [BC-EF] based on a computational intelligence approach. The suggested method outperforms the state-of-the-art methods, with a training accuracy of 0.93 and a validation accuracy of 0.91. EHRs for financial gain or disclose the contents of EHRs to competitors in a direct manner. Recently, block-chain has emerged as one of the most effective tools for maintaining privacy and security. Eventually, this security method is expected to eradicate the risks associated with conventional remote health monitoring systems. To prevent unwanted parties from accessing encrypted data, block chain uses encryption. Different healthcare related security approaches [23-28] have been discussed in this related field.

Existing approaches such as BiiMED, F-ANP, BCT, EHR -BT, and BC-EF are utilized to ensure the security and privacy of electronic health records (EHRs), as well as the data integrity of patient records. As a result, the Block Chain based e- Health Report Management Model (BC-EHRMM) is created to assist in keeping tabs on the various aspects of electronic health record (EHR) administration, including security and patient confidentiality [29-32].

3. Block Chain based e- Health Report Management Model (BC-EHRMM):

Block chain is a distributed ledger mechanism that stores data as encrypted blocks of information linked together in chains [33-36]. Hence consensus algorithms, all the nodes in the block chain agree on which blocks can be viewed legitimately by which users. In order to be added to the data chain, a data block must first be checked to ensure it is correct and relevant. In typical setups, each node can store its own copy of the block chain and track exactly when and by whom any given piece of data is viewed [37-39].

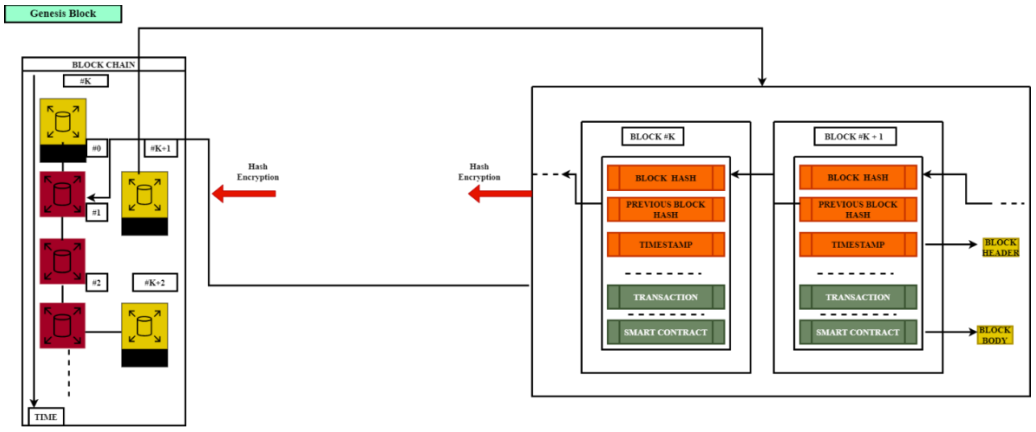

Fig 1. Block chain Structure

Block chain's advantages include greater decentralization, more transparent data, and enhanced privacy and security. This article argues that further research in health informatics, data sciences, and ethics is required before block chain-based EHRs may be implemented. Potential inequalities in healthcare resources, the enormous environmental impact of computing demands, and patient mistrust all need to be factored into block chain-based EHR systems. In addition, the network as a whole, rather than a single authority, decides if a given block should be included to the chain. In Figure 1, we can see the structure of a block chain, down to the individual blocks. Since each node in the block chain stores an identical copy of the block chain, it is impossible to make any changes to the data without alerting all of the other nodes. Encrypting the information in each block using a hash function, such an encryption algorithm, is essential for the privacy and security of block chain. Since cryptographic hashes are strong one-way functions, it is extremely impossible to reconstruct the original plain text from the hash value, making the block chain impenetrable to malicious actors. The cryptocurrency market is a pioneer adopter of block chain technology. Its decentralized nature, openness, and security characteristics may help address the issue of poor interoperability and data leaks in electronic health records.

The Healthcare Block chain System is a framework for electronic health information and remote patient monitoring. For confidentiality purposes, it employs an Ethereum-based private block chain. It enables full transparency into all data transactions on the block chain and keeps a secure log of who started them. All stakeholders are notified of potential security issues in remote patient monitoring.

No central server is necessary in a peer-to-peer network, making it a truly decentralized system. Information on a block chain network is less likely to be compromised since it is based on decentralized peer-to-peer (P2P) network technology rather than a centralized server.

$$Bn = \frac{{K_p}^n(y)+(1-\exp(-k_{in}+K_n))}{K^n(y+1)-{K_p}^n(y)} \quad (1)$$

${K_p}^n(y)$ and ${K_p}^n(y+1)$ are nodes of the block chain p at time y and time $y+1$ as per equation (1). Bn be the centralized server, K^n be the nodes of the previous block chain components and k_{in} be the input of the same nodes . The data capacity of nth directional individual and the mass flow rate n th directional understanding for patient. y is the knowledge-based expertise of the understanding of patient. That is the rate of n th-dimensional understanding in health sector.

$${I_q}^n(y)^* = fI^m(y)e^{{K_q}^n(y)-K^n(y)} \quad (2)$$

The building blocks of information generation denoted by ${I_q}^n$ for the component y are the intellectual management skills of the information agent's development be fI^m. In equation (2), the n-dimensional data associated with the operator I grows at the instant y is symbolically represented as exponential factor.

One of the most pressing problems we face today is achieving the strategic goal of enhancing service quality through the development of dynamic, digitally benchmarked, and ever-evolving clinical data.

$$\mathrm{HI_K} = \sum_m[\mathrm{I(m)} - \mathrm{I_E(m)}] * \mathrm{D_p/P_D} \quad (3)$$

System Information of specific patient health record $\boldsymbol{HI_K}$ can be obtained from equation (3), in which $\boldsymbol{I(m)}$the Information is given to the system, $\boldsymbol{I_E(m)}$ is the individual components, $\boldsymbol{D_p}$ is the database, $\boldsymbol{P_D}$ and is the patient database and $\boldsymbol{m}$ be the m number of vectors.

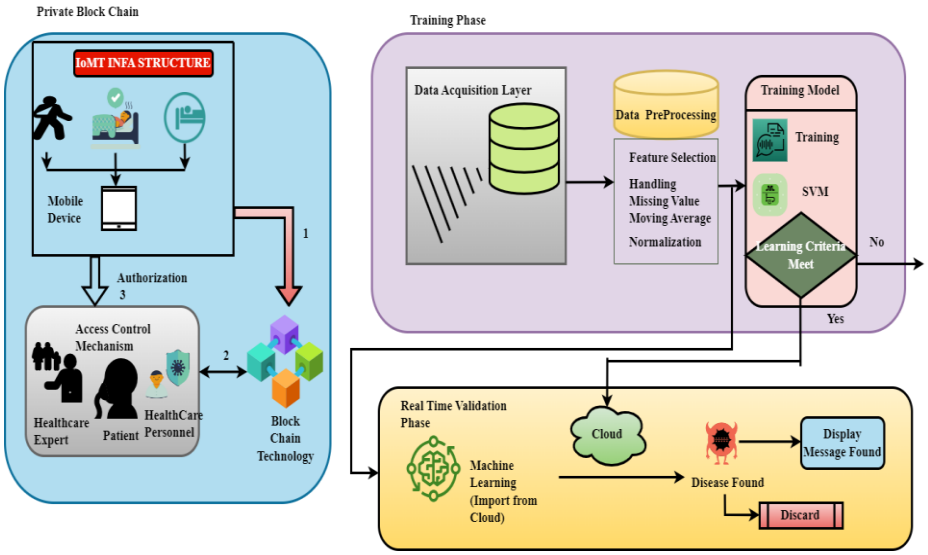

Fig 2. Secure communication Framework Proposal

Many advanced tools have been developed and integrated into the healthcare monitoring system with the advent of Internet of Medical Things (IoMT) technology. However, there are substantial difficulties with privacy and security when transmitting patient healthcare data. Recent planning and the interaction protocols (primary system) are unable to appropriately respond to system requests like verification, permission, and access management due to the ever-increasing number of devices and users.

$$\mathrm{P.I(n)} = \mathrm{N(P)}.\frac{\mathrm{I_{max}}}{\mathrm{n}} + \mathrm{A_t} + \mathrm{Add_t} + \mathrm{DOB} + \mathrm{DB} \quad \textbf{(4)}$$

As inferred from the above equation (4) $P.I(n)$ is the personalized information of the patient, $N(P)$ be the number of health records, I_{max} be the Information for the maximum patient, A_t be the age of the person, Add_t be the address of the information of the patient, DOB be the date of birth of the patient and DB be the database of the health records of the patient.

$$P.I_i = \frac{Z_i - X_i}{R_i} * \sum_{i=j}^{n}(Z + X_i), \qquad Z_i = (\,(1) + I_i\,/\,\sum_{i=1}^{n} 1 - I_i\,) \quad \textbf{(5)}$$

$P.I_i$ is the personal account of the patient

X_i is the given information of the system to block chain

I_i is the information gained through the proposed method

R_i is the output measured with the product of a standard block chain of given information included.

Z_i is the Encryption factor

$1 - I_i$ is used for finding the whole value from the central unit

The research presented here proposes private block chain-based encryption architecture as a solution to the many steps of authorization and authentication problems. The suggested research structure depicted in figure 2 safeguards patients' electronic health records while providing effective e-health monitoring. Figure 2 depicts the proposed system's breakdown into its component parts: the private block chain, the training phase, and the validation phase. The first step in the proposed framework's resource authorization and access control process is for the IoMT infrastructure to sense patient data and send that information to the block chain. Patients' medical histories must be accessible to all legitimate users of the healthcare IT infrastructure, including physicians, patients, and other healthcare professionals. Health records from various providers, including clinics, hospitals, and doctors' offices, are recognized by the IoMT framework. Patients, doctors, nurses, and other medical staff members must all submit requests for access to a patient's medical records to be able to view those records.

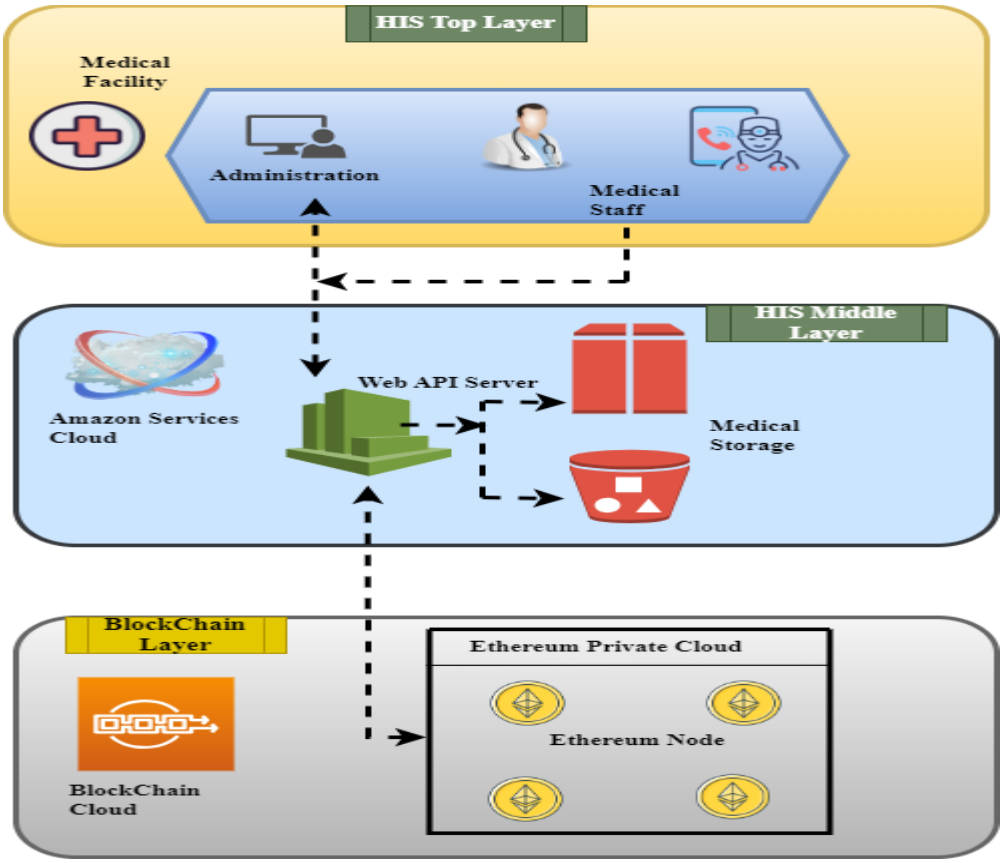

Fig 3. Design of the proposed system

The goal of this paper is to provide an overview of the created health intelligent system (HIS) and to discuss about the Block chain architecture BiiMED.

Health Intelligent System (HIS):

Health-related information systems (HIS) are created with the intention of managing healthcare data, such as managing a hospital's day-to-day operations, reviewing healthcare policy choices, collecting and storing electronic medical records (EMR), and exchanging EMR. This comprehensive index includes classifications for diseases, symptoms, indications, environmental factors, social setting, complaints, and exceptional situations. In addition, the DICOM standard (Digital Imaging and Communications in Medicine) is used here. It's the gold standard for sharing and managing medical imaging data and information, such as storing and sending images. This allows for multiple brands of PACS, networking hardware, printers, workstations, servers, and scanners to function together. Finally, the HIS makes use of the virtual Medical Record (vMR), a standardized data model for electronic health records that is designed to facilitate the integration of CDS. Electronic health records (EHRs) can be shared throughout several hospitals and clinics. The suggested HIS design is shown in Figure 3, and it consists of a Top layer, a Middle layer, and a Bottom layer.

There are several different web portals for different types of healthcare providers. The layout allow for communication between the healthcare system and medical professionals. It is a web service hosted in the cloud that facilitates information sharing between various parts of the system's software. In addition, Binary Large Objects (BLOB) like Computed Tomography (CT) scans and radiology images are stored on the Medical Record server in this tier. BiiMED is in charge of overseeing and verifying all inter-hospital data exchanges. Ethereum is used in the development of the Block chain Framework. Many Ethereum nodes made up the Block chain Framework. Two of them have been put to work mining on Amazon servers.

Hospitals are able to link with one another through the AMS to exchange electronic health records and have the authority to verify the accuracy of the data exchanged. Module for Managing Users includes the Management Agreement for Healthcare Organizations, which can be used to add, edit, or remove healthcare organizations from the system. The contracts in the Exchange Management Module are of two different types: those governing access to medical facilities and those governing access to independent auditors. The first agreement is in charge of controlling who has access to what information. A key that permits the healthcare facility's HIS to access the shared data and retrieve patient information must be requested via the access management contract. The

second agreement gives the Medical Facility System's Trusted Third Party Auditor (TTPA) access to the combined data for verification purposes.

$$Ey = \frac{Qy}{(N)} \sum_{x=0}^{N} \quad N * \pi_x(yx + x(\pi_x - 1)) \tag{6}$$

Equation (6) reflects the effectiveness with which hospital resources are managed represented by Ey. Qy Stands for quality, $yx + x(\pi_x - 1)$ is the condition for the feature function. N represents the entire sum of patients admitted in the hospital for treatment analysis.

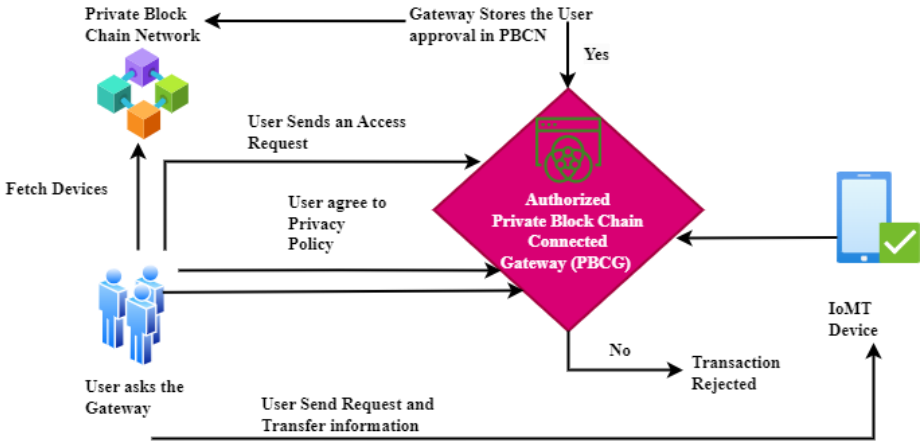

Fig 4. Security through Isolated Block chain Verification

The authentication process includes a section on what a smart contract is and what risks come with using one. All device-to-device and PBCG-to-PBCG interactions are managed by smart contracts to ensure the highest level of security and anonymity. As shown in figure. 4, the PBCG's contact with the devices is recorded and carried out within the block chain. One way to view the block chain is as a TTP, or trusted third party. As a result, the protocol's participants are immune to abuse. Raw data from the private block chain layer is transferred to the data acquisition layer for use in the training phase. The raw data is transmitted to the pre-processing layer, where feature selection, missing value handling, moving averages, and normalization are applied to reduce the noise. The SVM algorithm is then used to feed the cleansed data to the training model. Based on the sequence given in the above figure 4 the process is done and authentication is done.

1. $$AF = min\left(\sum_{j=1}^{n} \emptyset . f(\sqrt{Y_j^{1/2}})\right) . p(Y_j)) \tag{7}$$

2. *Equation (7) implies that AF is the first authentication function; as long as the user file remains consistent which is denoted by* $\sum_{j=1}^{n} \emptyset . f(\sqrt{Y_j^{1/2}}$, *new files can be added to it.*

Y_j be the input mechanism taken for consideration and which is to be authenticated. $\emptyset$ be the encryption constant. f be the frequency of the same.

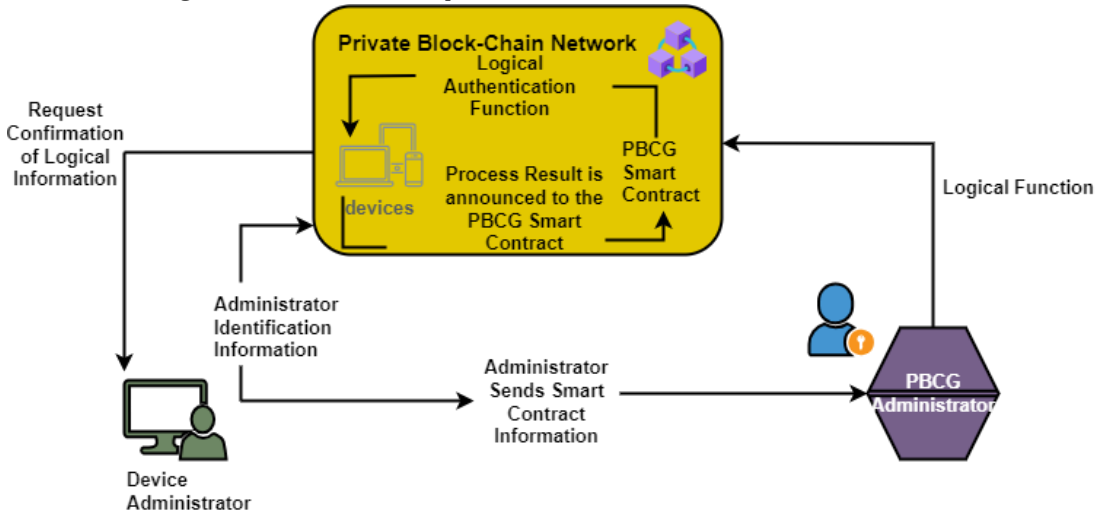

Fig 5. Block chain-based Authentication Mechanism

The above figure 5 shows the communication between devices using a block chain based authentication mechanism. Here two administrators are taken for consideration. Private block chain network is used with the rotation mechanism using logical authentication function and the process result is send to the PBCG Smart contract. Admin identification Information is send to the devices and admin sends smart contract information and other data to PBCG administrator. PBCG requests for logical information from the device administrator and PBCG admin contact PBCN through logical function and hence the communication is done between the devices using the Block chain based authentication mechanism.

Algorithm for Security for Healthcare Record Management Model: (S-HRMM)

Choice (S = (N, P), D)

Begin
***Step 1**: $N \leftarrow$ max level of patient records*
***Step 2**: $DB_N \leftarrow \emptyset$; (DB be the database of the health care record system)*
***Step 3**: Security (S);*
***Step 4**: $N \leftarrow \{S \mid DB_d \leq C_w,\ w \in V\}$ Multiple records with the same degree of database of each health record may exist.*
***Step 5**: For each $R_d \leftarrow 0,\ N \in V$, $R_y = 1, y \in N$;*
***Step 6**: for $S - 1 \geq G \geq N$ do*
***Step 7**: for $DB_N - \{ DB_N V \mid N = S \}$ do*
***Step 8**: if$(S, P) \in N$ then*
***Step 9**: $R_d + = P_R + N$ for all N ;*
***Step 10**: For all health records $Security \leftarrow \mid \{ R_d \mid R_d = N \} \mid < R_d$;*
***Step 11**: Privacy $\leftarrow \mid \{ P_d \mid R_d = N \} \mid < N_d$;*
End

Use Choice () in the above algorithm to select a patient's health record at a given tier. Let DB represent the health care record system's database, N represent the number of patients utilizing block chain-based devices, and R represent the average number of patients examined daily. N is the number of records, and Pd is the condition for maintaining confidentiality. With choose (), you may identify which node on a certain level represents a patient for the purposes of the record. There are N total patients in a block. After calculating each patient's connectedness, a single patient is selected as the navigator. Second, the patients () function determines the inverse connections between all patients on a given level. At last, the K most linked blocks are selected as the patients who will use block chain-based e-devices.

Next, we verify that the learning conditions are satisfied by examining the trained patterns. The learned output is saved in the cloud; otherwise, it is refreshed, and forth. In the validation stage, predictions are made using the trained patterns that were downloaded from the cloud. We double-checked our logic, making sure that if the sickness is indeed discovered, a message would be displayed to that effect, and that the procedure would be scrapped in the absence of such a finding. In the most common implementations of Block chains, operators of nodes in the network are rewarded in bitcoin for their part in maintaining data integrity and facilitating consensus within the decentralized ecosystem. The incentive, however, comes with costs for Block chain users in terms of computational performance and data storage. A cost-benefit analysis comparing the services provided by a healthcare to the current centralized and proprietary systems is thus required. To improve healthcare interoperability, block chain technology is being used to replace some traditional components. As an example, in this context, the quantity of data that can be saved in a medical center's patient register before the Block chain platform (like Ethereum) shuts down is being discussed. This section will discuss the "base case" for EHR exchange between hospitals. This is demonstrated in the authentication and authorization management for the healthcare facility is handled by the data access management module.

Tabulation 1: Comparison of Performance Analysis:

Number of Samples	BiiMED	F-ANP	BCT	EHR -BT	BC-EF	BC-EHRMM
10	12.4	35.4	46.7	50.1	58.2	60.3

20	15.5	24.8	48.5	50.4	59.3	62.2
30	19.3	29	45.2	52	63	64
40	21	32.8	43.9	58.7	66.1	68.9
50	25.8	30.6	48.6	53.5	69.5	74.4
60	24.4	30.3	41.3	55.1	72.2	76.6
70	29.2	39.1	59	59.9	74.3	77.9
80	32.6	41	57.8	63.7	76.7	79.6
90	30.1	43.7	55.6	67.4	77.9	80.2
100	30.7	48.6	50.4	69.1	80.7	81.3

The above table 1 shows that the comparison of performance analysis of different existing methods available. The research's authors propose a block chain-based IoMT platform for electronic health records. Users' medical records are stored safely because to the solution's usage of block chain technology and the Internet of Medical things. Users' privacy is protected since encrypted health data is first collected by a network of smart sensors and then stored on the Ethereum block chain's nodes. There is hope that block chain technology can assist EHR standardize, improve interoperability, and safeguard patient privacy. Block chain technology allows for decentralized data storage and sharing, yet it is not without its problems.

The proposed model, the Block Chain based e- Health Report Management Model (BC-EHRMM), is meant to be used in the development of EHR preservation and management methods. This research found that a cloud-based block chain management solution increased data integrity and efficiency prediction in smart systems. There have been extensive evaluations for accuracy, effectiveness, performance, security, and privacy have all been tested and measured.

4. Results & Discussion:

Despite the capacity of smart contracts to follow data requests, healthcare providers and individuals may continue to worry about the security of their personal information. Because of block chain's decentralized and transparent nature, despite the increased safety and security of data sharing, data regulation is more crucial than ever. Lack of regulation and education about block chain technology may cause distrust between healthcare providers and their patients. Support for minimally required structural interoperability, user identity and authentication, and Turing-complete operations are all guaranteed by this framework. To ascertain if the healthcare system's database management quality has improved, we propose simulating the system using the framework we've developed (BC-EHRMM). The results of various numerical simulations of efficacy, etc., are tested on representative samples and shared with the relevant parties. It is difficult to ensure the reliability of medical data stored in a centralized database. Sensitive patient information is generally stored in the records of a hospital or clinic in such a system, making it vulnerable to deletion or alteration by an intruder with access to the system [40].

Data loss can be avoided due to this simulation research, which assesses and addresses recommended efficiencies and other improvements in the intelligent healthcare system. BC-EHRMM is compared to other models including BiiMED, F-ANP, BCT, EHR -BT, and BC-EF in terms of accuracy, security performance efficiency, and privacy interval. Finally, problems with trust between patients and healthcare providers are a problem. The present research presents a computational intelligence-based system for improved and more efficient disease prediction.

4.1 Accuracy Analysis:

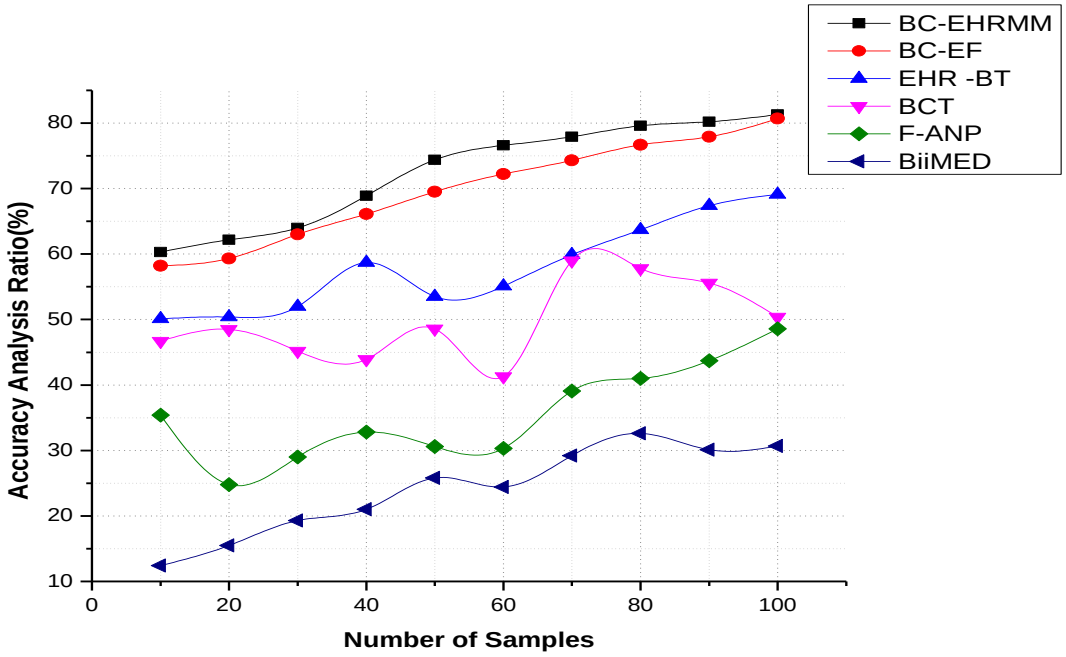

Figure 6. Accuracy Analysis

Accuracy analysis is shown in Figure 6. In the preceding graph, total samples are plotted along x, while accuracy analysis ratio is shown along y axis. Each method's samples are compared to one another. BC-EHRMM is the most precise approach available. The proposed strategy outperforms competing models in terms of accuracy.

4.2 Performance Analysis:

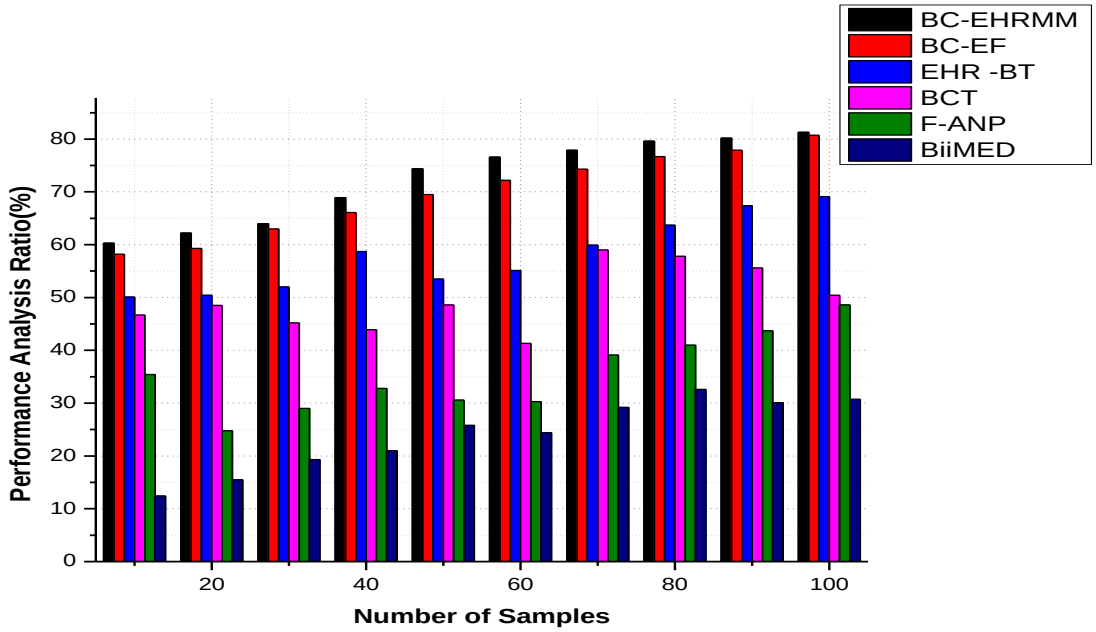

Figure 7. Performance Analysis

Figure 7 is a graph exhibiting a performance analysis, which shows the results of applying several existing proposed approaches to many different types of data. The ratio of performance analysis to total samples is plotted along the y axis of the above graph. Each method's samples are compared to one another. As may be seen in the graphic, BC-EHRMM outperforms its competitors.

4.3 Efficiency Analysis:

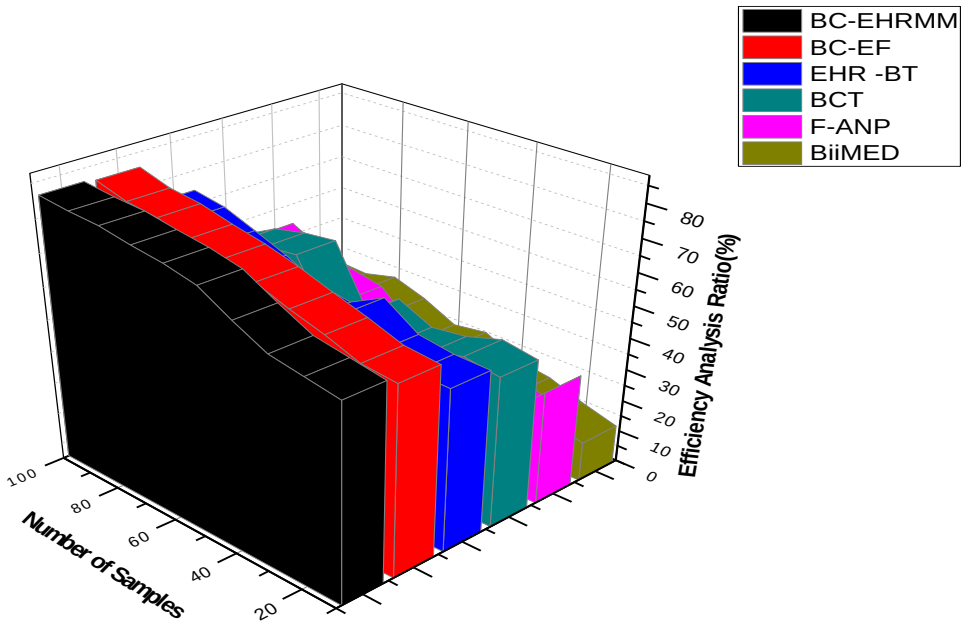

Figure 8. Efficiency Analysis

As can be seen in Figure 8, the BC-EHRMM method provides superior results to the status quo when it comes to uniformity and efficiency in physical health monitoring systems. The y-axis in the previous graph represents the efficiency analysis ratio, while the x-axis represents the total number of samples. There is a comparison of samples obtained using each technique. The proposed block chain-based health monitoring systems have been demonstrated to be superior to any currently available alternatives.

4.4 Security Analysis:

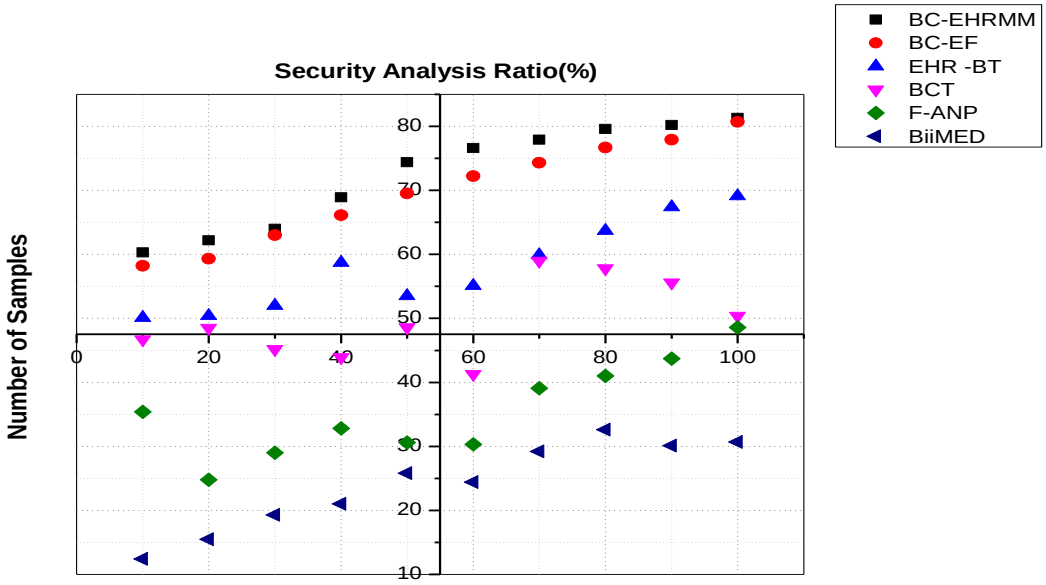

Figure 9. Security Analysis

Figure 9 shows how, in comparison to standard healthcare data security methods, analysis of user node security rates and reduced, optimized monitoring periods are achieved. Having accurate medical data on file is beneficial for several reasons. Access to medical records is granted using block chain indications and the user's selections from the formula. Over and over, you'll need to utilize many blocks to probe the state next door, and you'll have to keep track of your findings. Information from the user nodes is used to make predictions about individual patients. By keeping close tabs on the patient's movements, resources can be used more effectively.

4.5 Privacy Analysis:

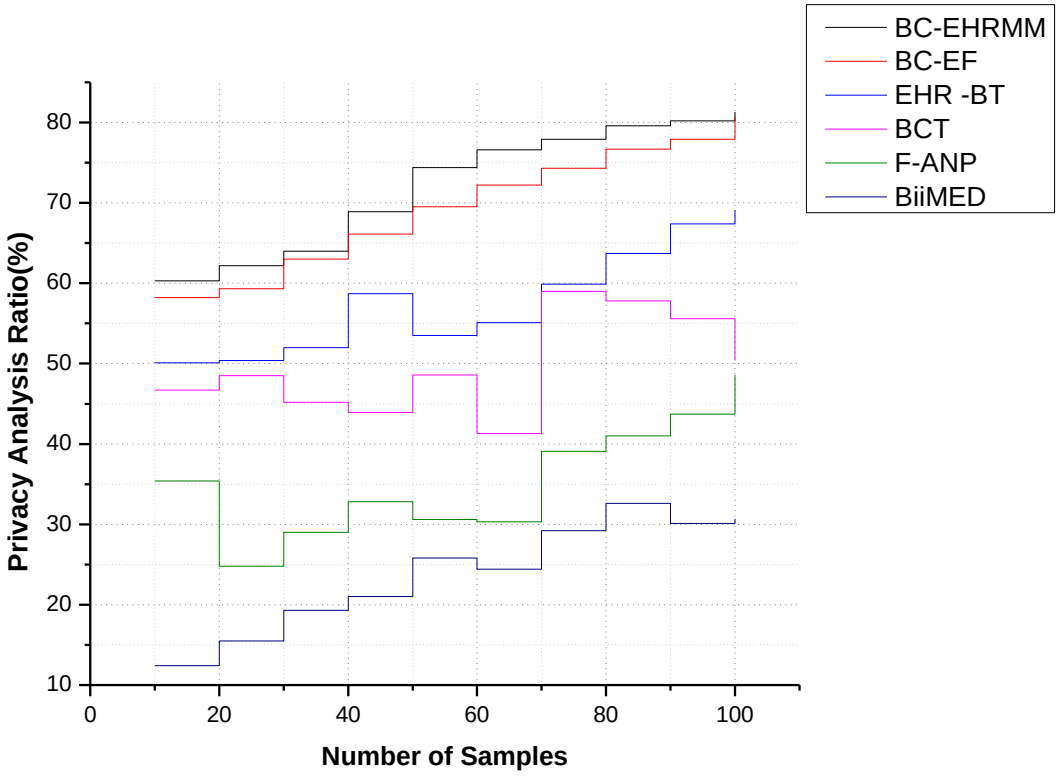

Figure 10. Privacy Analysis

The most consistent approach is the BC-EHRMM method, as shown in Figure (10), which compares the privacy of various methods and physical monitoring equipment. The expected number of iterations for health monitoring systems is higher than the usual. A reaction space is generated for the points in biometric and medical data, which might be continuous or discrete. The study's goal is to provide a model for protecting individuals' privacy in healthcare settings, one that adheres to the standards set by the public sector. This block chain-based scheme aspires to improve healthcare security.

4.6 Reliability Analysis:

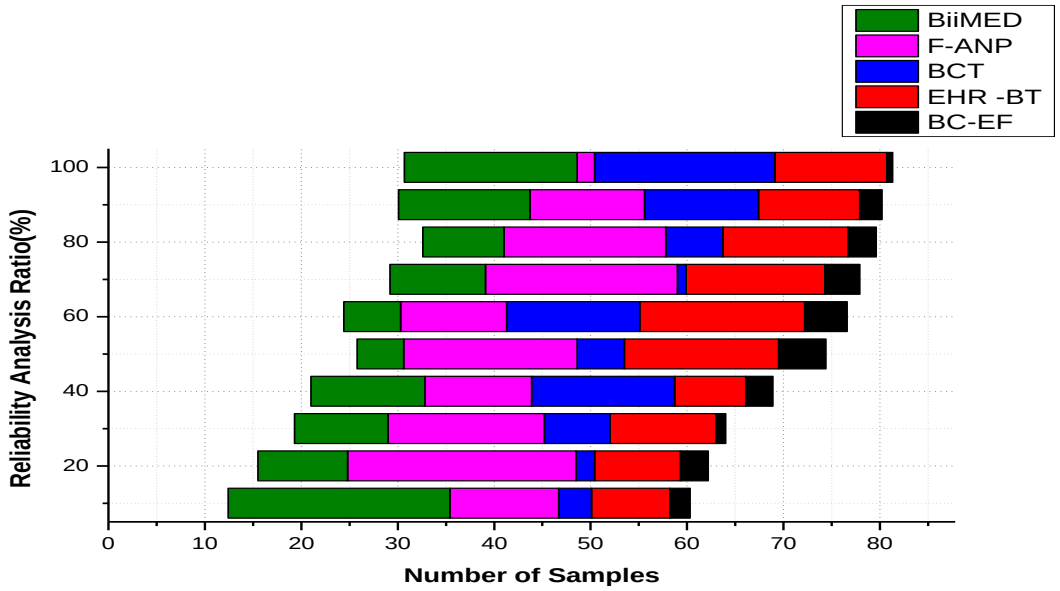

Fig 11. Reliability Analysis

Figure 11 depicts the adaptability aspect for the reliability, therefore keeping an eye on its data and being ready for problems is an essential input. Having a system in place to inspect all equipment on a regular basis ensures the continued smooth operation of crucial data. This not only serves as oversight, yet verifies that all conditions for a valid evaluation are met. Block chains are widely used for this purpose since they have been shown to boost data dependability in studies. The success reliable rate is maximal for a given input level when comparing the reliability with which one can save the data.

4.7 Safety Analysis:

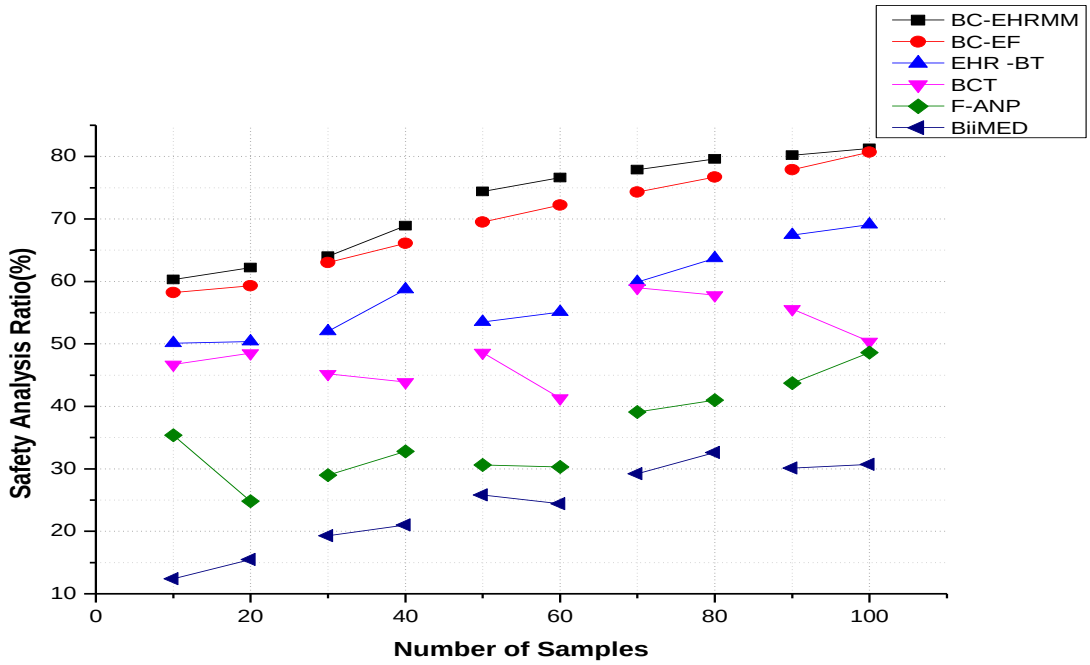

Fig 12. Safety Analysis

Figure 12 demonstrates that this methodology is superior than others for spotting flaws in input-based reasoning. Safety analysis, the first step in fixing any issue, is the most important. To make sure a system can withstand and recover from a variety of threats, safety testing must be performed. Research have demonstrated that block chains increase data reliability, hence they are extensively employed for this purpose. When contrasting the certainty with which one can store the data, the success safety rate is at its highest for a given input level.

In terms of smart environment performance, security, efficiency, privacy, and accuracy analysis, the proposed BC-EHRMM is shown to be superior to BiiMED, F-ANP, BCT, and EHR -BT. the various benefits of the new model become apparent when compared to the conventional methods of safeguarding healthcare information.

5. Conclusion:

The healthcare industry is using block chain technology as a means of protecting patient privacy and data. While we now have the capacity to retain this deluge of information, the security and privacy safeguards in place to protect it are inadequate, especially when discussing a computerized medical history (EMR) of a patient. A patient's medical history is personal information that should not be shared without the patient's explicit permission. Therefore, the block chain network may prove to be quite helpful. Concerning the confidentiality of the data, studies have been done. This research proposal presents a private block chain-based encryption architecture that takes a computational intelligence approach to security. The results of the tests conducted on a simple encryption framework demonstrate the efficacy of a private block chain infrastructure combined with computational intelligence. Results show the benefits of using a large amount of training data. The BC-EHRMM framework provides a powerful tool for conducting in-depth analyses of complex security and privacy problems, including evaluations of block chain systems. It has been determined that the Private Block chain alternative model is the preferred method of providing reliable and efficient healthcare block chain services to the public. Patients' electronic health records (EHRs) could be handled differently to private Block chain technology, which provides safer platforms for data sharing in healthcare by shielding data across a decentralized peer-to-peer infrastructure. To effect good change in the healthcare industry, future research could focus on evaluating the relative significance of different healthcare block chain

service deployments. We anticipate that in the not-too-distant future, we will be able to employ block chain technology to establish a more secure method of securing patients' medical records.

References:

[1] Rai, B. K. (2023). PcBEHR: patient-controlled blockchain enabled electronic health records for healthcare 4.0. *Health Services and Outcomes Research Methodology*, *23*(1), 80-102.

[2] Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M., & Abid, M. (2021). HealthBlock: A secure blockchain-based healthcare data management system. *Computer Networks*, *200*, 108500.

[3] Fatima, N., Agarwal, P., & Sohail, S. S. (2022). Security and privacy issues of blockchain technology in health care—A review. *ICT Analysis and Applications*, 193-201.

[4] Dwivedi, S. K., Amin, R., Lazarus, J. D., & Pandi, V. (2022). Blockchain-Based Electronic Medical Records System with Smart Contract and Consensus Algorithm in Cloud Environment. *Security & Communication Networks*, *2022*.

[5] Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks*, *2*, 130-139.

[6] Jain, M., Pandey, D., & Sharma, K. K. (2022). A Granular Approach to Secure the Privacy of Electronic Health Records Through Blockchain Technology. *International Journal of Distributed Systems and Technologies (IJDST)*, *13*(8), 1-20.

[7] Mohammed, R., Alubady, R., & Sherbaz, A. (2021, March). Utilizing blockchain technology for IoT-based healthcare systems. In *Journal of Physics: Conference Series* (Vol. 1818, No. 1, p. 012111). IOP Publishing.

[8] Roosan, D., Wu, Y., Tatla, V., Li, Y., Kugler, A., Chok, J., & Roosan, M. R. (2022). Framework to enable pharmacist access to health care data using Blockchain technology and artificial intelligence. *Journal of the American Pharmacists Association*, *62*(4), 1124-1132.

[9] Srivastava, S., Singh, S. V., Singh, R. B., & Shukla, H. K. (2021). Digital Transformation of Healthcare: A blockchain study. *International Journal of Innovative Science, Engineering & Technology*, *8*(5).

[10] Hashim, F., Shuaib, K., & Sallabi, F. (2022). Connected blockchain federations for sharing electronic health records. *Cryptography*, *6*(3), 47.

[11] Jabarulla, M. Y., & Lee, H. N. (2021, August). A blockchain and artificial intelligence-based, patient-centric healthcare system for combating the COVID-19 pandemic: Opportunities and applications. In *Healthcare* (Vol. 9, No. 8, p. 1019). MDPI.

[12] Pandey, P., & Litoriya, R. (2020). Implementing healthcare services on a large scale: challenges and remedies based on blockchain technology. *Health Policy and Technology*, *9*(1), 69-78.

[13] Ali, A., Rahim, H. A., Pasha, M. F., Dowsley, R., Masud, M., Ali, J., & Baz, M. (2021). Security, privacy, and reliability in digital healthcare systems using blockchain. *Electronics*, *10*(16), 2034.

[14] Elangovan, D., Long, C. S., Bakrin, F. S., Tan, C. S., Goh, K. W., Yeoh, S. F., ... & Ming, L. C. (2022). The use of blockchain technology in the health care sector: systematic review. *JMIR medical informatics*, *10*(1), e17278.

[15] Díaz, Á., & Kaschel, H. (2023). Scalable Electronic Health Record Management System Using a Dual-Channel Blockchain Hyperledger Fabric. *Systems*, *11*(7), 346.

[16] Singal, P., Sharma, G., & Gautam, S. (2020). Transforming healthcare with blockchain. *International Journal of Blockchains and Cryptocurrencies*, *1*(3), 302-311.

[17] Sharma, A., Kaur, S., & Singh, M. (2021). A comprehensive review on blockchain and Internet of Things in healthcare. *Transactions on Emerging Telecommunications Technologies*, *32*(10), e4333.

[18] Jabbar, R., Fetais, N., Krichen, M., & Barkaoui, K. (2020, February). Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)* (pp. 310-317). IEEE.

[19] Zarour, M., Ansari, M. T. J., Alenezi, M., Sarkar, A. K., Faizan, M., Agrawal, A., ... & Khan, R. A. (2020). Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records. *IEEE Access*, *8*, 157959-157973.

[20] Sharma, Y., & Balamurugan, B. (2020). A survey on privacy preserving methods of electronic medical record using blockchain. *J. Mech. Contin. Math. Sci*, *15*(2), 32-47.

[21] Han, Y., Zhang, Y., & Vermund, S. H. (2022). Blockchain Technology for Electronic Health Records. *International Journal of Environmental Research and Public Health*, *19*(23), 15577.

[22] Ghazal, T. M., Hasan, M. K., Abdullah, S. N. H. S., Bakar, K. A. A., & Al Hamadi, H. (2022). Private blockchain-based encryption framework using computational intelligence approach. *Egyptian Informatics Journal*, *23*(4), 69-75.

[23] Doss, S., Paranthaman, J., Gopalakrishnan, S., Duraisamy, A., Pal, S., Duraisamy, B. and Le, D.N.,

2021. Memetic optimization with cryptographic encryption for secure medical data transmission in IoT-based distributed systems. Computers, Materials & Continua, 66(2), pp.1577-1594.

[24] Dutta, P., Paul, S., Obaid, A.J., Pal, S. and Mukhopadhyay, K., 2021, July. Feature selection based artificial intelligence techniques for the prediction of COVID like diseases. In Journal of Physics: Conference Series, Vol. 1963, No. 1, pp. 012167.

[25] Rakshit, P., Nath, I. and Pal, S., 2020. Application of IoT in healthcare. Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm, pp.263-277.

[26] Biswas, R., Pal, S., Sarkar, B. and Chakrabarty, A., 2020. Health-care paradigm and classification in IOT ecosystem using big data analytics: an analytical survey. In Intelligent Computing in Engineering: Select Proceedings of RICE 2019, Springer, pp. 261-268.

[27] Tuan, N.A., Akila, D., Pal, S., Sarkar, B., Tran, T.K., Nehru, G.M. and Le, D.N., 2022. Dynamic Data Optimization in IoT-Assisted Sensor Networks on Cloud Platform. Computers, Materials & Continua, 72(1).

[28] Mukhopadhyay, K., Chattopadhyay, S., Dutta, S.P., Bhattacharyya, S., Pal, S. and Alzeyadi, A.K., 2023, September. Recent advancement of block chain in health care. In AIP Conference Proceedings, AIP Publishing, Vol. 2845, No. 1.

[29] Gaur, L., Afaq, A., Solanki, A., Singh, G., Sharma, S., Jhanjhi, N. Z., ... & Le, D. N. (2021). Capitalizing on big data and revolutionary 5G technology: Extracting and visualizing ratings and reviews of global chain hotels. Computers and Electrical Engineering, 95, 107374.

[30] Attaullah, M., Ali, M., Almufareh, M. F., Ahmad, M., Hussain, L., Jhanjhi, N., & Humayun, M. (2022). Initial stage COVID-19 detection system based on patients' symptoms and chest X-ray images. Applied Artificial Intelligence, 36(1), 2055398.

[31] Ghosh, G., Verma, S., Jhanjhi, N. Z., & Talib, M. N. (2020, December). Secure surveillance system using chaotic image encryption technique. In IOP conference series: materials science and engineering (Vol. 993, No. 1, p. 012062). IOP Publishing.

[32] Singhal, V., Jain, S. S., Anand, D., Singh, A., Verma, S., Rodrigues, J. J., ... & Iwendi, C. (2020). Artificial intelligence enabled road vehicle-train collision risk assessment framework for unmanned railway level crossings. IEEE Access, 8, 113790-113806.

[33] Gaur, L., Singh, G., Solanki, A., Jhanjhi, N. Z., Bhatia, U., Sharma, S., ... & Kim, W. (2021). Disposition of youth in predicting sustainable development goals using the neuro-fuzzy and random forest algorithms. Human-Centric Computing and Information Sciences, 11, NA.

[34] Nanglia, S., Ahmad, M., Khan, F. A., & Jhanjhi, N. Z. (2022). An enhanced Predictive heterogeneous ensemble model for breast cancer prediction. Biomedical Signal Processing and Control, 72, 103279.

[35] Humayun, M., Ashfaq, F., Jhanjhi, N. Z., & Alsadun, M. K. (2022). Traffic management: Multi-scale vehicle detection in varying weather conditions using yolov4 and spatial pyramid pooling network. Electronics, 11(17), 2748.

[36] Lim, M., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). Hidden link prediction in criminal networks using the deep reinforcement learning technique. Computers, 8(1), 8.

[37] Jhanjhi, N. Z., Ahmad, M., Khan, M. A., & Hussain, M. (2022). The Impact of Cyber Attacks on E-Governance During the COVID-19 Pandemic. In Cybersecurity Measures for E-Government Frameworks (pp. 123-140). IGI Global.

[38] Hussain, K., Hussain, S. J., Jhanjhi, N. Z., & Humayun, M. (2019, April). SYN flood attack detection based on bayes estimator (SFADBE) for MANET. In 2019 International Conference on Computer and Information Sciences (ICCIS) (pp. 1-4). IEEE.

[39] Sennan, S., Somula, R., Luhach, A. K., Deverajan, G. G., Alnumay, W., Jhanjhi, N. Z., ... & Sharma, P. (2021). Energy efficient optimal parent selection based routing protocol for Internet of Things using firefly optimization algorithm. Transactions on Emerging Telecommunications Technologies, 32(8), e4171.

[40] Kumar, T., Pandey, B., Mussavi, S. H. A., & Zaman, N. (2015). CTHS based energy efficient thermal aware image ALU design on FPGA. Wireless Personal Communications, 85, 671-696.