Electronic Research Archive

http://www.aimspress.com/journal/era

ERA, 31(2): 708–728.
DOI: 10.3934/era.2023035
Received: 20 October 2022
Revised: 03 November 2022
Accepted: 07 November 2022
Published: 22 November 2022

Research article

Blockchain-assisted cyber security in medical things using artificial intelligence

Mohammed Alshehri*

Department of Information Technology, College of Computer and Information Technology, Majmaah University, Majmaah 11952, Saudi Arabia

* **Correspondence:** Email: ma.alshehri@mu.edu.sa.

Abstract: The Internet of Medical Things (IoMT) significantly impacts our healthcare system because it allows us to track and verify patient medical data before storing it in the cloud for future use. A rapidly expanding platform like IoMT requires high security to keep all data safe. The patient's prescription history and other sensitive information must be encrypted and managed with great care. Nevertheless, it is challenging to determine what data uses are acceptable while protecting patient privacy and security. Understanding the limits of current technologies and envisioning future research paths is crucial for establishing a safe and reliable data environment. An untrustworthy person can communicate with a trustworthy person via blockchain, a decentralized digital ledger that allows for end-to-end communication. Therefore, this research suggests that the healthcare industry with blockchain-integrated cyber-security based on artificial intelligence (BICS-AI) in medical care to preserve medical-related things. Blockchain applications have the potential to consistently identify the most severe, potentially life-threatening mistakes in the medical field. The use of blockchain for decentralized data protection helps to protect patient health records from compromise. With the help of an access control provider (ACP), here came up with a lightweight solution that addresses this issue by allowing the delegating of security operations. Medical data from IoMT and integrated devices can be collected and stored securely and distributed using a conventional in-depth approach combined with blockchain, making it suitable for healthcare professionals such as nursing homes, hospitals, and the healthcare industry where data exchange is required. The research findings indicate that the suggested system is viable and has a 94.84% security rate, a security performance of 96.4%, a success rate of 89.9%, and a 5.1% latency rate compared to traditional methods.

Keywords: blockchain; cyber security; artificial intelligence; medical care; IoMT

1. Overview of blockchain-assisted cyber security in Medical Things using AI

Internet connectivity is currently accessible in an ever-increasing number of worldwide areas. The widespread use of cloud computing has brought about a revolution in the outsourcing of data and processing, which has paved the way for the development of the Internet of Things (IoT) [1]. Even though IoT devices are exploding, network technology is rapidly changing. 5G technology has recently been developed that allows devices to be permanently connected to a network at high speeds and with low latency [2].

Industrial Revolution (IR) brought rapid changes in large-scale industry automation, safety, and surveillance [3]. As a result, the Industrial IoT (IIoT) has sparked great interest by incorporating a wide range of wireless sensors and detectors for huge machinery observation and fault detection [4].

Some countries extend the pandemic and infection control measures to other countries [5]. More than a hundred thousand people thought to be infected have been quarantined, and countries worldwide have been put on lockdown to prevent the sudden emergence of new diseases [6]. It is possible to use AI to detect cyber threats and potentially harmful activity [7]. Even the tiniest ransomware or ransomware attacks can be detected by AI systems thanks to advanced methodologies that can identify even the tiniest patterns [8].

Patients' medical histories are kept in an electronic format by their doctors, who use it to track their progress and keep track of any problems or medications they've been prescribed [9]. An Electronic Health Record (EHR) is a digital version of this information and can include anything from demographics to progress notes to problems or medications the patient has been prescribed [10].

According to experts, both the positive and negative effects of AI and machine learning on cybersecurity can be expected [11]. It is done using historical data, and AI algorithms can learn how to deal with new situations [12]. They pick up new skills and knowledge by copying and adding new information. AI can help primary care doctors with tasks like note-taking, patient dialogue analysis, and EHR data entry. [13]. By utilizing these applications, primary care physicians can gain insight into their patient's medical conditions and better serve their patients' needs [14]. Based on similar or previously observed activity, tools and techniques that use artificial intelligence (AI) can identify and respond to possible cyber threats [15].

A variety of healthcare services can benefit from integrating blockchain and artificial intelligence (AI), with wireless body area networks (WBANs) playing a key role from an IoT perspective [16]. There is a growing interest in decentralized approaches to trust management as connectivity and cloud services become more widely used and the IoT grows in popularity [17]. In various fields of application, the research community is paying close attention to blockchain technologies because they provide a distributed ledger [18].

There are expected to be billions of sensing devices connected to the internet in the IoT devices of the future [19]. The massive amount of data this network of connected phones is expected to generate and access will open up new possibilities for innovative applications, raising significant security and privacy issues that will obstruct its further adoption and development [20]. It is realistic to predict that the number of internet-connected devices will continue to climb consistently over the future years due to the falling prices of devices with handling and networking capabilities. [21].

Emerging technologies like blockchain are being used to provide cutting-edge solutions in various settings, one of which is the healthcare industry [22]. Blockchain technology is being used in the

healthcare industry to ensure the security of patient records and to streamline the sharing of information among healthcare providers, laboratories, pharmaceutical firms, and other healthcare providers. [23]. In the world of medicine, apps built on blockchain technology have the potential to precisely detect significant and even hazardous errors. As a result, it has the potential to enhance the efficiency, safety, and openness of the system for exchanging medical data in the healthcare industry [24]. It is beneficial for medical institutions to use this technology to acquire insight and improve the analysis of medical records [25].

The primary benefits of Blockchain technology in healthcare were the subject of this investigation. The different capabilities, accelerators, and unified workflows of blockchains and how they might improve healthcare delivery throughout the globe are diagrammed and discussed. Blockchain technology plays a crucial role in identifying and avoiding dishonesty in clinical studies, and it can boost data efficiency in the healthcare industry. Concerns concerning data manipulation in the healthcare business may be alleviated by the system's provision of a one-of-a-kind computer storage pattern and maintenance of the highest possible safety. Access to data may be dynamic, interoperable, accountable, and authenticated. There are several reasons why it is crucial to protect the confidentiality of patients' medical information. Decentralized data protection and risk mitigation are improved by using blockchain technology in the healthcare sector.

The paper's significant contributions are as follows:

- Designing the proposed BICS-AI method to link an untrustworthy party to a trustworthy one utilizing blockchain.
- The suggested model (BICS-AI) uses an access control provider (ACP) to delegate security functions in this lightweight solution.
- An in-depth development of such systems with blockchain makes it suitable for health professionals to collect medical information from IoMT securely.
- The mathematical results have been performed and the proposed BICS-AI to achieve a security rate, success rate, and low latency rate compared to traditional methods.

The rest of the investigation went like this. Section 2 provides a related work comparing existing methods. Section 3 outlines the proposed advanced Blockchain-integrated cyber-security based on artificial intelligence (BICS-AI) design and implementation. Software analysis and performance testing are depicted in sections 4 and 5, which concludes the overall paper.

2. Background & literature research

This section discusses several works that various researchers have carried out; The existing models are discussed here to compare each analysis's performance.

Cybersecurity in blockchain-based systems (CS-BS). There was a growing interest in decentralized approaches to trust management as connectivity and cloud services became more widely used and the IoT grew in popularity [26]. It's no surprise that blockchain technologies are getting lots of attention from the scientific community because of their distributed ledger capabilities. Blockchain-based systems need to be secure, and this research will show how these systems can be secured using various techniques and elements.

A security architecture (SA) that integrates the Blockchain and the Software-defined Network

(SDN) technologies (SA-SDN). Humans and their surroundings are at risk from increasingly sophisticated cyberattacks on industrial control systems, and these issues necessitate new technologies and approaches [27]. In this study, we looked at how to prevent falsified commands and commands in the IIoT. The suggested fully connected is put through its paces using cyber attack information on industrial automation systems and an investigational architecture that leverages software-defined networking and blockchain technology.

The blockchain-assisted information distribution system for the IoT (BC-AIDS) has been proposed here. It was anticipated that the IoT would include billions of pervasive and mission-critical sensors and devices [28]. It's anticipated that this network of networked phones would generate and access massive quantities of data, open up new avenues for developing applications, and raise serious privacy and security issues that will slow its spread. According to this paper, a system that relies on blockchain systems and smart contracts can meet its security needs. In addition, here present a conceptual design for the system and a list of key technologies that make it possible.

Researchers reverted by implementing a firewall in the network (IFN), keeping track of every connected device and providing services based on a predefined threshold for each host. Many threats have arisen due to the new 4G LTE network's arrival [29]. 4G, instead of 2G and 3G, uses IP-based communication. It has been exposed to various worldwide web attacks and security risks due to excessive internet usage in mobile infrastructure. Our focus was the web access interface or GI interface responsible for linking the mobile device to the Internet and exposing it to various web threats, such as DoS (Denial of Service) and malware.

Deep learning with blockchain-assisted secure image transmission and diagnosis model (BASIT & DM) for the IoMT environment [30]. Data collection, transaction security, and hash value encryption are all included in this model. A grasshopper and fruit fly optimization hybrid, the GO-FFO algorithm was used to generate the optimal elliptic curve cryptography (ECC) key. Extensive experiments are carried out to validate the model's optimal performance, and the results are examined from multiple angles.

M. O. Lawal [31] described the modified YOLOv3 model for detection purposes. The robotic harvesting platform includes a fruit-detecting system that is an essential component. To address these issues, a modified version of the YOLOv3 model known as the YOLO-Tomato model has been developed to identify tomatoes in environments with high environmental complexity. The YOLO-Tomato models, in their entirety, provide improved generalization and real-time tomato identification, both of which are suitable for harvesting robots.

A novel approach for the effectiveness of producing pseudo-examples should be improved by addressing the flaws that are now present in the state-of-the-art methodologies that are currently in use deliberated by W. Khan et al [32]. Training a decoder network was simpler and more efficient than both encoder-decoder designs. Another perk was that unlike encoder-decoder systems, which can produce pictures that belong to the same training class, a decoder trained with random variables and pictures might produce variants of the same class. The suggested is superior to the state-of-the-art models currently available for both SSL and FSL, as shown by comparing their median classification accuracy performances.

As a result of BICS-AI research, the IoMT has been proposed as a means of providing security and authentication. With valid mathematical formulas and diagrams, this proposed model design is superior to all other existing methods, such as CS-BS, SA-SDN, BC-AIDS, IFN and BCSIT-DM.

3. Blockchain-integrated cyber-security based on artificial intelligence

In this research, the healthcare industry uses blockchain-integrated cyber security (BICS)–AI for IoMT. End-to-end communication and interaction between untrustworthy parties have contributed to the blockchain, and a fully decentralized blockchain is distributed. This cutting-edge innovation may improve efficiency and safety in keeping track of property. Blockchain technology may be considered a decentralized peer-to-peer (P2P) network that uses a replicated and distributed ledger. Sensitive health information is often stored in many locations, which may lead to delays in receiving necessary updates and affect patient outcomes. Additionally, there is a rising need for people to access and manage their data as patient engagement in health rises. Improved health outcomes may result from using blockchain technology since it is a secure decentralized online ledger that may be utilized to manage EHRs effectively.

Medical data from IoMT and integrated devices can be collected and stored securely or distributed using a conventional in-depth approach combined with blockchain, making it suitable for healthcare providers such as hospitals, clinics, and the health sector where data exchange is required.

In between private and open blockchains, collaborative blockchains are formed. Generally speaking, open blockchains are less stable than private ones because of the lower capacity of cryptographic techniques, which are measured in the number of transactions confirmed per second. Collaboration blockchains are less efficient than personal blockchains and more efficient than open blockchains.

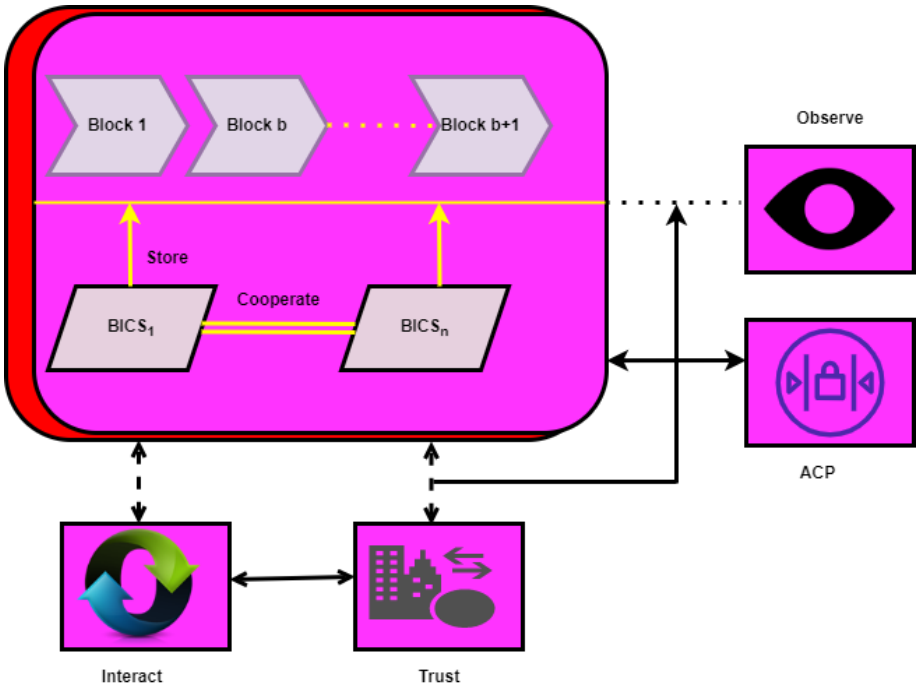

Figure 1. BICS framework representation.

Except for the first block1, each subsequent block in this functional architecture is connected to the one before it via a reverse connection and hash code of the previous block b up to block b+1. A block with the same hash code as its predecessor. An identification number, authentication code, hash of

all operations, and hash of all commitments in each block in the BICS system are in Figure 1. Hash values for operations and commitments are irreversible because even a single bit change can produce a unique hash code using ACP. The development of blockchain technology has generated yet another revolutionary innovation: intelligent contracts. Automating contractual agreements and restrictions is possible with intelligent contracts running on the blockchain's upper end when certain criteria are met. The irreversibility of blockchains and the fundamental hash of all intelligent contracts are linked to the synthesis and recording of executable code of intelligent contracts in blockchains. With smart contracts, trust and interaction between business operations observations can be more efficient while reducing the risk of a security breach.

Data stored in the blockchain is immutable, which means that even the smallest changes could result in incorrect data. Digital signs, non-symmetric encryption/decryption methods, and decentralized consensus procedures can all help to enable transactional non-repudiation. Blockchain data with accompanying metadata can be used to trace a data source referred to as traceability.

$$ID_{a,b} = ED_s(E, K) \rightarrow Dt(D_a(K, K_a, K_b)) \tag{1}$$

As shown in Eq (1) intrusion detection has been described. The information a,b to be prevented from the intrusion detection ID is shown in Eq (1), while the encrypted data ED is shown here in symmetric encryption s. An online cloud storage service(K) can be used to store the data(E). Using asymmetrical decryption Dt scheme, the application and the provider D_a each has a private key that is used to decrypt encrypted data(K, K_a, K_b) using key-value (K).

$$MR = \alpha \times \ pa.t - (1 - \alpha) \times \ qt \tag{2}$$

As found in Eq (2) medical report has been discussed. Successful IoMT data trading requires a high level of trust between parties. As a result, the healthcare system can use trustworthiness assessment techniques to gauge the trustworthiness of business partners. For the medical report MR, the trustworthiness of potential medical care is highly regarded. When there is a level of objective confidence in the person's abilities pa, the qt is the level of trustworthiness and the factor used for weighting α. First, medical report MRconsults mentioned in Eq (2), patients' records can have their trustworthiness evaluated using the trust assessment service. Trustworthiness evaluations can occur if all the information is accessible for hacking purposes. Many healthcare settings use them, including e-medicine, remote rehabilitation, and pandemic containment. Many diverse healthcare records have been generated due to IoMT's integration of various healthcare instruments and infrastructures.

Using a large amount of IoMT data, healthcare providers can quickly identify and diagnose health issues and treat patients. An overview of IoMT architecture is depicted in Figure 2. A large amount of IoMT data is generated by medical sensors in IoMTarchitecture, and this data is gathered, analyzed, and evaluated by healthcare professionals in real-time. Healthcare providers and patients can benefit from IoMT's reliable and efficient healthcare services such as a medical interpreter, medical emergency, and medical library.

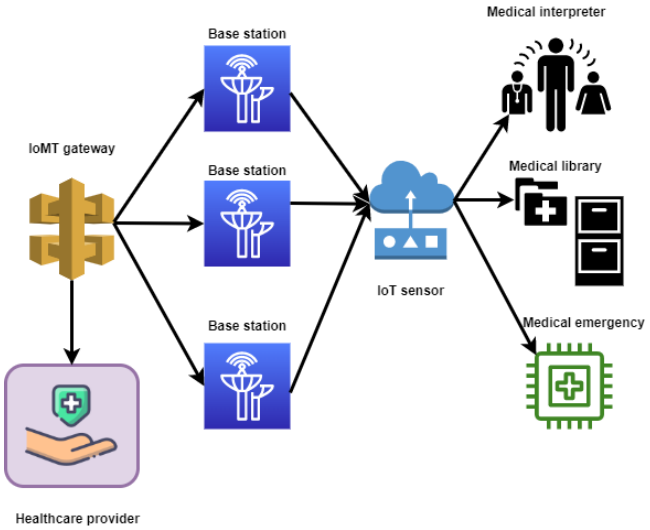

Figure 2. IoMT in BICS-AI.

Two problems arise with other conventional methods with the rise of IoMT: 1) a lack of interoperability between different IoMT domains and 2) flaws in secrecy and cybersecurity in IoMT instruments and networks. Heterogeneous IoMT systems include a variety of biosensors, healthcare systems, Internet of Things interfaces, and wireless networks. Near-field transmission and bluetooth technology, WBAN are examples of IoMT's wide range of wireless systems. Various data barriers are created due to the lack of compatibility between distributed IoMT systems. Transmitting health information between facilities and organizations is therefore difficult. Medical professionals depend on transmitting patient data to help prevent and control pandemics. The IoT faces a number of serious security and privacy concerns.

$$PH.cs = \alpha(SD_aXUD_b) \tag{3}$$

As initialized in Eq (3), serious security and privacy concerns have been deliberated. Research shows that patients' health PH is more closely linked to their cyber security environment csthan previously thought from Eq (3). It is a strange dataset SD that collects and preserves useful data UD for the environment α. Air quality, noise, temperature, and other factors are covered factors with healthcare-based information a and b.

$$I_m(sr+1) = max\left[I_m(hp) \times MA_m + hc_m fr_m(t)\right] \tag{4}$$

$$I_m = max\left[sr + I_m(t)\right] \tag{5}$$

As evaluated in Eqs (4) and (5), information has been demonstrated. Information I_m is gathered through the use of sensors sr strategically placed throughout a space. Sensors are strategically placed throughout the area to aid in this process. Regular health problems(hp) necessitate a bed rest regimen. Prolonged bed rest causes discomfort, stress, and restlessness in patients is defined using Eqs (4) and (5). All of the patient's body and the bed are outfitted with sensors that monitor(t) their actions. Malicious attacks MA_m such as eavesdropping, interference and malware and worm threats are inherent

weaknesses in healthcare sensors hc_m and medical equipment that is frequently resource-constrained fr_m. This research looked at strategies for lowering operational expenses, strengthening data transfer security, and improving the quality of digital communications. As a relatively new idea in computing, blockchain may help increase trustworthiness and facilitate patient monitoring using sensors with little resources. In addition, when consensus mechanism evolves, they become suitable for usage in low-power systems.

$$Bm_i(sr) = ad(ms) - \sum (ms)^{1/2}.t_i(ms) \tag{6}$$

As explored in Eq (6) IoMT in cyber security Bm sensors can perform analytics(sr) on many devices and in a distributed environment i using Eq (6). It is possible to enhance the computing framework at the edge networks using numerous options and capabilities in BICS-AI. This new technology employs ACP and real-time discrepancy detection to help people succeed. IoT-based remote monitoring systems ms are highly effective in giving patients timely t and accurate data ad. In addition, IoMT data is extremely private compared to other IoT data types. Patient data may be compromised during the collection, processing, and analysis phases of IoMT. This can happen either intentionally or accidentally.

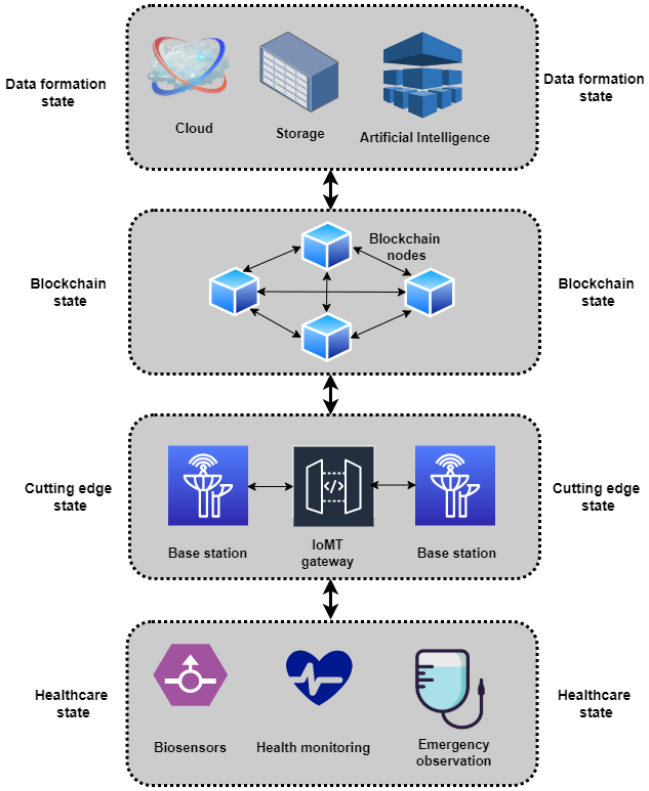

Figure 3. Framework of BICS using AI.

It is possible to solve cybersecurity and privacy issues by integrating blockchain with IoMT. The IoMT'sblockchain-assisted cybersecurity architecture is shown in Figure 3. The design has four possible states: 1) medical instrument state, 2) cutting edge state, 3) blockchain state and 4) data formation state. Biosensors, health monitoring, and emergency observation are some of the IoMT healthcare instruments available in this state of readiness. Communications infrastructure and computational resources are all needed to create a cutting-edge state. Embedded wireless networks, base stations, and IoMT gateways can collect and preprocess data. In addition, the blockchain state serves as a critical gateway to provide reliable analysis of multiple resources across the preceding levels. It includes cloud computing, digital storage, and artificial intelligence algorithms in the data formation stage. Objects and capabilities in the data synthesis state are connected to nodes in the blockchain state via the edge network. With blockchain-aided IoMT, both the cutting-edge state and the blockchain can benefit from excellent authentication and authentication protocols. There is less complexity in IoMT devices and interactions when cutting-edge and blockchain states are used. Other programs can take advantage of blockchain-assisted features provided by the blockchain state, making the development process easier.

$$ST_d = \frac{ST_q(t)}{ST_u(t)} \tag{7}$$

$$sT_e = sT_q(t) + sT_b(t) \times ST_d \tag{8}$$

As expressed in Eqs (7) and (8) security threats has been derived. To get an idea of how much time it takes to reach a consensus, security threats use ST_d. The fabrication of data encryption and the verification of AI, as well as the communication of information and verification of data, such as the authenticity of the signatures using Eqs (7) and (8), are vital for optimizing efficiency sT_u (t) in the decision-making process. Slot acceptance is being held up because of a backlog sTe of applications in the intrusion process, t is equaled. Here, sTq and sT_b is the propagation and validation time for slot communications.

$$DS = CD \times (1 + hpS(D)) \tag{9}$$

As obtained in Eq (9), propagation and validation time slots have been described. The security process of any data provided by the healthcare provider hpSas described in (9), can be expressed in the above general form the number of security issues and is the network connection generated by the IoMT. A trust-aware knowledge-based security system's primary goal is to determine how much profit it can increase for specific intrusion methods. The cost structure is based on the perceived patient paradigm of the demanders. The blockchain state uses the built-in augmented reality network to connect various IoMT sub-networks across the entire IoMT network. Because of this, various IoMT modules are combined into a single unit to meet the needs of other applications. As a result, IoMT system compatibility will be improved. Healthcare providers and other healthcare sectors provide health care, including everything from surgery to medicine, counseling to sports medicine, and everything in between. This includes primary, secondary, and tertiary care and public health care. Many of the IoMT-based models that have been mentioned can be implemented by utilizing already existing data infrastructure.

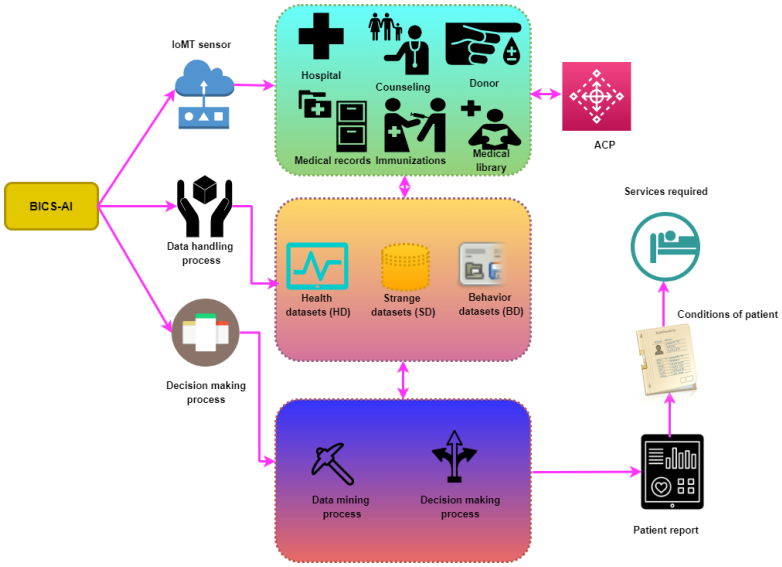

Figure 4. Overview of BICS-AI using ACP method.

Figure 4 depicts the BICS-AI framework. An ACP sends location information to a server via the mobile data network. The proposed architecture has two layers: (i) one that regulates the data flow and storage and (ii) an additional layer that regulates the healthcare data hub. The design is driven by a patient's private sensor network, with data collected and then sent to a third-party healthcare data aggregator. The generated information is sent to a server that serves as the patient data agent and is in charge of data module administration, the data mining module, and data security. If patient data transfers are extra secure and reliable may have heard that they have to go via a blockchain network before they get to the end consumers. The wireless sensor principle can transmit real-time data from these hardware solutions. Medical sensors and biosensors collect data that is combined. The BICS-AI design collects quantitative and qualitative data from the patient. Immunity levels are lower in people who are generally healthy than in cyber threats. The sensitivity of those who suffer from long-term illnesses is increased. The BICS-AI architecture and the various datasets must constantly monitor these patients. The first step in a decision-making framework is gathering all BICS-AI data through mining. Real-time data from IoMT data providers can be mined for useful information using data mining techniques. In other words, many types of research are predicated on a chronological examination of a wide range of IoMT data. Due to the time-sensitive nature of patient well-being.

The Internet of Medical Things (IoMT) links the digital and physical worlds to improve patient health and well-being by expediting diagnosis and treatment and making real-time adjustments to a patient's way of life or health conditions. The integration of medically relevant technologies will profoundly impact patients and healthcare providers.

$$IV = (ptv(ht), \Delta T) = pqt(\frac{wgt}{ht_1 U ht_2 U ht_n}) \tag{10}$$

As demonstrated in Eq (10), the profound impact on patients and healthcare providers has been discussed. Patients with a lower patient valueptv have worse health; while patients with higher health index valuesIV have better health(ht) can be calculated from Eq (10). The healthcare practitioner must be informed to take proper action whenever a *patient's* health is threatened. Using the average

weightwgt technique for conditional probability pqt, it is possible to calculate the index values from $ht_1 \cup ht_2 \cup ht_n$

$$ID = \frac{b * SD}{2^{DT_i}} \sqrt{\frac{\sum_{b*ES}}{ITO}} \tag{11}$$

Intrusion detection process duration ID active period is divided into 16 equal-sized time slots to allow data transfer. It is defined by two parameters, iterative order ITO and encoding scheme ES are calculated using the square root function with summation of base value b and SD using the above Eq (11),

$$ID = \frac{b * S\ D}{2^{DT_i}} * \sqrt{\frac{\sum b * E\ S}{ITO}} \tag{12}$$

where, $(L = 1, 2, 3, ...n)$ the hidden layer Lth neuron processes the incoming data by measuring the amount of weight and applying the $term\theta_w htfrom$ Eq (4). Transform the net value of the input into an accurate data transfer function and transfer the result to the next level of neurons using Eq (12).

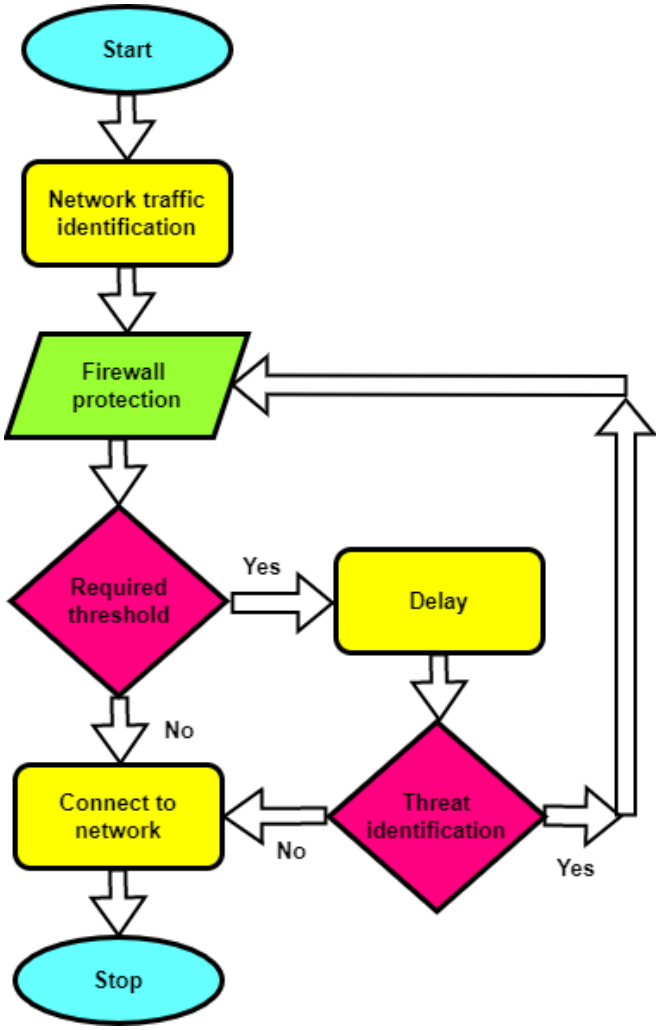

Figure 5. Overview of BICS-AI using ACP method.

Figure 5 depicts the proposed security system's flow chart. Data requests from various mobile hosts enter a firewall security system, which first checks the IP address of each mobile host and then checks the request rate of each mobile host concerning its IP address. Any mobile host's request rate must fall below a predetermined threshold before accessing the server over the Internet. If the request rate is equal to or greater than the threshold, the requesting host receives a timeout and is allowed internet service facilities when the timeout expires. Mobile hosts with a lower request rate than the threshold are granted web services during the delay. As a result, a complete system shutdown caused by an overabundance of data requests is avoided.

$$ve(xt) = \frac{1}{1 + e^{-sl}} + f(wht_{nL}) \tag{13}$$

As shown in Eq (13), wht_{nL} denotes the training procedure used to iteratively alter the values of the weights that connect each node. The sigmoid function is the most commonly used transfer function. Weights are changed using the steepest descent approach to limit the number of training stops. The improved virtual environment ve(xt) can be expressed as seen in the above equation with signal sl. The parameter $f(wt_{nL})$ defines the transfer function of the maximum number of times for learning from n^th output respect to m^th input, (wht_{nL}).

$$CT = \frac{1}{2}\sum_{n=1}^{i}\sum_{m=1}^{j}(wht_{nL} - wht^{*}_{nL})^2 \tag{14}$$

There are three identifiers in Eq (10) that are utilized to generate weight values wht_{nL} for n = 1 to i and L = 1 to j using summation for the steepest descent algorithm. The maximum bandwidth of a blockchain, measured in transactions per second (tps), is limited by the proportion of the block transaction capacity to the block acceptability period. Bitcoin's block size is proportional to its weight, representing the total of all the transaction weights inside it. When calculating the total transaction size in Bytes, the witness contributes less than the other components. The significance of a given transaction is determined by the kind and quantity of its inputs and outputs. The combination of the block weight restriction and the difficulty adjustment yields a throughput of around 2500 tpb or 4 tps. The number of squared residuals $(wht*_{nL})$ is one of the most widely used functions given in Eq (14), a layer's current weight change is determined Ct.

They focused on abnormality identification ab_i and prediction P_i As well as decision-making when it came to time-series data TS_{i-1} The experimental validation section discusses the appropriateness of specific machine-learning algorithms $\widehat{TS}_i$. Artificial intelligence approaches like classification, clustering, and association analysis in the healthcare industry can be helpful using Eq (15). The usefulness of databases is discussed. A resource-based collection and processing method has been developed for use in emergency healthcare facilities using Figure 6.

$$ab_i = (1 - P_i) \times TS_{i-1} + \left[P_i \times \widehat{TS}_i\right] \tag{15}$$

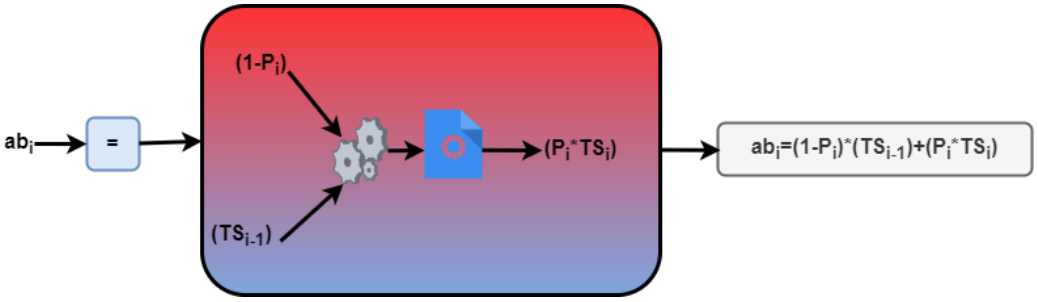

Figure 6. Representation of conventional in-depth approach.

Remote monitoring is made possible by constantly updating the web application with health data using biomedical sensors. Multiple sensors are employed in hospitals to monitor all the patients. Each hospital in the proposed system has an IoT node that analyses sensor data for health monitoring. The system's resilience must be considered in regularly securing justice and accountability in the implementation process. The following are the most critical issues in implementing an IoMT device. As various image centers and ACP models for images of a single domain are expected to be implemented, the distribution of healthcare environments is expected to alter. Medical data from IoMT and integrated devices can be collected and stored in a secure and distributed manner using a conventional in-depth approach combined with blockchain in our proposed system BICS-AI, making it ideal for healthcare providers such as nursing homes, hospitals, and the healthcare industry who need to exchange data in this format by analyzing the below parameters.

4. Results and discussion

The healthcare management system is decentralized, uses blockchain technology, and is based on the current industry standard. The proposed solution utilizes blockchain technology and medical IoT devices to develop an RPM and EHR management system that is reliable and efficient. The suggested system's design uses the decentralized storage idea and a permissionless blockchain network as an ACP to monitor a patient's vital signs. Both of these concepts were taken from the notion of blockchain technology. This section explains the OPNET simulations used to evaluate the proposed BICS-AI performance. 20 user devices and 80 sensor nodes make up this model. As shown in Figure 1, a centralized server serves as the network's data analyst. This system makes use of the well-established 15-interval response recommendation. 1 TB of storage and a processing speed of 2.4 GHz is included in the security rate, security performance, success rate, and latency rate compared to traditional methods. Additionally, other traditional methods will be compared to the proposed method to assess its reliability in BICS-AI. In this study, the x-axis considers several sensors and y axes such as overall performance (%), security performance (%), security rate (%), and latency rate (%) when compared to CS-BS, SA-SDN, BC-AIDS, and IFN with our method BICS-AI.

4.1. Security performance analysis

Table 1 shows the proposed framework's user node security rate and monitoring intervals for IoMT healthcare cybersecurity. Nodes receive healthcare data and control the mapping parameters with the

model expressed $\alpha \times \ pa.t - (1 - \alpha)$ in Eq (2). The data is divided into secure and unsecured, and mapping determines the user's expectations. Patients' historical data is compared to the anticipated model, and the condensed costs to trace actions are indicated. The outcome of the provision is transferred regularly, and it has a high degree of precision. Many IoMT sensor networks benefit from the proposed model's ability to increase security. Healthcare data is collected and connected using the proposed model to create an Internet of Medical Things (IoMT) network for authentication and cybersecurity. When a patient's request is classified as an emergency, the healthcare providers respond immediately.

Table 1. Security analysis.

Number of Sensors	CS-BS	SA-SDN	BC-AIDS	IFN	BICS-AI
10	25.3	63.3	76.6	84.8	96.2
20	85.9	71.4	65.8	57.7	25.1
30	55.5	67.5	76.9	87.8	94.5
40	52.3	68.2	72.7	86.7	92.4
50	52.6	66.7	77.9	87.9	91.5
60	54.1	65.2	75.0	87.0	92.9
70	57.9	68.9	76.8	82.6	93.8
80	50.8	67.5	75.78	86.9	96.2

4.2. Security performance comparison

The patient is engaging in physical activity, and the attending physician must monitor the patient's heart rate during the activity. Because of this, the sensors implanted inside the patient's body transmit a packet to the device that serves as the gateway. After that, the packages are sent to the blockchain network, where they engage in conversation with the smart contracts to complete the duties and save the data. The information in the blockchain is then sent to a medical facility so that doctors there may do more secure queries on the data. In addition, the graphic illustrates several different devices that may be used as gateways to transmit data over the blockchain.

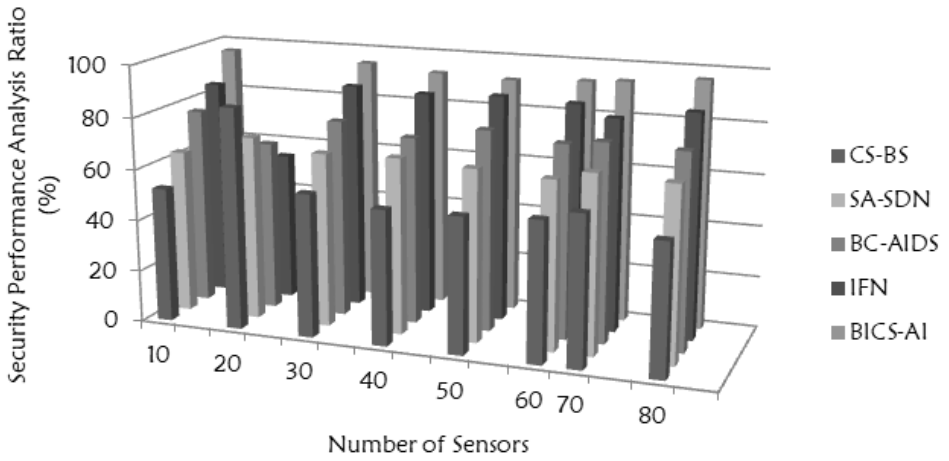

Figure 7. Security performance analysis.

Figure 7 shows that user node performance rates and monitoring intervals are reduced and performed optimally compared to conventional IoMT healthcare data security approaches. From the patient's medical history, healthcare data can improve functional performance. Medical records can be accessed using biometric signs and the user's preferences from Eq (5). It is necessary to investigate a neighboring state repeatedly using multiple IoMT sensors, and the results are then recorded. The user nodes' data predict data mapped to the patient's historical data. For optimal resource utilization, the patient's actions are accurately observed.

4.3. Success rate analysis comparison

This action could be better understood with the aid of sensors that have been activated in the past. Because an observation history is being used, the model has the potential to include more knowledge from the past. When a public blockchain is used, the validation process is lengthened since all nodes are required to participate, which takes more time. Only a select number of nodes can participate in the validation process when this problem occurs. This helps save time and improves the overall performance of the system.

Table 2. Security analysis.

Number of Sensors	CS-BS	BC-AIDS	BICS-AI
10	65.1	79.1	89.6
20	75.4	82.8	84.5
30	65.2	84.6	92.9
40	73.5	79.3	87.1
50	64.0	75.1	82.6
60	75.3	83.0	95.3
70	68.6	77.5	89.5
80	60.8	86.2	90.6
90	71.1	88.4	91.3

The IoMT remote cloud can receive healthcare data from user nodes. The outcome is referred to as a warning. According to the schedule, this alert is sent out, and the healthcare data relates to the domain state of matching the literature data from Table 2. Patient behavior in the healthcare industry differentiates in this match state because of the blockchain-assisted cybersecurity model. Classifying whether an activity is secure is done in conjunction with the amount of data generated by IoMT sensors. In this assessment, the accuracy of the patient's activity is improved, and the range of security is expanded using Eq (9). The warning indication is not sent if the patient's behavior is secured; it is sent if not. In terms of understanding the patient's behavior, tracing states are used.

4.4. Latency rate analysis

Figure 8 shows the latency comparison among the various approaches to physical health monitoring, and the BICS-AI approach outperforms the ACP method in terms of standardization and effectiveness. Concerning the number of iterations estimated using Eq (7), IoMT-based physical sensor-based health

monitoring systems outperform conventional methods. Continuous and discontinuous medical and biometric data create a response space for the data points. Using the BICS-AI model, this research provides a safe healthcare industry for IoMT sensor networks using a healthcare data protection and privacy model. Using blockchain technology, this model aims to improve healthcare security.

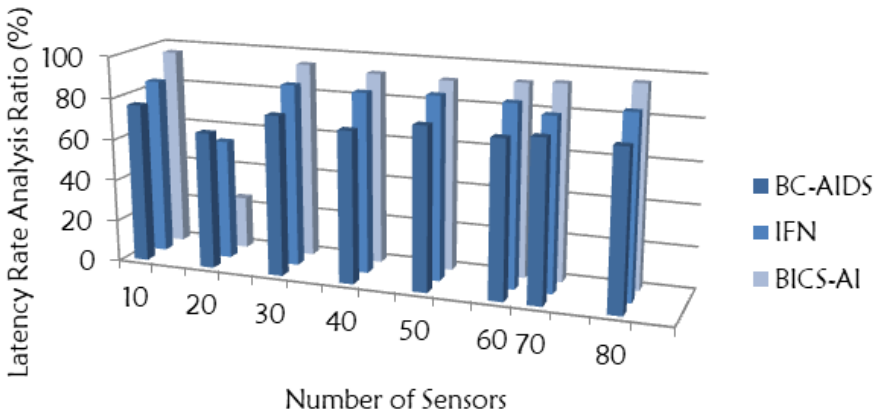

Figure 8. Comparison of latency aate.

4.5. Accuracy ratio (%)

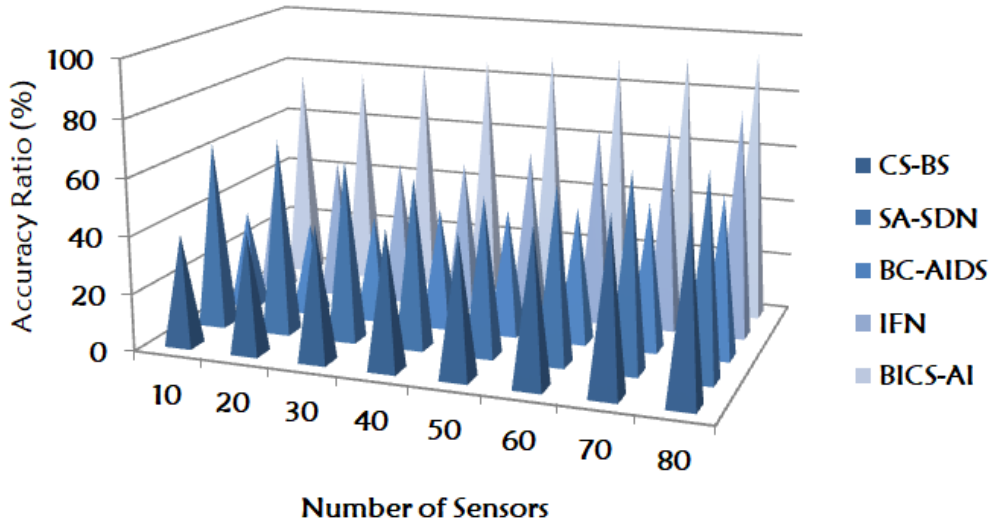

Figure 9. Comparison of accuracy ratio (%).

Patients are better served by medical records that are complete and accurate. Maintaining patient confidentiality and safely archiving medical information are necessary when providing medical care. For a considerable time, the general public has been worried about the safe storage and use of sensitive medical information; however, this problem may now be handled using blockchain technology. Blockchain technology is decentralized, verifiable, and incorruptible, making it an ideal candidate for

storing sensitive medical information. Figure 9 illustrates the precision that may be achieved using blockchain technology for monitoring patient health.

The pulse and temperature of the body are each measured three times to ensure accuracy. Blockchain technology makes it possible to recover patients' medical records promptly and accurately. An advanced computer analyzes blood pressure readings to determine whether or not they are low, normal, or high. The results of this analysis are then shown on a screen. The chance of the doctor's physical condition is evaluated after doing research that involves looking at the doctor's overall health indicator's dispersion in the higher dimensional space.

4.6. Data transmission ratio (%)

The patient data and blockchain models perform much better than the others compared to the amount of data traded to update medical records. This illustrates that the throughput for data transmission offered by the blockchain platform is superior to that offered by a client/server network. The leader nodes in a network are responsible for boosting the amount of data exchange by broadcasting the applications necessary to update medical records to all other nodes throughout the network. Figure 10 discusses the data transfer ratio of other technologies currently in use.

Additional data processing can occur because every peer node on the network broadcasts the ciphertext of a block in real-time to all of the other nodes in the network. Compared to the client/server design, blockchain technology can transport around ten times the amount of data.

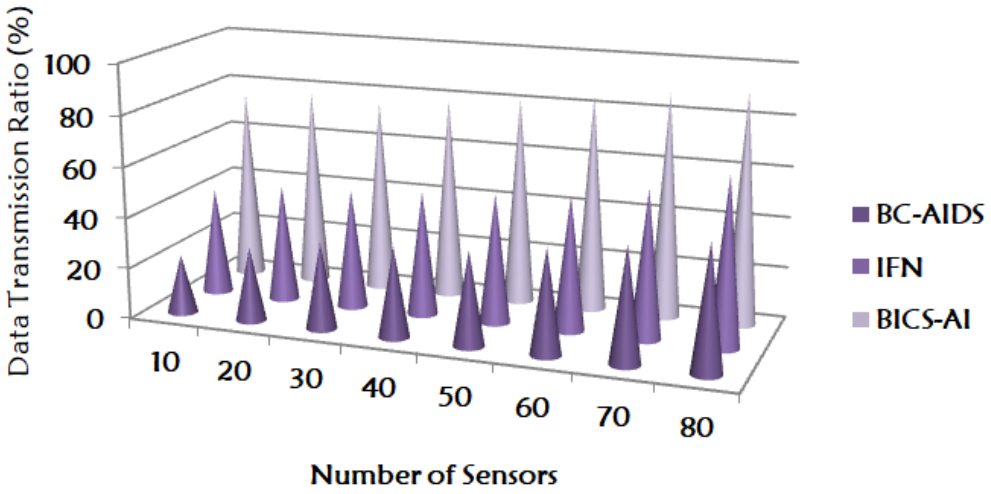

Figure 10. Comparison of data transmission rate (%).

4.7. Overall comparison of the BICS-AI approach

Regarding physical health monitoring systems, the BICS-AI approach outperforms the ACP method in terms of standardization and effectiveness. In terms of maintaining standards and efficacy over an estimated number of iterations based on Eq (13), IoMT-based physical sensor-based health monitoring systems outperform other conventional methods of monitoring intervals as shown in Table 3.

Table 3. Result analysis of the BICS-AI approach.

Performance Metrics	CS-BS	SA-SDN	BC-AIDS	IFN	BICS-AI
Overall performance (%)	67.6	77.4	86.9	84.1	89.2
Security performance (%)	73.1	73.9	73.9	72.1	96.4
Security Rate (%)	65.1	65.2	77.1	75.9	94.8
Latency Rate (%)	13.1	14.9	8.6	13.9	5.1

Comparing model (BICS-AI) performance metrics with traditional IoMT healthcare data security approaches for improved precision, reliability, security, and latency are all the new model's advantages. The experimental results show that the proposed system has a 94.8% security rate, a security performance of 96.4%, a success rate of 89.9%, and a 5.1% latency rate compared to traditional methods.

5. Conclusions

Blockchain technology has the potential to improve the infrastructure supporting healthcare services significantly. In this article, several frameworks and methods to assess the performance of such systems and potential improvements to present shortcomings in healthcare system design are investigated as potential applications of blockchain technology. To accurately prescribe medicine to patients access to their medical history is important. IoMT healthcare data can be protected by the built-in security features of blockchain, such as heterogeneous encrypted communications methods and digital signatures. Another way to improve cybersecurity is integrating blockchain with currently used safety measures like authorization and access control providers in our proposed system (BICS-AI). It is possible to use IoT sensors to automatically activate auto-updating programs to ensure that IoT instrument software is always updated. Works presenting a prototype that utilizes the blockchain concept in healthcare now have plans to produce a fully operational system shortly for user testing with actual patients. The capacity to communicate patient information through a secure channel is subject to several restrictions regarding the process's reliability, efficiency, and consistency. The experimental results show that the proposed system has a 94.8% security rate, a security performance of 96.4%, a success rate of 89.9%, and a 5.1% latency rate compared to traditional methods.

Acknowledgments

The authors extend their appreciation to the deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number (IFP-2020-78).

Conflict of interest

The authors declare there is no conflicts of interest.

References

1. B. Alqaralleh, T. Vaiyapuri, V. S. Parvathy, D. Gupta, A. Khanna, K. Shankar, Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment, *Pers. Ubiquitous Comput.*, **5** (2021). https://doi.org/10.1007/s00779-021-01543-2

2. O. Diekmann, M. Gyllenberg, H. Huang, M. Kirkilionis, J. A. J. Metz, H. R. Thieme, On the formulation and analysis of general deterministic structured population models. II. Nonlinear theory, *J. Math. Biol.*, **43** (2001), 157–189. https://doi.org/10.1007/s002850170002

3. S. Marchesseau, H. Delingette, M. Sermesant, R. Cabrera-Lozoya, C. Tobon-Gomez, P. Moireau, et al., Personalization of a cardiac electromechanical model using reduced order unscented Kalman filtering from regional volumes, *Med. Image Anal.*, **17** (2013), 816–829. https://doi.org/10.1016/j.media.2013.04.012

4. A. K. Das, B. Bera, D. Giri, AI and blockchain-based cloud-assisted secure vaccine distribution and tracking in the iomt-enabled covid-19 environment, *IEEE Internet Things Mag.*, **4** (2021), 26–32. https://doi.org/10.1109/IOTM.0001.2100016

5. A. Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal, F. M. Almansour, Blockchain-assisted secured data management framework for health information analysis based on the Internet of Medical Things, *Pers. Ubiquitous Comput.*, **19** (2021), 1–4. https://doi.org/10.1007/s00779-021-01583-8

6. S. Razdan, S. Sharma, Internet of Medical Things (IoMT): overview, emerging technologies, and case studies, *IETE Tech. Rev.*, **39** (2022), 775–788. https://doi.org/10.1080/02564602.2021.1927863

7. M. Elsayeh, K. A. Ezzat, H. El-Nashar, L. N. Omran, Cybersecurity architecture for the Internet of Medical Things and connected devices using blockchain, *Biomed. Eng. Appl. Basis Commun.*, **33** (2021), 2150013. https://doi.org/10.4015/S1016237221500137

8. A. Sharma, Sarishma, R. Tomar, N. Chilamkurti, B. G. Kim, Blockchain-based smart contracts for the Internet of Medical Things in e-healthcare, *Electronics*, **9** (2020), 1609. https://doi.org/10.3390/electronics9101609

9. B. S. Egala, A. K. Pradhan, V. R. Badarla, S. P. Mohanty, Fortified-Chain: a blockchain-based framework for security and privacy assured Internet of medical things with effective access control, *IEEE Internet Things J.*, **8** (2021), 11717–11731. https://doi.org/10.1109/JIOT.2021.3058946

10. X. Li , B. Tao, H. N. Dai, M. Imran, D. Wan, D. Li, Is blockchain for the Internet of Medical Things a panacea for COVID-19 pandemic? *Pervasive Mob. Comput.*, **75** (2021), 101434. https://doi.org/10.1016/j.pmcj.2021.101434

11. M. Wazid, A. K. Das, S. Shetty, M. Jo, A tutorial and future research for building a blockchain-based secure communication scheme for the Internet of intelligent things, *IEEE Access*, **8** (2020), 88700–88716. https://doi.org/10.1109/ACCESS.2020.2992467

12. M. Wazid, A. K. Das, S. Shetty, M. Jo, Blockchain-enabled internet of medical things to combat COVID-19, *IEEE Internet Things Mag.*, **3** (2020), 52–57. https://doi.org/10.1109/IOTM.0001.2000087

13. R. Kumar, R. Tripathi, Towards design and implementation of security and privacy framework for Internet of medical things (iomt) by leveraging blockchain and ipfs technology, *J. Supercomputing*, **77** (2021), 7916–7955. https://doi.org/10.1007/s11227-020-03570-x

14. R. A. Rayan, C. Tsagkaris, *Blockchain-Based IoT for Personalized Pharmaceuticals*, in *Internet of Medical Things*, (2021), 51–62. https://doi.org/10.1201/9780429296864-4

15. P. P. Ray, D. Dash, K. Salah, N. Kumar, Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases, *IEEE Syst. J.*, **15** (2020), 85–94. https://doi.org/10.1109/JSYST.2020.2963840

16. M. A. Rahman, M. S. Hossain, An internet of medical things-enabled edge computing framework for tackling COVID-19, *IEEE Syst. J.*, **8** (2020), 15847–15854. https://doi.org/10.1109/JIOT.2021.3051080

17. W. Meng, W. Li, L. Zhu, Enhancing medical smartphone networks via blockchain-based trust management against insider attacks, *IEEE Trans. Eng. Manage.*, **67** (2020), 1377–1386. https://doi.org/10.1109/TEM.2019.2921736

18. P. A. Catherwood, D. Steele, M. Little, S. McComb, J. McLaughlin, A community-based IoT personalized wireless healthcare solution trial, *IEEE J. Transl. Eng. Health Med.*, **6** (2021), 1–13. https://doi.org/10.1109/JTEHM.2018.2822302

19. H. Liao, Z. Zhou, X. Zhao, L. Zhang, S. Mumtaz, A. Jolfaei, et al., Learning-based context-aware resource allocation for edge-computing-empowered industrial IoT, *IEEE Internet Things J.*, **7** (2019), 4260–4277. https://doi.org/10.1109/JIOT.2019.2963371

20. S. Chakraborty, V. Bhatt, T. Chakravorty, Impact of IoT adoption on agility and flexibility of healthcare organization, *Int. J. Innovative Technol. Exploring Eng.*, **8** (2019), 2673–2681. https://doi.org/10.35940/ijitee.K2119.0981119

21. X. Chen, M. Ma, A. Liu, Dynamic power management and adaptive packet size selection for IoT in e-Healthcare, *Comput. Electr. Eng.*, **65** (2018), 357–375. https://doi.org/10.1016/j.compeleceng.2017.06.010

22. A. Choi, H. Shin, Longitudinal healthcare data management platform of healthcare IoT devices for personalized services, *J. Universal Comput. Sci.*, **24** (2018), 1153–1169. Available from: https://scholarworks.bwise.kr/gachon/handle/2020.sw.gachon/5295.

23. M. M. Dhanvijay, S. C. Patil, Internet of Things: A survey of enabling technologies in healthcare and its applications, *Comput. Networks*, **153** (2019), 113–131. https://doi.org/10.1016/j.comnet.2019.03.006

24. O. I. Khalaf, G. M. Abdulsahib, N. A. Zghair, IOT fire detection system using sensor with Arduino, *AUS*, **26** (2019), 74–78.

25. B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, K. Mankodiya, Towards fog-driven IoTeHealth: promises and challenges of IoT in medicine and healthcare, *Future Gener. Comput. Syst.*, **78** (2018), 659–676. https://doi.org/10.1016/j.future.2017.04.036

26. G. García, P. Sánchez-Alonso, C. E. M. Marín, Visualization of information: a proposal to improve the search and access to digital resources in repositories, *Ing. Invest.*, **34** (2014), 83–89. https://doi.org/10.15446/ing.investig.v34n1.39449

27. M. M. Islam, A. Rahaman, M. R. Islam, Development of smart healthcare monitoring system in IoT environment, *SN Comput. Sci.*, **1** (2020), 185. https://doi.org/10.1007/s42979-020-00195-y

28. V. E. Sathishkumar, C. Shin, Y. Cho, Efficient energy consumption prediction model for a data analytics-enabled industry building in a smart city, *Build. Res. Inf.*, **49** (2021), 127–143. https://doi.org/10.1080/09613218.2020.1809983

29. Y. S. Jeong, S. S. Shin, An IoT healthcare service model of a vehicle using implantable devices, *Cluster Comput.*, **21** (2018), 1059–1068. https://doi.org/10.1007/s10586-016-0689-z

30. W. Li, C. Jung, J. Park, IoT healthcare communication system for IEEE 11073 PhD and IHE PCD-01 integration using CoAP, *KSII Trans. Internet Inf. Syst.*, **12** (2018), 1396–1414. https://doi.org/10.3837/tiis.2018.04.001

31. M. O. Lawal, Tomato detection based on modified YOLOv3 framework, *Sci. Rep.*, **11** (2021), 1447. https://doi.org/10.1038/s41598-021-81216-5

32. W. Khan, K. Raj, T. Kumar, A. M. Roy, B. Luo, Introducing urdu digits dataset with demonstration of an efficient and robust noisy decoder-based pseudo example generator, *Symmetry*, **14** (2022), 1976. https://doi.org/10.3390/sym14101976

AIMS Press