The Journal of Supercomputing (2025) 81:271
https://doi.org/10.1007/s11227-024-06782-7

BDLT-IoMT—a novel architecture: SVM machine learning for robust and secure data processing in Internet of Medical Things with blockchain cybersecurity

Abdullah Ayub Khan[1] · Asif Ali Laghari[2] · Abdullah M. Baqasah[6] · Rex Bacarra[4] · Roobaea Alroobaea[3] · Majed Alsafyani[3] · Jamil Abedalrahim Jamil Alsayaydeh[5]

Accepted: 27 November 2024

Abstract

The integration of artificial intelligence (AI) has caused information and communication technology (ICT) to undergo a number of recent rapid fluctuations. These changes have primarily affected the areas of management, end-to-end device interconnectivity, resource organization, communication, networking, and application-related aspects of ICT. Owing to the complex structure of applicational connectedness, evaluating each of the aforementioned opportunities concurrently reflects the idea of heterogeneity. The association of multiple end devices, particularly in interoperable space, integrity, privacy protection, security, provenance, and the massive volume of everyday media data generated in the modern healthcare setting could also provide significant issues. To address these issues, decentralized, secure, economical resource optimization, and intelligent network activities and organization are necessary. Blockchain technology plays a crucial role in providing distributed storage data organization, sharing, and exchange for automated decision-making, privacy, and security in AI-enabled machine learning (ML) models. However, machine learning models—support vector machine, in particular—have a significant impact on the growth of distributed consortium networks and the exchange of information among connected nodes, resolving issues with resource management, scalability, and data processing. By resolving the three main problems of seamless data integrity, peer-to-peer communication between nodes, and infrastructure security, we provide a novel interoperable technique in this proposed architecture. The approach is unique, as demonstrated by the simulation-based results, which display huge differences of 1.37%, 1.56%, and 1.87%, respectively. The background for the evaluation consists of the following three areas: (i) infrastructure security to protect automated decision-making; (ii) integrity between smooth data sharing and exchange; and (iii) network resource optimization to enable smooth communication across heterogeneous devices.

Extended author information available on the last page of the article

Published online: 10 December 2024

Keywords Internet of Medical Things (IoMT) · Internet of Things (IoT) · Machine learning (ML) · Support vector machine (SVM) · Blockchain · Cybersecurity

1 Introduction

The innovations brought about by the convergence of the Internet of Things (IoT) with the healthcare sector have resulted in a sharp increase in interest in the Internet of Medical Things (IoMT) over the past ten years. The cyber-physical system (CPS) is essential for balancing this equation since it offers a multi-dimensional scheme that primarily takes into account the industrial prospects across the network [1, 2]. Create a budget-friendly atmosphere for electronic healthcare systems as a result. In fact, cyber-physical systems can be used in pharma, pharmaceutical, telehealth, and other healthcare applicational environments [1–3]. Here is a highlighted list of popular run-time programs [4, 5]: (i) HealthTap; (iv) MyChart; (v) Pocket Pharmacist; (ii) Medisafe Medication; and (iii) Teladoc Health. But in terms of applicational connectivity, telemediation, virtual diagnosis and cost-effectiveness, and stakeholder registration verification and validation, the evolution of cyber-physical systems in the healthcare sector makes a significant impact. Moreover, this technology integrates digital-to-analog and analog-to-digital components, as well as logical and physical systems working together to manage intercommunication transmission [4, 6]. Actuators, wireless network sensors, and networking modules are all part of the cyber-physical system network, which aids in the management of suitable automation, particularly in the healthcare platforms [5, 6].

In general, IoT requires integral support of cyber-physical systems in a healthcare environment, which is considered a complex prospect where the external operations are performed on cyber applications, as shown in Fig. 1. Undoubtedly, this integrated manner not only provides information and communication technology (ICT) progressive. On the other side, it also helps in more positive fluctuation in the acquisition of data transmission, management, organization, preservation, and optimization. On the other end, cybersecurity is considered in terms of major challenging issues, where vulnerability can be measured, such as intrusion hazards, malicious attacks, or attempts of malicious insiders [4, 6]. These days, the experts of CPS are highly concerned about the privacy and security of the

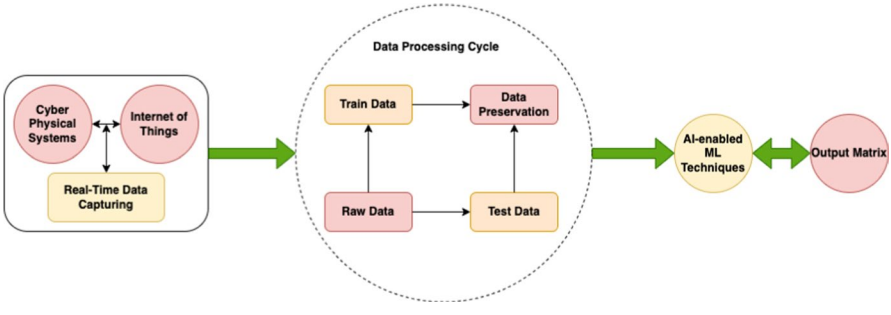

Fig. 1 Current environment of data processing using cyber-physical systems and Internet of Things

technology, especially in collaborative prospects with electronic healthcare. However, the intrusion detection system (IDS) performs a vital role, where intrusion detection is one of the key applications that maximize the integrity of the system. Recently, most of the IDS has been employed for effective and efficient prevention of malicious attacks [6, 7]. The working operation is to classify anomalies, where IDS is categorized into two parts, such as identifying misuse predictions and analysis of anomaly occurrence in the running environment. In both aspects, the feature of similarities in terms of malicious attacks examination, which helps in misuse prediction and evaluation. Nowadays, every auditable information requires an authenticated dataset, which needs to be associated with it in order to examine the impact of intrusions [6–8]. In fact, a misuse detector generates a minimized effect in the function point. However, the detector has different types of challenging prospects, like working with another line of defense, identifying intrusions that are unable to be adopted in the evaluation of security procedures, and no role of safeguard integration.

On the other end, the detection of anomalies in IDS is constructed to evaluate a routine profile behavior with a categorized one, where marching the usual behavior and separate unusual activities, such as malicious attacks [7–9]. Comparatively, IDS-enabled anomaly detection performs better but is not accurate enough to say that it finds unknown malicious activity with a hundred percent ratio. However, this technology interconnects a broad range of ubiquitous devices, where the management of computational resources fluctuates, along with the cycle of battery consumption, transmission protocols, software connectivity, and operation of deliverance [8, 9]. Such type of device heterogeneity makes this system more limited, including the placement of security challenges, and the design of the surface raises the rate of attacks in the recent environment. Whereas the adaptation of blockchain technology makes these differences more lesser in terms of providing a distributed environment with node heterogeneity connectivity [8, 10]. Due to this, the system can fetch overall vulnerability occurrences and resist them for future endorsement.

In the recent healthcare environment, machine learning (ML) techniques have been presented for examining patterns from collected data, and then effectively identifying and detecting points of interest in terms of cybercriminal activities effectively [10, 11]. However, it affects, while loading a large number of datasets, where the efficiency scale and their point of revealed prospects cannot be accomplished the mark, including a low performance for identifying malicious attacks when nodes of the network are in distributed mode. On the other side, deep learning (DL) models stimulate such identification patterns in a complex way, but the results count as sophisticatedly [11, 12]. Although the complex network of DL requires more computation power, experts can rely on the generated results due to its reliability and efficiency. In fact, the experts of AI majorly focus on the investigation of the malicious ubiquitous; in order to provide a novel design that fulfills a trustworthiness environment, which supports cybercrime-enabled behavioral profiling analysis [13–15]. In addition, node reputation is evaluated as another prospect that needs to be resolved while applying a list of attacks detection and recognition because it violates the Euclidean distance measurement between profiles.

1.1 Research motivation and objectives

This study examines all of these difficult possibilities, but it primarily focuses on creating a secure infrastructure for IoMT. To ensure privacy, security, and automated decision-making using blockchain and machine learning, data must be stored, shared, and organized in a distributed node-to-node environment. This paper proposes a novel concept for a distributed consortium network in which member nodes build intercommunication. The ML-enabled SVM algorithm has a significant impact on this process. SVM's primary responsibility during interconnectivity is to handle crucial situations including data processing, resource management, scalability, and security. This article thus discusses three important issues that arise in the current e-healthcare interoperable environment: peer-to-peer communication between nodes connected to the same network, easy data protection and confidentiality maintenance, and the general security of the health infrastructure. Through the proposed architecture, this study offers a novel, interoperable method to preserve these. The main contribution of this research is expounded upon in the following definition of the research objectives and contributions argument:

- A list of research gaps that are assessed throughout the problem-solving process is provided in this publication. These gaps have been compiled from a variety of reputable academic research publisher sources, including IEEE, ACM, Elsevier, Springer, Wiley, and Taylor & Francis.
- "BDLT-IoMT" is a suggested secure architecture for the Internet of Medical Things (IoMT) that combines ML and blockchain DLT. Furthermore, one of the main functions of this suggested architecture is that blockchain is essential for supplying training data for machine learning models, like support vector machines (SVMs), which in particular seek to arrange, distribute, and trade data from dispersed storage in order to ensure security, protection, and automation in decision-making.
- To facilitate communication between participating nodes and handle both technologies simultaneously, a consortium network is created with the goal of offering a channel for data processing, resource management, scalability, and security.
- As a result, the suggested design offers peer-to-peer communication between nodes, seamless data integrity, and infrastructure security while addressing issues with platform interoperability.
- A list of issues related to the deployment of distributed applications (DApps) is provided, together with a justification statement and an explanation of potential remedies.

1.2 Outline of this research work

The further description of this paper is aligned and presented as follows: In Sect. 2, the detailed argument based on exiting blockchain applications running, infrastructural weakness, and protocols, along with the provisional statement of IoMT

integrations are discussed. However, Sect. 3 presents the working objective of the proposed study, along with the activities of executions. The brief discussion of the proposed architectural simulations and results in Sect. 4, whereas a list of implementation, deployment, and further research gaps that have emerged in the organization of this work in Sect. 5. At the end, this paper concludes with the well-defined statement of conclusion in Sect. 6.

2 Related work

Recently, most of the running systems of e-healthcare considered as highly consumed energy resources due to the association of IoT and connectivity. Undoubtedly, it fulfills a basic form of industrial healthcare ecosystem but requires more in-depth investigation to overcome it. Considering the ad hoc nature of this technology is one of the reasons that the emergent list of threats needs to be captured and estimated in real time, including botnets [16]. This may be raised while collaborating edge devices with the host IoT devices for designing successful cyber-physical systems for making cybersecurity prospects that minimize transmission overhead and energy consumption. However, the existing proposal received on the development of an effective trust-based e-healthcare platform that follows the concept of autonomous vehicular network [16, 17]. It is one of the first trusted proposal received by the technology in 2021, which aim to assist associative methods of AI for autonomous driving vehicles, where assisted data can be exploited for calculating the exact trust values. After the integration of reinforcement learning, these healthcare-based autonomous driving vehicles stimulate a self-warning alert and report vulnerabilities. However, further details regarding the technological developments are addressed in the next subsections as follows:

2.1 Existing blockchain applications, infrastructure, and protocols

These days, the development of blockchain distributed ledger technology (BDLT) creates new paradigms, especially the topology of healthcare network management which has changed, including stakeholder registration, adding new data, and updating records in a decentralized manner [18, 19]. Undoubtedly, blockchain enhances information security and privacy procedures, integrity, confidentiality, trustworthiness, provenance, transparency, and platform interoperability. While distributed nodes are connected like patients are interconnected in the designed ecosystem networks via ubiquitous devices. However, the bibliometric analysis of blockchain in the health industry is quite limited. It is because a rate of growing bodies examines a potential fluctuation received by this collaborative technology. During the investigation, we found a lack of technical improvement received by the blockchain-enabled healthcare technology, majorly because of the high theoretical description available compared to real-time implementation. However, Table 1 presents an investigational report that highlights what factors still emerge as current research gaps, which can be transformed into future developments and maybe research trends. The evaluation

Table 1 Current research gaps on the Internet of Medical Things environment and the role of blockchain

List of References	Major research gaps analysis	A list of research contributions	Targeted research objectives	Answered research question
[20]	Platform interoperability limitation	Proposal of modular architectural design	Multi-stakeholder authentication	This paper addressed a multi-stakeholder registration verification and validation of protocols like ECMQV-MAC
[21]	Limitation in sizing of node during transmission	Cross-platform-based node interconnectivity	Distributed storage management using Filecoin	The author of this paper presented a solution for IoMT data management, where the role of AI-enabled ML-based artificial neural network is mentioned
[22]	Distributed channels design for intercommunication, including implicit and explicit	Two intercommunication channels are designed, on-chain and off-chain over consortium network	A novel proposal is presented, named CARE	This paper proposed a carbon-aware computing environment for blockchain-enabled Internet of Medical Things-based data organization and optimization
[23]	Hash calculating and hashing organization problem	Presented a list of most occurrence attacks in the current IoMT environment	Revolutionaries AI in IoMT for more sophisticated developments	In this paper, the author highlighted a list of cyberattacks that involved in AI-enabled IoMT environment, along with a discussion of countermeasures
[24]	Technological integration requirement and fulfillment is addressed	Resource management and allocation hierarchy is proposed	Maintaining heterogeneous node-to-node data sharing and exchange	The role of federated learning in healthcare is discussed, where the integration of blockchain impacts the IoMT platform in terms of data management, privacy, and security throughout distributed environments
[25]	Efficient transaction processor's scheduling hierarchy and management related challenges	A secure node-to-node interconnectivity is proposed	Collaborative approach of blockchain and cryptography	This paper presents enhanced IoMT data communication for smart healthcare platforms using blockchain and cryptographic algorithms, especially hashing

metrics of this table are mentioned as follows: (i) a list of references, (ii) a major research gaps analysis, (iii) a list of research contributions, (iv) targeted research objectives, and (v) answered research questions.

2.2 Security hierarchy in Medical Internet of Things (IoMT) and the role of machine learning

Recent developments have shown that healthcare data management systems encounter problems like data availability, central storage, grant access, and operational controls. But not fulfill the requirements of advanced digital technology, including integrity, traceability, provenance, data transparency, immutability, flexible access controls, audit, trustworthiness, and privacy protection. However, the revolution of BDLT resolves the mentioned challenges, but there is a need to specify resource usage due to high computing requirements for managing a distributed environment; this technology suffers in terms of balancing the allocation of computational resources [26–29]. Undoubtedly, blockchain technology establishes confidence in the health hierarchy for data organization by enabling the tracking of changes from a collection of data sources and related forms. Current case studies elaborate on the importance of blockchain as a range of diverse fulfillment of health applications. The need is to address critical the concept of rescheduling the limited capability of computational resource optimization so that blockchain can be adapted successfully in every domain of the health industry. To overcome these challenging prospects, this paper investigates the factors affecting of possible adaptation of blockchain and their role in cost-efficient data management and organization is highlighted as follows:

- Use of Hyperledger technology
- Design cost-effective function in smart contracts
- Customize consensus mechanisms
- Define blockchain protocols
- Association of NuCypher Re-Encryption mechanism
- Immutable storage and connectivity
- Specify communication channels

3 Research material and methodology

3.1 Problem description, formation, and notations

With the use of SVM, we can handle the issues of data processing, resource management (especially computational cost), and scalability, as shown in Fig. 2; due to this, we design a function that follows the mentioned constraints, such as the calculation of the distance of data points, reflect false negative and false positive values, and the margin data values. Here we explain this in a mathematical manner:

$f(a) = w * A + b' \leq -1$; for all false positive.

$f(b) = w * B + b' \geq 1$; for all false negative. Where two constraints are taken together, we can achieve to simplify the calculation of both constraints into 1. Let us assume the negative value y = − 1 and the positive value y = 1, as mentioned in Table 2.

In order to evaluate every point in terms of classifying correctly, the equation is designed as follows:

$$y'\left(w' * (A * B) + b'\right) \geq 1$$

To maintain computational resources, the total cost of data processing is scheduled with this equation as follows:

$$(a2 - a1) * (w'/w)$$

where $(a2 * w' - a1 * w')/w$

Here a2 and a1 are the variables that define positive data processing hierarchy and loss function in accordance with the designed resource limitations as follows: $y' * (2 * (f(a) + f(b)) = 1$

For positive data processing, y must be equal to 1. Here, we define the possibilities of memory scalability during processing as follows: $1 * (w * a1 + b') = 1$;where $w' * a1 = 1 - b'$;

By adding both equations together to achieve data optimization, along with organization and management (as shown in Fig. 3), we present the equation as follows:

$$\left(\left(1 - b'\right) - (-b' - 1)\right)/w$$

$$\frac{\left(1 - b'\right) + \left(b' + 1\right)}{w} = \frac{2}{w} = f(a)$$

Hence, the maximum scalability that the proposed architecture can be handled is defined as follows:

$$\max\left(w'', b''\right) = \frac{2}{w} \text{such that } y'(w' * (A * B) + b')'' \geq 1$$

However, the minimization of memory scalability is integrated and illustrated as follows:

$$\min\left(w'', b''\right) = \frac{w}{2} + (\text{Sum of value c})$$

Effective data classification, especially in binary classification tasks, is the SVM model's primary strength. When combined with blockchain, the model benefits from the additional security, transparency, and trust it provides, fortifying and improving the dependability of the entire data pipeline from training to deployment. The security and verifiability of the decisions and updates made by SVM-based systems are additionally ensured by the decentralized and immutable nature of blockchain.

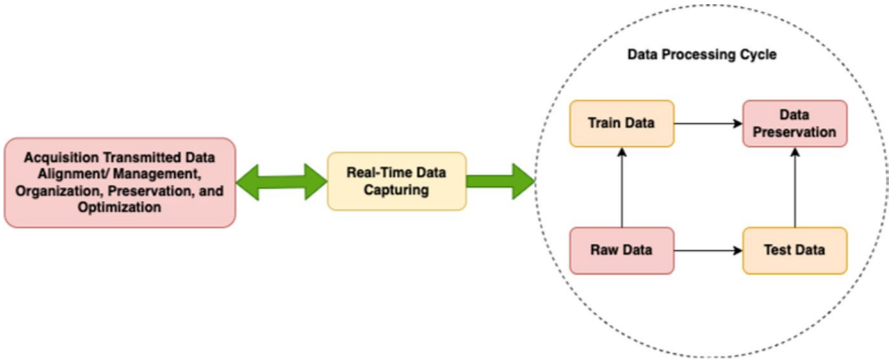

Fig. 2 Working cycle of data processing and memory management

3.2 Proposed architecture and working sequences

A proposed distributed application (DApp) for Fig. 3 serves as a mediator between several stakeholders and the BDLT infrastructure. Maintaining privacy security procedures when Internet of Medical Things (IoMT) transactions are planned for transmission in an economical way, which is chosen by the system's patients, is the main goal of such an implementation. But in order to ensure seamless transmission, this suggested BDLT-IoMT created a consortium network, with an administrator tasked with looking into any instances of fault tolerance that may arise during the processing cycle. Conversely, as illustrated in Fig. 3, two distinct channels—referred to as off-chain and on-chain—are suggested in order to rearrange the list of explicit and implicit transactions.

Table 2 Notations

Symbols	Elaboration
f(a)	Function that evaluates data processing sequences
A	False positive
f(b)	Function that evaluates data processing scheduling for minimize resource consumption
B	False negative
b'	Bias value
W	Weight
y	Output constraint
y'	Change in output constraint
w'	Change in weight
a	Fluctuation receives
w''	Final weight update
b''	Final bias update
c	Constant variable

The BDLT-IoMT architecture, which combines blockchain technology with AI-enabled machine learning to avoid cyberattacks, is presented in this section and is illustrated in Fig. 4. Three sections cover the explanation of this proposed work: (i) ML-enabled SVM association and implementation; (ii) blockchain infrastructure solution; and (iii) IoT connectivity to facilitate health transactions. The first section of our proposed work relies heavily on ML-enabled SVM. Here, we performed data scheduling, resource management, and scalability tasks so that real-time captured data could be extracted, examined, filtered, aggregated, analyzed, and stored in an immutable blockchain that was predefined, like InterPlanetary File Storage (IPFS), as illustrated in Fig. 3. As a result of its implementation, the suggested BDLT-IoMT is able to meet the following three main restrictions (as shown in Fig. 4): infrastructure security (i) to protect automated decision-making; integrity (ii) to allow for smooth data sharing and exchange; and network resource optimization (iii) to enable smooth communication between disparate devices.

But as Fig. 5 illustrates, the technology behind blockchain is broken down into nine distinct sub-components: node interconnectivity, REST API, intercommunication channels, states, chaincode, consensus mechanism, proof-of-work (PoW) integration, and digital signature. The transaction processor manages every step of the BDLT hierarchy that has been described. Node interconnectivity offers a framework for connecting various nodes based on block size, where blocks are derived from transaction data, size, public key, hashing (n − 1) SHA-256, and hashing (n). REST API, on the other hand, plans transactions as they are completed, as mentioned in Table 3. Conversely, as was already said, intercommunication can be divided into two categories: on-chain and off-chain. The BDLT infrastructure (predefined) manages each individual transaction's state when a new transaction is listed.

Table 3 provides a concise description of the consensus policy and chaincode working objective along the digital signature procedure.

4 Simulations and results

The originality of the proposed work is discussed in this section with regard to the presentation of simulations and their distinct outcomes. To test the overall infrastructural security with regard to data preservation, we have divided the simulations

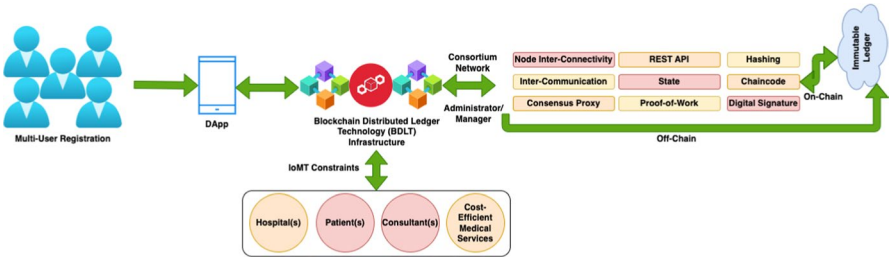

Fig. 3 Cycle for achieving data optimization and memory hierarchy

into six distinct scenarios. These include the working cycle of BDLT-IoMT evaluation—false positive (Tests 1 and 2), BDLT-IoMT evaluation—false negative (Tests 1 and 2), the working cycle of BDLT-IoMT resource management (Test 1), the working cycle of BDLT-IoMT resource management (Test 2), and the overall infrastructural security test with regard to data protection throughout. Prior to commencing these tests, the following prerequisite must be satisfied:

- System requirement—13th generation core i7 vPro processor is used, along with the 3.0 GHz clock speed.
- 32 GB main memory is installed with the connectivity of 1 TB SSD.
- Integrated/shared GPU is mandatory.
- 10–100 Mbps Network bandwidth is required.
- Software requirement—JavaScript installation, Truffle, Ganache, visual studio code, and additional plugins to support JavaScript program execution is mandatory.

Figure 6 illustrates the simulation result of the proposed BDLT-IoMT working cycle in terms of data processing. This scheduled test is based on both perspectives,

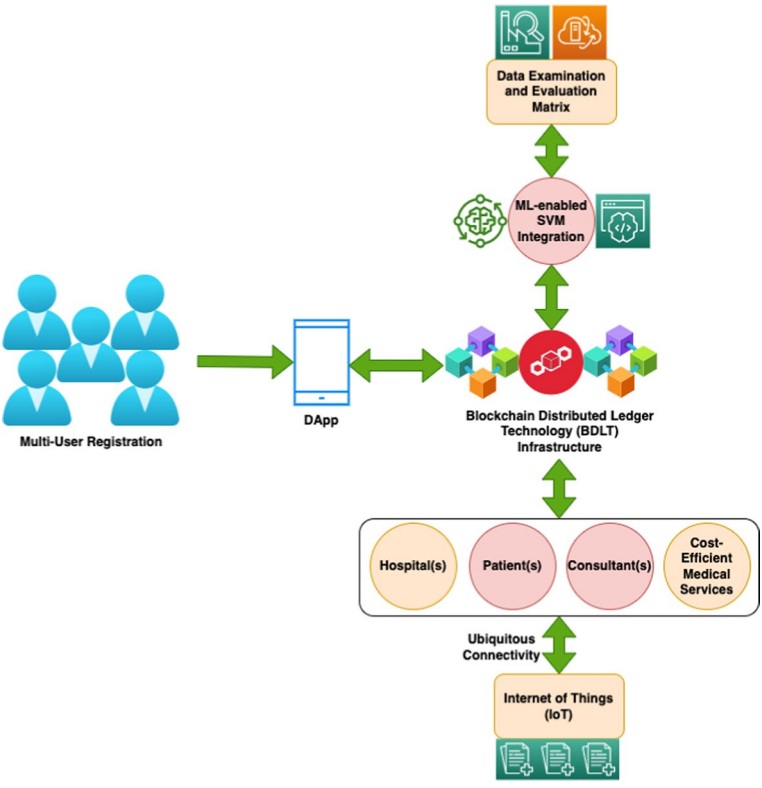

Fig. 4 Proposed BDLT-IoMT architecture

like false positive—Test 1 (as shown in Fig. 6a) and false negative—Test 1 (as shown in Fig. 6b), where the metric of evaluation is the fluctuation received in the data processing cycle with respect to scheduling data per second (s). However, the analytics of false positive is the sum of 277 cycles per 3511 s, which is equal to 0.0788 cycles of data investigated per second. The uniqueness of these results shows that the proposed BDLT-IoMT is processing data better as compared to the previously published methods [30–33].

Figure 7 shows the result of the proposed BDLT-IoMT simulations, which are based on the data processing cycle and related hierarchy. The test is conducted on two points of manner, like false positive—Test 2 (as shown in Fig. 7a) and false negative—Test 2 (as shown in Fig. 7b), where the metric of evaluation is the fluctuation received in the data processing cycle with respect to scheduling data per second (s). However, the analytics of false positive is the sum of 256 cycles per 2503 s, which is equal to 0.1022 cycles of data investigated per second. (Where the meaning of 2 is the second test, P is the false positive, and N is the true negative.)

The overall infrastructural security test is presented in Fig. 8, where evaluation is conducted twice to investigate the successful deployment of the proposed BDLT-IoMT, which mainly highlights the role of blockchain-enabling technology for data preservation prospects. The examination metric of this simulation is the sum of the cycle of resource management used with respect to data management and preservation slots delivered per second(s).

Decentralized machine learning environments, where preserving data integrity is crucial, were considered in the simulation. This represents real-world applications where data provenance and tamper resistance (as guaranteed by blockchain) are crucial, including those in the financial, legal, or medical records sectors. By ensuring that the simulations account for constraints, real-world scenarios, and data complexities, we believe that the results can be safely extended to real-world settings. We demonstrate that the simulated results translate well into broader, real-world contexts with our plans for field testing and matching simulation conditions with real applications.

However, Fig. 9 illustrates the simulation test of the complete cycle of computational resource consumption (Test 1), where the investigation metrics is the sum of fluctuation received in resource management during scheduling data and related hierarchy with respect to time (s). Whereas the total number of fluctuations received is 221 cycles in the 1500 s, which is a total of 0.1473 cycle/s. On the other side, the result of Fig. 10 (Test 2) is the sum of fluctuations received, is 243 cycles in 727 s, which is a total of 0.3342 cycle/s.

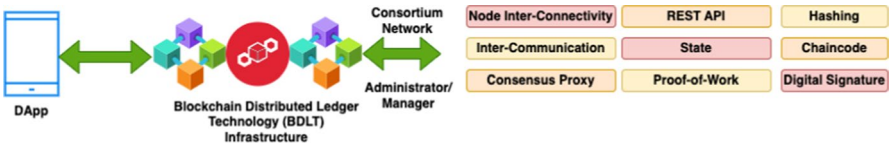

Fig. 5 Steps of BDLT

Table 3 Pseudocode of the proposed BDLT-IoMT

```
Regulatory and Compliances: Administrator manages the occurrence of fault tolerance;
Immutable preservation structure is associated (as IPFS is integrated);
Initial Declarations:
data scheduling,
dS();
resource management,
rM();
scalability,
sC();
captured data,
cD();
extract,
eX();
examine,
eY();
filter,
fI();
aggregate,
aG();
analysis,
aY();
preserved,
pS();
stakeholder registration,
sR();
Blockchain timestamp, [run];
Method Execution: int main:[File->chaincode.js]
if      user != sR();
        then, enroll in sR();
        if user != sR();
        then, verify request dS(), rM(), sC();
        and validate IoMT-based transaction according to cD(), eX(), eY(), fI(), aG(), and aY();
        blockchain timestamp [run];
        and maintain pS(IPFS);
        else state change, share, exchange, and reschedule,
              stop,
              programs terminate;
else state change, share, exchange, and reschedule,
stop,
programs terminate;
Consensus Policy = PoW;
Consensus procedure = 51% vote required;
Digital signature->Authentication/approval = True;
User = Read/Request ->Patient/Consultant;
Verification = True;
Validation = True;
Storage = IPFS;
Other stakeholders = Read/Write->Hospital/Administrator;
Output: dS(), rM(), sC(), pS(), sR();
```

The combined outcomes of Tests 1 and 2 across the board for all three environments are displayed in this scenario, including enhanced infrastructure security, higher network resource consumption, and higher integrity of smooth data transfer by up to 1.87%, 1.37%, and 1.56%, respectively.

Overall infrastructural security test is conducted via the proposed BDLT-IoMT, as shown in Fig. 8, where evaluation is scheduled only once to investigate the successful deployment of the work, which mainly highlights the pop-up of the use of blockchain technology in the data protection scenario. Whereas the evaluation criteria are mentioned as the sum of the cycle of resource management used with respect to data management and preservation slots delivered per second(s), where 266 cycles are managed in 683 s (Fig. 11).

However, the list of state-of-the-art publications is mentioned that are used as the comparative analysis as follows [30–35]:

- A blockchain-based federated learning mechanism for the privacy preservation of healthcare IoT data;
- A blockchain-based federated artificial intelligence system of intrusion detection for IoT healthcare system;
- An original research article on a blockchain-based secure Internet of Medical Things framework for smart healthcare;
- Efficient personal health records sharing on the Internet of Medical Things using searchable symmetric encryption, blockchain, and IPFS; and
- Blockchain-based AI model for industrial healthcare applications

Tables 4 and 5 present a report of comparative analysis between the proposed BDLT-IoMT and other state-of-the-art methods, where the context of evaluation is addressed as follows: (i) data processing cycle, (ii) computational cost, (iii) memory scalability, (iv) trustworthiness environment, and (v) overall efficiency and accuracy.

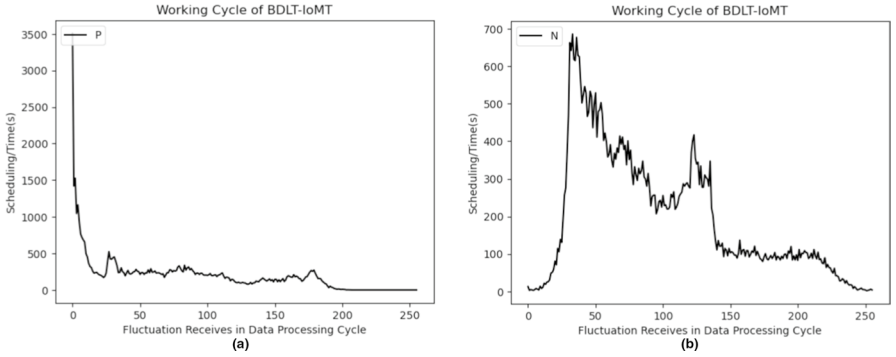

Fig. 6 Working cycle of BDLT-IoMT (Test 1), where the metrix is the fluctuation receives in data processing cycle and scheduling data per second, **a** test of false positive, and **b** test of false negative

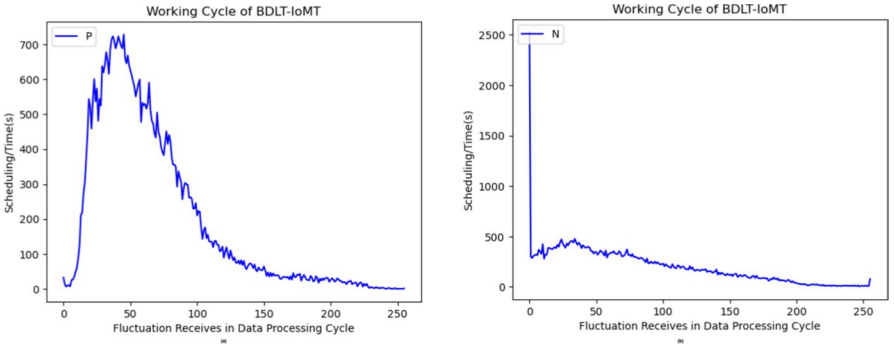

Fig. 7 Working cycle of BDLT-IoMT (Test w), where the metrix is the fluctuation receives in data processing cycle and scheduling data per second, **a** test of false positive, and **b** test of false negative

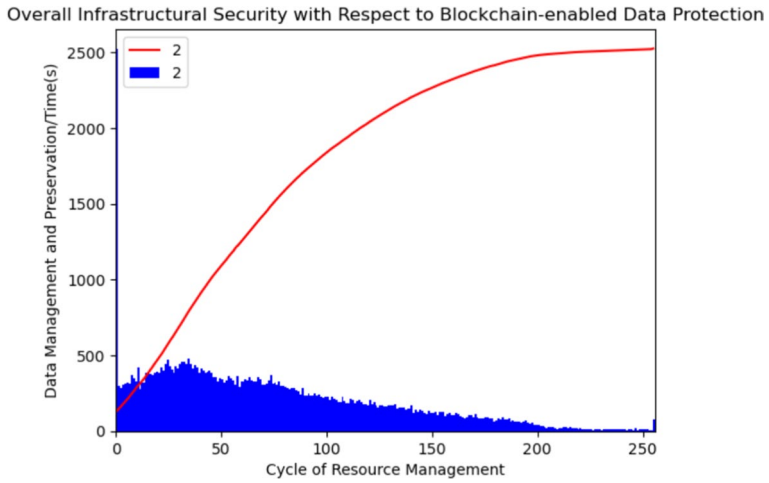

Fig. 8 Overall infrastructural security solution using blockchain-enabling technology for data preservation prospects

5 List of limitations in implementation, deployment, and the current research gaps

In this section, we present a report that is based on a critical investigation raised during the implementation of this proposed BDLT-IoMT, where the major prospects of design and deployment are highlighted. In addition, this paper tries to provide a possible solution to the mentioned problems, which need to be fulfilled near future and most probably require technological maturity.

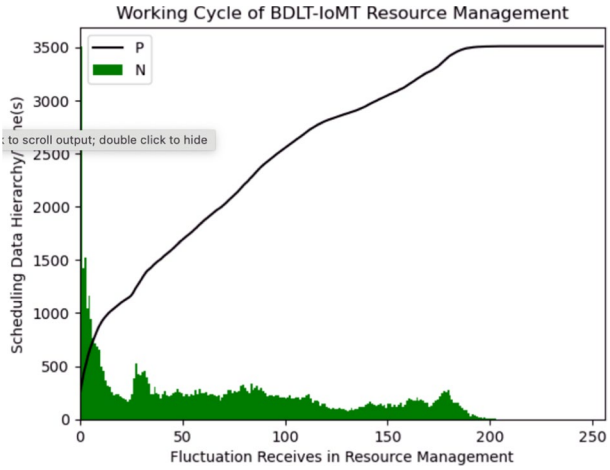

Fig. 9 Working cycle of BDLT-IoMT for resource management Test 1

5.1 Seamless e-healthcare data collection and management

Due to the high demand of healthcare, the usage of interoperable platform is going on peak day-to-day and their integration-seamless information share and exchange between hospital-to-hospital or hospital-to-patient and vice versa, within consortium network, and even cross-border transactions. In this whole scenario, an effort is underway while initiate streamline healthcare data exchange because the current architecture is based on centralized system, which is not feasible to handle and transmit transactions in a distributed environment [36, 37]. Blockchain is the only solution that enhance interoperable effectiveness and provide improve integration

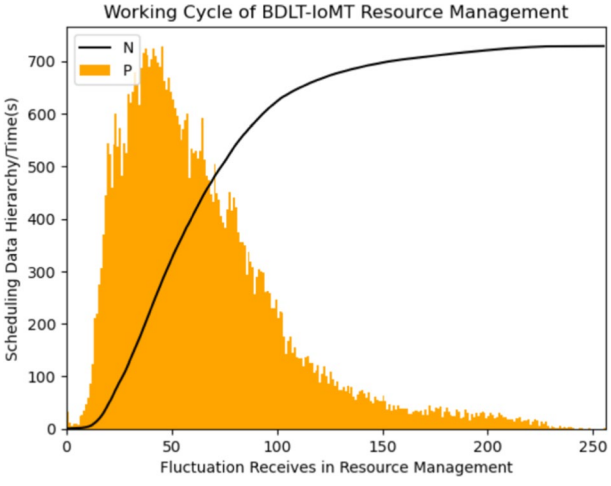

Fig. 10 Working cycle of BDLT-IoMT for resource management Test 2

between nodes. In addition, it provides a greater consistency in terms of platform standardization and related protocols, which directly effects on the design of cost-efficiency, where patient cannot be retested. However, the involvement of regulatory and compliances by the government, the ecosystem perform actively in technological supplies, quality assessment, experience, and monitoring. Furthermore, this blockchain-enabled solution not only answers the seamless data exchange problem but also addressed a list improvement in healthcare domain, which is highlighted as follows:

- Digital transformation-frictionless secure data sharing can be leverage.
- Platform interdependency-provide ease workforce data management.
- Data exchange-provide framework for share data in a standard manner.
- International border law-provide interoperability between explicit node interconnectivity within easier and more efficient manner.

5.2 Fine-grained stakeholder authentication and privacy

Recently, different methods are introduced that addresses secure data access and controls. However, fine-grained is one of them, which not only provide a controlling scenario but ensure certain data accessibility and availability [36, 38]. In healthcare, we compare generalized data access and control scenario with coarse-grained method, where fine-grained perform more sophisticated in terms of following nuanced steps and variable operations for access enrollment purpose. Substantially, this adaptation mainly ensures a list of limitation that are involved in the existing healthcare environment as follows:

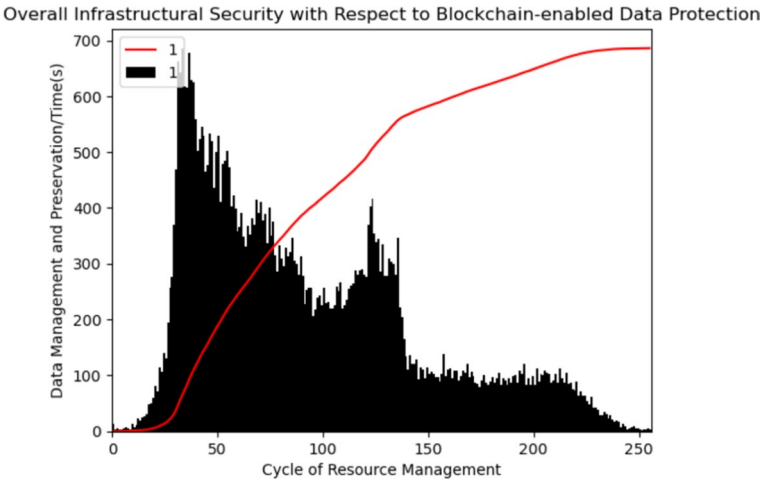

Fig. 11 Overall infrastructural security solution using blockchain-enabling technology for data protection scenario

Table 4 Report of systematic analysis (1)

Context of discussion	State-of-the-art method (1) [30]	State-of-the-art method (2) [31]	State-of-the-art method (3) [32]
Data processing cycle	Yes	Yes	Yes
Computational cost evaluation	Yes	No	Yes
Memory scalability	N/A	N/A	N/A
Trustworthiness environment	No	Yes	Yes
Overall efficiency/accuracy	+88%	+90%	+90%

Table 5 Report of systematic analysis (2)

Context of discussion	State-of-the-art method (4) [33]	State-of-the-art method (5) [34]	State-of-the-art method (6) [35]
Data processing cycle	Yes	Yes	Yes
Computational cost evaluation	No	No	No
Memory scalability	No	No	N/A
Trustworthiness environment	Yes	Yes	Yes
Overall efficiency/accuracy	+80%	+85%	+90%

- Multi-data source storage, exchange, and access facility
- Provide degree of access in accordance with the assigned roles
- Mobile access and security facility
- Ensuring third-party accessibility

5.3 Security loopholes and storage cost-effectiveness

A large number of healthcare applications are running on an outdated design, protocols, compliances, or even operating systems, which drastically exacerbating security and privacy challenges. A list of common vulnerability raises in the healthcare environment is mentioned as follows [39–42]:

- Cryptographic attacks
- Cybercrime like malicious insider attacks
- Denial of service (DoS)
- Distributed denial of service (DDoS)
- Injection exploits
- Malware
- Web security exploits
- Privilege escalation

Blockchain Hyperledger technology plays a significant role in addressing these issues by offering an affordable, effective, and adaptable architectural

environment for transforming seamless, interoperable healthcare data, or even managing cross-border information exchanges within the designated computing resources.

6 Conclusions

This paper explored the real-time trends in IoMT, wherein advanced digital technology plays a significant role. The goal is to offer a novel approach to the design and development of healthcare apps that are interoperable and directly contribute to the advancements in the healthcare industry. Throughout the investigation process, this study uncovers a few difficult issues, particularly one pertaining to interoperability, that have a significant impact on the present lifetime of IoMT. In order to manage and safeguard the current IoMT functioning, including data processing, organizing, optimizing, resource management, scalability, and data exchange via distributed preservation (such as IPFS—InterPlanetary File Storage System) to ensure automation in decision-making, along with the security and privacy, this paper evaluated all such possibilities and proposed a novel and secure architecture (named BDLT-IoMT). This architecture uses the collaborative technique of blockchain with SVM. In order to protect automated decision-making, the suggested BDLT-IoMT experiences significant changes in infrastructure security, according to simulation data. Furthermore, in order to enable smooth intercommunication among heterogeneous devices, the proposed BDLT-IoMT guarantees integrity between seamless data sharing and exchanging and network resource optimization. Nonetheless, the evaluation findings demonstrate the importance of the work in the following ways: (i) increased network resource consumption by 1.87%, improved infrastructure security by up to 1.37%, and increased integrity of seamless data transfer by up to 1.56%.

Acknowledgements The authors extend their appreciation to Universiti Teknikal Malaysia Melaka (UTeM) and to the Ministry of Higher Education of Malaysia (MOHE) for their support in this research; and the authors extend their appreciation to Taif University, Saudi Arabia, for supporting this work through project number (TU-DSPP-2024-229).

Author contributions All the authors contribute equally.

Data availability No datasets were generated or analyzed during the current study.

Declarations

Conflict of interest The authors declare there is no conflict of interest.
The authors declare no competing interests.

Ethics approval Not applicable.

Consent to publish Not applicable.

References

1. Ameen AH, Mohammed MA, Rashid AN (2023) Dimensions of artificial intelligence techniques, blockchain, and cyber security in the Internet of Medical Things: opportunities, challenges, and future directions. J Intell Syst 32(1):20220267
2. Lian Z, Wang W, Han Z, Su C (2023) Blockchain-based personalized federated learning for internet of medical things. IEEE Trans Sustain Comput 8(4):694–702
3. Chaudhury S, Sau K (2023) A blockchain-enabled internet of medical things system for breast cancer detection in healthcare. Healthc Anal 4:100221
4. Khan AA, Laghari AA, Awan SA (2021) Machine learning in computer vision: a review. EAI Endorsed Trans Scalable Inf Syst 8(32):e4–e4
5. Qi P, Chiaro D, Giampaolo F, Piccialli F (2023) A blockchain-based secure Internet of Medical Things framework for stress detection. Inf Sci 628:377–390
6. Rahman A, Wadud MAH, Islam MJ, Kundu D, Bhuiyan TAUH, Muhammad G, Ali Z (2024) Internet of medical things and blockchain-enabled patient-centric agent through SDN for remote patient monitoring in 5G network. Sci Rep 14(1):5297
7. Khan AA, Bourouis S, Kamruzzaman MM, Hadjouni M, Shaikh ZA, Laghari AA, Dhahbi S (2023) Data security in healthcare industrial internet of things with blockchain. IEEE Sensors Journal. 23(20):25144–25151
8. Albakri A, Alqahtani YM (2023) Internet of Medical Things with a blockchain-assisted smart healthcare system using metaheuristics with a deep learning model. Appl Sci 13(10):6108
9. Messinis S, Temenos N, Protonotarios NE, Rallis I, Kalogeras D, Doulamis N (2024) Enhancing Internet of Medical Things security with artificial intelligence: A comprehensive review. Comput Biol Med 170:108036
10. Khan AA, Wagan AA, Laghari AA, Gilal AR, Aziz IA, Talpur BA (2022) BIoMT: A state-of-the-art consortium serverless network architecture for healthcare system using blockchain smart contracts. IEEE Access 10:78887–78898
11. Osama M, Ateya AA, Sayed MS, Hammad M, Pławiak P, Abd El-Latif AA, Elsayed RA (2023) Internet of medical things and healthcare 4.0: trends, requirements, challenges, and research directions. Sensors 23(17):7435
12. Mitra A, Bera B, Das AK, Jamal SS, You I (2023) Impact on blockchain-based AI/ML-enabled big data analytics for cognitive Internet of Things environment. Comput Commun 197:173–185
13. Khan MF, AbaOud M (2023) Blockchain-integrated security for real-time patient monitoring in the Internet of Medical Things using federated learning. IEEE Access 11:117826–117850
14. Sankaran KS, Kim TH, Renjith PN (2023) An improved AI based secure M-trust Privacy protocol for medical Internet of Things in smart healthcare system. IEEE Internet Things J 10(21):18477–18485
15. Ali A, Pasha MF, Guerrieri A, Guzzo A, Sun X, Saeed A, Fortino G (2023) A novel homomorphic encryption and consortium blockchain-based hybrid deep learning model for industrial Internet of Medical Things. IEEE Trans Netw Sci Eng. 10(5):2402–2418
16. Dhasarathan C et al (2023) User privacy prevention model using supervised federated learning-based block chain approach for Internet of Medical Things. CAAI Trans Intell Technol. https://doi.org/10.1049/cit2.12218

17. Alatawi MN (2023) An approach based on machine learning for the cybersecurity of blockchain-based smart Internet of Medical Things (IoMT) networks. Int J Software Eng Knowl Eng 33(10):1513–1535
18. Aldhyani, T. H., Khan, M. A., Almaiah, M. A., Alnazzawi, N., Hwaitat, A. K. A., Elhag, A., Alshebami, A. S. (2023). A secure internet of medical things framework for breast cancer detection in sustainable smart cities. Electronics, 12(4), 858.
19. Egala BS, Pradhan AK, Dey P, Badarla V, Mohanty SP (2023) Fortified-chain 2.0: intelligent blockchain for decentralized smart healthcare system. IEEE Internet Things J 12:858
20. Lin Q, Li X, Cai K, Prakash M, Paulraj D (2024) Secure Internet of medical Things (IoMT) based on ECMQV-MAC authentication protocol and EKMC-SCP blockchain networking. Inf Sci 654:119783
21. Khurana R, Choudhary M, Singh A, Singh KK (2023) AIML-based blockchain solutions for IoMT. In: Singh A (ed) Blockchain and Deep Learning for Smart Healthcare. Wiley, Hoboken
22. Ghosh P, Mazumder A, Banerjee PS, De D (2024) CARE: carbon-aware computing for blockchain-enabled internet of medical things. Innov Syst Softw Eng 3:373–391
23. Rufai AU, Fasina EP, Uwadia CO, Rufai AT, Imoize AL (2023) Cyberattacks against artificial intelligence-enabled Internet of Medical Things. In: Agbotiname LI, Valentina EB, Vijender KS, Cheng-Chi L, Mohammad SO (eds) Handbook of Security and Privacy of AI-Enabled Healthcare Systems and Internet of Medical Things. CRC Press, Boca Raton
24. Myrzashova R, Alsamhi SH, Shvetsov AV, Hawbani A, Wei X (2023) Blockchain meets federated learning in healthcare: a systematic review with challenges and opportunities. IEEE Internet of Things J 10:14418–14437
25. Awotunde JB, Farhaoui Y, Imoize AL, Folorunso SO, Adeniyi AE (2023) An Enhanced Internet of Medical Things Data Communication Based on blockchain and Cryptography for Smart Healthcare Applications. In The International Conference on Artificial Intelligence and Smart Environment (pp. 305–313). Cham: Springer Nature Switzerland.
26. Kumar R, Rana R, Jha SK (2023) Scalable blockchain architecture of Internet of Medical Things (IoMT) for Indian smart healthcare system. AI Models for Blockchain-Based Intelligent Networks in IoT Systems: Concepts, Methodologies, Tools, and Applications. Springer International Publishing, Cham, pp 231–259
27. Sakly H, Said M, Al-Sayed AA, Loussaief C, Sakly R, Seekins J (2023) Blockchain technologies for internet of medical things (BIoMT) based healthcare systems: a new paradigm for COVID-19 pandemic. Trends of Artificial Intelligence and Big Data for E-Health. Springer International Publishing, Cham, pp 139–165
28. Awotunde JB, Chakraborty C, AbdulRaheem M, Jimoh RG, Oladipo ID, Bhoi AK (2023) Internet of medical things for enhanced smart healthcare systems. In: Chinmay C, Subhendukumar P, Mohd AA, Qin X (eds) Implementation of smart healthcare systems using AI, IoT, and blockchain. Elsevier, Amsterdam
29. Subhan F, Mirza A, Su'ud MBM, Alam MM, Nisar S, Habib U, Iqbal MZ (2023) AI-enabled wearable medical internet of things in healthcare system: a survey. Appl Sci 13(3):1394
30. Panchal B, Parmar S, Rathod T, Jadav NK, Gupta R, Tanwar S (2023). AI and Blockchain-Based Secure message Exchange Framework for Medical Internet of Things. In 2023 International Conference on Network, Multimedia and Information Technology (NMITCON) (pp. 1–6). IEEE.
31. Dalal S, Lilhore UK, Simaiya S, Sharma A, Jaglan V, Kumar M, Rana AK (2023) Original research article a blockchain-based secure Internet of Medical Things framework for smart healthcare. J Auton Intell. https://doi.org/10.32629/jai.v6i3.592
32. Tyagi P, Bargavi SM (2023) Using federated artificial intelligence system of intrusion detection for IoT healthcare system based on blockchain. Int J Data Inf Intell Comput 2(1):1–10
33. Moulahi W, Jdey I, Moulahi T, Alawida M, Alabdulatif A (2023) A blockchain-based federated learning mechanism for privacy preservation of healthcare IoT data. Comput Biol Med 167:107630
34. Bisht A, Das AK, Niyato D, Park Y (2023) Efficient personal-health-records sharing in Internet of Medical Things using searchable symmetric encryption, blockchain and IPFS. IEEE Open J Commun Soc 4:2225–2244
35. Bibhu V, Das L, Rana A, Sharma S, Salagrama S (2023) AI model for blockchain based industrial application in healthcare IoT. AI Models for Blockchain-Based Intelligent Networks in IoT Systems: Concepts, Methodologies, Tools, and Applications. Springer International Publishing, Cham, pp 163–184

36. Khan AA, Laghari AA, Shafiq M, Cheikhrouhou O, Alhakami W, Hamam H, Shaikh ZA (2022) Healthcare ledger management: a blockchain and machine learning-enabled novel and secure architecture for medical industry. Hum Cent Comput Inf Sci 12:55
37. Hong Y, Yang L, Liang W, Xie A (2023) Secure access control for electronic health records in blockchain-enabled consumer internet of medical things. IEEE Trans Consumer Electron 70:4574–4584
38. Khan AA, Laghari AA, Shaikh ZA, Dacko-Pikiewicz Z, Kot S (2022) Internet of Things (IoT) security with blockchain technology: A state-of-the-art review. IEEE Access 10:122679–122695
39. Khan AA, Shaikh ZA, Baitenova L, Mutaliyeva L, Moiseev N, Mikhaylov A, Alshazly H (2021) QoS-ledger: Smart contracts and metaheuristic for secure quality-of-service and cost-efficient scheduling of medical-data processing. Electronics 10(24):3083
40. Abou El Houda Z, Moudoud H, Brik B, Khoukhi L (2023). Securing Federated Learning Through Blockchain and Explainable AI for Robust Intrusion Detection in IoT Networks. In IEEE INFOCOM 2023-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 1–6). IEEE.
41. Moudoud H, Cherkaoui S (2023) Empowering security and trust in 5G and Beyond: a deep reinforcement learning approach. IEEE Open J Commun Soc 4:2410
42. Moudoud H, Cherkaoui S, Khoukhi L (2021). Towards a Secure and Reliable Federated Learning Using Blockchain. In 2021 IEEE Global Communications Conference (GLOBECOM) (pp. 01–06). IEEE.

Authors and Affiliations

Abdullah Ayub Khan[1] · Asif Ali Laghari[2] · Abdullah M. Baqasah[6] · Rex Bacarra[4] · Roobaea Alroobaea[3] · Majed Alsafyani[3] · Jamil Abedalrahim Jamil Alsayaydeh[5]

✉ Abdullah Ayub Khan
abdullah.khan00763@gmail.com; abdullahayub.bukc@bahria.edu.pk

✉ Jamil Abedalrahim Jamil Alsayaydeh
jamil@utem.edu.my

Asif Ali Laghari
asiflaghari@synu.edu.cn

[1] Department of Computer Science, Bahria University Karachi Campus, Karachi 73500, Pakistan

[2] Software Collage, Shenyang Normal University, Shenyang, China

[3] Department of Computer Science, College of Computers and Information Technology, Taif University, P. O. Box 11099, 21944 Taif, Saudi Arabia

[4] Department of General Education and Foundation, Rabdan Academy, Abu Dhabi, United Arab Emirates

[5] Department of Engineering Technology, Fakulti Teknologi Dan Kejuruteraan Elektronik Dan Komputer (FTKEK), Universiti Teknikal Malaysia Melaka (UTeM), 76100 Melaka, Malaysia

[6] Department of Information Technology, College of Computers and Information Technology, Taif University, 21974 Taif, Saudi Arabia