[1]D. Baby Sathiya

[2]L. Nalini Joseph

Securing the Patient's Breast Cancer Data using Blockchain-based IBE with Deep Learning Model in IoT

Abstract: - Computational intelligence (CI) and artificial intelligence (AI) have a portion to offer in the way of making healthcare systems smart and long-lasting. These technological advances have the potential to lessen our environmental impact while simultaneously increasing expectations for performance. The use of electronic health monitoring systems in healthcare management has been crucial. E-health has the potential to offer patients useful and efficient tracking tools. However, the existing E-Health system has protection disputes. However, there are safety concerns with the present online healthcare system. Doctors with bad intentions might collude with CSPs to compromise their patients' electronic health records (EHRs) or quickly leak EHR information to other opponents for financial gain. Patients might be manipulated by clinicians who work in collusion with a Patient Healthcare Monitoring Service Provider (PHMSP). EHRs for financial gain or disclose the HER content of EHRs directly to other adversaries. Recently, block-chain has emerged as one of the most potent strategies for maintaining privacy and security. The current security issues in e-health monitoring systems are expected to be replaced by this promising security method. To prevent unauthorised parties from accessing encrypted data, blockchain uses encryption. Using a computational intelligence approach, this study presented a blockchain-based encryption framework based on identity-based encryption (IBE) to deliver secure solutions. Furthermore, the study effort utilises optimised deep learning (ODL) to forecast the patient's condition from breast cancer input data. The suggested method improves performance, with an accuracy of 0.93 during training and 0.91 during validation.

Keywords: Electronic Health monitoring system; Blockchain; Optimized deep learning; Patient Healthcare Monitoring Service Provider; Encryption; Breast cancer.

Introduction

The (IoT) makes it conceivable for electronic gadgets to interconnect with one another. The agricultural, smart home, and healthcare sectors have all benefited greatly from the IoT in fresh years. Using the Internet of Things, medical personnel may save time and improve patient care [1]. In the healthcare sector, IoT facilitates a number of tasks, including remote patient monitoring and tracking of treatment outcomes [2]. Disease prediction, in which a patient's health is tracked throughout time to look for signs of a certain illness, has the potential to dramatically enhance medical care. This means there has to be a massive datacenter to house all this information. The interoperability issue also emerges when combining data across many devices. The goal of IoT devices is to collect, process, and communicate high-priority sensitive information related to health [3, 4]. Internet of Things devices used in healthcare settings deal with sensitive information [4]. The centralization of the IoT's underlying architecture poses serious challenges to data privacy and integrity. Traditional cryptographic methods of providing security pose risks to sensitive medical data. Therefore, a decentralised method of ensuring security is necessary [5].

Some examples of IoT security systems that employ CI approaches are malware detection, cyberattack finding [6]. The Internet of Things (IoT) might apply CI methods to strengthen its cybersecurity measures, ensuring the safety of IoT apps and users. Protecting sensitive healthcare information and ensuring confidential interactions among the User, Database Service provider, and Owner necessitates a secure and computationally savvy solution [7]. Blockchain is the answer to the problem of how to provide security and integration in a decentralised manner. Potential advantages of the blockchain include data encryption and digitally signed blocks for increased trustworthiness [8]. Due to the complexity and high degree of trust required in the healthcare business, blockchain may be an appropriate option. In general, block chain is most useful for widely dispersed systems where the need for trustworthy data is paramount and the potential of tracking actions is great [9].

[1] Research Scholar, Department of Computer Science, Bharath Institute of Higher Education and Research, Chennai. babysathiya10@gmail.com

[2]Professor, Department of Computer Science, Bharath Institute of Higher Education and Research, Chennai.

Blockchain can function on a vast network of devices, protecting the confidentiality of countless reports in the process. When it comes to the use of ICT, healthcare is currently at the forefront. The (IoT) has revolutionised healthcare by enabling electronic health records and remote patient monitoring [10]. Concerns concerning the quality of the data are exacerbated by the volume and variety of healthcare data supplied by multiple sources. Furthermore, there are other uses for medical data, including illness prediction. Integrating data from several devices necessitates strict adherence to quality standards, which is no easy task [11, 12]. Sharing healthcare data over a network raises data confidentiality concerns, and storing data in a single, highly visible location increases the risk of a catastrophic data loss event. When legitimate data is stored in one central location, a denial-of-service attack can occur. The blockchain facilitates the solution that can fix the problems we've been discussing. Blockchain is a distributed ledger that can let hospitals and clinics share and update patient records in real time. Each block contains private medical data that is only accessible to those with proper access [13]. Blockchain's appeal stems from its many desirable characteristics, which include decentralised data storage, permission, immutability, and expanded storage capacity. Any illness prediction model may be constructed using ML algorithms, as the blockchain data is immutable and cannot be altered by malicious actors. MeDShare was developed specifically for cloud providers as a blockchain-based, trustless medical data exchange solution. Mainly, it employs blockchain technology to switch out the centralised data processing unit with a decentralised one. Using blockchain technology, medical service frameworks have been created to safeguard patients' personal information [14].

The blockchain makes use of hash functions, asymmetric key procedures, and cryptographic procedures. With the use of hash roles, all blockchain participants may see the same information. The Secure Hash Algorithm 256 (SHA-256) is often used for this purpose in blockchains [15]. Encryption techniques are used to ensure security features including data privacy and access control. However, securing adequate access control is a major challenge. Combining the decentralised nature of blockchain technology with traditional security measures is not a straightforward task [16]. A lot of progress has to be made in this environment. While many academics have studied blockchain-based security systems in recent years, few have provided concrete designs for them. Thus, it is important to study and develop secure models of encryption frameworks based on blockchain technology.

The initial step of this study is a disease prediction, and then the data is stowed in the cloud. Finally, the data is encrypted using the IBE based on the blockchain and used for analysis. The remaining units of the paper are as shadows: The relevant literature is presented in Section 2, and the suggested model is explained in outline form in Section 3. In Section 4, we compare and contrast the projected model to some usually used validation methods. Section 5 provides the final analysis.

2. Related works

For blockchain security in healthcare networks, Miriam et al. [17] present a Lionised Golden Eagle based (LGE-HES) method. The hash function performed by the blockchain algorithm keeps the medical picture secure. MATLAB is used to carry out this study's calculations. Simulation findings using Computed Tumour (CT) images and MRI image datasets confirmed the usefulness of the proposed system. According to the sum results data, during the simulation, 94.9% were successfully recognised and detected, and other measures are used to contrast the proposed model's performance with those of conventional methods.

A proxy re-encryption-based data sharing technique is proposed by Keshta et al. [18]. To begin, we build a proxy re-encryption method that uses SM2 and the blockchain. Sharing data via the blockchain might provide a safe and reliable method for companies to exchange information. Since this network is decentralised, data is signed cryptographically and sent between peers without any possibility of tampering. Data stored on a blockchain is harder to hack or change. To ensure the privacy of transactions and to realise data security sharing, the data-controlled sharing system employs proxy re-encryption. Second, we suggest a system whereby user permissions may be dynamically modified. For user access rights determinism in a blockchain, nodes split up the work and control the re-encryption key settings independently. With each update, the amount of hidden transaction data is changed automatically. Finally, the performance and security assessment shows that this scheme is more appropriate to the Controlled sharing of blockchain data and can realise dynamic sharing of blockchain data while ensuring transaction privacy and having advantages in processing overhead. Based on these findings, we propose

a supervised blockchain-based data sharing system that employs proxy re-encryption. To ensure the complete confidentiality of financial transactions and to enable the identification of appropriate data access authorities, they are implementing SM2 into a proxy re-encryption method. To allow users with fewer resources to gain access to encrypted content, it is recommended that they adopt a hybrid attribute-based proxy re-encryption approach that allows the proxy server to convert attribute-encrypted cypher texts into texts.

A new Elliptic Curve Cryptography–based blockchain-based secure data exchange (BSDCE-IoV) technique has been proposed and evaluated by Karim et al. [19]. Multiple assaults on the IoV ecosystem are prevented by our proposed solution. In addition to the informal security study, a thorough evaluation utilising the Real-or-Random oracle model and the Scyther tool verifies the scheme's security and privacy. In order to gauge the computational and communication load, the Multi-precision Integer and Rational Arithmetic Cryptographic Library (MIRACL) is used. The Multi-precision Integer and Rational Arithmetic Cryptographic Library (MIRACL) was used to assess computational and communication costs. BSDCE-IoV outperforms several recent selective works in IoV security in terms of security, functionality, and latency. de Moraes Rossetto et.al. [20] presents an architecture for protecting the confidentiality of health records that are distributed across a blockchain network and encrypted using RSA, ECC, and AES. The influence of encryption on the proposed architecture was tested using several evaluation metrics including computational effort, memory utilisation, and execution time. The results show that the design and encryption improve privacy and security, but come at the cost of more execution time and computing effort when transmitting data to the blockchain.

In order to safeguard the exchange of electronic health records (EHRs) between various EHR systems, Amanat et al. [21] offer a blockchain-based architecture that verifies the identification of users using a Proof of Stake (POS) cryptographic consensus mechanism and a Secure Hash Algorithm (SHA256). When gathering and sending data to the cloud, EHR sensors are verified using an (ECDSA). In terms of power consumption, authenticity, and security of healthcare data, the suggested approach performs extraordinarily well in comparison to existing systems such as Proof-Of-Work (POW), Secure (MD5).

Using UBCCSP (Upgraded BCCSP), Yang et al. [22] have created a transaction mechanism and proposed a novel smart contract. After that, UCBIS (Consortium Blockchain Information System based on UBCCSP) is offered as an enhanced consortium blockchain information system built on top of UBCCSP. The SM2 and SM3 algorithms provide security for identities and transaction data in Hyperledger Fabric transactions, and SM3 is also utilised in the creation of smart contracts. Our smart contracts provide more effective querying while decreasing overall data volume. The UBCCSP-based info query scheme has been fully deployed. The blockchain system has been evaluated and found to have superior performance and higher query efficiency, with an average query time of only 31.162 ms.

To encourage the use of blockchain knowledge and two-factor authentication in electoral procedures, Ajao et al. [23] recommend integrating security countermeasures. The private blockchain method is implemented to safeguard the integrity and veracity of record transactions against tampering and to guarantee the immutability of data. The blockchain and electronic voting system based on the decentralised system use bi-factor certification and secrecy (Iris and Fingerprint) to implement the Paillier homomorphic encryption technique. Testing demonstrated an improvement in system performance, with a FAR of 0.02% and a FRR of 0.1%, correspondingly. When it comes to certification execution and data retrieval latency, the Paillier homomorphic encryption used in the crypto-blockchain approach works admirably.

2.1. Research Gap

It is evident from the aforementioned methods that data security is the primary focus. However, hardly a single research forecasts future disease outbreaks and then guarantees the safety of that information. The main foci of this study are prediction and blockchain-based encryption. Predicting the likelihood that a given person will have a disease (or experience a given incident) in the future is the central challenge of disease prediction. Disease prediction will be defined based on a person's various characteristics, and a time limit for a specific prediction target such as stroke, etc. will be set, serving as the time node for making forecast judgements, to guarantee a certain level of accuracy in predicting the likelihood of occurrence of a given disease risk.

In the procedure of data sharing, however, it is important to think about the privacy protection of data and the effectiveness of the model in the process of data protection since medical data contains data privacy concerns and the data is held independently at medical institutions. The paper presents a solution to data privacy concerns by employing dispersed and locally stored data to patients, as well as decentralised learning and blockchain-based security.

3. Proposed Framework of IoT

There are two phases to this study, the first being illness prediction and the second being data security..

3.1. Stage 1: Disease Prediction

Several cities have used deep learning (DL) methods, which collect massive amounts of data from a wide variety of IoT devices. Practical operations of DL models, such as Recurrent Neural Networks (RNN), are used to successfully classify data. Detecting anomalies and diagnosing diseases are two examples of useful uses. Since training a classifier often requires a large amount of tagged Internet of Things data collected from many sources, data privacy has arisen as an essential concern. Most current solutions make the flawed assumption that they can efficiently obtain training data from several data suppliers. We evaluated the methods using the Wisconsin datasets that may be found in the UCI machine learning repository [24].

The WDBC is computed from a digital picture of a breast tumour aspirate, and its properties characterise the quality of the cell nuclei present in the image. These features are seen in a digitally acquired, microscopic aspirate from a breast tumour. Cases are classified as benign or malignant based on the information gathered. The training data accounted for 70% of the dataset, while the test data made up the remaining 30%. Future applications include using this method to treat conditions related to brain tumours.

3.1.1. Data sampling

The Wisconsin Breast Cancer Data Set, used for research and diagnosis, was obtained using Kaggle. Breast cancer develops when cells in breast tissue proliferate and divide unchecked for an extended period of time. It's possible that there will be a lot more cases of breast cancer diagnosed. Perhaps you are correct in thinking this. How many cellular subtypes might potentially arise in breast tissue? Malignant breast cancer is the deadliest kind. The WDBC data samples are analysed to determine whether or not a tumour is cancerous. This is done so that a correct diagnosis may be made. One of the 569 instances was selected from a recent study that presents 32 distinctive traits. The identification/diagnosis data set includes two categories. There were 31 characteristics and their actual values utilised as input.

3.1.2. Prediction of disease using deep learning model

Here, we apply an optimised CNN to the problem of identifying breast cancer in clinical samples. The input for CNN is the appropriate target class y, and the training information is a vector X of trained samples based on the backpropagation method [25]. The output of each CNN is compared to the target, and the difference between the two represents the learning error. Using maths to play the part of the next CNN,

$$E(\omega) = \frac{1}{2}\sum_{\rho=1}^{p}\sum_{j=1}^{N_\iota}(o_{j,p}^{l} - y_{j,p})^2 \qquad (1)$$

Our goal is the minimalizing of cost function $E(\omega)$, finding a minimizer $\tilde{\omega} = \tilde{\omega}^1, \tilde{\omega}^2, \dots, \tilde{\omega}^v \in \mathbb{R}^v$,where $v = \sum_{k=1}^{L} \mathrm{WeightNum}\ (k)$ and signify that the space of weight $\mathbb{R}^v$is $(\mathrm{WeigtNum}(.))$ at each k layer of entireL layers of the CNN network.

$$\nabla E_i(\omega_i) = \left(\frac{\partial E_i}{\partial \omega_i^1}, \dots, \frac{\partial E_i}{\partial \omega_i^v}\right) \qquad (2)$$

$$\omega_{i+1} = \omega_i - n\nabla E_i(\omega_i) \qquad (3)$$

Where n is the pace of learning (in steps). The COA method was used to determine the value of n, as will be shown below.

Canis latrans (coyotes) are a population-based, behaviorally-driven evolutionary heuristic species [26]. The COA is not the same as the (GWO), which is enthused by the Canis lupus species (for reasons that will become clear shortly). While the GWO is solely concerned with hunting, the COA also investigates coyote social structures and experiences.

The N pN* packs in the COA are home to a total of N cN* individual coyotes. In this initial plan, it is suggested that there be a certain number of pack. The entire population of the algorithm is thus calculated by multiplying N p by N c. For the sake of simplicity, lone or transient coyotes are ignored in this initial implementation of the algorithm. Coyote's social standing pays the price for the reader's comfort. Both internal (such as the coyote's gender, social status, and membership in a pack) and external factors are considered to affect the animal's conduct. In light of these considerations, an optimisation problem was used to create the COA mechanism, with coyote social conditions serving as the decision variable x. Thus, the social condition soc (set of determinants) of the pth pack's cth coyote may be written as:

$$soc_c^{p,t} = \vec{x} = (x_1, x_2, \dots, x_D) \quad (4)$$

And it proposes in the coyote's version to the condition $fit_c^{p,t} \in \mathbb{R}$.

Since COA is a stochastic algorithm, it must first construct the global coyote population, with each individual coyote's initial social circumstances being determined by chance.:

$$soc_{c,j}^{p,t} = lb_j + r_j.(ub_j - lb_j) \quad (5)$$

For the jth decision variable, the bounds of the decision variable are represented by random values with a fixed probability in the range [0,1]. The coyote's capacity to adapt to the current social setting is then evaluated.:

$$fit_c^{p,t} = f(soc_c^{p,t}) \quad (6)$$

Coyotes can, however, leave their packs at any moment and go solitary or join a new pack. The risk of a coyote getting kicked out of the pack increases to P e if there are more than two coyotes there..

$$P_e = 0.005 \,.\, N_c^2 \quad (7)$$

Only 14 coyotes make up a pack since P e may be greater than 1 for Nc less than 200. As a result of this process, cultural interchange occurs all around the world, which helps the COA increase social diversity.

Even though there are normally two alphas in this species, only the one most matched to the environment is considered by the COA. Using a constraint minimization problem, we may define the alpha of the t-th moment in the p-th pack as:

$$alpha^{p,t} = \left\{ sco_c^{p,t} | arg_c = \{1,2,\dots N_c\} \min f(sco_c^{p,t}) \right\} \quad (8)$$

Because of the clear signs of swarm intellect in this species, the COA coyotes are well-organized enough to share the social circumstances and help maintain the pack. As a result, the COA links all of the coyote data to create a compilation of the pack's cultural tendencies.:

$$cult_j^{p,t} = \begin{cases} O^{p,t}_{\frac{(N_c+1)}{2},j} N_c \; is \; odd \\ \frac{o^{p,t}_{\frac{NC}{2}} + o^{p,t}_{\left(\frac{N_c}{2}+1\right),j}}{2}, \quad otherwise \end{cases} \quad (9)$$

For each j in [1,D], O(p,t) represents the order in which the members of the pth pack find themselves socially at the tth time instant. The cultural inclinations of a pack may be estimated by averaging the average social coyotes.

The COA calculates the age of a coyote by considering just its date of birth and date of death. A coyote's origin narrative is shaped by the interactions between chance and chance in the lives of two parents.

:

$$pup_j^{p,t} = \begin{cases} soc_{r1,j}^{p,t} & rnd_j < P_s \text{ or } j = j_1 \\ soc_{r2,j}^{p,t}, & rnd_j \geq P_s + P_a \text{ or } j = j_2 \\ R_j & otherwise \end{cases} \quad (10)$$

in where $c$and Coyotes with random loss are chosen at random from the pth pack, problem dimensions j 1 and j 2 are chosen at random, and the values P s, P a, R j, and rnd j are chosen at random from variable boundaries of the jth dimension. The principles of dispersion and association probability shape the cultural diversity of a pack. In this preliminary version of the COA, the P_s and the P_a are defined as follows::

$$P_s = 1/D \quad (11)$$

$$P_a = (1 - P_s)/D \quad (12)$$

According to some research, coyote pups have a 10% probability of dying even before they are born, and this risk upsurges with age. According to Algorithm 1, the sum of coyotes in the worst-adjusted coyote group is and the total of prairie wolf in this group is to keep the population size steady. Line 4 suggests thinking about the potential that coyotes of similar ages may congregate. The less adaptable coyote will perish under these conditions.

Algorithm 1: Birth and death privileged a pack.
1: $Compute\ \omega\ and\ \phi.$
2: $if\ \phi\ =\ 1\ then$
3: $The\ pup\ survives\ and\ the\ only$ $coyote\ in\ \omega\ dies.$
4: $elseif\ \phi\ >\ 1\ then$
5: $The\ pup\ survives\ and\ the\ oldest\ coyote\ in\ \omega\ dies.$
6: $else$
7: $The\ pup\ dies.$
8: $end\ if$

Coyotes' seeming subservience to the alpha and the pack is used by the COA to illustrate social dynamics within packs. Two examples are given, one contrasting the culture of the pack with that of a random coyote (cr 2) and the other contrasting a member of the pack (cr 1) with an alpha coyote (cr 2). The formulas for picking random coyotes from a probability distribution are as follows:

$$\delta_1 = alpha^{p,t} - sco_{cr_1}^{p,t} \text{ and } (13)$$

$$\delta_2 = cult^{p,t} - soc_{cr_2}^{p,t} \quad (14)$$

$$new\_soc_c^{p,t} = soc_c^{p,t} + r_1, \delta_1 + r_2 . \delta_2 \quad (15)$$

where r_1 and $r_2$characterize the alpha correspondingly. It was initially stated that the two random statistics, r_1 and r_2, in the interval [0,1] were generated with equal probability. After then, we take stock of the altered social climate.:

$$new\_fit_c^{p,t} = f(new\_soc_c^{p,t}) \quad (16)$$

The cognitive abilities of an animal are what decide whether or not a different social setting is more favourable than the one previously experienced.:

$$soc_c^{p,t+1} = \begin{cases} new\_soc_c^{p,t}, & new\_fit_c^{p,t} < fit_c^{p,t} \\ soc_c^{p,t}, & otherewise \end{cases} \quad (17)$$

Coyote society is selected as the greatest example since it has successfully adapted to its natural habitat. process 2 of the COA pseudo code allows for an initial guess of Nc in the range [5,10], with Np being the population size for the whole process..

Algorithm 2: COA's Pseudo code
1: $Initialize\ Np\ packs\ with\ Nc\ coyotes\ each\ (Eq.5)$.
2: $Verify\ the\ coyote's\ adaptation\ (Eq.6)$.
3: $while\ stopping\ criterion\ is\ not\ achieved\ do$
4: $for\ each\ p\ pack\ do$
5: $Define\ the\ alpha\ coyote\ of\ the\ pack\ (Eq.8)$.
6: $Compute\ the\ social\ tendency\ of\ the\ pack\ (Eq.9)$.
7: $for\ each\ c\ coyotes\ of\ the\ p\ pack\ do$
8: $Update\ the\ social\ condition\ (Eq.15)$.
9: $Evaluate\ the\ new\ social\ condition\ (Eq.16)$.
10: $Adaptation\ (Eq.17)$.
11: $end\ for$
12: $Birth\ and\ death\ (Eq.10\ and\ Algorithm\ 1)$.
13: $end\ for$
14: $Transition\ between\ packs\ (Eq.13)$.
15: $Update\ the\ coyotes'\ ages$.
16: $end\ while$
17: $Select\ the\ best\ adapted\ coyote$.

3.2. Stage 2: Encryption based Blockchain System

Medical and healthcare facilities have used IoT so that patient records may be accessed remotely at any time. People are wary of transmitting sensitive information online because of the prevalence of hacking and other malicious activities. Blockchain ledger that may be used to transactions across the global digital network. It consists of interconnected blocks that cannot be altered at the key reference level. However, when the number of chains is grown, this characteristic might cause an issue known as illness overlapping, which is a drawback of blockchain technology in healthcare and other related fields. Patients are worried that untrustworthy third parties may acquire access to their personal medical records and use that knowledge against them. The use of Blockchain knowledge into healthcare institutions is meant to reduce stress for patients. There have been several proposals throughout the years for Blockchain-based healthcare systems to improve data dependability and accessibility. However, these methods required too much time and were unique to each hospital or medical centre. As a result, new information regarding a patient's allergies, symptoms, and prescriptions cannot be entered to the records, and the previous medical history cannot be retrieved if the patient transfers to a different hospital for treatment of any ailment due to the differing BCs. The resulting overlap in diseases creates inconsistencies that slow down the healing process.

This framework considers a Blockchain-based solution to this problem by adding a new-fangled block to the chain whenever there is an update to a patient's medical file, such as the addition of a new allergy, symptom, or medication. This is done without requiring any special permissions or information from the hospitals involved. This ensures that the patient's information is always up-to-date without duplicating any previously collected data, and that the doctor can provide accurate care by consulting the file. Our BC-based paradigm for managing illness overlap is described in full in [27]. This study proposes a security architecture that will increase security by storing patient information in an encrypted form over the network, therefore protecting the privacy of patients' medical records. Using an encryption algorithm and a public Blockchain, the proposed Blockchain-based IoT architecture aims to provide an efficient and reliable security mechanism [28]. As data security is one of the largest issues in IoT healthcare systems that cannot be overheard, the primary goal of the proposed project is to develop an IoT Blockchain system in which patient data is safer and more scalable.

Patients will feel more comfortable disclosing private health information to their doctors and health information hubs, increasing confidence in the system as a whole [29]. In light of these goals, this study sets out to provide a protocol for managing the healthcare system in the cloud while protecting sensitive data stored on servers connected to the (IoT). The suggested Blockchain-based Things healthcare system is depicted in Figure 1 [30].

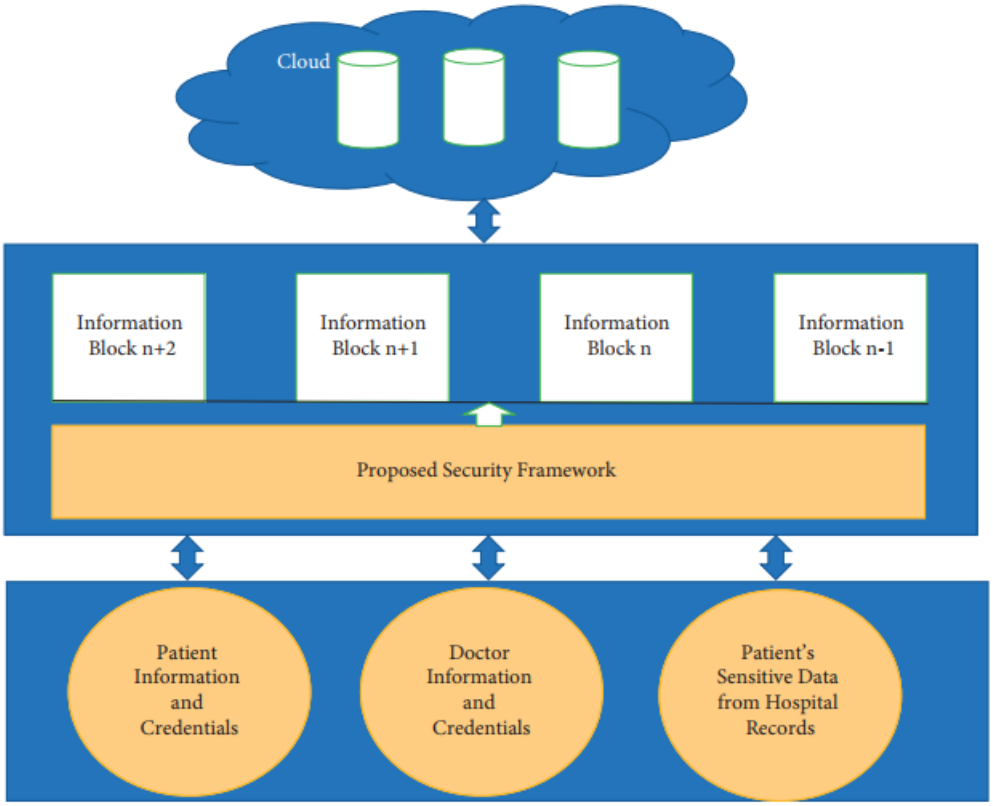

Figure 1: Presence of Blockchain in Secure IoT data

There are typically three stages involved in the broadcast of data from the physical world to the cloud server in any Blockchain system based on the Internet of Things. Data is gathered at a lower level, where sensors and actuators are placed. In the third and final tier, the data is delivered to a cloud server, having first been passed straight to layer, where it is split into many blocks. Securing IoT architecture is critical [31] because patient data comprises sensitive information that must not be accessed or exposed to any unauthorised person. Modifications are made to the IoT system's second layer (shown in Figure 1) to prevent unauthorised and unauthenticated access to this data. The second layer's additional data security technique increases confidence and trustworthiness among both patients and data hubs. Information is gathered under the proposed framework from patients, physicians, and healthcare facilities. A real-time dataset gathered from Kaggle.com has been utilised to sidestep complexity and dimensionality problems.

As was noted before, the information gathered in the previous stage is very private and must be protected. The patient's information is encrypted using the suggested technique (identity-based encryption (IBE)) to add an extra layer of protection.

3.2.1. Proposed IBE Algorithm

Consider the group G to be of prime order p. The bilinear map from Group G to Group 1 can be efficiently computed. The definition of G1's bilinear map representation e : G × G1➔G2, and g is the producer of group G.

$$ID = (id_1, id_2, id_3, \dots, id_n) \quad (18)$$

From ID bits of arbitrary length, the collision- function can produce strings of set length n. The suggested IBE algorithm consists of the following steps:

3.2.1.1. Setup Phase.

First, generate the scheme parameters. A secret is designated at random from Z_p. Choose a random that $g \in G$, and fix the value $g1 = g^{\alpha}$ and select g2 randomly in G. After parameter, first-rate a random sum u such that

$u' \in G$ and a random n-length vector such that $U = \{u_i\}$. To conclude, $g, g1, g2, u'$ and U are published as public limits and g_2^a as master key.

3.2.1.2. Generation Phase.

Let $v$represents $n$bit string uniqueness for a user, *ith* bit of $v$is signified by *vi*, where $V \subseteq \{1, \cdots, n\}$ be different, i.e., $V = \{v_1, v_2, \cdots, v_m\}$ and $\{v_{r1}, v_{r2}, .., v_{rm}\}$ such that $m + r_m = n$, where v_{ri}stands for a random value that was thrown into the mix to make the suggested approach more bulletproof. Identity v is produced by first selecting a random number and then using the matching identity's private key..

$d_v = (g_2^a (u' \prod_{i \in V} v_i)^r, g^r)$ (19)

$U = \{u_1, u_2 - - - -u_n\}$ *and* $V = \{v_1, v_2 - - - -u_m\}$enough so that m n. Now, build a polynomial function with the Lagrange coefficient approach and utilise it for polynomial interpolation. Some values of v that are recoverable from the current data points can be concealed with the use of polynomial interpolation. The proposed method can be represented by the polynomial equation

$P(x) = \frac{(x-x_1)(x-x_2)--(x-x_n)}{(x_0-x_1)(x_0-x_2)--(x_0-x_n)} y_0 + \frac{(x-x_0)(x-x_1)--(x-x_{n-1})}{(x_1-x_0)(x_1-x_2)--(x_1-x_n)} y_1 - - \frac{(x-x_1)(x-x_2)--(x-x_n)}{(x_n-x_0)(x_n-x_1)--(x_n-x_{n-1})} y_n$ (20)

Lagrange coefficient is

$\Delta_{i,v}(x) = \sum_{i=0,k \in V}^{n} \left(\prod_{0<i<n, j \neq i} \frac{x-x_j}{x_i-x_j} \right) y_k$ (21)

where x = u_i and y = y_k:

Each user identity has its own unique random set, u_i, and each Lagrange coefficient is created with the same u_i value. In order to prevent a challenger from discovering the real identity of an authorised user, the expert will employ m-terms of identification value. It will therefore be challenging to acquire or guess the key created for a certain ID. Now consider the scenario in which all of the user identities and U values are identical; in this case, P(x) produces no error, meaning that the challenger cannot guess the key.

This situation is unique. The resulting error will be zero, and the maximum error between any two nodes may be calculated.

3.2.1.3. Encryption Segment.

Let "c" be a random worthselected from Z_{p} and communication$M (M \in G_1)$. For approximatelyindividuality v, can be achieved using Equation (22).

$C = (e(g_1, g_2)M, g^c, (u' \prod_{i=v} v_i)^c)$ (22)

3.2.1.4. Decryption Phase.

Let $C = (C_1, C_2, C_3)$meet the requirements for ciphertext M with user id v. Then, we may use to decipher cypher text C by $d_v = (d_1, d_2)$ as given in Equation (23)–(26):

$= (e(g_1, g_2)^c M) \frac{e(g^r, (u' \prod_{i=V} v_i)^c)}{e(g_2^a, (u, \prod_{i=v} v_i)^r, g^c)}$ (23)

$= (e(g_1, g_2)^c M) \frac{e(g^r, (u' \prod_{i=V} v_i)^{rc})}{e(g_1, g_2)^c, e((u, \prod_{i=v} v_i)^{rc}, g)}$ (24)

$= (e(g_1, g_2)^c M) \frac{e(g, (u' \prod_{i=V} v_i)^{rc})}{e(g_1, g_2)^c e(g, (u' \prod_{i=V} v_i)^{rc})}$ (25)

$= M$ (26)

By using encryption, not only is patients' personal health information protected from prying eyes, but trust between patients and information hubs like hospitals is strengthened as well. In this way, it strengthens the safety measures already in place for the Internet of Things. After encryption, the data is divided into disparate chunks. The patient's

information is then double protected by a hashing method applied to these blocks. The patient's encrypted and secured data is sent to the cloud layer in the proposed model's third and final tier, where it is kept and may be retrieved at any time. The specified objectives must be met by implementing the proposed IoT architecture in accordance with the listed layers [32].

1. Authentication: Access Blockchain relies on user authentication and authorization.
2. Privacy protection: Our concept employs a layered security system (encryption and Blockchain) to protect user privacy.
3. Trust: The suggested IoT framework needs to foster confidence amongst connected devices.

3.3. Interface of the Projected IoT Healthcare Scheme.

The challenge now is how the planned healthcare actually works to accomplish these goals. This is accomplished by creating an API-driven paradigm where users may sign up with just their own credentials. The various components of the projected Blockchain-based IoT healthcare system consist of a registering unit, a login unit, an form, and a data centre. Each part will be simply and sequentially explained below.

The initial step in using the scheme is registering as a user; this might be either a doctor or a patient. Important data such as a user's name, phone number, user ID, password, and even a photo is captured and kept throughout this procedure. The user category indicates whether the new member is a healthcare provider or a patient. In addition, the information is entered into the database in preparation for verification. In addition, an improved deep learning model is used to provide illness predictions. When a user provides the obligatory data, it is automatically protected in the cloud.

(ii) Authentication: After registering, users may quickly access the arrangement with their credentials. To admittance the proposed IoT scheme, the user inputs their user id, password, and user type beforehandsnapping the login button. When a user clicks the module sends a request to the cloud storage, which then verifies whether or not the provided credentials match the ones on file. To ensure that only legitimate users are granted entrée to the system, the cloud service verifies each user's credentials against a database of registered users, sending a response to the login module if a match is found and rejecting the request otherwise. As was previously said, the user may play the role of either a physician or a patient. Information entered by one party can be seen by the other and vice versa.

When the user is a patient, just the patient's name, phone number, age, and sex need to be input or seen. Also shown are the patient's blood pressure and other vitals, as well as the name of the attending physician.

However, when a doctor logs into the system with his credentials, a page emerges where he may inspect and analyse the health by selecting the patient's name. However, since the data collected thus far is encrypted, the doctor will have a difficult time accessing the patients' files.

(v) Data-based authentication: for the doctor to admission the patient's private data, he must provide the decoding credentials at the location where his data has been posted. When a request is made to admittance a patient's medical records, the system performs a secondary authentication check with the credentials; if they match, the records are made obtainable to the elected doctor; otherwise, the request is denied, providing an extra layer of security.

4. Results and Discussion

4.1. Implementing Proposed IoT Network Architecture.

The projected Blockchain-based Internet of Things (IoT) health care scheme must be fully security compatible to assure its reliability and longevity. In this part, we focus on the most important aspects of our proposed system, including its safety features, compatibility requirements, and aims.

(a) Scalability is the system's capacity to handle larger models without degrading performance. According to the proposed framework, a P2P network may support not just related but also aggregated requests for information. The first makes use of a public Blockchain to manage association inquiries, while the second makes use of a

health-edge to provide controlled communiqué on summative requests among members located in different geographic regions.

(b) Authentication and authorization: The projected framework uses a blockchain- authentication way to verify the identities of IoT participants. The model is protected from spoofing thanks to this method. In addition, the data saved in the cloud database is only accessible to the authorised user after their credentials have been verified.

(c) Reliability was measured by hashing and signing of exchanged messages in traditional IoT-based healthcare systems. Our suggested strategy improves safety by encrypting user data at rest in the cloud. The fact that this encrypted information may be decoded by only the authorised parties increases confidence in the IoT as a whole.

(d) Data integrity guarantees the correctness of all statistics in the scheme. In additional words, it's the rule that prevents any user from making any changes to or adding new information to previously traded conversations at any point in time. The system is protected since only the genuine and authorised individual may make the necessary adjustments.

The effectiveness of the projected Blockchain scheme is evaluated not only in terms of the aforementioned important criteria, but also in footings of encryption time and decryption period. To show its efficacy, all three metrics should have high values. In the next part, we describe in detail the efficiency of the suggested encryption model.

4.2. Validation Analysis of proposed model

Table 1.Processor utilization rate.

Methods	1st trial	2nd trial	3rd trial	4th trial
Proposed IBE	401	156	103	357
AES	460	869	956	986
Blowfish	480	990	998	1010
DES	520	230	303	340
RC5	1530	660	740	980
3DES	410	580	300	301

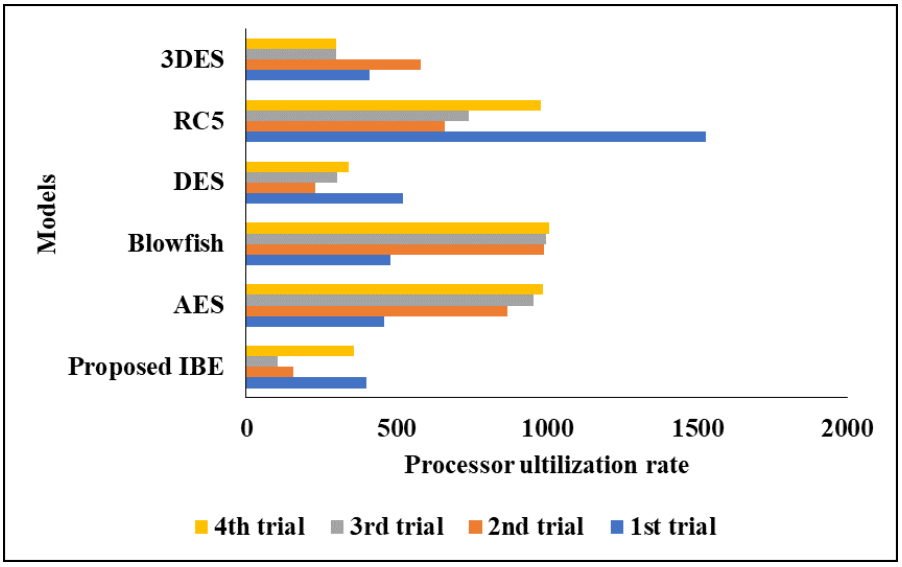

Figure 2: Graphical Comparison for Processor utilization rate

Each round's CPU time was studied by altering the amount of the input data. In comparison to the other IBE modules, key transformation often requires greater processing time. The obtained findings show how useful IBE may be. Performance comparison of IBE with various cryptographic algorithms as a function of CPU utilisation

is shown in Table 1. This section contrasts the data security provided by certain widely-used cryptographic block cyphers with that provided by IBE in a blockchain setting.

Understanding how much time a central processing unit (CPU) spends on a given task is called "processor usage." It indicates how much work is being done by the CPU. The higher the CPU load, the more CPU power was required in the encipherment method. The purpose of these tests is to examine the precision and precision of the processor time estimation across a variety of platforms and input sizes.

Table 2: Value parameters gotten in traditional RSA, DSA, and projected model.

Parameters	DSA	RSA	Proposed
MSE	3620.966	2884.1	19695.03
Enc time	11.1202	0.253194	0.032955
MAE	59.11055	45.22305	119.6063
RMSE	60.17446	53.70382	140.339
Dec time	10.8254	0.254536	0.024304

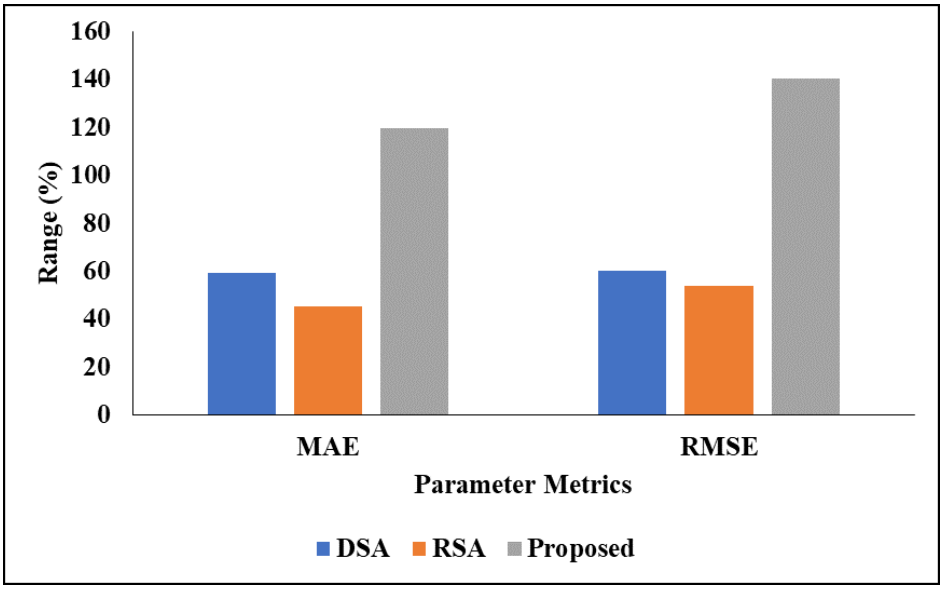

Figure 3: Graphical Representation of proposed model in terms of two metrics

In above table 2 represent that the Value parameters found in traditional RSA, DSA, and projectedperfect. In the comparisons analysis of RSA model reached the MAE value as 45.22305 and the RMSE value as 53.70382 and also, the MSE value as 2884.1 and the encryption time as 0.253194 and finally, the description time as 0.254536 respectively. And also,another comparisons analysis ofDSA model reached the MAE value as and the RMSE value as 59.11055 and also, the MSE value as 60.17446 and also, the MSE value as 3620.966 and the encryption time as 11.1202 and finally, the description time as 10.8254respectively. And also, another comparisons analysis ofproposed model reached the MAE value as and the RMSE value as 119.6063 and also, the MSE value as 140.339 and also, the MSE value as 19695.03 and the encryption time as 0.032955 and finally, the description time as 0.024304respectively. In the Value parameters analysis of different models, the projected model reaches the better consequences than other compared models.

5. Conclusion and Future Scope

The penalty area of this study was to develop and authenticate a cutting-edge method for detecting breast cancer at an early stage through the blockchain. We accomplished a great deal by demonstrating the system outperforms standard methods of breast cancer diagnosis. Two major issues in the healthcare industry that blockchain technology helps solve are the protection of sensitive patient data and the restriction of unauthorised access. These

findings show the uniqueness of the technology and its latent to drastically improve breast cancer diagnosis. The blockchain is crucial for the private and secure electronic storage of health records. This study investigates the custom of blockchain technology in healthcare records and demonstrates how putting medical information on a distributed ledger solves the underlying problem. Second, the ability to make accurate forecasts is crucial in the sector.

The potential impact of a Blockchain for breast cancer diagnosis in the future is enormous. More study, development of algorithms, and construction of machine learning models may help improve accuracy. Beyond its current application in breast cancer diagnostics, blockchain technology has the ability to open the way for the development of IoMT medications for a wide diversity of disorders. Integrating with telemedicine schemes allows for remote monitoring and diagnosis, expanding access to high-quality medical care for more people. The study may be expanded to anticipate numerous chronic diseases that impact internal organs including the kidneys and the liver, and to solve the latency issue that arises as a result of blockchain integration.

References

[1] Rathee, G., Sharma, A., Saini, H., Kumar, R. and Iqbal, R., 2020. A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. Multimedia Tools and Applications, 79(15-16), pp.9711-9733.

[2] Qahtan, S., Sharif, K.Y., Zaidan, A.A., Alsattar, H.A., Albahri, O.S., Zaidan, B.B., Zulzalil, H., Osman, M.H., Alamoodi, A.H. and Mohammed, R.T., 2022. Novel multi security and privacy benchmarking framework for blockchain-based IoT healthcare industry 4.0 systems. IEEE Transactions on Industrial Informatics, 18(9), pp.6415-6423.

[3] Singh, S., Rathore, S., Alfarraj, O., Tolba, A. and Yoon, B., 2022. A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. Future Generation Computer Systems, 129, pp.380-388.

[4] Mehbodniya, A., Webber, J.L., Neware, R., Arslan, F., Pamba, R.V. and Shabaz, M., 2022. Modified Lamport Merkle Digital Signature blockchain framework for authentication of internet of things healthcare data. Expert Systems, 39(10), p.e12978.

[5] Kelli, V., Sarigiannidis, P., Argyriou, V., Lagkas, T. and Vitsas, V., 2021, June. A cyber resilience framework for NG-IoT healthcare using machine learning and blockchain. In ICC 2021-IEEE International Conference on Communications (pp. 1-6). IEEE.

[6] Badr, S., Gomaa, I. and Abd-Elrahman, E., 2018. Multi-tier blockchain framework for IoT-EHRs systems. Procedia Computer Science, 141, pp.159-166.

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

[8] Al-Megren, S., Alsalamah, S., Altoaimy, L., Alsalamah, H., Soltanisehat, L. and Almutairi, E., 2018, July. Blockchain use cases in digital sectors: A review of the literature. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 1417-1424). IEEE.

[9] Alzubi, J.A., 2021. Blockchain-based Lamport Merkle digital signature: authentication tool in IoT healthcare. Computer Communications, 170, pp.200-208.

[10] Attia, O., Khoufi, I., Laouiti, A. and Adjih, C., 2019, June. An IoT-blockchain architecture based on hyperledger framework for health care monitoring application. In NTMS 2019-10th IFIP International Conference on New Technologies, Mobility and Security (pp. 1-5). IEEE Computer Society.

[11] Chakraborty, S., Aich, S. and Kim, H.C., 2019, February. A secure healthcare system design framework using blockchain technology. In 2019 21st International Conference on Advanced Communication Technology (ICACT) (pp. 260-264). IEEE.

[12] Wang, D.H., 2020. IoT based clinical sensor data management and transfer using blockchain technology. Journal of IoT in Social, Mobile, Analytics, and Cloud, 2(3), pp.154-159.

[13] Abou-Nassar, E.M., Iliyasu, A.M., El-Kafrawy, P.M., Song, O.Y., Bashir, A.K. and Abd El-Latif, A.A., 2020. DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems. IEEE access, 8, pp.111223-111238.

[14] Tahir, M., Sardaraz, M., Muhammad, S. and Saud Khan, M., 2020. A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics. Sustainability, 12(17), p.6960.

[15] ElRahman, S.A. and Alluhaidan, A.S., 2021. Blockchain technology and IoT-edge framework for sharing healthcare services. Soft Computing, 25(21), pp.13753-13777.

[16] Satamraju, K.P., 2020. Proof of concept of scalable integration of internet of things and blockchain in healthcare. Sensors, 20(5), p.1389.

[17] Miriam, H., Doreen, D., Dahiya, D., & Rene Robin, C. R. (2023). Secured Cyber Security Algorithm for Healthcare System Using Blockchain Technology. Intelligent Automation & Soft Computing, 35(2).

[18] Keshta, I., Aoudni, Y., Sandhu, M., Singh, A., Xalikovich, P. A., Rizwan, A., ... &Lalar, S. (2023). Blockchain aware proxy re-encryption algorithm-based data sharing scheme. Physical Communication, 58, 102048.

[19] Karim, S. M., Habbal, A., Chaudhry, S. A., & Irshad, A. (2023). BSDCE-IoV: Blockchain-Based Secure Data Collection and Exchange Scheme for IoV in 5G Environment. IEEE Access.

[20] de Moraes Rossetto, A. G., Sega, C., &Leithardt, V. R. Q. (2022). An Architecture for Managing Data Privacy in Healthcare with Blockchain. Sensors, 22(21), 8292.

[21] Amanat, A., Rizwan, M., Maple, C., Zikria, Y. B., Almadhor, A. S., & Kim, S. W. (2022). Blockchain and cloud computing-based secure electronic healthcare records storage and sharing. Frontiers in Public Health, 10, 938707.

[22] Yang, Y., Lin, T., Liu, P., Zeng, P., & Xiao, S. (2022). UCBIS: An improved consortium blockchain information system based on UBCCSP. Blockchain: Research and Applications, 3(2), 100064.

[23] Ajao, L. A., Umar, B. U., Olajide, D. O., & Misra, S. (2022). Application of crypto-blockchain technology for securing electronic voting systems. In Blockchain Applications in the Smart Era (pp. 85-105). Cham: Springer International Publishing.

[24] Chaudhury, S. and Sau, K., 2023. A blockchain-enabled internet of medical things system for breast cancer detection in healthcare. Healthcare Analytics, p.100221.

[25] Babu, P.A., Rao, B.S., Reddy, Y.V.B., Kumar, G.R., Rao, J.N., Koduru, S.K.R. and Kumar, G.S., 2023. Optimized CNN-based Brain Tumor Segmentation and Classification using Artificial Bee Colony and Thresholding. INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL, 18(1).

[26] Pierezan, J. and Coelho, L.D.S., 2018, July. Coyote optimization algorithm: a new metaheuristic for global optimization problems. In 2018 IEEE congress on evolutionary computation (CEC) (pp. 1-8). IEEE.

[27] D. K. Meena, R. Dwivedi, and S. Shukla, “Preserving patient’s privacy using proxy Re-encryption in permissioned blockchain,” in Proceedings of the 2019 Sixth International Conference on Internet of ?ings: Systems, Management and Security (IOTSMS), pp. 450–457, Granada, Spain, October 2019.

[28] R. Jabbar, N. Fetais, M. Krichen, and K. Barkaoui, “Blockchain technology for healthcare: enhancing shared electronic health record interoperability and integrity,” in Proceedings of the

2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), pp. 310–317, Doha, Qatar, February 2020.

[29] M. S. Christo, P. Sarathy, and C. Priyanka, “An efficient data security in medical report using block chain technology,” in Proceedings of the 2019 International Conference on Communication and Signal Processing (ICCSP), pp. 0606–0610, Chennai, India, April 2019.

[30] Jeet, R., Kang, S.S., Safiul Hoque, S.M. and Dugbakie, B.N., 2022. Secure model for IoT healthcare system under encrypted blockchain framework. Security and Communication Networks, 2022.

[31] A. A. Vazirani, O. O’Donoghue, D. Brindley, and E. Meinert, “Blockchain vehicles for efficient Medical Record management,” NPJ Digital Medicine, vol. 3, p. 1, 2020.

[32] R. Jeet and S. S. Kang, “E-biomedical: a positive prospect to monitor human healthcare system using blockchain technology,” World Journal of Engineering, vol. 19, no. 1, pp. 13–20, 2020.