Journal of Information Systems Engineering and Management
2025, 10(5s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Security Control Strategy Based on Blockchain for Attack Detection in the Health Care Environment

[1*]M.Sandhya, [2]Dhanesh Kumar, [3]Dr G Bhuvaneswari, [4]Dr G Manikandan, [5]Mr. Ramesh Krishnamaneni, [6]Mr. Ashwin Narasimha Murthy

[1*]Assistant Professor, Department of Electronics & Communications Engineering, Faculty of Science & Technology, IcfaiTech, ICFAI Foundation for Higher Education (IFHE), Hyderabad, India

[2]Assistant Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India

[3]Professor / CSE, Department of Computer Science and Engineering, Saveetha Engineering College, Saveetha Nagar, Sriperumbadur Taluk, Chennai, Tamil Nadu, India

[4]Professor, Department of Artificial intelligence and Data Science, RMK ENGINEERING COLLEGE RSM Nagar, Kavaraipettai, Gummidipoondi Taluk, Tiruvallur District, Tamil Nadu, India.

[5]Researcher, Jurypicks AI, Tampa, Florida US,

[5]Email: ramesh@jurypicks.ai, Researcher, Jurypicks AI, San Francisco, CA US

[6]Email: ashwin@jurypicks.ai, [1*]Corresponding Author Mail: msandhyaresearch@gmail.com

ARTICLE INFO

Received: 11 Oct 2024
Revised: 12 Dec 2024
Accepted: 24 Dec 2024

ABSTRACT

The usage of blockchain in healthcare spans a wide range of applications, including secure patient identification, clinical research, medication management, insurance, and the detection of medical fraud. In the hospital system, attack detection is also the most challenging responsibility. As a result, the data will be protected in this research by a revolutionary Blockchain-based African Buffalo Identity-Based Encryption (BABIBE) system. The system that is built in the Python program also collects and trains Electronic Health Records (EHR). Update the blockchain security to detect and ignore threats while also continuously monitoring them. The IBE approach, which encrypts data using the public key and decrypts it by private key, is used to secure data. As a result, blocks receive encrypted data that is then added to the blockchain using the private key. Additionally, depending on the threshold value, identify attacks, and compare the created technique's performance results with those of other traditional models, like energy consumption, throughput, latency, computation time, and detection rate.

Keywords: Healthcare System, Attacks, Unauthorized Access, Identity Based Encryption, Session Key, Private and Public Key.

INTRODUCTION

Originally, EHR encompasses sensitive information about the patient that is accomplished by several healthcare providers [1]. Frequently, attackers steal the EHR present in the health application which causes wrong surgery and hacking patient personal information [2]. The loss of health records tends to attain the wrong medication for a patient; as a result, loss of life is possible [3]. So, securing the medical and health care data is more important to save the patient life [4]. Moreover, blockchain is a distributed, decentralized system that allows nodes to share immutable medical records with one another without the need for an intermediary [5]. Furthermore, the distributed ledger stored blocks in the blockchain are linked [6]. Hash, data, timestamp, difficulty, nonce, previous hash, public key, and private key are all contained in each block [7].

The timestamp is used to determine the block's creation or identification time, and a hashing algorithm is employed to encrypt the contents [8]. Furthermore, an arbitrary variable known as a nonce is used to guarantee the uniqueness of every block in the blockchain and to protect it against attacks [9]. The block hash that comes right before the current block is the reference to the previous hash [10]. Moreover, healthcare data is encrypted and decrypted using private and public keys [11]. Lastly, a value known as difficulty is applied to hash value prefixes as zeros. The timing is modified in accordance with the requirements of the communication process [12, 13]. Figure 1 depicts the fundamental architecture of blockchain technology.

In particular, there are three types of blockchain: consortium, private, and public [14]. Everyone has taken part in the consortium blockchain, which is utilized by corporations, and the public blockchain

[15]. Similar to this, a private blockchain is utilized for rigorous data access management, and node contributions are limited to the entirety of the blockchain [16]. As a result, blockchain is applied in numerous industries, including finance, healthcare, and agriculture [17]. Generally, the blockchain is used in numerous areas in healthcare for health reports, secure patient identity, clinical research, managing medicine, insurance, and medical fraud detection [18]. In healthcare applications, patients' EHR are securely stored in the blockchain and the stored data of the patient are noticed and confirmed by the patient [19].

The most challenging task in blockchain-based healthcare is attack it contains different kinds of attacks such as smart contrast attacks, user wallet attacks, mining pool attacks, blockchain network attacks, dictionary-based attacks, and so on [20]. So design an optimization-based blockchain framework for enhancing security and detecting attacks. Consequently, blockchain helps perform a cryptographic technique that encrypts and decrypts the data securely and stored in the blocks. Also, secure the healthcare information containing medical education, EHR, insurance details, biomedical information, etc. It improves the reliability of stored data and also shares patient records securely between healthcare providers.

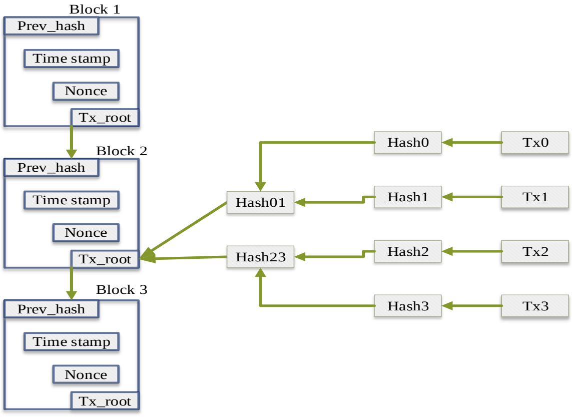

Fig.1 Blockchain structure

Attack detection is one of the most difficult issues in the healthcare setting because of its low scalability, low dependability, and long communication latency. Certain methods for data security have low throughput rates and need longer encryption and decryption times. Create a blockchain-based security control method for attack detection in a healthcare setting to address these problems. Moreover, the high energy consumption rate is caused by time complexity. It uses cryptographic techniques to secure the data and keeps an eye out for attacks.

The primary goals of the suggested model are to improve the security and privacy of the healthcare environment and to create an efficient security control method for identifying network threats. Designing an optimization-based blockchain model with cryptographic approaches to secure the data into distinct blocks is the primary contribution of the designed model. A hash function built into each block improves the EHR's security.

Below is a summary of the designed model's primary contribution.

- First, EHRs are gathered, and the Python tool is used to test and train them in the system.
- Next, create BABIBE with the right settings to protect the medical data from intrusions.
- Additionally, the plain text is transformed into ciphertext using IBE encryption, and the encrypted data is transferred to the block.
- Consequently, the African Buffalo (AB) fitness is updated in the blockchain for detecting attacks by continuous monitoring.
- The EHR is secured by the final model, and its effectiveness is evaluated against other traditional models.

The research article structure can be summed up as follows: Blockchain-based attack detection research was covered in part 2, and the system model and problem statement are covered in section 3. In the same way, section 5 included findings and debates, while section 4 detailed the methodology's procedure. In section 6, the designed model's conclusion is finally covered.

2. RELATED WORKS

Mitigation and malicious attacks are the most important issues in the Internet of Everything (IoE). Moreover, sensing data are securely processed with a fog server. PandiVijayakumar *et al* [21] proposed Blockchain based Artificial Intelligence (BAI) access control model to detect malicious attacks. The designed model measures the computation time of the blockchain which may vary the number of transactions per block. However, encryption time is more while compared to other techniques.

WeizhiMeng *et al* [22] devised the trust management scheme with blockchain for minimizing communication delay and enhancing efficiency. Furthermore, Bayesian inference-based trust management is developed for malicious nodes detection in the medical smartphone network. Additionally, experimental outcomes show efficiency and improve malicious node detection but computation time is high because of data complexity.

Because of rapid digitization, Machine Learning (ML) techniques are plays a massive role that is applicable in the area of engineering, healthcare, finance, etc. Neerajkumar *et al* [23] introduced an ML with blockchain scheme for securing the generated dataset for healthcare applications. It contains a private cloud system for tackling the aforementioned problems and also secures the data but computation delay is high.

Anik Islam and Young Shin [24] developed a secure and efficient healthcare technique using blockchain for securing healthcare data. Initially, healthcare data are collected from the patient through Unmanned Aerial Vehicle (UAV) and that is kept in the nearest server. Moreover, security analysis discussion shows the feasibility of the designed model and they are investigated through implementation and simulations. But the attack rate is high.

The HER retains health history and patient medications that are attracting more attention from attackers. The loss of EHR leads to attaining wrong surgery and wrong medication. Radhakrishnan *et al* [25] developed a blockchain-based multilevel authentication scheme for protecting the EHR from attacks. Moreover, blockchain secures the data and transactions by decentralized and distributed ledger, however, less scalability and optimality problems.

Hritu Raj et al [27] discussed the challenges related to privacy and security in the healthcare environment. This research is useful for the next generation of the healthcare industry using fog computing and IoT sensors. Also, the designed model contains several papers related to security, IoT, privacy, cloud, and the fog computing. It addresses the privacy and security issues of healthcare.

One of the powerful machine learning models is a classification that is frequently used for the prediction process. Beulah *et al* [28] introduced an ensemble method to enhance a prediction accuracy of heart diseases. The designed model predicts heart diseases in an early stage and the experimental outcomes improve the weak classifier prediction accuracy but the execution time is high.

Mohit and Shadan [29] designed an emerging computing model called edge computing for overcoming the bandwidth, and security challenges and handling time-sensitive data. Moreover, Artificial Intelligence (AI) based service placement model is proposed to improve the Quality of Service (QoS). It attains better efficiency and improves the quality but the error rate is high because of data complexity.

The most challenging and complex tasks in cloud services are gratifying the end users' QoS; optimizing cost and execution time and scheduling algorithms. Mohit Kumar et al [30] proposed autonomic scheduling and resource prevising model for scheduling the jobs and optimizing cost, energy consumption, and the processing time. Furthermore, the efficiency of the designed model is analyzed with cloudsim. However, the attack rate is maximal.

Kalka et al [31] have devised a security-based allocation model for solving an allocation of IoT services in fog and cloud environments. Here, the performance metrics are evaluated with synthetic datasets. Moreover, an experimental outcome proves the outperformance of the designed model and enhances several influential parameters. However, it has scheduling issues. Table 1. provides a full description of the literature survey.

Table.1 Summary of recent literature survey

Author	Technique	Advantage	Disadvantage
PandiVijayakumar *et al* [21]	BAI access control model	● Detect malicious attacks	● Encryption time is more

		● Measures the computation time	● Imbalance utilization
WeizhiMeng *et al* [22]	Trust management scheme with blockchain	● Minimizing the communication delay ● Enhance efficiency ● Improve malicious node detection	● Computation time is high because of data complexity ● Unable to optimize energy
Neerajkumar *et al* [23]	ML-based blockchain scheme	● Tackling the aforementioned problems ● Secure data	● Computation delay is high ● Less availability
Anik Islam and Young Shin [24]	Secure and efficient healthcare technique using blockchain	● Securing healthcare data ● Better scheduling process	● The attack rate is high ● High makespan time
Radhakrishnan *et al* [25]	Blockchain-based multilevel authentication scheme	● Protecting the EHR from attacks	● Less scalability ● Optimality problems
Beulah et al [28]	Ensemble learning method to predict heart disease	● Predicts heart diseases in an early stage ● Improve the weak classifier prediction accuracy	● Execution time is high. ● High complexity
Mohit and Shadan [29]	Emerging edge computing model	● Handle time-sensitive data ● Improve the Quality of Service (QoS) ● Attains better efficiency	● The error rate is high because of data complexity ● Overhead issue
Mohit Kumar et al [30]	Autonomic scheduling and resource prevising model	● Scheduling the jobs ● Optimize energy consumption, cost, and processing time	● The attack rate is high ● Scheduling problems
Kalka et al [31]	Security-based allocation model	● Enhances the several influential parameters	● Scheduling issues ● High resource utilization

3. PROPOSED METHODOLOGY

Developing the Blockchain-based African Buffalo Identity Based Encryption (BABIBE) Scheme would protect healthcare data from threats and unwanted access. By using a threshold value, this approach is able to identify assaults in the network by continuously monitoring their presence. Additionally, some patients' EHRs have been updated to the planned cloud system. Figure 2 shows the architecture of the suggested methodology. System administrators often become aware of patient data and provide related public data. EHR is then forwarded to IBE, which will encrypt the data by transforming plain text into ciphertext. Data are encrypted using the session key, and then the encrypted data are transferred to the block via a private key. In order to secure the data, blocks are also moved to the blockchain. This phase updates the AB fitness for ongoing network attack monitoring. Lastly, the model's design safeguards the information while also identifying threats based on their threshold value.

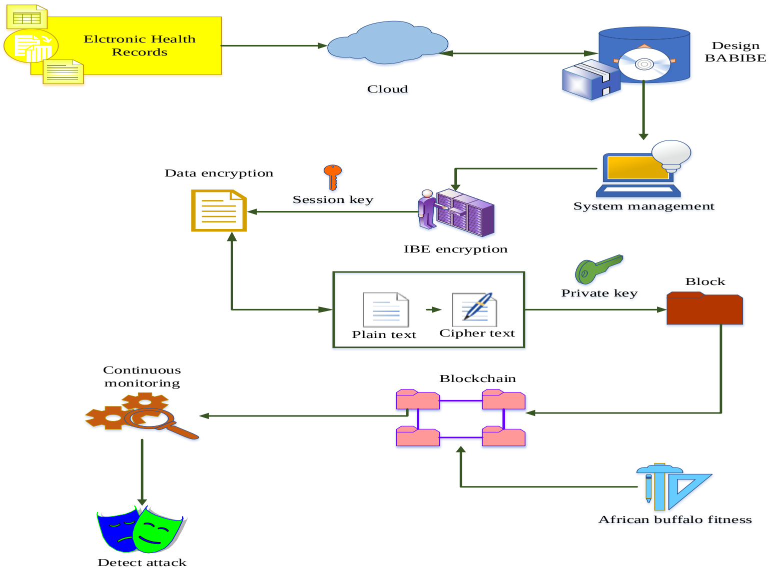

Fig.2 Proposed methodology

3.1 Encryption using Identity-Based Encryption (IBE)

The generated EHR is updated to the designed model and the system manager recognizes the patient information using generated EHR. Then generate the public information based on the patient information. To secure the data from unauthorized access and attacks cryptographic techniques are used. Each patient contains a pair of IBE private and public keys. Furthermore, all private keys are kept through the patient. In particular, data owners safely send their information to an unreliable cloud server. The data that is transferred is encrypted and kept in ciphertext format. Only those who have been granted permission by the data owners can view it. Data encryption, data decryption, key generation, and system initialization are among the four processes that make up the IBE.

Electronic health record

The EHR is a patient's medical history that is maintained throughout time by the provider. It is the organized collection of population and patient, automatically stored health information in a digital format. Moreover, EHR is generated if the patient consults the doctor that contains medication and diagnosis information. After the generation of EHR, a notification goes to the patient.

- **System initialization**

Initially, generate the system parameters S_p, and secrete key is selected randomly from M. Moreover, system parameters contain the description of the plaintext space Q and ciphertext space R. Furthermore, the security parameters M as input that runs the secrete key and system parameters. Then select the random generator R_g form M that $R_g \in M$. Afterward, fix the value $R_{g1} = R_g \alpha$ and select randomly R_{g2} in M. Moreover, select the security parameter by selecting the random number j such that $j^{'} \in M$. At last, $R_g, R_{g1,} R_{g2},$ and $j^{'}$ are the public parameter and $R_{g2}\alpha$ are represented as a master key.

- **Key generation**

The EHR of the patient ID is considered as input and returns the secret value x_d of the patient ID and the session key as Sx_d. Consequently, neither the session key nor the created secret value are revealed.

Then generate the random number k for the identity of the patient that offers security to the designed technique. Thus, the k has decided to use Equation (1) to determine the matching private key.

$$P_k^s = \left(R_{g2}\alpha \left(j^{'} \prod_{i\in k} k_i \right), Sx_d \right) \tag{1}$$

Let, k_i is denoted as the i^{th} bit of patient identity, $R_{g2}\alpha$ is represented as the master key, $j^{'}$ is called as the public parameter and Sx_d is denoted as the session key. Moreover, patient ID contains mailbox, ID number, IP, and other information.

- **Data encryption**

Patient identifying information is represented by the letter I_d, and system settings S_p, a master key $R_{g2}\alpha$, and the plain text are utilized to turn it into ciphertext. The plain text is denoted as W_p, and C_p is considered as ciphertext, and A_k^s is deliberated as a public key. Using Equation (2), ordinary text is transformed into ciphertext.

$$D_e = S_p \left(W_p \left(R_{g2}\alpha\right) A_k^s \left(j^{'} \prod_{i\in k} k_i \right), C_p \right) \tag{2}$$

An erroneous public key A_k^s in an encryption failure. Additionally, IBE encryption protects the data from attacks and unwanted access, and the private keys are used to securely store the encrypted data in the blockchain.

- **Data decryption**

A system parameter and private key are required to decrypt the ciphertext into plaintext and extract the data from it. Additionally, Eqn (3) is used to process the decryption of the designed model.

$$D_{de} = S_p \left(C_p \left(R_g, R_{g1}, R_{g2}\right) P_k^s, \frac{C_p \left(R_g\right) \left(j^{'} \prod_{i\in k} k_i \right)}{C_p \left(R_{g2}\alpha\right) \left(j^{'} \prod_{i\in k} k_i \right)}, W_p \right) \tag{3}$$

Using the private key, the encrypted data are sent to the blocks, which are subsequently moved to the blockchain. The EHR is hashed using the supplied key generation, just like every other block in the blockchain. As a result, the process of key generation produces the keys needed to build blockchain blocks. Lastly, use secret keys to lock down the EHR on the blockchain. The algorithm 1 provides a detailed process of the designed model .

Design BABIBE framework for securing healthcare data from attacks

```
Input: EHR
Output: detect an attack
Start
    {
            Set dataset
            // patient ID, patient information, etc
Design BABIBE
        Update dataset to BABIBE
```

```
IBE
//Encrypt a data for enhancing security
System initialization
        // plain text, input. system parameter
Key generation
        // produce session key
            For all k=1
            {
            session key, $Sx_d$
            }
            End for
Data encryption
        Create public key, $A_k^s$
        Encrypt a data
Data decryption
            Produce private key, $P_k^s$
            Decrypt a data
Attack detection
        // continuous monitoring of attack
        Update AB fitness
        Calculate threshold value using Eqn. (4)
             if $(k(s) \le 0.1$
             {
             Attack
             }
              else if $(k(s) \ge 0.1$
              {
              No attack
              }
              End if
Detect attacks
Secure the data
   }
End
```

-
- **Attack detection**

Moreover, healthcare provider accesses the data using the private key but it has the chance to hack the healthcare data using attacks and unauthorized access. The most challenging task in healthcare data is the detection of attacks because of improper prediction, failure in key generation, and high latency. Update the AB fitness in the blockchain during this phase to keep an eye out for any ongoing network threats. The "waa" (alert) and "maa" (alarm) noises are used to distinguish the food and an attacker in the AB fitness process.

Utilizing the threshold value for ongoing monitoring, the proposed model aims to detect any assaults that may be present in the network. The threshold value is obtained using Eqn. (4).

$$T_m^s = \frac{D_e(b) - k(s)}{p_k^s \times B(n)} \tag{4}$$

Let, $D_{e(b)}$ is denoted as encrypted data from the blockchain, $k(s)$ is considered as a threshold value, and $B(n)$ is AB fitness function. Furthermore, detection of attacks is obtained using Eqn. (5).

$$A_d^r(s) = \begin{Bmatrix} if\,(k(s) \leq 0.1, & 1 \\ if\,(k(s) \geq 0.1, & 0 \end{Bmatrix} \tag{5}$$

While the threshold value is less than 0.1, detect attacks but a threshold value is greater than 0.1, no attacks present in a network. Lastly designed model continuously monitors the network and whether any attacks are presented in the network. Figure 3 illustrates the intended model workflow. Numerous data blocks make up a blockchain. These data blocks are kept on nodes that allow for comparison. On a blockchain, every node is linked to every other node. This makes sure that every node is updated. The blockchain is stored, distributed, and maintained by the nodes. Nodes are a key component of a blockchain's framework.

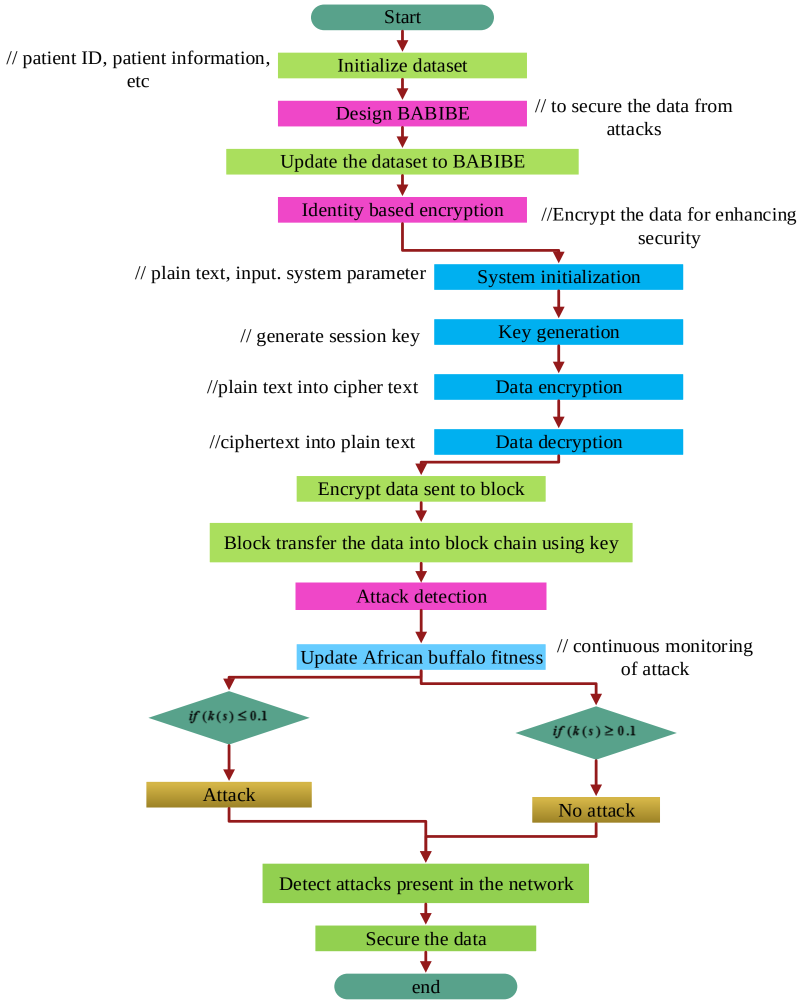
Start
// patient ID, patient information, etc
Initialize dataset
Design BABIBE
// to secure the data from attacks
Update the dataset to BABIBE
Identity based encryption
//Encrypt the data for enhancing security
// plain text, input. system parameter
System initialization
// generate session key
Key generation
//plain text into cipher text
Data encryption
//ciphertext into plain text
Data decryption
Encrypt data sent to block
Block transfer the data into block chain using key
Attack detection
Update African buffalo fitness
// continuous monitoring of attack
if (k(s) ≤ 0.1
if (k(s) ≥ 0.1
Attack
No attack
Detect attacks present in the network
Secure the data
end

Fig.3 Workflow of the designed model

4. RESULTS AND DISCUSSIONS

Create the BABIBE model that is used in the Python tool to protect the healthcare data from intrusions. Patients' electronic health records are first tested and trained on the system before being upgraded to the intended model. Additionally, blockchain is implemented in a consensus mechanism which is one of the fault-tolerant mechanisms helpful for blockchain systems and computers. It validates, verifies, and confirms the datasets by generating block records. Additionally, IBE is used to process data encryption, safely encrypting the data using the created session key. Next, use the private key to transform the plain text into ciphertext, which is then sent to the blocks. Subsequently, the blocks are moved to the blockchain for data security. Additionally, update AB's fitness on the blockchain to identify threats through ongoing system monitoring. Lastly, obtained performance outcomes are contrasted with those of other traditional models.

4.1 Performance metrics

The results obtained from the proposed BABIBE model are verified in terms of energy consumption, throughput, latency, calculation time, and detection rate using other pertinent methodologies. Additionally, the efficiency of the designed model is contrasted with several traditional methods, including AI-based Access Control Blockchain (AIACB) [21], Blockchain-based Secure Healthcare (BbSH) Technique [24], and Multi-Security Level Cloud Storage (MSLCS) scheme [26].

- **Energy Consumption (EC)**

EC denotes the energy used for performing an action, processing, or manufacturing something which is measured by gaining energy from the production process. For securing the healthcare data, energy consumption is essential to transmit the EHR to cloud server. It is measured by multiplying by the wattage of several working hours or operational hours. The proposed technique energy consumption is compared with other models that are shown in table.2.

Table.2 Validation of energy consumption

Data size	Energy consumption (J)			
	AIACB	BbSH	MSLCS	Proposed
50	3.27	1.25	4.54	0.65
100	3.65	1.45	5.12	0.94
150	4.21	2.32	5.98	1.21
200	4.77	2.42	6.43	1.43

The energy consumption of the designed model is associated AIACB, BbSH, and MSLCS. Moreover, the AIACB technique attained energy consumption is 3.27J for 50 data sizes; the BbSH technique attained energy consumption is 1.25J for 50 data sizes. The energy consumption comparison is in fig.4.

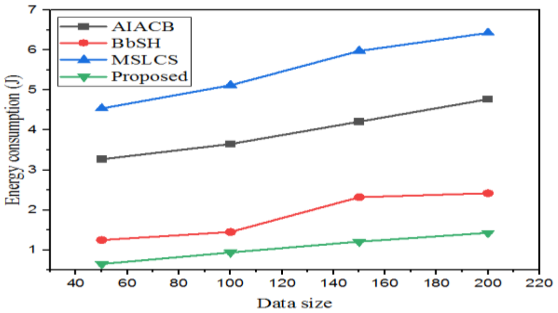

Fig.4 Comparison of energy consumption

Furthermore, the MSLCS model attains 4.54J in energy consumption and the developed model attains 0.65J in energy consumption for using a 50 data size. While comparing other techniques developed techniques attain low energy consumption.

- **Throughput**

- It is the number of units within an assured period that is passed by the production process which is measured by the unit moving rate from beginning to end. The amount of information or product in the server that is generated and delivered to the client at a specific time is called throughput.

The designed model's increased throughput performance is contrasted with alternative methods, which are listed in the table.3.

Table.3 Validation of throughput

Data size	Throughput (kB/s)			
	AIACB	BbSH	MSLCS	Proposed
50	28.5	37.9	43.5	83.7
100	26.7	36.5	41.4	81.1
150	24.8	35	39.4	78.5
200	23.4	34.4	37.1	76.3

Generally, the AIACB model gained a throughput rate of 28.5kB/s, the BbSH model attained a throughput rate of 37.9kB/s, and the MSLCS model attained a throughput rate of 43,5kB/s for using 50 data sizes. Figure 5 displays the throughput comparison.

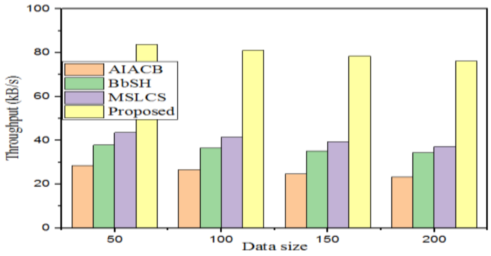

Fig.5 Comparison of throughput

In particular, the proposed model outperformed other traditional models in terms of throughput, with an achieved throughput rate of 83.7 kB/s. It displays the designed model's effectiveness and performance.

- **Latency**

Latency refers to how much time is taken to transmit a data packet to a destination point. Moreover, low latency is considered positive communication but high latency is considered poor communication. Furthermore, the time taken for transferring the data between the source and destination as well as high latency causes the internet connections, communication process, and data transmission process. Figure 6 and Table 4 provide a full comparison of latency.

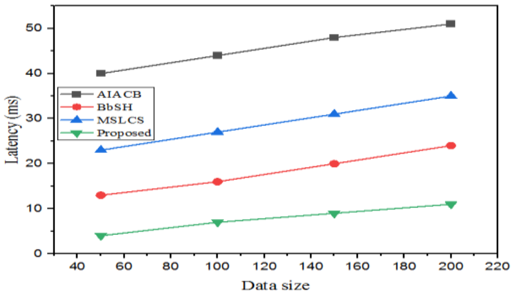

Fig.6 Comparison of latency

Furthermore, the MSLCS model attains 23ms in latency and the developed model attains 4ms in latency for using a 50 data size. While comparing other techniques developed techniques attain low latency.

Table.4 Validation of latency

Data size	Latency (ms)			
	AIACB	BbSH	MSLCS	Proposed
50	40	13	23	4

100	44	16	27	7
150	48	20	31	9
200	51	24	35	11

The created model's latency is contrasted with that of other traditional models, such as AIACB, BbSH, and MSLCS. Moreover, the AIACB technique attained a latency is 40ms for 50 data sizes; the BbSH technique attained a latency is 13ms for 50 data sizes.

- **Detection Rate (DR)**

Generally, the detection rate is denoted as a fraction of all health dataset who has the attacks and the percentage of attacks identified during data transmission. It proves the efficiency of the developed framework by identifying the attacks present in the cloud server. Furthermore, the system continuously monitors the network traffic to detect attacks or unauthorized access in the network environment. Table 5.5 provides specifics on the designed model's detection rate gain performance.

Table.5 Validation of Detection Rate

Data size	Detection Rate (%)			
	AIACB	BbSH	MSLCS	Proposed
50	76.4	85.4	92.2	98.5
100	73	83.2	90	98
150	71.1	81	88.2	97.6
200	68.4	78.12	86.3	97.2

Generally, the AIACB model gained a detection rate of 76.4%, the BbSH model attained a detection rate of 85.4%, and the MSLCS model attained a detection rate of 92.2% for using 50 data sizes. The comparison of detection is shown in fig.7.

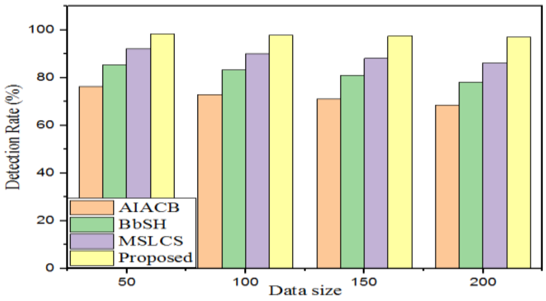

Fig.7 Comparison of detection rate

In particular, developed models achieved a detection rate of 98.5% and got superior detection when compared to other traditional models. It illustrates the performance and efficacy of the specified model.

- **Computation Time (CT)**

It is the length of the required time for performing the computational process. And the computation time is proportional to the number of rule applications. Moreover, it is spending time performing computations on the data. Table 6.6 provides a detailed comparison of the designed model's gained calculation time with alternative methods currently in use.

Table.6 Validation of computation time

Data size	Computation time (ms)			
	AIACB	BbSH	MSLCS	Proposed
50	28.64	15	22.5	8

100	29.65	17.2	25.8	10
150	31.70	20	29.34	12.3
200	33.08	22.45	33	14

The developed model computation time is contrasted with those of other traditional models, such as AIACB, BbSH, and MSLCS. Moreover, the AIACB technique attained a computation time is 28.64ms for 50 data sizes; the BbSH technique attained a computation time is 15ms for 50 data sizes. The computation time comparison is shown in fig.8.

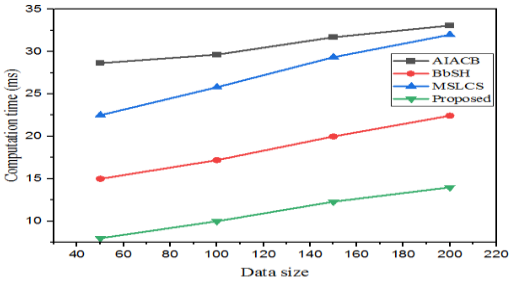

Fig.8 Comparison of computation time

Furthermore, the MSLCS model attains 22.5ms in computation time and the developed model attains 8ms in computation time by 50 data sizes. Low computation times are achieved by developed strategies as compared to others.

5.2 Discussion

The BABIBE has shown good performance with high throughput, detection rate, energy consumption, latency, and computation time. Thus, the designed model detects the attacks presented in the network. It continuously monitors the threshold value of users using AB fitness. Thus, the developed technique attains less time for detecting attacks and gained energy consumption is low. Table 7 provides a detailed analysis of the intended model's overall performance using current approaches.

Table.7 Overall performance assessment

Performance assessment	Methods			
	AIACB	BbSH	MSLCS	Proposed
Energy consumption (J)	3.27	1.25	4.54	0.65
Throughput (kB/s)	28.5	37.9	43.5	83.7
Detection Rate (%)	76.4	85.4	92.2	98.5
Computation time (ms)	28.64	15	22.5	8

Generally, the designed model attains better results while comparing other models like AIACB, BbSH, and MSLCS. The designed model archives 0.65J of energy consumption, 83.7 kB/s of throughput, 98.5% of detection rate, and 8ms of computation time for 50 data sizes. Thus, the developed model enhances the security by encrypting the data, and the encrypted data are secured and stored in several blocks which improve the security and privacy of the healthcare environment. Also, the proposed blockchain is used for securing the data from sensors.

6. CONCLUSIONS

To secure the healthcare data from attacks designed BABIBE model stores the encrypted data securely in a cloud server. The main aim of the designed model is to detect the attacks present in the system also secure the data by IBE and securely store it in the blockchain. Also continuously monitor the attacks present in the network using the fitness of AB. Consequently, the IBE scheme involves four processes to encrypt and decrypt the data. Moreover, the session key is generated to secure the data and encrypt the data using the public key. Additionally, decryption used a private key and the encrypted data is stored in the blocks. That block is securely transferred to the blockchain with the hash function and generated keys. Finally, attained results of the designed model prove the efficiency and scalability. The achieved energy consumption rate is 0.65J, throughput 83.7 kB/s, latency 4ms, and detection rate 98.5%. Thus the designed model can detect the attacks and secure the data in the healthcare environment. In the future, blockchain-based artificial intelligence techniques enhance the QoS in healthcare and also will reduce the medical industry cost. Moreover, combing cryptographic techniques into AI reduce the vulnerabilities.

Compliance with Ethical Standards

Conflict of interest

The authors declare that they have no conflict of interest.

Human and Animal Rights

This article does not contain any studies with human or animal subjects performed by any of the authors.

Informed Consent

Informed consent does not apply as this was a retrospective review with no identifying patient information.

Funding: Not applicable

Conflicts of interest Statement: Not applicable

Consent to participate: Not applicable

Consent for publication: Not applicable

Availability of data and material:

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Code availability: Not applicable

REFERENCES

[1] Pai, Manohara MM, et al. "Standard electronic health record (EHR) framework for Indian healthcare system." Health Services and Outcomes Research Methodology 21.3 (2021): 339-362.

[2] Ibarra, Jaime, Hamid Jahankhani, and Stefan Kendzierskyj. "Cyber-physical attacks and the value of healthcare data: facing an era of cyber extortion and organised crime." Blockchain and Clinical Trial. Springer, Cham, 2019. 115-137.

[3] Nemati, Mohammadreza, Jamal Ansary, and NazafarinNemati. "Machine-learning approaches in COVID-19 survival analysis and discharge-time likelihood prediction using clinical data." Patterns 1.5 (2020): 100074.

[4] Kumar, Dinesh, and S. Smys. "Enhancing security mechanisms for healthcare informatics using ubiquitous cloud." Journal of Ubiquitous Computing and Communication Technologies 2.1 (2020): 19-28.

[5] De Aguiar, Erikson Júlio, et al. "A survey of blockchain-based strategies for healthcare." ACM Computing Surveys (CSUR) 53.2 (2020): 1-27.

[6] Sunyaev, Ali. "Distributed ledger technology." Internet Computing. Springer, Cham, 2020. 265-299.

[7] Zhai, Sheping, et al. "Research on the Application of Cryptography on the Blockchain." Journal of Physics: Conference Series. Vol. 1168. No. 3. IOP Publishing, 2019.

[8] Velmurugadass, P., et al. "Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm." Materials Today: Proceedings 37 (2021): 2653-2659.

[9] Kumar, Ranjith, and N. Bhalaji. "Blockchain based chameleon hashing technique for privacy preservation in E-governance system." Wireless Personal Communications 117.2 (2021): 987-1006.

[10] Huang, Ziqing, and Shiguang Liu. "Perceptual hashing with visual content understanding for reduced-reference screen content image quality assessment." IEEE Transactions on Circuits and Systems for Video Technology 31.7 (2020): 2808-2823.

[11] Chenthara, Shekha, et al. "Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology." Plos one 15.12 (2020): e0243043.

[12] Zhang, Lejun, et al. "A covert communication method using special bitcoin addresses generated by vanitygen." Computers, Materials & Continua 65.1 (2020): 597-616.

[13] Li, Fengyin, et al. "Aitac: an identity-based traceable anonymous communication model." Journal of Ambient Intelligence and Humanized Computing (2020): 1-10.

[14] Assaqty, Mohammad IqbalSaryuddin, et al. "Private-blockchain-based industrial IoT for material and product tracking in smart manufacturing." IEEE Network 34.5 (2020): 91-97.

[15] Madhura, K., and R. Mahalakshmi. "Usage of block chain in real estate business for transparency and improved security." 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI). IEEE, 2022.

[16] Albanese, Giuseppe, et al. "Dynamic consent management for clinical trials via private blockchain technology." Journal of Ambient Intelligence and Humanized Computing 11.11 (2020): 4909-4926.

[17] Swetha, M. S., et al. "Blockchain enabled secure healthcare Systems." 2020 IEEE International Conference on Machine Learning and Applied Network Technologies (ICMLANT). IEEE, 2020.

[18] KamelBoulos, Maged N., James T. Wilson, and Kevin A. Clauson. "Geospatial blockchain: promises, challenges, and scenarios in health and healthcare." International Journal of Health Geographics 17.1 (2018): 1-10.

[19] Mahajan, Hemant B., et al. "Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems." Applied Nanoscience (2022): 1-14.

[20] Akbar, NurArifin, et al. "Distributed Hybrid Double-Spending Attack Prevention Mechanism for Proof-of-Work and Proof-of-Stake Blockchain Consensuses." Future Internet 13.11 (2021): 285.

[21] Bera, Basudeb, et al. "AI-enabled blockchain-based access Control for malicious attacks detection and mitigation in IoE." IEEE Consumer Electronics Magazine 10.5 (2020): 82-92.

[22] Meng, Weizhi, Wenjuan Li, and Liqiu Zhu. "Enhancing medical smartphone networks via blockchain-based trust management against insider attacks." IEEE Transactions on Engineering Management 67.4 (2019): 1377-1386.

[23] Gadekallu, Thippa Reddy, et al. "Blockchain-Based Attack Detection on Machine Learning Algorithms for IoT-Based e-Health Applications." IEEE Internet of Things Magazine 4.3 (2021): 30-33.

[24] Islam, Anik, and Soo Young Shin. "A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things." Computers & Electrical Engineering 84 (2020): 106627.

[25] Radhakrishnan, B. L., A. Sam Joseph, and S. Sudhakar. "Securing blockchain based electronic health record using multilevel authentication." 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS). IEEE, 2019.

[26] Shen, Jinan, Xuejian Deng, and ZhenwuXu. "Multi-security-level cloud storage system based on improved proxy re-encryption." EURASIP Journal on Wireless Communications and Networking 2019.1 (2019): 1-12.

[27] Raj, Hritu, et al. "Issues and challenges related to privacy and security in healthcare using iot, fog, and cloud computing." Advanced Healthcare Systems: Empowering Physicians with IoT-Enabled Technologies (2022): 21-32.

[28] Latha, C. Beulah Christalin, and S. Carolin Jeeva. "Improving the accuracy of prediction of heart disease risk based on ensemble classification techniques." Informatics in Medicine Unlocked 16 (2019): 100203.

[29] Ali, Shadan, and Mohit Kumar. "Service Placement in Edge Computing with AI Based Techniques." International Conference on Computing in Engineering & Technology. Springer, Singapore, 2022.

[30] Kumar, Mohit, et al. "ARPS: An autonomic resource provisioning and scheduling framework for cloud platforms." IEEE Transactions on Sustainable Computing 7.2 (2021): 386-399.

[31] Dubey, Kalka, S. C. Sharma, and Mohit Kumar. "A Secure IoT Applications Allocation Framework for Integrated Fog-Cloud Environment." Journal of Grid Computing 20.1 (2022): 1-23.