IJISAE

International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Fog-Assisted Anomaly Detection in Healthcare IoT Networks using Lightweight Blockchain and Collaborative Intrusion Detection Systems

R. Mageswaran[1*], Ponnam Lalitha[2], Y.M.Mahaboob John[3],G. Vennila[4], R. Kesavan[5], N. Kumaran[6]

Submitted: 14/05/2024 **Revised**: 27/06/2024 **Accepted**: 07/07/2024

Abstract*:* The Internet of Things (IoT) has its footprint in each and every industry all over the world. Most industries are using IoT predominantly for its eminent performance, and the Internet of Medical Things (IoMT) is specifically used in Medical industries for providing effective and timely healthcare systems. Each and every data is counted as a precious thing in the medical field because a single alteration or modification in a patient's data will lead to wrong treatment and may cause serious issues in the patient's life. In the proposed work fog, fog-based anomaly detection is incorporated by using a lightweight blockchain approach. The raw data in a network is initially stored in local blocks, and after performing data aggregation and filtration, the selective blocks are transferred to the global block. These are further used for analysis purposes. The lightweight blockchain reduces the latency and improves efficiency. These blocks can be easily corrupted by malicious users or attackers. So, to enhance the security of the system, we have implemented a collaborative intrusion detection system based on the Lion Salp swarm optimization algorithm, which is a branch of the Metaheuristic algorithm. The proposed system has achieved 99.7% accuracy and 99.2% precision. This shows that the proposed work outperformed all other existing algorithms.

Keywords: *Internet Of Things (IoT), Internet Of Medical Things (IoMT), Fog Computing, Blockchain Approach, Intrusion Detection System (IDS), Lion Salp Swarm Optimization Algorithm, Metaheuristic Algorithm and Healthcare.*

1. Introduction

In recent days, there have been numerous health issues, particularly post-COVID-19, where individuals are exposed to new viruses daily. Many immune systems are weakening due to environmental neglect, escalating global warming, and heat waves, leading to various health problems. The medical industry witnesses continuous advancements in technology to combat these challenges. Additionally, managing patient records poses a significant challenge. Storing patient medical data in the cloud for future reference emerges as a viable solution. This enables healthcare professionals to monitor patients' medical conditions and administer timely treatment.

Consistently updating and maintaining patient records is paramount for accurate medical diagnoses. Even minor alterations in a patient's record could result in incorrect treatment, potentially leading to severe consequences or, in some cases, posing a life-threatening risk.

Cybersecurity emerges as a critical component in the Internet of Medical Things (IoMT) due to the storage of data in the cloud, rendering it vulnerable to cyberattacks. Unauthorized individuals can potentially access and manipulate patient records, posing serious risks. The majority of cyberattacks occur at the application layer of the network, making them challenging to detect through conventional verification methods, as they occur post-validation. Effective optimization techniques are essential to enhance the privacy and security of healthcare systems. Initially, the establishment of a database containing information on both legitimate and anonymous users serves as a preventive measure against malicious attacks. Subsequently, the implementation of specific optimization techniques utilizing metaheuristic algorithms fortifies our healthcare infrastructure. Intrusion detection systems based on metaheuristic algorithms play a pivotal role in bolstering the privacy and security of our healthcare systems.

Privacy concerns are addressed through the implementation of a lightweight blockchain approach, enhancing transparency and privacy for legitimate users. This method begins by obtaining authorization from the user, facilitating access to their database. Subsequently, the Electronic Health Record (EHR) is maintained for future

[1] *Assistant Professor, Department of EEE, S.A. Engineering College, Anna University, Thiruverkadu, Tamil Nadu-600077, India,* ***Email: mageswaranrr@gmail.com*(Corresponding Author)***

[2] *Assistant Professor, Department of Computer Science and Engineering (Data Science), VNR Vignana Jyothi Institute of Engineering and Technology, Pragati Nagar, Bachupally, Hyderabad.*
Email: lalitha_p@vnrvjiet.in

[3] *Assistant Professor, Department of ECE, Mahendra College of Engineering, Salem-636106, Tamil Nadu.* ***Email: mehaboobece712@gmail.com***

[4] *Assistant Professor, Department of Artificial Intelligence and Machine Learning, School of Computing, Mohan Babu University, Tirupati – 517102 Andra Pradesh*
Email: drvennilam@gmail.com

[5] *Assistant Professor, Department of Artificial intelligence and data science P.S.R Engineering College, Sivakasi – 626140, Tamil Nadu.* ***Email: kesavan@psr.edu.in***

[6] *Assistant Professor, Department of Mathematics, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai - 600062, Tamil Nadu. India*
Email: nkumaran@veltech.edu.in

reference. Recognizing that traditional blockchain systems demand substantial computational resources, the adoption of lightweight blockchains is favored. To overcome limitations, integration of fog computing is employed, enhancing the effectiveness and efficiency of the system.

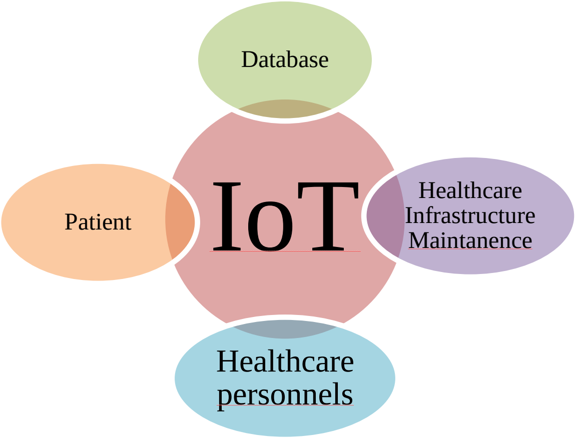

Fig 1 General block diagram of Internet of Things in medical industries.

Figure 1 represents the general block diagram of the Internet of Things in the medical industry. The block diagram demonstrates that the IoT comprises patient details stored in a database, which are used in healthcare industries for further reference by doctors and nurses.

2. Literature review

The Internet of Medical Things (IoMT) plays a vital role in developing healthcare industries. It is a field where we require accurate data with low execution time. These are evergreen industries and require day-to-day innovation of new technologies [1]. Blockchain-based IoT serves best in the field. In the review paper, the studies are carried out for the last five years with existing technologies, and proven blockchain-based approaches serve well. The study discusses all factors, starting from the tools used, hardware components utilized, and the software used [2]. As a further development, the healthcare monitoring system requires an effective and cost-efficient structure to meet the requirement. RFID plays a vital role in such criteria. To reduce the cost, chip-less devices are introduced, and various studies have been carried out to project the design structure and fabrication mechanism of such devices. These chip-less devices are prone to external and internal losses [3].

The modernized healthcare system should provide all the services remotely, and that should fit into our palm. The 5G technology is used to achieve our requirements. Under this modernized healthcare system, patients' databases are customized based on their personal requirements, and they are secured by indulging primitive measures [4]. Authentication is the most important factor in safeguarding the data. That too in a healthcare system requires a strong authentication mechanism to secure the personal physical data of individual patients [5]. In some cases, the adequacy of the system is interrupted by malicious users and hackers. To sort out this issue, various authentication algorithms are followed [6].

The data stored in the cloud, termed big data, comprises bundles of raw data. With such vast amounts of data, suitable computational strategies are necessary to make accurate decisions and provide correct treatment. Maintaining the privacy and confidentiality of both patients and healthcare providers is crucial. While blockchain-based healthcare systems offer security, the adoption of the holochain approach aims to enhance privacy and security levels further. This approach delves into resource management and privacy constraints to improve overall system integrity.

An increase in the number of IoT devices increases both pros and cons in the network. These networks can be easily hacked by sending spam messages and guessing the keys. So, the network has to prevent those intruders by following specific approaches in a precise manner. The study follows a hybrid model to solve the issue [10]. Another drawback is the difficulty of dynamically detecting the unknown drifts or attacks that happen in normal traffic of a system. These drifts have to be assed properly to maintain a secured network. Cutting-edge techniques are implanted to resolve these issues [11]. These can also be sorted out by using a prototyping mechanism [12]. Proper classification mechanisms should be included to protect our network from intruders. The study has employed an ensemble classifier to meet the requirement [13].

3. Proposed work

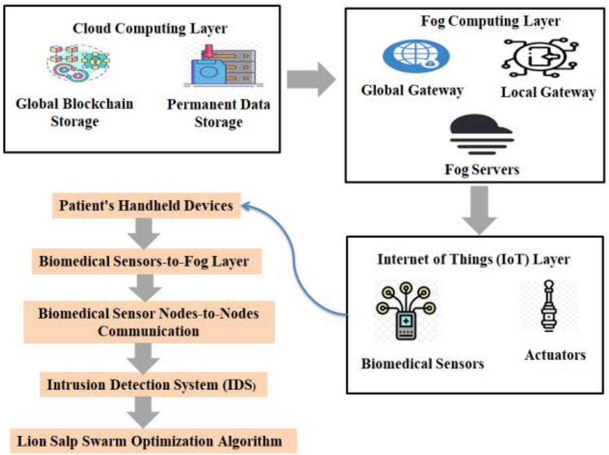
Cloud Computing Layer
Global Blockchain Storage
Permanent Data Storage
Fog Computing Layer
Global Gateway
Local Gateway
Fog Servers
Patient's Handheld Devices
Biomedical Sensors-to-Fog Layer
Biomedical Sensor Nodes-to-Nodes Communication
Intrusion Detection System (IDS)
Lion Salp Swarm Optimization Algorithm
Internet of Things (IoT) Layer
Biomedical Sensors
Actuators

Fig 2 Comprehensive Architecture for Healthcare IoT with Fog Computing and Blockchain

In the proposed work, we discuss anomaly detection techniques in Healthcare IoT using fog-based lightweight blockchain and an Intrusion detection system. The proposed work has three modules: patient healthcare system Architecture, Lightweight blockchain module, and Intrusion Detection system.

3.1 Patient's Healthcare System Architecture

Patient's Healthcare System Architecture comprises three layers, namely

3.1.1 Internet of Things (IoT) device layer

The First layer corresponds to the Internet of Things (IoT) device layer. This layer is responsible for data collection. Initially, data aggregation is performed. Various sensor nodes are deployed to gather the patient's biomedical information and other data. This process is carried out periodically and then the collected data is transferred to the fog computing layer. All the information is noted by the doctors and corresponding nurses to assist with the procedure.

3.1.2 Fog Computing Layer

The second layer corresponds to the Fog computing layer. The fog computing layer has many gateways, and it collects data from subnetworks and performs all computational operations starting from data aggregation, filtration, and protocol translation and finally providing high-level services. Initially, the data obtained from the first layer will be processed, and then it will be stored in the cloud. The fog computing layer filters the necessary data that has to be stored in the cloud and omits the temporary information. Sensor nodes will be continuously monitoring the patient's biomedical reports, and they will immediately inform both the patient and doctor if there is any abnormal result obtained. The corresponding doctor will note the records and give treatment accordingly. Fog maintains two gateways for blockchain namely local gateway and global gateway. If there is any interruption occurs, the fog stops communicating with the cloud and starts storing the data in the local gateway. Because of the diversified functionalities, fog reduces the latency constraints and improves timely response to the end user.

3.1.3 Cloud Computing Layer

The Third layer corresponds to the cloud computing layer. The cloud is nothing but blockchains. This layer performs analytical operations and stores the data. The data stored here are permanent data that are considered while giving treatment. This layer is responsible for classifying the data and predicting the disorder or diagnosing the disease. Doctors will plan the type of treatment based on this prediction. These data can only be accessed by authorized authorities. It provides an anonymous ID to the user where he/she can hide their data from external users. This provides a high-security level. Alert message will be sent to all the corresponding authorities who are linked to the patient's ID.

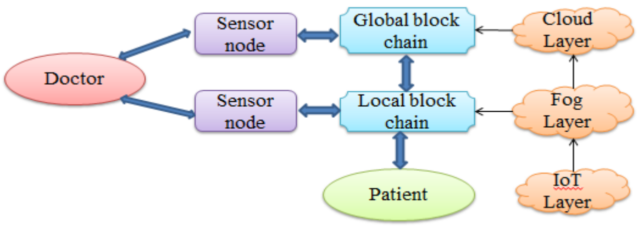

Fig 3 General Block Diagram of Three layered Patient's Healthcare System Architecture

Figure 3 represents the general block diagram of a three-layered patient healthcare system architecture, which demonstrates the architecture's working procedure.

3.2 Data transmission

The data transmission occurs in the blockchain module. The consensus algorithm is used for transferring the data. It is done only after processing the following steps namely

1. Verification

2. Consent

3. Secured communication harmonization

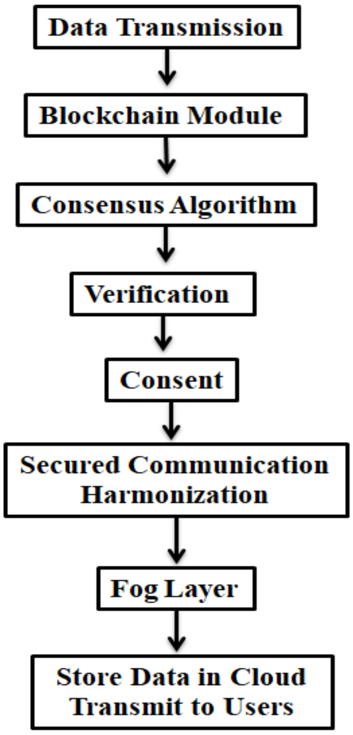

Figure 4 Data Transmission Process in Healthcare IoT

The fog layer serves as the point of control between the IoT layer and the cloud layer, where it controls and assists a specific group of IoT devices. Once the fog layer completes all the above-mentioned steps, the data is stored in the cloud and transferred to the corresponding persons connected to each individual ID in four different forms.

3.2.1 End user to Fog layer

Whenever the end user requires to get access to the patient's data, he/she has to send a request to the fog layer along with specific authentication functionalities. The fog layer has a list of authorized individuals who can access the patient's database. It includes healthcare professionals such as doctors and nurses, caretakers, and the patient themself. It also has included a particular authorized person to whom all the data has to be handed over in the event of diminish. Initially, the fog layer verifies the requested users ID with the existing accessible individuals list, and if the ID matches with the listed personality, the fog layer gives access to the user along with a unique ID that is used for accessing the data, the time period of accessing the data and corresponding block address. If the ID doesn't match with the existing list, the fog layer rejects the request and intimates the user regarding an unauthorized attempt to get access.

3.2.2 Biomedical sensor nodes-to-fog layer

In a healthcare system, many sensor nodes will be deployed in various positions based on the medical requirements. The group of sensor nodes with similar functionalities will form a cluster, and these clusters will have a cluster head, and they are called a block header. The data collected by the sensory nodes are called blocks, and they are transferred to the block header. The block header contains raw data, and it will perform data aggregation and cumulate the fused data blocks. These data blocks will be further transferred to the fog layer. To avoid congestion, it schedules time slots for every individual node. Each node within the network will be aware of the blocks that are transferred. These detailing will be fed into the handheld devices that monitor the patient's health condition. Whenever a request arises from such devices, the fog layer performs two operations, namely validation and authorization. If the obtained request is from the authorized device, the fog layer gives access to the device, and if it doesn't satisfy the condition, it will send a rejection message to the corresponding device.

3.2.2 Fog layer-to-fog layer

The medical sensor nodes will collect all the data with different parameters like biomedical conditions, physical conditions, etc. These are the predominated requisites through which a doctor can assist the patient remotely. It periodically monitors the patient's readings and checks for abnormalities. If any abnormality occurs, the fog layer will intimate an alert message to the health care provides fog layer. After the medical assessments, the doctor decides whether the patient should visit in person for treatment or they can be treated remotely. This also maintains a smooth data transmission when the patients move around the hospital as well as at home. It maintains an uninterrupted data transmission. It improves efficiency and mobility.

3.2.4 Biomedical sensor nodes -to Biomedical sensor nodes

The Biomedical sensor nodes -to-medical sensor node communication ensures the patient's medical condition is stable after the hospitalized treatment is over. It helps to monitor the patient's medical condition remotely and transfers the data to the medical authorities periodically. These sensor nodes are bonded with the patients, and these will monitor the patient's preliminary health conditions like BP level, blood glucose level, and heart rate. Similarly, there will be some sensor nodes placed in hospitals. Both the nodes that are placed remotely and in the hospital will be connected to the block-enabled fog layer. These nodes can communicate with each other. The communication link will be enabled only when they are enabled to the fog layer. The remotely placed sensors will intimate the sensor nodes that are connected in the hospital when there is an abnormality in a patient's health condition. These nodes will search for the availability of beds in the hospital for emergency admission purposes.

3.3 Blockchain Architecture

The blockchain approach is used to establish reliable and transparent data transmission. We utilize a consensus algorithm to achieve a blockchain module.

In the medical field, each patients are monitored by using sensor nodes. Similar nodes will form a cluster, and there will be a cluster head who communicates with the end user, and he decides which data to store and which data is to be removed. Data in the system is referred to as blocks. Periodically, these blocks undergo examination, and expired blocks that are no longer required for further processing are removed. This helps to improve the efficiency of the system and improves the speed of the system.

Authorized users can alone look into these blocks. The sensor nodes in each cluster will continuously collect the data and send it to the cluster head. Similarly, the healthcare personnel will send data to the cluster head. The cluster head will collect all the data and store it in a transitory memory, and after a certain time, it segregates all the data, and a cumulative result block will be stored. Each block contains multiple cumulative data. After a certain time, it will request the server for block transmission, and the server verifies the request, and if it is an authorized request, the server sends an acknowledgment. After receiving the acknowledgment, the cluster head will send the blocks to the server. These are stored in the global blockchain. Those transitory memory blocks are stored in the local blockchain.

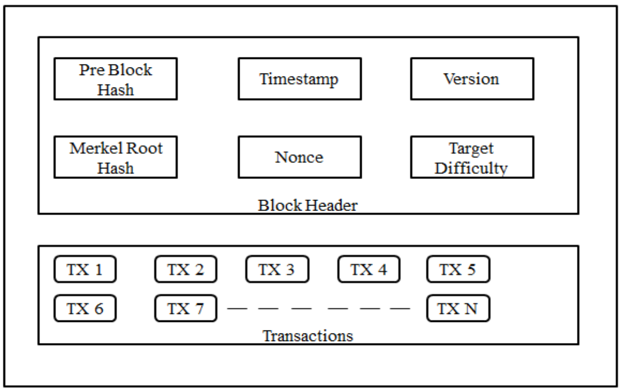

Fig 5. Individual Block Structure in a Global Blockchain

Figure 5 illustrates the structure of each block stored in the global blockchain. These blocks consist of two sections: the block header and transactions. Under the block header, all the details about the blocks, such as the previous block hash, time, version, etc., are included. The transaction section comprises of all the details about the block transactions. These are stored under the global block for further reference.

These blocks are pre-processed by the fog layer by established distributed networks and repository networks. Pre-processing helps segregate the data and store the necessary data, improving latency and efficiency. The pre-processing also includes a filtration process. Since patient biomedical signals are collected, they are often interrupted by signals from the external environment and internal sensor alignment. Biomedical signals are similar to each other and difficult to differentiate if affected by noise. A lightweight filtration approach is adopted to perform data filtration.

Followed by data filtration, a deep learning technique is adopted to analyze the data. It continuously monitors the readings and compares them with the existing ones. If the reading goes down or exceeds the threshold value, it alerts the healthcare personnel. This is the most important part because it is the part where the abnormality in the patient is predicted. It helps to provide the correct treatment at the correct time. It is used to assist patients who take treatment remotely. The medical sensor nodes are made energy efficient because they continuously collect the patient's reading and transfer huge amounts of data to the healthcare personnel. If the energy goes down, accurate data and accurate time cannot be obtained. This can lead to serious conditions and also be life-threatening for the patients at times.

3.4 Intrusion Detection System

The intrusion detection system is mainly used to secure our data from cyber-attacks. In the proposed system, precise data are collected in huge amounts and transferred in bulk. The blocks could be easily altered by any malicious user or anonymous user. So, these data are preserved for establishing a secured network [14]. Healthcare systems work both in online and offline modes, so they can use both hardware and software to secure the system [15].

Here, machine learning approaches are incorporated for detecting cyber-attacks. Initially, the intruders are analyzed using training parameters. Then, they are compared with the predefined dataset to detect altered blocks. A novel approach is proposed by integrating both machine learning and metaheuristic algorithms.

In the proposed work, two optimization algorithms are combined, such as linear optimization and salp swarm optimization. The obtained algorithm is termed the Lion Salp swarm optimization algorithm. By utilizing authentication and optimizing existing resources, cyber-attacks can be prevented. The procedure is proposed by initiating with salp swarm optimization for authenticating and then proposing linear optimization for confirming.

The authentication process is used to reduce the login count. This allows only the authorized users and offends the anonymous user [16]. The linear optimization algorithm allows the user to get access to only particular resources that are readily available. This is achieved by following three steps namely

3.4.1 Observing Traffic Configuration

By Observing Traffic Configuration, abnormal data flow is predicted. Initially, the system with sample configuration is trained and has set some threshold values. The LSSOA algorithm simultaneously compares the obtained value with the trained data set. If it exceeds the threshold value, it immediately activates the alarm signal. Proper monitoring helps to predict cyber-attacks at the correct time. This is an important factor because it is easy to protect the system at the gateway, and it can avoid data recovery constraints [17].

3.4.2 Rate Constraint Implementation

A malicious user can send a spam request to the IP of the cloud layer, and if unknowingly the request is accepted, it may lead to severe cyber-attack or loss of data [18]. To avoid this situation, two restriction methodologies are followed. One is by restricting the number of requests, and the other one is by restricting the number of IP addresses [19]. By doing so, unnecessary transducers are avoided. In certain cases, the intruder may guess the accessing key or make the system busy by sending unwanted requests and may raise request flooding issues. By using the restriction methodologies, the systems can limit requests and access.

3.4.3 Blacklist Implementation

Blacklisting is another way of protecting the system from hackers. In some cases, specific IP addresses are known that belong to malicious users, or specific regions are known that belong to corresponding malicious users. So by blocking or blacklisting these regions, the system is protected from malicious user. These are the steps that are used in the proposed work to prevent the data from malicious users.

$$NP = OP + (rand() * ((LP + GLP)/2 - OP)) * HW \quad (1)$$

The above-mentioned equation (1) is used to combine the linear optimization algorithm and the slap swarm algorithm. In the above equation (1), NP denotes the new position that is the updated future potion of the algorithm. OP denotes the old position, which is the current position of each node in the algorithm. LP denotes the leader position, which is the position of the header node. GLP denotes the global leader position, and HW denotes the hybrid weight of the proposed network. This has control over the position of the node and their sizes [20].

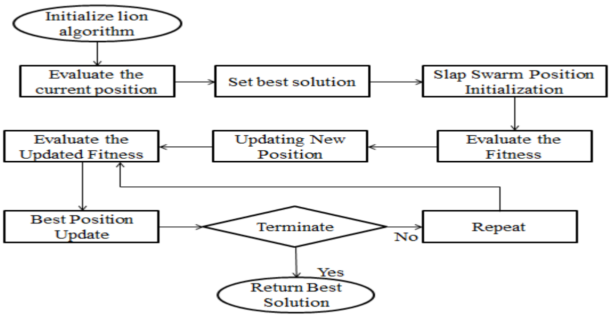

Figure 6 Flow Diagram of Line Slap Swarm Algorithm

Initially, the population is initialized using the Lion algorithm. Then, each single bit solution is evaluated, and its fitness is predicted. From the obtained values, the best one is set as the initial value for the Slap Swarm algorithm. By implementing a random distribution, every position is allocated. Again, fitness parameters are evaluated for obtained solutions. Then, corresponding salp positions and their values are updated. This process repeats until the best solutions are found.

The lion salp swarm optimization algorithm initializes a population using the lion algorithm and evaluates their fitness. Positions are updated using hybrid equations that combine local and global leader positions with a hybrid weight. Salp positions are further refined through a process influenced by both new and leader positions. This iterative process continues until the optimal solution is found or a stopping criterion is met, effectively enhancing the detection of cyber-attacks by optimizing the resource allocation and authentication steps.

Algorithm: Lion Salp Swarm Optimization Algorithm

```
NP = new position (updated future position)
OP = old position (current position of each node)
LP = leader position (position of the header node)
GLP = global leader position
HW = hybrid weight (controls position of the node and their sizes)
FW = fitness weight
α, β = coefficients for global and local positions
SP = salp position
SP_old = previous salp position
c1, c2 = learning factors
Input: Initial population P, maximum number of iterations MaxIter
Output: Optimal solution NP
Initialize population P using lion algorithm
Evaluate fitness of each individual in P
Set the best solution as the initial value for the salp swarm algorithm
for iter = 1 to MaxIter do
for each individual in P do
NP = OP + (rand() * ((LP + GLP)/2 - OP)) * HW
FW = α * (GLP - OP) + β * (LP - OP)
Evaluate fitness of each updated individual
end for
Update salp positions and their values
SP = $SP_{old}$ + c1 * rand() * (NP - $SP_{old}$) + c2 * rand() * (LP - $SP_{old}$)
Evaluate fitness parameters for updated solutions
Update lion position based on the previous salp update
if stopping criterion is met then
break
Return NP as the optimal solution
```

4. Experimental Analysis

To evaluate the performance of the system hyper-ledger platform is used. It is an open-source platform to implement blockchain-based applications. This sets a benchmark value for the proposed work. The hyper-ledger platform makes an easy configuration mechanism and aids API users [21]. For back-end processing, a restful API system is used. All the contact information is stored in the .bna extension file. This is a business network archive file. Hyper-ledger composer is used for designing and implementing the blockchain module [22]. These modules consist of contributors, possessions, and operations in a particular network. The contributors are the users of the system, possession is the services that are provided by the network, and operation is the communication that happens within the network. If a query is raised, it is validated, and a token is provided to the user to get access to the data.

Various experiments are carried out to evaluate the performance of the system. Execution time is one of the most important parameters in a healthcare monitoring system. To evaluate this execution time postman tool is utilized. This execution time depends on the number of devices accessing the network. The execution time varies in three different processes, namely registration, retrieval, and block agreement time. Three sets of devices are considered, such as 200, 400, and 600 devices in each process, and the execution time is segregated as least, middling, and extreme value.

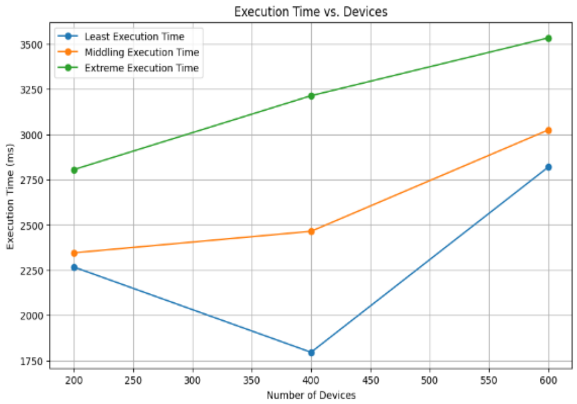

Figure 7 Registration execution time of Healthcare Devices

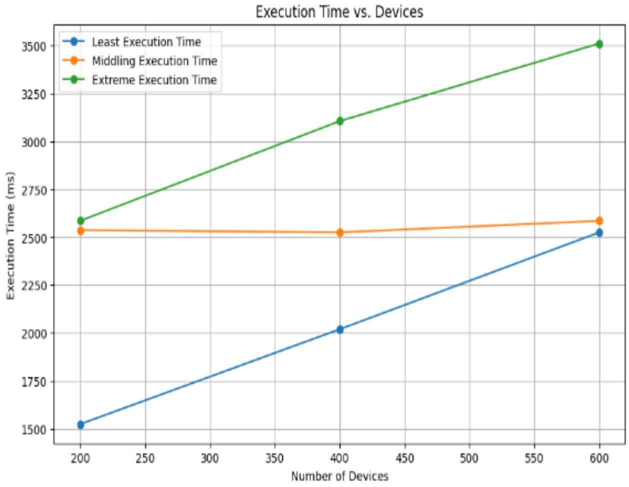

Figure 8 Retrieval execution time of Healthcare Devices

Figure 7 represents the execution time of healthcare registration with a varied number of devices, such as 200, 400, and 600. From the graphical representation, it is evident that the increase in the number of devices will increase the execution time. Proper scheduling is maintained to avoid collision. Similarly, from figures 8 and 9, it is visualized that when the number of queries increases, it also increases the execution time. The number of devices and execution time are proportional to each other. From figure 9 it is shown that in an average of 10ms, it is possible to execute from 200 devices to 600 devices.

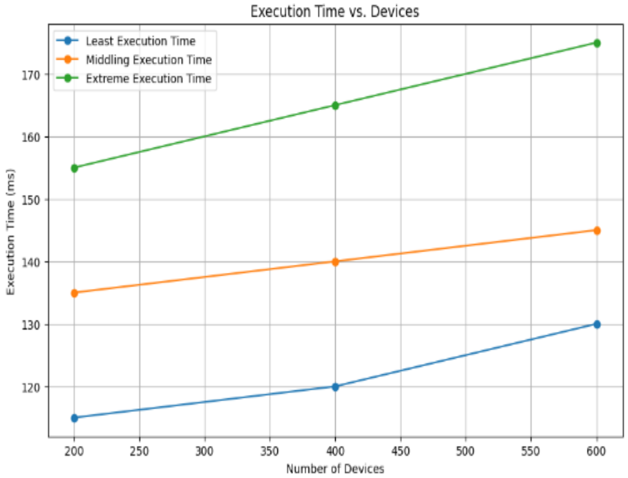

Figure 9 Block consensus execution time of Healthcare Devices

ifogsim simulating tool is used to perform simulation of the proposed network. It is a combination of fog and cloud computing environment. In the IoT layer, 24 ECG machines are connected along with corresponding ECG sensors. It is connected to an emergency alert system. The IoT layer is further connected to the Fog layer, and it has 4 local servers in it. The IoT-layered devices can communicate with any of the four fog-enabled local servers. These local servers are connected to a regional server set at the cloud layer. It provides seamless data transmission among the lower level data transmission.

Table 1 Simulator Parameters

Name	Speed (MIPS)	Downlink BW (MB)	Uplink BW (MB)	Memory (GB)	Busy power (MWh)	Idle power (MWh)
EM	1100	12	7	8	1.2	0.3
LS	7050	10	5	12	1.4	0.5
RS	15100	8	4	16	1.7	0.8
cloud	40200	5	6	32	3.3	1.5

Table 1 represents the parameters of our simulation module. From the simulation process, a simulation frequency of 450 seconds is achieved, and it also can sense 6 signals per second

.

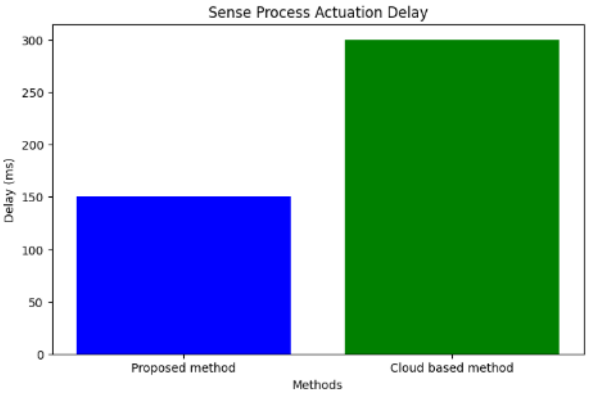

Fig 10 Reduction of sense process actuation delay

Figure 10 shows that the proposed method has reduced the sensing process actuation delay to 150ms. Figure 11 shows that the proposed work has reduced energy consumption as well. It is recorded that it consumes only 0.17MWh of energy for its execution. Figure 12 shows that the proposed method reduced the retrieval time with respect to transaction size. For 400KB of transaction size, it is recorded as 7ms, and for 2000KB of transaction size, it is recorded as 17ms. This is evident that the proposed work outperforms the existing cloud-based method.

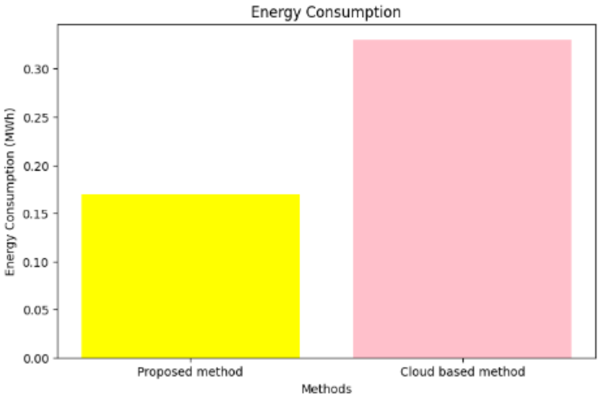

Fig 11 Reduction of energy consumption

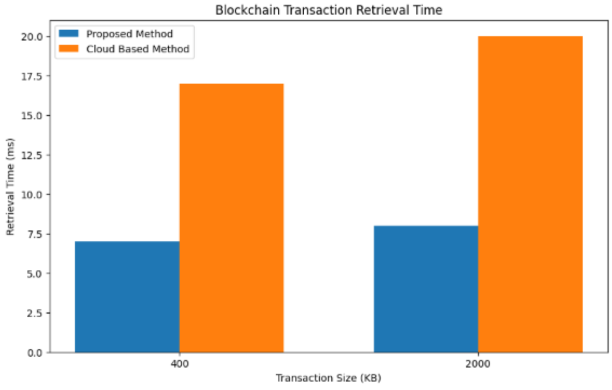

Fig 12 Reduction of blockchain transaction retrieval time

Further, the performance of the system with respect to the intrusion detection system is evaluated by four analysing metrics, namely precision, recall, accuracy, and FI score.

4.1 Precision

This performance metric determines the accurate number of cyber-attacks that have taken place during the course of execution.

$$P = \frac{PV}{PV+PI} \times 100$$

(2)

Where P denotes the Precision value, PV denotes the positive value, and PI denotes the positive invalid value. PV is nothing but the accurately detected number of attacks, and PI is the wrongly detected number of attack values.

4.2 Recall

This performance metric is used to determine the system's capability to remind the occurrence of the attack.

$$R = \frac{NV}{NV+NI} \times 100 \qquad (3)$$

Where R denotes the Recall value, NV denotes the negative value, and NI denotes the invalid negative value. NV is nothing but the number of events without attacks, and NI is a wrongly predicted value in the cases of an attack occurring.

4.3 Accuracy

This performance metric is used to predict the accuracy of the system in determining the accurate value of intrusion detection.

$$A = \frac{PV+NV}{PV+PI+NV+NI} \times 100 \qquad (4)$$

Where A denotes the accuracy and other terminologies are referred to in equations (2) and (3).

4.4 FI Score

The FI score is determined by

$$FI = 2 \times \frac{P*R}{P+R} \qquad (5)$$

We consider two ratios based on the positive values and the negative values to determine the system performance.

$$PVR = \frac{PV}{PV+NI} \times 100 \qquad (6)$$

$$NIR = \frac{PI}{PI+NV} \times 100 \qquad (7)$$

Where PVR is the positive valid rate and NIR denotes a negative invalid rate.

Equation (1) is used in the proposed algorithm to improve performance by utilizing two effective optimization algorithms, and the rest of the equations are used for analytical purposes.

Table 2 Performance evaluation of five different optimization techniques

Method	Accuracy	PIR	NIR	Precision	Recall	FI score
Lion	86.1%	3.5%	12.2%	88.4%	88.1%	88.1%
Salp swarm	82.2%	6.5%	18.6%	84.4%	82.3%	83.4%
Spider monkey	83.3%	5.5%	16.4%	86.6%	84.1%	85.2%
Wale	89.1%	2.5%	11.1%	90.4%	90.1%	90.2%
LSSOA	99.7%	7.5%	18.6%	99.2%	98.7%	97.6%

Table 2 compares the performance of four different optimization techniques with the proposed algorithm. It visualizes that the proposed algorithm performs better than any other algorithm.

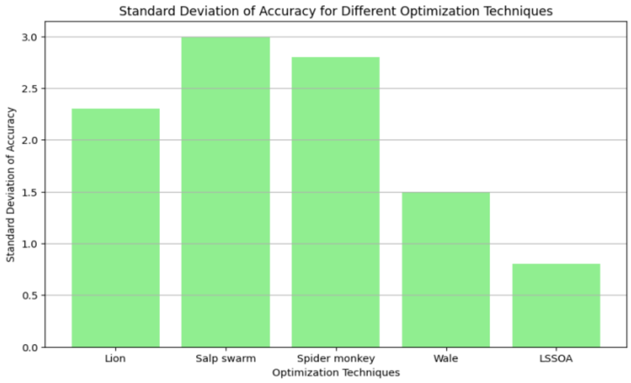

Figure 13 Standard Deviation of Accuracy for Different Optimization Techniques

Figure 13 represents the standard deviation of accuracy for different optimization techniques. The LSSOA method has the lowest standard deviation in accuracy at 0.8, indicating that it has the most consistent performance among the five methods. This suggests that the accuracy of LSSOA is more stable and less prone to fluctuations compared to the others. In contrast, the salp swarm technique has the highest standard deviation at 3.0, showing greater variability in its accuracy measurements, which implies that its performance is less predictable. The lion method has a standard deviation of 2.3, while the spider monkey method shows a slightly higher value at 2.8. Both of these methods exhibit moderate variability in their accuracy. The whale optimization technique, with a standard deviation of 1.5, performs better than lion and spider monkey in terms of consistency but not as well as LSSOA.

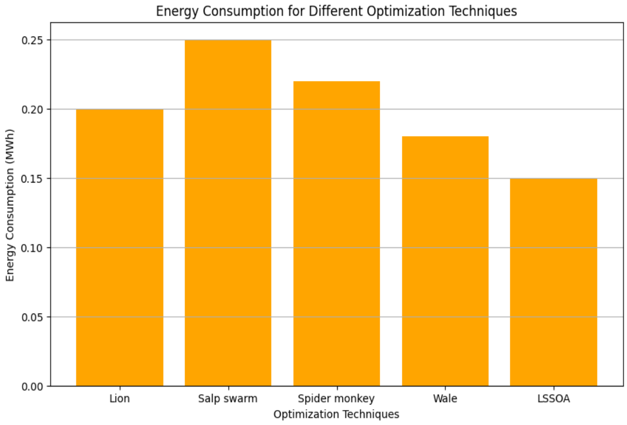

Fig 14 Energy Consumption for Different Optimization Techniques

Figure 14 illustrates energy consumption for different optimization techniques. LSSOA method has the lowest energy consumption, recorded at 0.15 MWh, making it the most energy-efficient among the five techniques. This low energy requirement is particularly advantageous for IoT applications, where power efficiency is crucial. On the other end of the spectrum, the salp swarm technique has the highest energy consumption at 0.25 mwh, indicating it requires more power to operate compared to the others. The lion and spider monkey methods have moderate energy consumption levels, at 0.20 mwh and 0.22 mwh, respectively. These values suggest that while they are not the most efficient, they are still more energy-efficient than salp swarm. The wale technique also shows good energy efficiency with a consumption of 0.18 mwh, making it the second most efficient after LSSOA.

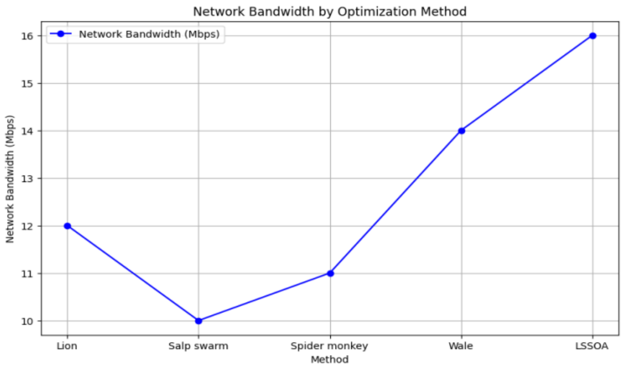

Fig 15 Network Bandwidth by Optimization Method

Figure 15 shows network bandwidth by optimization method. LSSOA has the highest network bandwidth demand at 16 Mbps, indicating it requires the most data transfer capacity among the techniques. The wale method follows with a network bandwidth of 14 Mbps, slightly lower than LSSOA but still relatively high. The lion method, on the other hand, utilizes 12 mbps, positioning it in the middle range. The spider monkey method has a bandwidth requirement of 11 Mbps, while the salp swarm method has the lowest bandwidth demand at 10 Mbps.

This lower demand can be beneficial in scenarios where network resources are limited.

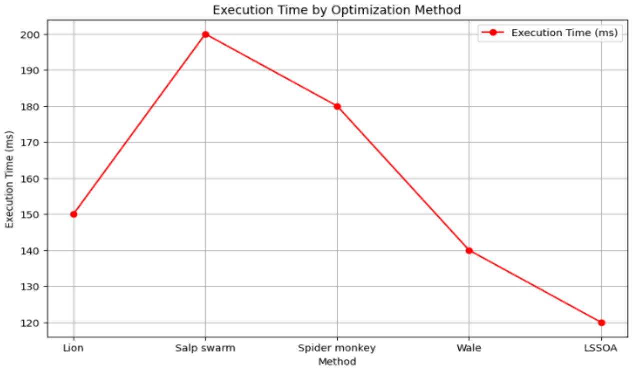

Fig 16 Execution Time by Optimization Method

Figure 16 depicts execution time by optimization method. The LSSOA method has the shortest execution time at 120 ms, making it the fastest among the methods analyzed. The wale method follows with an execution time of 140 ms, which is slightly slower than LSSOA but still efficient. The lion method has an execution time of 150 ms, placing it in the middle range. The spider monkey method requires 180 ms to execute, showing a higher execution time compared to Lion and Wale. The salp swarm method has the longest execution time at 200 ms, indicating it is the slowest among the five techniques.

5. Conclusion

In the proposed work, fog-assisted anomaly detection in healthcare IoT has been implemented. Lightweight blockchain and collaborative intrusion detection systems have been incorporated to achieve an effective healthcare monitoring system. Healthcare authorities can easily access the blocks stored in global blocks. The Metaheuristic algorithm utilizes optimization techniques to preserve data. The proposed method has reduced latency by precisely optimizing execution time and improved system efficiency. Various performance analysis metrics such as Accuracy, Precision, Recall, F1 score, NIR, and PIR are used to compare the effectiveness of the system. As a result, a 99.7% accuracy and 99.2% precision have been achieved. In future work, the system can be improved by adopting the federated learning approach. This approach performs filtration and analysis simultaneously, reducing latency and providing accurate values. Using a clustering mechanism, channels can be equally distributed among all block nodes in the network. Proper scheduling helps reduce congestion.

Declaration Statement

Ethical Statement

I will conduct myself with integrity, fidelity, and honesty. I will openly take responsibility for my actions, and only make agreements, which I intend to keep. I will not intentionally engage in or participate in any form of malicious harm to another person or animal.

Informed Consent for data Used

All subjects gave their informed consent for inclusion before they participated in the study. The study was conducted in accordance with the Declaration of Helsinki.

I consent to participate in the research project and the following has been explained to me: the research may not be of direct benefit to me. my participation is completely voluntary. my right to withdraw from the study at any time without any implications to me.

Data Availability

- Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.
- The datasets used and/or analysed during the current study are available from the corresponding author on reasonable request.
- All data generated or analysed during this study are included in this published article

Conflict of Interest

The authors declare that they have no conflict of interest.

Competing Interests

The authors have no competing interests to declare that are relevant to the content of this article.

Funding Details

No funding was received to assist with the preparation of this manuscript.

Acknowledgments

I am grateful to all of those with whom I have had the pleasure to work during this and other related Research Work. Each of the members of my Dissertation Committee has provided me extensive personal and professional guidance and taught me a great deal about both scientific research and life in general.

Reference

[1] W. A. N. A. Al-Nbhany, A. T. Zahary and A. A. Al-Shargabi, "Blockchain-IoT Healthcare Applications and Trends: A Review," in *IEEE Access*, vol. 12, pp. 4178-4212, 2024, doi: 10.1109/ACCESS.2023.3349187.

[2] A. Subrahmannian and S. K. Behera, "Chipless RFID Sensors for IoT-Based Healthcare Applications: A Review of State of the Art," in *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1-20, 2022, Art no. 8003920, doi: 10.1109/TIM.2022.3180422.

[3] N. Taimoor and S. Rehman, "Reliable and Resilient AI and IoT-Based Personalised Healthcare Services: A Survey," in *IEEE Access*, vol. 10, pp. 535-563, 2022, doi: 10.1109/ACCESS.2021.3137364.

[4] S. Wang, X. Zhou, K. Wen, B. Weng and P. Zeng, "Security Analysis of a User Authentication Scheme for IoT-Based Healthcare," in *IEEE Internet of Things Journal*, vol. 10, no. 7, pp. 6527-6530, 1 April1, 2023, doi: 10.1109/JIOT.2022.3228921.

[5] U. Demirbaga and G. S. Aujla, "MapChain: A Blockchain-Based Verifiable Healthcare Service Management in IoT-Based Big Data Ecosystem," in *IEEE Transactions on Network and Service Management*, vol. 19, no. 4, pp. 3896-3907, Dec. 2022, doi: 10.1109/TNSM.2022.3204851.

[6] S. Zaman, M. R. A. Khandaker, R. T. Khan, F. Tariq and K. -K. Wong, "Thinking Out of the Blocks: Holochain for Distributed Security in IoT Healthcare," in *IEEE Access*, vol. 10, pp. 37064-37081, 2022, doi: 10.1109/ACCESS.2022.3163580.

[7] M. Naveed, S. M. Usman, M. I. Satti, S. Aleshaiker and A. Anwar, "Intrusion Detection in Smart IoT Devices for People with Disabilities," *2022 IEEE International Smart Cities Conference (ISC2)*, Pafos, Cyprus, 2022, pp. 1-5, doi: 10.1109/ISC255366.2022.9921991.

[8] O. A. Mahdi, A. Alazab, S. Bevinakoppa, N. Ali and A. Khraisat, "Enhancing IoT Intrusion Detection System Performance with the Diversity Measure as a Novel Drift Detection Method," *2023 9th International Conference on Information Technology Trends (ITT)*, Dubai, United Arab Emirates, 2023, pp. 50-54, doi: 10.1109/ITT59889.2023.10184268.

[9] G. Zachos, G. Mantas, I. Essop, K. Porfyrakis, J. C. Ribeiro and J. Rodriguez, "Prototyping an Anomaly-Based Intrusion Detection System for Internet of Medical Things Networks," *2022 IEEE 27th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, Paris, France, 2022, pp. 179-183, doi: 10.1109/CAMAD55695.2022.9966912.

[10] T. Saba, "Intrusion Detection in Smart City Hospitals using Ensemble Classifiers," *2020 13th International Conference on Developments in eSystems Engineering (DeSE)*, Liverpool, United Kingdom, 2020, pp. 418-422, doi: 10.1109/DeSE51703.2020.9450247.

[11] H. Alamro *et al.*, "Modeling of Blockchain Assisted Intrusion Detection on IoT Healthcare System Using Ant Lion Optimizer With Hybrid Deep Learning," in *IEEE Access*, vol. 11, pp. 82199-82207, 2023, doi: 10.1109/ACCESS.2023.3299589.

[12] S. Racherla, P. Sripathi, N. Faruqui, M. Alamgir Kabir, M. Whaiduzzaman and S. Aziz Shah, "Deep-IDS: A Real-Time Intrusion Detector for IoT Nodes Using Deep Learning," in *IEEE Access*, vol. 12, pp. 63584-63597, 2024, doi: 10.1109/ACCESS.2024.3396461.

[13] M. Fouda, R. Ksantini and W. Elmedany, "A Novel Intrusion Detection System for Internet of Healthcare Things Based on Deep Subclasses Dispersion Information," in *IEEE Internet of Things Journal*, vol. 10, no. 10, pp. 8395-8407, 15 May15, 2023, doi: 10.1109/JIOT.2022.3230694.

[14] S. Arisdakessian, O. A. Wahab, A. Mourad, H. Otrok and M. Guizani, "A Survey on IoT Intrusion Detection: Federated Learning, Game Theory, Social Psychology, and Explainable AI as Future Directions," in *IEEE Internet of Things Journal*, vol. 10, no. 5, pp. 4059-4092, 1 March1, 2023, doi: 10.1109/JIOT.2022.3203249.

[15] D. Breitenbacher, I. Homoliak, Y. L. Aung, Y. Elovici and N. O. Tippenhauer, "HADES-IoT: A Practical and Effective Host-Based Anomaly Detection System for IoT Devices (Extended Version)," in *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9640-9658, 15 June15, 2022, doi: 10.1109/JIOT.2021.3135789.

[16] M. Wazid, J. Singh, A. K. Das and J. J. P. C. Rodrigues, "An Ensemble-Based Machine Learning-Envisioned Intrusion Detection in Industry 5.0-Driven Healthcare Applications," in *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 1903-1912, Feb. 2024, doi: 10.1109/TCE.2023.3318850

[17] A. Ghourabi, "A Security Model Based on LightGBM and Transformer to Protect Healthcare Systems From Cyberattacks," in *IEEE Access*, vol. 10, pp. 48890-48903, 2022, doi: 10.1109/ACCESS.2022.3172432.

[18] M. A. Khatun, S. F. Memon, C. Eising and L. L. Dhirani, "Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation," in *IEEE Access*, vol. 11, pp. 145869-145896, 2023, doi: 10.1109/ACCESS.2023.3346320.

[19] Alsalman, "A Comparative Study of Anomaly Detection Techniques for IoT Security Using Adaptive Machine Learning for IoT Threats," in *IEEE Access*, vol. 12, pp. 14719-14730, 2024, doi: 10.1109/ACCESS.2024.3359033.

[20] M. M. Alani and A. I. Awad, "An Intelligent Two-Layer Intrusion Detection System for the Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 19, no. 1, pp. 683-692, Jan. 2023, doi: 10.1109/TII.2022.3192035.

[21] Perumal, G., Subburayalu, G., Abbas, Q., Naqi, S. M., & Qureshi, I. (2023). VBQ-Net: A Novel Vectorization-Based Boost Quantized Network Model for Maximizing the Security Level of IoT System to Prevent Intrusions. Systems, 11(8), 436.

[22] Hemanand, D., Reddy, G. V., Babu, S. S., Balmuri, K. R., Chitra, T., & Gopalakrishnan, S. (2022). An intelligent intrusion detection and classification

system using CSGO-LSVM model for wireless sensor networks (WSNs). International Journal of Intelligent Systems and Applications in Engineering, 10(3), 285-293.