Secure IoMT Pattern Recognition and Exploitation for Multimedia Information Processing using Private Blockchain and Fuzzy Logic

Taher M.Ghazal[1,2*,] Mohammad Kamrul Hasan[1], Siti Norul Huda Abdallah[1], Khairul Azmi Abubakkar[1]

[1]Center for cyber Security, Faculty of Information Science and Technology, UniversitiKebangsaan Malaysia (UKM), 43600 Bangi, Selangor, Malaysia

[2]School of Information Technology, Skyline University college, University City Sharjah, 1797, Sharjah, UAE

*Taher M.Ghazal: Taher.ghazal@skylineuniversity.ac.ae

Mohammad Kamrul Hasan: mkhasan@ukm.edu.my

Siti Norul Huda Abdallah :Snhsabdullah@ukm.edu.my

Khairul Azmi Abubakkar: khairul.azmi@ukm.edu.my

The Internet of Medical Things (IoMT) is a definite IoT connecting atmosphere that contracts with communication via intelligent medical equipment. Activity detection, motion tracking, information extraction, consumer retrieval, etc., have all been solved due to advances in the autonomous study of human behavior from multimedia information processing. Though the IoT connecting atmosphere enables and provisions our daily actions, it too has certain disadvantages. IoTgrieves from numerous safety and confidentiality challenges, such as reiteration, impersonation, man-in-the-middle, remote hijacking, privileged-insider attack, denial of service (DoS) attacks, password guessing, and malware bouts. Hence, in this paper, Private Blockchain and Fuzzy Logic based Attack Detection system (PBFL-ADS) has been proposed for secure IoMT disease prediction using Multimedia Information Processing techniques. The proposed method utilizes Bayesian inference-based trust administration to perceived malevolent nodes in Health Smartphone Structures (HSS) for PBFL-ADS. This paper focuses on the specific form of IoMT called HSS because smartphones have been widely used in the healthcare profession. Then, blockchains have been utilized to improve Bayesian trust management's efficacy in detecting hostile nodes in HSSs. The effectiveness of the suggested technique has been assessed, and test results show that blockchain technology helps identify fraudulent nodes with an acceptable workload. The proposed PBFL-ADS method increases the HS2 scenario 1.1, processor utilization at nodes 33.5%, pattern recognition ratio 92.1%.and server utilization 40.1%.

Keywords: IoMT, Pattern Recognition, Disease Prediction, Private Blockchain, Multimedia Information Processing, Smartphone structures, Fuzzy Logic, Security

1. INTRODUCTION TO BLOCKCHAIN AND IOMT

The Internet of Things (IoT) is a system that connects elements such as intelligent equipment and intelligent household items. They possess a strong Internet address (IP), which allows them to talk to the external systems of the network (i.e., the user of an intelligent home) [1]. The users are interconnected and exchanged using a sensor and application programming interface (API).In computerized sensing and multimedia information processing, several problems have been addressed, including studying human behavior. [2]–[3]. An electronic gateway is an application-specific micro-computing device except for typical embedded functional devices.

Another IoT connecting atmosphere is the Internet of Medical Things (IoMT) [4]. It includes medical products such as intelligent healthcare and monitors (i.e., an intelligent pacemaker, an intelligent blood glucose meter, etc.) and programs connecting to IoT healthcare networks and the internet. Medical equipment is provided with some connected devices (i.e., Bluetooth and Wi-Fi) for the machine, which provides the basis for IoMT connectivity [5]-[6]. IoMT senses the medical data of the customer and transmits the information to some computer (monitors) through intelligent medical devices (for example, cloud server). Like Amazon Web Services (AWS), specific cloud systems may be required to record medical information and analyze it to make decisions and prescriptions for health[7]. A medical sentencing hearing performance is continually monitored as part of healthcare monitoring. The procedure, excellent medical practice, applicable regulations,

2375-4699/2022/1-ART1 $15.00
http://dx.doi.org/10.1145/3523283

and operational procedures must all be adhered to. Users' anonymity is not sacrificed to protect health; this process allows information security, including both downloading and recovery and safe processing and networking.

Vulnerabilities in IoT nodes will rise slowly than surely as IoT applications develop and implement quickly. It enables the prospect of initiating several kinds of assaults over the internet in the IoT ecosystem [8]. Automated pattern detection is a data analysis technique that uses classification technique algorithms to identify patterns in data sets automatically. This data set can include anything from text and photos to sounds or any other definable quality. Pattern recognition systems can swiftly and reliably identify known patterns. In IoMT, the connectivity and regulation of intelligent electronic instruments are a particularly severe problem [9]. Picture lookup results variation is a prominent topic in multimedia exploration, and this can be handled by multimedia information processing. For example, if the attacker successfully controls innovative medical equipment remotely, they may endanger the patient's life (i.e., an intelligent pacemaker may cause a patient to die). There are continuously developing varieties of IoT infections. These developing malware can influence IoMT's connectivity and can be exploited to manipulate intelligent medical devices[10]-[11].

For malware detection and analysis, the present techniques are not sufficient. As seen later, the Mirai and Brickerbot assaults were being carried out [12]. There are important issues in multimedia systems relating to image and video processing methodologies and implementations addressed in multimedia information processing applications. Compression and indexing algorithms for images or videos are part of this set of tools. It is due to the lack of robust security supervision and security measures. These assaults lead to disseminated Denial-of-Service (DDoS) assaults. It is thus essential to have a solid security framework to identify and resist threats of this sort in IoT. (especially in IoMT) [13]–[14]. Many studies have shown that the growing importance of the mobile health industry is related to the introduction of cellphones, and smartphones are an excellent data transfer station for the customized gathering of medical data. In the monitoring and exchanging electrical cardiogram (ECG) data with an IoT environment, the smartphone can play a significant role in helping to diagnose certain cardiac diseases[15]-[16].

Public health insurance providers could benefit from disease prediction and determine whether a patient is susceptible to health problems. Predictive models can swiftly assess and give findings using both data and information. Healthcare professionals can make smart choices about patients' diagnosis and patient management with computer vision, which ultimately results in higher efficiency of health care operations.

Consequently, these technologies are developing a specific network called the HSS. It can be considered a particular form of IoMT, where different Internet-enabled healthcare devices link and simplify healthcare providers' activities. Medical institutions commonly use a centralized system to hold maximum operations, like faith administration [17]. It can make many tasks more accessible; nonetheless, the design itself might be susceptible to excessive traffic or events in a single point of failure. Because blockchain technology has been recently adopted and popularised, it has been discovered to give a platform for communicating with unfamiliar parties without relying upon a third party for trust[18].

This article focuses on intruders and tries to develop a trust management system based on Blockchain to help protect HSSs against intruders' attacks. This paper addressed the accomplishments as follows.

1) The backdrop of HSS and then developing a trust management system based on Bayesian inference has been suggested in this article to improve detecting harmful intruders.
2) The proposed technique uses multimedia information processing technology to find the patient's data.
3) A fuzzy logic-based neural network model for the proposed PBFL-ADS system in health and risk prediction has to been proposed.
4) In the assessment, tests were carried out in conjunction with two healthcare organizations to evaluate the effectiveness of trusted governance in Blockchain. Furthermore, the technique presented has been tested in the medical sector, then it can too be used for other application areas.

The remaining sections of the document are organized as follows. Section 2 explores related works on the security issues in IoMT and Blockchain. Private Blockchain and Fuzzy Logic based Attack Detection system has been proposed in section 3 for secure IoMT using HSS. Section 4 consists of the analysis and findings obtained from the proposed model. Finally, the conclusion and possible studies have been outlined in Section 5.

2. RELATED RESEARCH ON SECURE IOMT USING BLOCKCHAIN

Information and communications technology is being steadily used in the healthcare business, making it more straightforward for individuals and specialists to interact. In many healthcare companies, smartphones are essential gadgets used to cut costs, regulate data access and monitor outcomes. It likewise enables a wide range of patient apps for data recording and prompt notification to health experts of the status[19].

The IoMT brings good results to the medical industry and allows a more humanistic approach to patient care and well-being. It has several cyber risks and weaknesses, though. The authors in [20] identified the high prevalence of cyber assaults in IoMT as possible: (1) The exchange of sensitive patient data is mainly for medical subjects. (2) inconsistency and complication resulting from a large variety of sensors and diverse networks being connected. (3) An expanding sector significantly increases by adopting IoMT solutions without considering healthcare manufacturers' safety problems. As a result, authenticity, non - repudiation, and availability concerns occur. (4) As most IoT elements wirelessly send and receive data, it opens IoMT to the risk of security violations of the wireless sensor network (WSN). (5) Another critical worry is the risk of applications, such as breaches of the authorization and authentication, and the general safety and validity of the request. (6) Some computations for security take significant amounts of processing power.

These are some of the significant reasons why IoMTs are exposed. Many of these linked devices are unsecured, and the potential implications on the patient data and patient treatment result from any inaccuracy in a patient's data report or analysis. Therefore, it is imperative to examine how medical equipment assaults may be identified and protected. Most vulnerabilities of IoTs too apply to IoMTs. However, particular vulnerabilities target IoMTs, because the medical information is significant. Cyber assaults include data breach, MiTM (Man in The Middle) attacks, spoofing and decryption of network traffic, DoS, and security and privacy risks, then are not limited. IoMT volunteer capabilities may be classified on a layer basis. An IBM analysis reveals that the most significant expenses connected with data breaches were incurred by health care institutions[21].

Moreover, in addition to the compromised outpatient medication data of 175,000 people [22], according to Help Net Security, hackers broke the health service and stole individual information from 1.45 million patients in Singapore. There are several information security problems in the health business continually. Those problems vary from malware that jeopardizes data consistency and patient privacy to DDoS assaults that impede the capacity of patient care centers [23]. The safety of confidential documents, such as health protection information passing through IoMT and continuous access privileges, is a growing issue for healthcare practitioners. Although other vital infrastructures experience similar attacks, there are particular obstacles to the nature of the objective of the health industry. It extends outside economic damage and infringement then directly affects people's lives. Any assault on the medical system, minor or massive, is a hazard for whatever cause. Given that IoMT is an essential element in medical treatment, safe and efficient management of IoMT has to be found [24].

Responsive medical systems may be transformed with the aid of IoT into proactive wellness systems. Some intelligent healthcare systems monitor and communicate health information to the closest node in such a system (i.e., cloud server). If a user (that is to say, a physician or a patient family) is accessing the system in real-time, they may be provided via IoT. IoT, therefore, provides access, computation, and analysis in real-time [25]-[26] of vital health information.

Kumar et al.[27] developed a confidence management technique to establish a dynamic confidence reputation for WSNs. They evaluated a collection of nodes with direct and indirect confidence and utilized a different algorithm to emphasize the trust values most recently received dynamically. Jiang et al. [28] have developed an environmentally friendly trustworthiness sensor relaying algorithm to deal with network dimensions using a similar approach with trust calculations that are direct and indirect. Gomathi et al. [29], who combined several criteria to assess the reputed HSS nodes, such as energy, information, connectivity, and recommendations, have created a routing protocol. Their way to detect attack frequency and evil occurrences rely, in particular, on the sliding time window.

Chen, G. et al. [30] presented the prototype-agnostic scene layout (PaSL) approach to constructing each picture's spatial configuration that does not follow any preexisting model. An important study direction in scene identification is utilizing the spatial organization in the photographs of a scene. Versatile structural arrangement to adapt to diverse image features is difficult due to the substantial intra-class structural variety. The results reveal that the improved approach may be used in invarious situations and competitively.

This development enables more devices to interact with one other in medical contexts, called IoMT. It seeks to make communication time more effective, reduce the number of patients being monitored, and notify strange occurrences. However, due to its dispersed nature, internal threats represent one of the main dangers to such an IoT system. The problem remains how they can enhance confidence management in IoMT. The general objective of this report is to examine the effectiveness of Blockchain and fluid-based trust management because of the popularity of blockchain technology.Multimedia information processing is used to find the pattern recognition of attacks and helps to monitor them.

3. PROPOSED PBFL-ADS FRAMEWORK FOR SECURE IOMT DISEASE PREDICTION

Blockchains' primary purpose is for payments without a link between companies and constructing a temperature resilient blockchain. A conventional blockchain comprises a collection of arranged entries sequentially by discrete-time markings (called blocks). One unit has an encrypted hatch, in which the first piece is termed the genesis, connected to the front block. Different implementations of Blockchain can lead to additional block content. A component contains a message and reference number and a specific hash class determined by all preceding blocks.Multimedia information processing systems employ filtering procedures to enhance a patient's medical record and other credentials. They can be used to change the image's luminance, clarity, density, and noise level. Typical image processing includes contouring, sharpening, blurring, embossing, and edge detection.

In principle, there are two main kinds of blockchains: permission-free or publicly known blockchains and permitted blockchains. The earlier enables any object to link the shackle as an author or bibliophile throughout the consensus process. Applications include Bitcoins, Zerocash, and Ethereum for such blockchains. However, the latter restricts the number of organizations to engage in the network. Even though blockchain technology can still be spread across many sites, a private blockchain authorized by a single company or centralized body is frequently managed. A blockchain consortium allows a group to reach consensus decisions that each member organization must registerbefore entering an agreement.

The newcomer can enter the embedded system and exchange intelligence with the consortium blockchain rather than start fresh. ' Using this platform, companies may come together to find answers and thus save money and effort on creation. The term "federalized blockchain networks" refers to blockchains that are part of a consortium. For financial aid reasons, a consortium agreement is a contract between two institutions of higher learning to recognize their enrollment at each site. One of the two universities is too authorized to handle federal financial assistance.

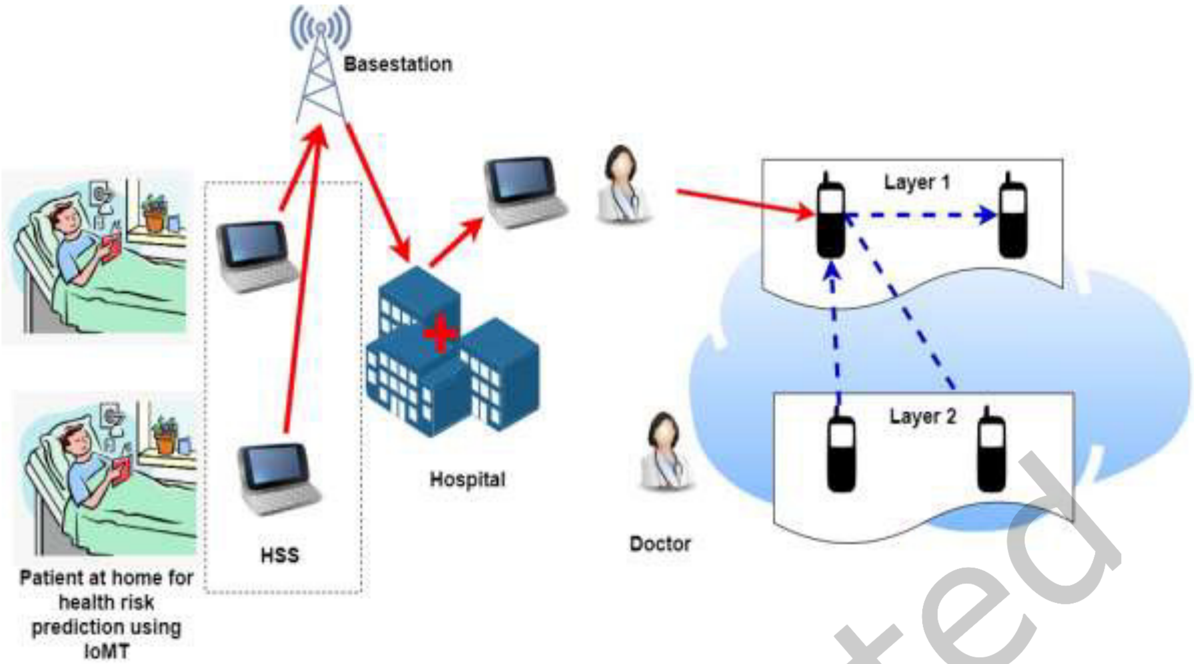


Fig. 1 Framework of HSS

The elevated HSS framework is depicted in Fig. 1. HSSs may be categorized into localized HSSs and extended HSSs based on the connection scope. The primarily former pertain to cellphones in a healthcare company, whereas the latter contains smartphones outside the business, that is, devices that patients use in their homes. Individuals' gadgets for broad HSSs can communicate over the internet with local HSSs. Each widget on the HSS can be considered a (network) hub, analogous to a network structure.

Layer 1 and layer 2 are end-users in healthcare, and appearing placed on personal computers can be accessed via portable devices in healthcare situations to assist in testing and therapy decisions. Mobile applications can indeed assist clinicians in determining which scans or tests they should order, lowering the variety of techniques performed without a need and the associated costs. Anyone with a pressing informational want seeks assistance from a searching expert or uses an information-gathering technology.

Predictive analytics is useful in various situations, including enhancing outcomes for patients. Patients' medical histories can be integrated with other healthcare data to detect early warning indications of significant medical occurrences and avoid their development. Lifelong illness prediction systems will allow people to receive early medical attention or manage and prevent unusual events in their lives. Patients will save time & expense as a result, which will help cut back on the number of people with chronic illnesses.

There are various primary techniques in the network to build a distributed consensus system to validate and update blocks.

1) Work evidence (WE) - If the contributor can demonstrate that a predetermined quantity of computing possessions (recognized as "work") is used, a network node can accept a block for such a scheme. An SHA-256 has already been deployed in the Bitcoin network.
2) Stake evidence - This approach reaches agreement by requiring users to expend a number of their tokens to validate and reward operations blocks. The more assets a user takes, the more excellent the opportunity.
3) Expired time evidence - This approach is much like the PoW method by substituting a random timing system for a demanding mining procedure. This fair lottery technique can enhance productivity.

3.1 Bayesian Interface for PBFL-ADS

Inference from the Bayesian theorem is a technique of explicitly applying previous information to the statistical probability calculation. It is particularly beneficial when there is insufficient information yet the likelihood of associated occurrences must be predicted. The theorem of the Bayes has been explored in computer networks, which asserts that a malicious packet has a 1/2 chance on the shared network. In a package or several containers, it means that harmful events may be detected in multiple ways. Equation (1) for log-normal distribution for a node can be computed as,

$$Prob(m(S) = l|q) = l^{M} \times (q/l) \times (q)^{S} \quad (1)$$

Consider a node that transmits data containing S packets. Among the S packets sent, m packages are considered regular packets. $m(S) = l$ is based on log-normal distribution. $m$common packets have been transmitted with the probability of occurrence q. The distribution of likelihood using Baye's theorem has been given by,

$$Prob(W_{S+1} = 1|W_S = l) = Prob(W_{S+1} = 1|m(S) = l)/Prob(W_S = l) \quad (2)$$

In Equation (2), the use of Baye's interface is to find$\Big(S + 1)th$packet is regular or being affected by the malicious node with probability given by $Prob(W_{S+1} = 1|m(S) = l)$.

The Bayes' theorem describes the likelihood of an event and the principle of maximum probability. One of the most important statistical rules is the law of calculated value. It deals with unconditional and residual probabilities associated with knowledge about the circumstances suitable for a given event. A random variable can be calculated using Bayes' theorem; for example, the moment of the day or that drive, the location one reserved, and what gatherings are taking place all affect the chances of finding a parking spot.

In mathematics, Bayesian is a method for estimating the probability of a given event. Probabilistic based on past outcomes is known as probabilistic reasoning. Using Bayes' theorem, it is possible to derive the likelihood function by adding a prior probability distribution function. In Bayesian probabilistic reasoning, the chance of an event occurring before obtaining fresh data is known as the posterior distribution.

For the Equation given (3), the residual conditional probability can be used that implies that one likelihood function is probable without any other random variables being influenced. Then two equations can be achieved:

$$Prob(m(S) = l) = \sum Prob(m(S) = l \times f(q)) \quad (3)$$

$$Prob(W_{S+1} = 1, m(S) = l) = \sum Prob(m(S) = l \times f(q) \times q) \quad (4)$$

As no previous information on q is available, anunvaryingpriordispersal of q of $f(q) = 1, q \in [0,1]$ is pretty supposed to determine q. From (1) to (4), the following objective Equation has been obtained:

$$Prob(W_{M+1} = 1, m(M) = l) = \frac{\sum Prob(m(M)=l \times f(q) \times q)}{\sum Prob(m(M)=l \times f(q))} = (l + 1)/(M + 1) \quad (5)$$

As with (5), the quantity of regular$l$ packets and total M packets may be assessed to determine the credibility of HSS nodes. Given a suitable confidence threshold, one can classify malicious or normal HSS nodes. Notably, the network may be observed longer than multiple negative messages to establish a robust trust calculation for a member. It is because certain security breaches may impair the precision of identification.

3.2 Private Blockchain-based Attack Detection system

It has been prudent to protect linked medical equipment from being hacked. SANS institute research found that cyber thieves have infiltrated up to 93.5 percent of different health organizations, including medical devices and infrastructure. Medical equipment needs to be integrated with security and privacy. For instance, if one piece of equipment in HSSs is attacked, intruders can use the compromised one to exploit other devices. Indicator assaults constitute a significant issue to IoMT and HSS since their nature is dispersed. As previously stated, integrity-based ADS is a powerful and crucial safety technique to prevent assaults by insiders.Medical picture preparation, virtual resources, virtual surveillance, network management systems, communications technology, emerging technologies like remote sensor and mesh systems, and advancements in learning, business, games, archaeology, and art are some of the latest multimedia research areas multimedia information processing is used.

These techniques are generally used to regulate the trust calculation process and make a conclusion. In reality, however, such a dynamic server can develop a solitary point of catastrophe as most healthcare IT workers are not security specialists, and updates and patches of the deployed software can be delayed. Consequently, the service provider is difficult to assure from a security perspective. More study has begun to merge ADS and blockchains with the prominence and use of distributed ledger technology.Blockchain technology allows unidentified (or even untrustworthy) people to communicate their information without the requirement for a trusted intermediary in a verifiable manner. Motivated by that finding, the intention is to develop a risk monitoring system for safeguarding healthcare companies from insider assaults based on a blockchain basis.

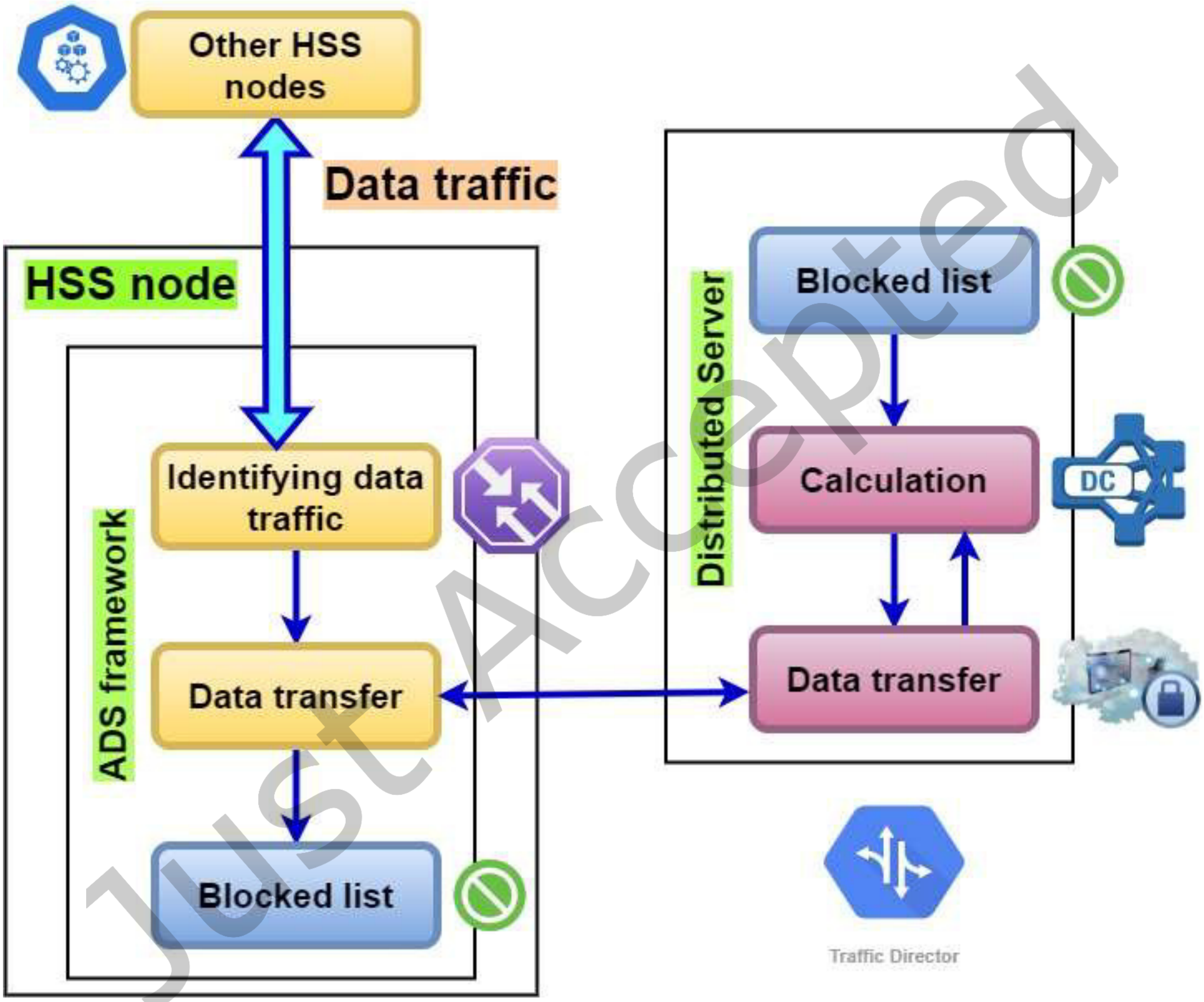


Fig. 2 Framework of ADS for HSS nodes

The standard ADS method depicts the precise interactions between different HSS and dispersed server nodes in Fig. 2. In particular, a minimalist variant of ADS is deployed on smartphones to support network information monitoring, traffic registration, and privacy rules. There are generally three main components: traffic monitors, connectivity, and a blocklist.

- Traffic monitoring: this component is utilized for traffic control, data acquisition, and message transmission to its connectivity element.
- Communication: This element connects and transmits necessary information to the data server that plays a vital role during the engagement. It likewise supports updating the blocklist depending on network statistics.

- Blocklist: This element provides a list of prohibited HSS nodes determined by the trust values generated on a server. The database will be adaptive to limit fake results based on medical service executive comments. On the other side, the central server manages the process of confidence calculation and anomaly-based monitoring. It generally has three main elements: trust calculation, connectivity, and a blocklist.

The Trust component helps compute HSS trust levels, identify malicious nodes and decide blocklists based on the data received. The Communication component is comparable to the mobile element,connecting different terminals to the domain controller. It helps collect the necessary data from nodes to aid trust calculation processes and transmit the updated blocklist to the appropriate HSS nodes. The blocklist is the list of delisted nodes most refreshed. Various security restrictions may be implemented to guarantee that the database is active and correct.This system is improved by combining multimedia information processing with blockchain technology.

The healthcare services' design is requested with a single dominant server and may develop a centralized failure point. Since blockchains allow many nodes to connect in a decentralized style without a centralized expert, building a trust administration system is necessary through integration with blockchains.

An attack detection system monitors for unusual behaviors and signals of an attempt, and it is capable of providing countermeasures to safeguard the system. Companies use this type of security solution to identify suspicious network connections, examine the issue further and do investigations to identify its origin before minimizing the problem. If anyone has an active Intrusion detection system, theycan not need any human interaction to stop a suspicious operation in the process.Like wiretapping, traffic monitoring assaults use what the assailant observes to access a system. By simply listening to network traffic, the attacker can gather location information of important nodes, the routing topology, and perhaps even program attitudes and behaviors.

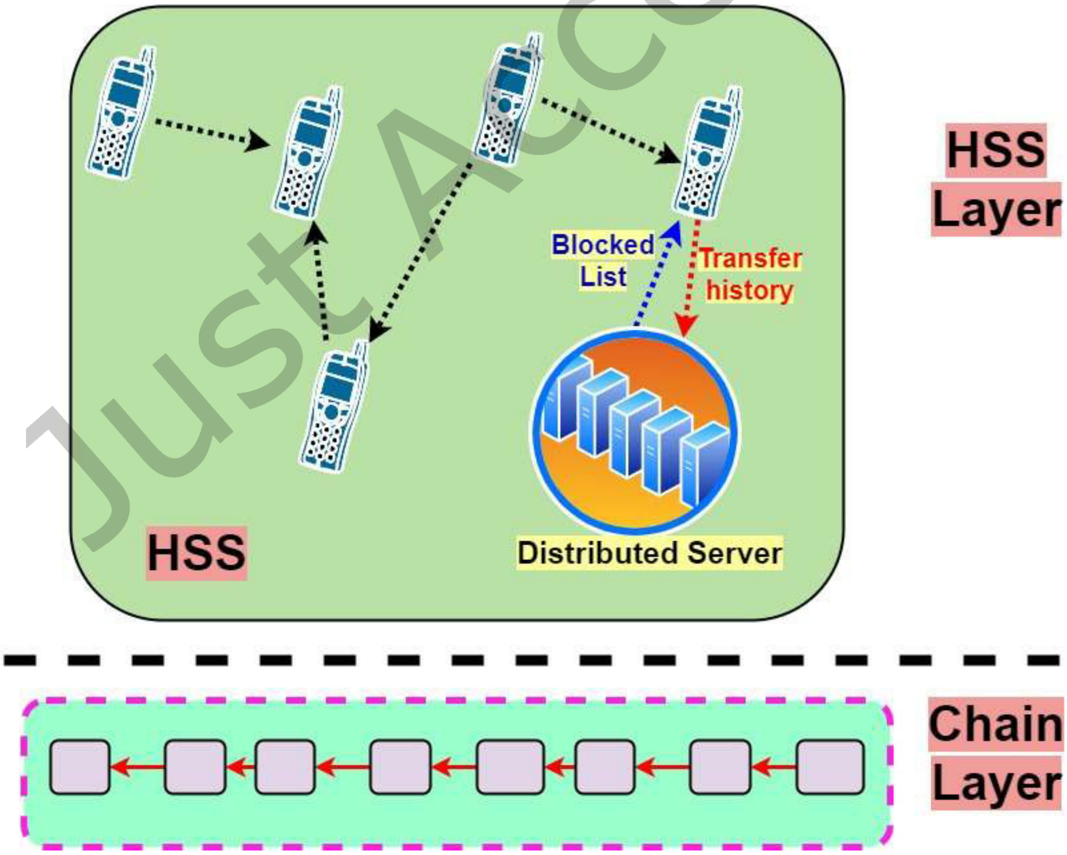


Fig. 3 Proposed ADS framework using Blockchain

Fig. 3 depicts the security monitoring system based on Blockchain, which divides HSS into two primary levels, the HSS level and the chain level.When applying previous information to specific patients and their families, pattern recognition is a lifesaver for healthcare practitioners. Children and their families benefit from the expertise of nurses who work with them and the doctors' growth in self-awareness.

1) HSS Level: Regular communication between HSS nodes and a database controller is possible through this layer. The current structure may be maintained and implementation costs in a medical institution reduced. Several different approaches to sustain blockchain trustworthiness, then present architecture may need to adapt.
2) Chain level: This level builds a blockchain associationthat lets any node add undesired or harmful packet characteristics. Since any node may visit the chain to verify the attributes of spitefulpacks, it can immediately apprise its blocklist and receive further information to send messages straight to the target node. It is not simple to refresh the database quickly in the original architecture. This Blockchain-based confidence maintenance system can offer two advantages: 1) it can assist to rapidly send the blocklist across HSS nodes by verifying the blockchains; 2) it may enable more influentialelements to interact with possibly aberrant entities. A fraudulent node might be immediately discovered, according to Equation (5), by reducing the cost of l.

Patients' lives and deaths are in the hands of healthcare professionals, and each health system must establish a solid basis of expertise, credibility, and integrity.

The following Equation may therefore assess the confidence of the HSS nodes:

$$T_{hv} = \Sigma_1^j l_t \mu^t + 1 \times \Sigma_1^j M_t \mu^t \qquad (6)$$

The viability of HSS nodes may be assessed based on Equation (5) if t is to indicate the time interval. Else if $T_{hv}$the value indicates a node's trustworthiness; it will be calculated from Equation (6). A factor that is μ ∈ [0, 1] has been applied to gradually emphasize the current untruthful occurrence to diminish the influence of past data. Let t indicate the period.M is the total number of nodes, and the number of normal nodes is denoted as l .

A blockchain is a digital ledger that stores data in a units chain of blocks, and whenever a piece is completed, it is sealed and connected to the preceding block, producing a trail of data ledger called the Blockchain. The bitcoin's safe characteristics can greatly improve the security of patient data. It would be difficult to hack because each user would have to be targeted one by one to access confidential information. As a result, healthcare data stored on blockchains can be verified unalterably.

3.3 Fuzzy logic based ADS

Sugeno form of fuzzy logic has too been developed to assess the suggested ADS model. Seven clinical factors are found, derived from HSS along with specified ranges. As seven factors and five pairs of conditions are available, 700 are the total rules to be produced.

$$D(r, I) = (r + I - 1) = [(r + I - 1)!]/[(I! \times (r - 1)!)] \qquad (7)$$

The above Equation (7) is determined by the total number of potential (D) combinations with seven parameters denoted as (r) and five input options for each state with iterations given by (I).

Algorithm 1:Biological input processing to detect health state of individual using HSS in the proposed PBFL-ADS framework

```
Input:   Snoring level, breathing, pulse rate, oxygen level, eye movement, leg movement, and body
temperature.
Output: Health state of individual using fuzzy logic and ADS framework

    1. Initialize Snoring level, breathing, pulse rate, oxygen level, eye movement, leg movement, and body
       temperature to 0.
    2. Check the equivalence of input data with the assigned constraints.
    3. While input value lies in the range, do
    4.  Give the value for variable/parameter
    5. If variable/parameter given value previously, then
Exchange variable/parameter based on updated input
Else
Give the value for the next variable/parameter
End if
    6. Repeat steps from 3 to 5 thus that values are given to all the variables/parameters
    7. End while
    8. If variable/parameter=0, then
         Repeat from step 2
End if
    9. Detect health state of individual using HSS
```

Algorithm 1 gives the biological input processing to detect the health state of individuals using HSS in the proposed PBFL-ADS framework.After receiving the input information as measured traits, it is analyzed with the range of parameters determining the patient's health status. The risk level is assigned to the initial conditions when the information is within the scope. The algorithm provides the detailed data processing flow using an example.

The input parameters include snoring level, breathing rate, pulse rate, oxygen level, eye movement, leg movement, and body temperature. The fuzzy logic and ADS framework is used to provide an individual's health state. Set the input parameters to 0 and verify that the supplied data is equivalent to the constraints. For each parameter, give its value and its condition, and then alter it if the input falls within that range or outside of it. Afterward, the next variable is examined, and it proceeds to the end, where the while function is terminated. The thing comes to an end and can be used to determine an individual's health status utilizing HSS if a criterion is met.

Table 1: Range of fuzzy output to detect health state of individual using HSS in the proposed PBFL-ADS framework

Health state	Range of output values
Low health risk	0-1
Moderate Low risk	1.1-2.1
Moderate risk	2.2-3.2
Moderate high risk	3.3-4.3
High risk	4.4-5.4

Table 1 shows the range of fuzzy output to detect the health state of individuals using HSS in the proposed PBFL-ADS framework. Based on the secure data obtained from HSS and fuzzy logic, individuals' health condition has been categorized into the following levels and is given in Table 1. The five states of an individual's health have been classified based on fuzzy values: low, moderately low, moderate, relatively high, and high risk.

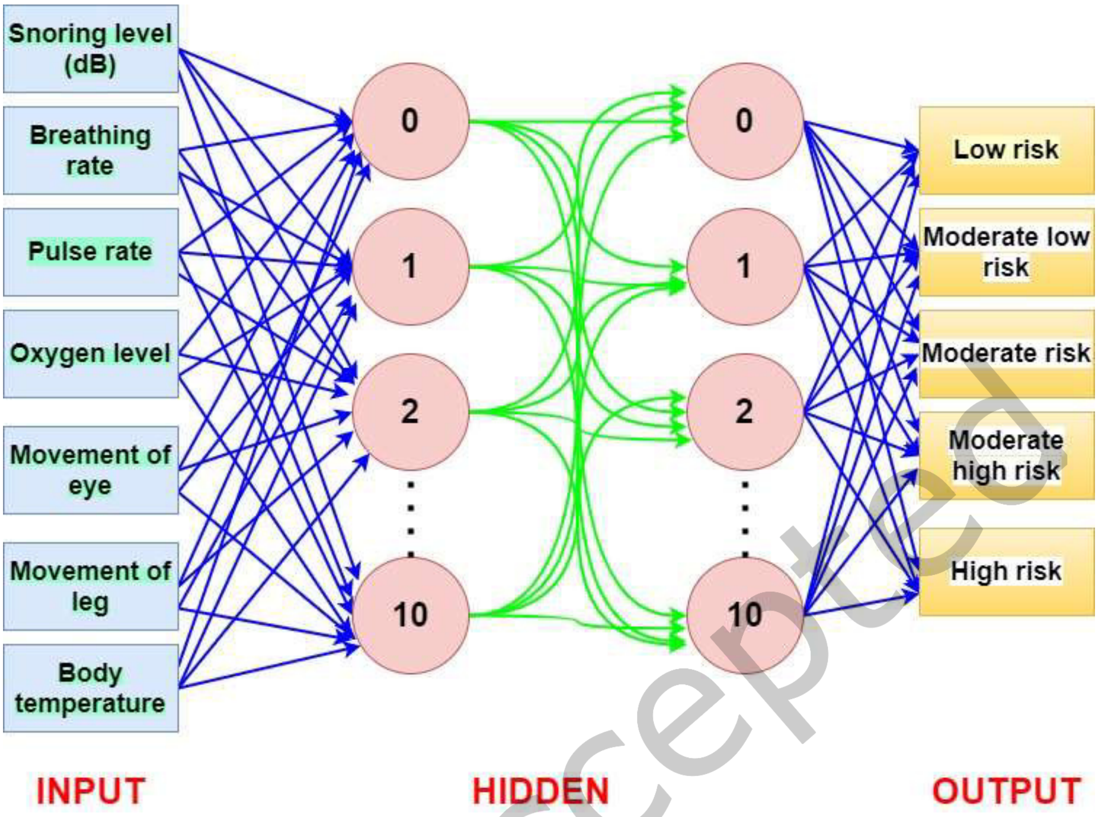


Fig. 4 Fuzzy logic-based neural network model for the proposed PBFL-ADS system in health and risk prediction.

Fig. 4 shows the fuzzy logic-based neural network model for the proposed PBFL-ADS system in health and risk prediction.A fully connected neural Network model is utilized to demonstrate the link between biological data and risk levels in health, as shown in the figure. A neural network based on fuzzy logic contains neurons in one level, and each neuron in the previous layer receives the input connections. One layer of input, two levels masked layer and one layer of output have been considered. A linear layer-stacked sequential model is developed. The hidden layer comprises ten groups of tightly linked neurons.Pattern recognition is a term used to describe the automatic non-analytical method of retrieving pertinent information. Doctor can quickly diagnose a patient's problem using automatic information integration processes like classification and problem representation.

Based on the degrees of state of the input, fuzzy logic is a fundamental control system that influences the output according to this state and how quickly it changes. In other words, a fuzzy logic system assigns a specific output based on the likelihood of the state of the input.

The assigned weights for each level in the hidden layer is given as:

$$Z(Y) = \sum_{j=1}^{M}(t_j\, y_j + t_0) \quad (8)$$

The information obtained from HSS has been given to the hidden layer, and its weights are computed. $Y = y_1, y_2, \dots\dots, y_m$ denotes the input with $m \times m$ measurement, $Z(Y)$Denotes the neural retort based on the parameter Y. t_j and t_0 are the weight of the input and output layers, respectively.

$$f(y) = \begin{cases} 1 & y > 1 \\ y & y = 1 \; and \; 0 \\ 0 & y < 1 \end{cases} \quad (9a)$$

$$q = SMx(t.y + i) \qquad (9b)$$

The linear transfer function is utilized as a hidden layer activation feature in Equation (9a). In contrast,the Softmax function (SMx) has been given in Equation (9b), used in the output layer. The variables $t, y, and\ i$ represent the weight, inference function, and prejudice function, respectively.

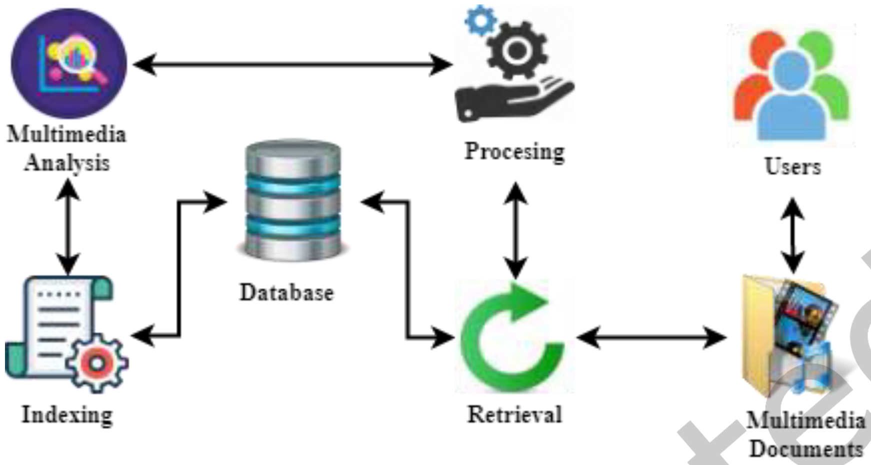


Fig. 5 Multimedia information processing of patients data

Media objects, generated metadata, and objects' spatially and temporally features are all part of multimedia database information. It is updated and edited by services regularly. Afterward, researchers will go through time-related models for multimedia information processing which is explained in fig. 5.Data sources appropriate to a certain requirement can be retrieved through multimedia information processing from a bundle of resources. A hospital's ability to provide users with the data they need is one of its most critical tasks.

$$M_i = Q(B_i)\Sigma_{i=1}^{n}\left(1 - Q(B_i)\right) \qquad i = 1,2,3,\ldots\ldots n \qquad (10)$$

$$I_p\left(p_1, p_2, p_3, \ldots\ldots . p_n\right) = \left(1 - \Pi_{i=1}^{n} 1 - Q\left(n_{p_i}\right)\right), \Pi_{i=1}^{n} m_{p_i}, \Pi_{i=1}^{n} q_{p_i} \qquad (11)$$

$$Where\, p_n = \left(n_{p_i}, m_{p_i}, q_{p_i}\right) \qquad (12)$$

As per equations 10, 11, and 12, the pattern recognition ratioI_p is the calculation of fuzzy weighted average M_i is used to assess the total preferred value $Q(B_i)$for each choice $i = 1,2,3,\ldots\ldots n$ and score function $p_n = \left(n_{p_i}, m_{p_i}, q_{p_i}\right)$is used to present the and rating$Q\left(n_{p_i}\right), m_{p_i}, q_{p_i}$of each option. The pattern recognition ratio is derived and improved with the help of equations 10,11, and 12.

Parameters	Explanation
S	packets sent
m	packages are considered to be regular packets
q	probability of occurrence
$(S + 1)$	Baye's interface
$Prob(W_{S+1} = 1\|m(S) = l)$	malicious node with probability
l	quantity of regular
M	totalpackets
t	time interval
T_{hv}	trustworthiness
D	total number of potential
r	combinations with seven parameters
$Y = y_1, y_2, \ldots\ldots, y_m$	input with $m \times m$ measurement
$Z(Y)$	neural retort based on the parameter Y
t_j and t_0	weight of the input and output layers
SMx	Softmax function
$t, y, and\ i$	weight, inference function

Thus, a decentralized system that provides visible and transparent storage space, i.e., maintains data integrity, frequently manages or controls the Blockchain. In particular, without most participants' consent, connected data in any block cannot be fraudulently altered. The storage is processed on the cloud at the edge of the proposed PBFL-ADS system. The system does not need to sacrifice user privacy; it offers secure data transfer for both download and retrieval and safe storage and communication.

4. RESULTS OBTAINED FOR THE PROPOSED PBFL-ADS FRAMEWORK

In cooperation with two healthcare organizations, the performance of the proposed PBFL-ADS Framework has been analyzed. The method has been adopted to assist appropriatesupervisors in privacy and control two healthcare settings, called HS1 and HS2. In particular, the HS1 and HS2 are 20 and 25 telecommunication nodes. A fully accessible ADS-based mobile intrusion version has been launched. Intel Core 2, Quad CPU with the speed of 2.6GHz central server processes the information gathered from each HSS node and appropriate information. It should be noted that both companies have introduced regulations for radio communications (145 for HS1 and 260 for HS2). The blockchain alliance has been implemented in multi-end PC with Intel Core i6, CPU 2.5GHz, 50GB storage system.

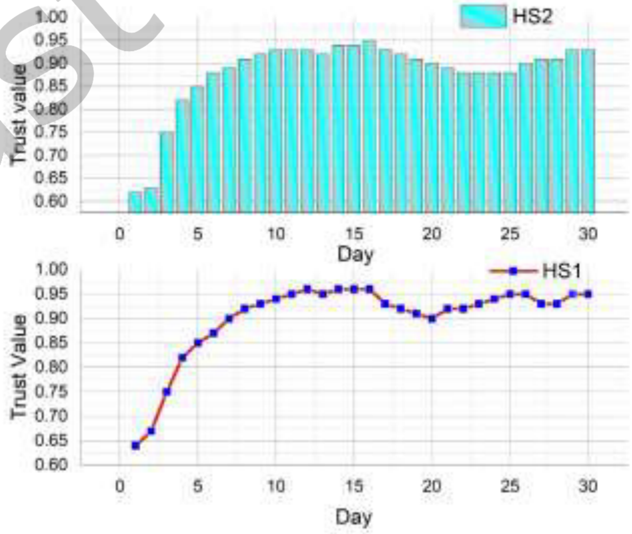
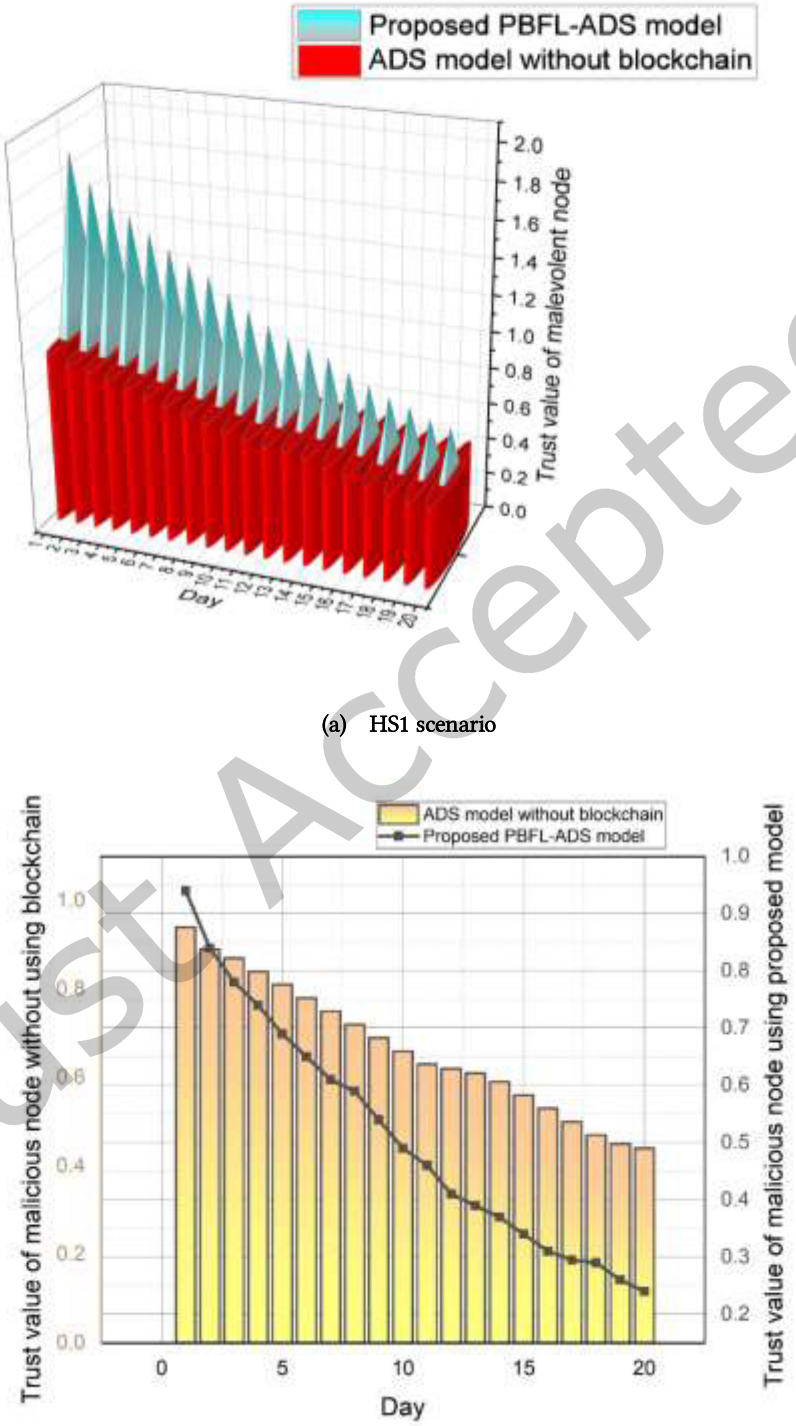


Fig. 6 Mean value of trust among HSS nodes under standard scenario

Fig. 6 depicts the mean value of trust among HSS nodes under a standard scenario. μ = 0.85 has been put forth in this work based on the practical analysis of the forgetting factor. After a time, the trust values might become stable, that is to say exceptionally near to one, following the data gathering on the cloud server. In practice, due to communications delays and various security considerations, it is tough to achieve the value of one according to the importance of $Prob(W_{M+1} = 1, m(M) = l)$and T_{hv}. Furthermore, the mean credibility for HS1 is slightly greater than that for HS2. The reason is that HS2 utilized more self-regulations to manage mobility, which leads to a safer scenario.



(a) HS1 scenario

(b) HS2 scenario

Fig. 7 Comparison of trust value (malevolent nodes) among ADS model without Blockchain and the proposed PBFL-ADS model

Comparison of trust value (malevolent nodes) among the ADS model without Blockchain and the proposed PBFL-ADS model for HS1 and HS2 scenarios have been given in Fig. 7. This study aims to assess the performance under adversarial conditions of the proposed trust management mechanism. To start internal assaults, four and six nodes have been randomly picked in the HS1 and HS2 nodes for malicious packets to be sent to other nodes. The software built, relying on the mobile ADS client application, delivered infected files with the capacity to send several types of modified packets such as the airjack signal packets. The forgetting factor has too been adjusted at $\mu = 0.85$.

To build a good reputation, a malicious node can work together with others, then it can too decide not to work together while launching assaults, and it is explained in figure 6.

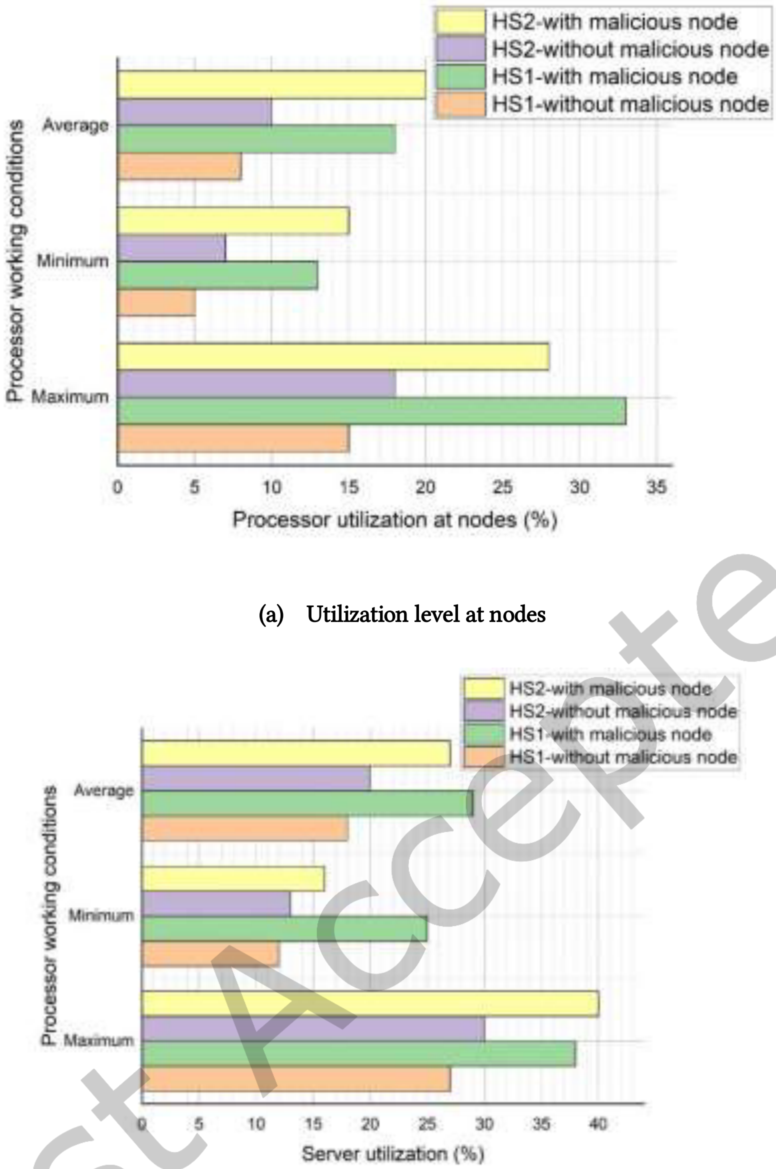
The inward assault has been initiated when the system and the confidence levels in both healthcare environments become steady. The research has been carried out seven times to decrease the influence of unexpected circumstances. Figures 6(a) and 6(b) illustrate the traditionalbelief values of malicious nodes. The credibility levels of attackers began to decrease under every kind of trust management once the assault had been launched.

Table 2: Fuzzy logic based classification of HSS node information using the proposed ADS framework

Input \ output	Low risk	Moderate low risk	Moderate risk	Moderate high risk	High risk
Snooring level (dB)	45-55	55-65	65-85	85-95	Above 95
Breathing rate (bpm)	15-19	19-22	22-25	25-28	Above 28
pulse rate (bpm)	40-50	50-60	60-70	70-80	Above 80
oxygen level	95-100	93-95	90-93	87-90	Below 87
eye movement	65-75	75-80	80-90	90-95	Above 95
leg movement	5-10	10-15	15-20	20-25	Above 25
body temperature (°F)	97-99	95-97	93-95	90-93	Below 93

Table 2 shows the fuzzy logic-based classification of HSS node information using the proposed ADS framework. The information entered is evaluated to the variety of characteristics that allow the users' health status to be recognized. Table 2 gives the range of values classified using fuzzy logic and neural network once the biological parameters have been obtained. The health status is assigned following the supplied factors after the information is within the limit. When comparing the PBFL-ADS approach to the original, it has been shown that the proposed model could further enhance the prediction performance.The proposed technique could lower the trustworthiness by below 0.85 one day quicker than the original scheme in both health care contexts. The primary reason is that HSS nodes can update their blocklist more rapidly in the proposed system than the existing model, and adjacent nodes can more often interact with suspect nodes for additional traffic data.

Biological factors are classified using fuzzy logic and neural networks in Table 2. To arrive at these numbers, researchers used equations 8 and 9.



(a) Utilization level at nodes

(b) Utilization level at the server

Fig. 8 Processor utilization level under various working conditions for the proposed PBFL-ADS model in HS1 and HS2 scenarios.

Fig. 8 depicts the processor utilization level under various working conditions for the proposed PBFL-ADS model in HS1 and HS2 scenarios. Due to the trust-based procedures, increasing the burden for both the node and the server is fair. 1) Interfaces, such as packet status collection, communication between nodes and a server, and blocklist updates, are essentially causing a burden on the centralized computer. 2) The node's workload is primarily due to interactions with elements like HSS communication, trust calculation, generating and updating the blocklist, enforcement of security policies, retrieval of blockchains, etc. Figure 7 shows the processor application in the studies' various node and server circumstances, including maximal, minimal, and average use of processors in two health environments (HS1 and HS2).

The distance between the lower and higher average of a set of values. The most numerous item in a collection of information and data with the smallest value is a minimal set. For example, a range of values is how much difference between a high and a little number. To put it simply, the range is the difference between the least and the greatest values in a collection.

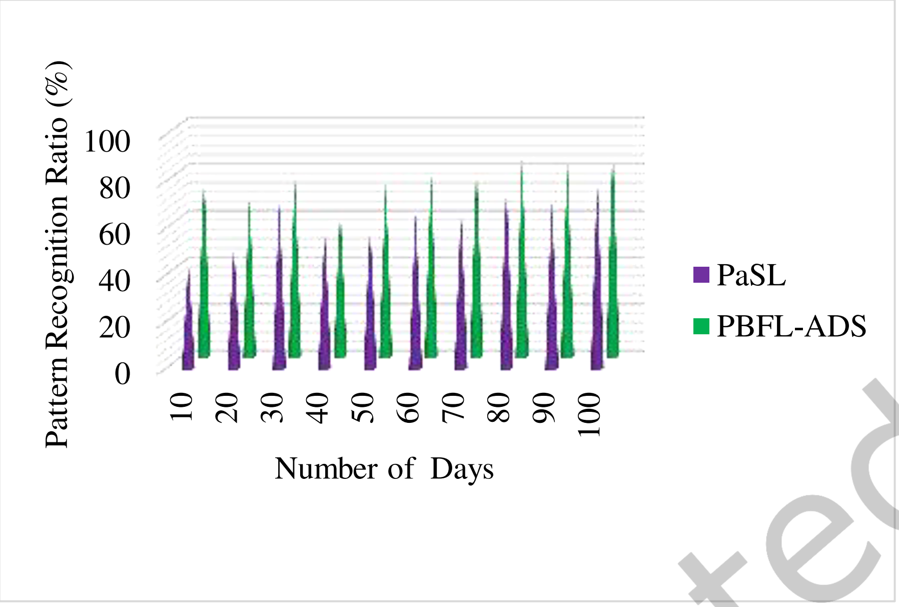


Fig. 9. Comparison of pattern recognition

Learning algorithms are used to recognize recurring patterns in data as part of a pattern recognition technique. Text, photos, audio, and other quantifiable data types are all acceptable. Systems that use predictive modeling can rapidly and reliably identify patterns that are familiar to them. Automated pattern identification is the process of identifying patterns and trends in a dataset. Aside from the collection and analysis of the signal, pattern recognition concentrates much more on the transmitter itself. Equation 11 is used to analyze the pattern recognition ratio, and it is greater than other methods, as shown in Fig. 9.

The utilization of the processor has been readily discovered to be much more significant in adverse node conditions (with malicious nodes) thanin the normal situation. For example, the mean processor utilization of the centralized computer is 18%, then it may rise to 30% in the case of attacks. Harmful information would lead to more excellent contact between various HSS nodes, between nodes, and the server. The server's stress is significantly larger than on the node side, which means that processor utilization is 18 percent and 7 percent correspondingly for the server and nodes in HS1. The reason is attributed to the fact that the server has a lot of duties, such as collecting and evaluating data, calculating trust, and generating blocklists and updating.

Multi-step transactions that require verification and traceability benefit from blockchain technology. Secure transactions, reduced compliance expenses, and faster data transfer processing can all be achieved through Blockchain. The auditing of a product's provenance can be made easier using blockchain technology.

To preserve the accuracy and security of the network as a whole, blockchain networks use encryption processes, including hashes techniques and public-key encryption. The system could be hacked if encryption keys are not properly managed. The results may have consequences for legislation, practice, philosophy, and continued studies, as well as for scientific literature. As a result of this research, they have provided suggestions for a particular policy, practice, theory, and future research.

5. CONCLUSION

Thus, a secure IoMT health prediction has been presented to the private Blockchain and the Fuzzy Logic-based attack detection system (PBFL-ADS). The approach uses Bayesian trust management based on infusion to detect nodes maliciously associated with PBFL-ADS in HSS. This article concentrates on the specific kind of IoMT termed HSS, as smartphones are frequently utilized in the medical sector. This proposed model enhances information retrieval using multimedia information processing.Blockchain was then used to increase the efficacy and detection of hostile nodes of HSSs via Bayesian trust management. Despite the advantages, excessive usage of smartphones may lead to substance abuse, harming human well-being. Many people suffer from despair, anxiety, and a lack of social contact because they are addicted to their smartphones. In addition, excessive smartphone use might lead to a loss of productivity. The experimental findings show that, compared to the original scheme and two ADS models, the suggested PBFL-ADS scheme can achieve higher detection performance. Moreover, the trend in both health settings for the reputation of harmful nodes is comparable and validates the adaptability of the proposed strategy. The findings showed that the suggested technique could recognizemalevolent nodes more quickly than the existingsystem. Likewise, the processor utilization of the proposed system was equivalent to the uniquedesign, making the method satisfactory and feasible for real-time implementation. The subsequent work might involve examining how to strengthen the trust management based on Blockchain by examining delay and computing resource factors. Moreover, it is important to explore how to develop suitable decentralized, secure communication for healthcare providers.The proposed PBFL-ADS method increases the HS2 scenario 1.1, processor utilization at nodes 33.5%,server utilization 40.1%, and pattern recognition ratio 92.1%. In a decentralized system, medical files may be rapidly and easily accessed by physicians, institutions, pharmacies, and anybody else participating in the care process. In this approach, the Blockchain could result in more accurate diagnostics and individualized treatment programs for patients.

REFERENCES

1. Gheisari, M., Najafabadi, H. E., Alzubi, J. A., Gao, J., Wang, G., Abbasi, A. A., & Castiglione, A. (2021). OBPP: An ontology-based framework for privacy-preserving in IoT-based smart city. *Future Generation Computer Systems*, *123*, 1-13.
2. Baskar, S., Shakeel, P. M., Sridhar, K. P., & Kanimozhi, R. (2019, July). Classification System for Lung Cancer Nodule Using Machine Learning Technique and CT Images. In *2019 International Conference on Communication and Electronics Systems (ICCES)* (pp. 1957-1962). IEEE.
3. Son, S., Lee, J., Kim, M., Yu, S., Das, A. K., & Park, Y. (2020). Design of secure authentication protocol for cloud-assisted telecare medical information system using Blockchain. IEEE Access, 8, 192177-192191.
4. Billah, M. F. R. M., Saoda, N., Gao, J., & Campbell, B. (2021, May). BLE Can See: A Reinforcement Learning Approach for RF-based Indoor Occupancy Detection. *In Proceedings of the 20th International Conference on Information Processing in Sensor Networks (co-located with CPS-IoT Week 2021)* (pp. 132-147).
5. Do, D. T., Van Nguyen, M. S., Nguyen, T. N., Li, X., & Choi, K. (2020). Enabling multiple power beacons for uplink of noma-enabled mobile edge computing in wirelessly powered IOT. *IEEE Access,* 8, 148892-148905.
6. Muthu, B., Sivaparthipan, C. B., Manogaran, G., Sundarasekar, R., Kadry, S., Shanthini, A., & Dasel, A. (2020). IOT based wearable sensor for diseases prediction and symptom analysis in healthcare sector. *Peer-to-peer networking and applications*, 13(6), 2123-2134.
7. Zhan, H., Wang, L., Chen, S., Kumar, P. M., & Shakeel, P. M. (2021). Detection and alerting system of nearby medical facilities during emergency using IoT sensors. *Journal of Ambient Intelligence and Humanized Computing*, 1-13. https://doi.org/10.1007/s12652-021-03007-0
8. Gao, J., Wang, H., & Shen, H. (2020, May). Smartly handling renewable energy instability in supporting a cloud datacenter*. In 2020 IEEE international parallel and distributed processing symposium (IPDPS)* (pp. 769-778). IEEE.
9. Krishnamoorthy, S., Shanthini, A., Manogaran, G., Saravanan, V., Manickam, A., & Samuel, R. D. J. (2021). Regression Model-based Feature Filtering for Improving Hemorrhage Detection Accuracy in Diabetic Retinopathy Treatment. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems,* 29(Supp01), 51-71.
10. Seyhan, K., Nguyen, T. N., Akleylek, S., Cengiz, K., & Islam, S. H. (2021). Bi-GISIS KE: Modified key exchange protocol with reusable keys for IoT security. *Journal of Information Security and Applications*, *58*, 102788.
11. Sedik, A., Hammad, M., Abd El-Latif, A. A., El-Banby, G. M., Khalaf, A. A., Abd El-Samie, F. E., & Iliyasu, A. M. (2021). Deep Learning Modalities for Biometric Alteration Detection in 5G Networks-Based Secure Smart Cities. *IEEE Access,* 9, 94780-94788.
12. Amudha, G., & Narayanasamy, P. (2018). Distributed location and trust based replica detection in wireless sensor networks. *Wireless Personal Communications*, 102(4), 3303-3321.
13. Dash, S., Abraham, A., Luhach, A. K., Mizera-Pietraszko, J., & Rodrigues, J. J. (2020). Hybrid chaotic firefly decision making model for Parkinson's disease diagnosis. *International Journal of Distributed Sensor Networks*, 16(1), 1550147719895210.
14. Gunasekaran, N., Thoiyab, N. M., Zhu, Q., Cao, J., &Muruganantham, P. (2021). New Global Asymptotic Robust Stability of Dynamical Delayed Neural Networks via Intervalized Interconnection Matrices. *IEEE Transactions on Cybernetics*.
15. Kaur, M., Singh, D., Kumar, V., Gupta, B. B., & Abd El-Latif, A. A. (2021). Secure and energy efficient based E-health Care Framework for Green Internet of Things. *IEEE Transactions on Green Communications and Networking*.
16. Amudha, G. (2021). Dilated Transaction Access and Retrieval: Improving the Information Retrieval of Blockchain-Assimilated Internet of Things Transactions. *Wireless Personal Communications,* 1-21.
17. Garg, S., Aujla, G. S., Erbad, A., Rodrigues, J. J., Chen, M., & Wang, X. (2021). Guest Editorial: Blockchain Envisioned Drones: Realizing 5G-Enabled Flying Automation. *IEEE Network*, 35(1), 16-19.
18. Dhasarathan, C., Kumar, M., Srivastava, A. K., Al-Turjman, F., Shankar, A., & Kumar, M. (2021). A bio-inspired privacy-preserving framework for healthcare systems. *The Journal of Supercomputing*, 1-36.
19. Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. EURASIP Journal on Information Security, 2020, 1-18.
20. Malamas, V., Chantzis, F., Dasaklis, T. K., Stergiopoulos, G., Kotzanikolaou, P., &Douligeris, C. (2021). Risk Assessment Methodologies for the Internet of Medical Things: A Survey and Comparative Appraisal. IEEE Access, 9, 40049-40075.
21. Xhafa, F., Kilic, B., & Krause, P. (2020). Evaluation of IoT stream processing at edge computing layer for semantic data enrichment. Future Generation Computer Systems, 105, 730-736.
22. Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. Current Psychiatry Reports, 23(4), 1-9.
23. Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. Journal of Management Analytics, 7(2), 189-208.
24. Alladi, T., Chamola, V., Sikdar, B., & Choo, K. K. R. (2020). Consumer IoT: Security vulnerability case studies and solutions. IEEE Consumer Electronics Magazine, 9(2), 17-25.
25. Miao, Y., Tong, Q., Choo, K. K. R., Liu, X., Deng, R. H., & Li, H. (2019). Secure online/offline data sharing framework for cloud-assisted industrial internet of things. IEEE Internet of Things Journal, 6(5), 8681-8691.

26. Ferrag, M. A., Shu, L., & Choo, K. K. R. (2021). Fighting COVID-19 and Future Pandemics With the Internet of Things: Security and Privacy Perspectives. IEEE/CAA Journal of AutomaticaSinica, 8(9), 1477-1499.
27. Kumar, M. H., Mohanraj, V., Suresh, Y., Senthilkumar, J., &Nagalalli, G. (2021). Trust aware localized routing and class based dynamic block chain encryption scheme for improved security in WSN. Journal of Ambient Intelligence and Humanized Computing, 12(5), 5287-5295.
28. Jiang, J., Zhu, X., Han, G., Guizani, M., & Shu, L. (2020). A dynamic trust evaluation and update mechanism based on C4. 5 decision tree in underwater wireless sensor networks. IEEE Transactions on Vehicular Technology, 69(8), 9031-9040.
29. Gomathi, S., & AM, A. B. (2021). High energy efficient lifetime management system and trust management framework for manet using self-configurable cluster mechanism. Peer-to-Peer Networking and Applications, 14(3), 1229-1241.
30. Chen, G., Song, X., Zeng, H., & Jiang, S. (2020). Scene recognition with prototype-agnostic scene layout. *IEEE Transactions on Image Processing*, *29*, 5877-5888.