Journal of Autonomous Intelligence (2024) Volume 7 Issue 5
doi: 10.32629/jai.v7i5.1478

ORIGINAL RESEARCH ARTICLE

A blockchain-based deep learning approach for cyber security in next-generation medical cyber-physical systems

Bukola Fatimah Balogun[1], Khushboo Tripathi[2,*], Shrikant Tiwari[3], Shyam Mohan J S[4], Amit Kumar Tyagi[5,*]

[1] *Department of Computer Science, Kwara State University, Malete 241103, Nigeria*

[2] *Department of Computer Science and Engineering, Amity University, Gurugram, Haryana 122412, India*

[3] *Department of Computer Science & Engineering, School of Computing Science and Engineering (SCSE), Galgotias University, Greater Noida, Uttar Pradesh 203201, India*

[4] *Department of CSE, GITAM University, Bengaluru 561203, Karnataka, India*

[5] *National Institute of Fashion Technology, New Delhi, Delhi 110016, India*

*** Corresponding authors:** Khushboo Tripathi, khushbootripathi.cse@gmail.com; Amit Kumar Tyagi, amitkrtyagi025@gmail.com

ABSTRACT

Cyber-physical systems (CPSs) have been employed to seamlessly integrate numerous processes and physical components with integrated computing facilities and data storage, aiming to achieve a heightened level of effectiveness and efficiency across various qualitative and quantitative metrics, including technical and organizational aspects. The increased use of the web and the prospering network through IoT (Internet of things) have given a critical open door to CPS to prevail. While this innovation is as of now utilized in programmed pilot flying, advanced mechanics frameworks, clinical checking, modern control frameworks, and so forth, the headway of these frameworks should understand undeniable spotlight on making them proficient and secure. To work on the strength, reliability, and security of these frameworks, specialists can integrate blockchain innovation which has an inbuilt mix of consensual calculations, secure conventions, and circulated information capacity, with the CPS. This introduces an efficient deep learning approach based on blockchain for medical cyber-physical systems (CPS), consisting primarily of two components: a) a blockchain based security framework to protect the medical data and b) the extraction of quintessential features from these data to a classifier for performing the anomaly scans using deep learning. The experimental evaluation demonstrates that the suggested system outperforms existing models, achieving exceptional performance with an accuracy rate of 0.96 and a sensitivity score of 0.95.

Keywords: blockchain; cyber-physical system; deep learning; proof of concept; medical CPS

ARTICLE INFO

Received: 11 December 2023
Accepted: 15 January 2024
Available online: 6 March 2024

1. Introduction

In recent times, there has been a notable upswing in interest surrounding cyber-physical systems (CPS), recognized as an advanced paradigm. CPS entails the seamless integration of processing and communication capabilities on a global scale. Substantial support for fundamental research in this field comes from the US National Science Foundation (NSF) and has garnered approval from the US President's Council of Advisors on Science and Technology. The essence of cyber-physical systems (CPS) lies in the amalgamation of sensing, computation, and networking. Noteworthy technological advancements, such as wireless sensor networks (WSN), medical sensors, and cloud computing (CC), have solidified CPS as a valuable framework for various clinical applications, particularly

within the domains of healthcare and home-based patient care. These innovations have the potential to remotely monitor patients' health status and provide enhanced treatment options. A comprehensive evaluation has been conducted on clinical sensors, which are utilized to gather extremely sensitive patient data. Wireless communication channels are utilized for transmitting this data, while wired sensors are incorporated to provide versatility to healthcare providers and patients. The information recorded by these sensors is safely stored on a server and is easily accessible to healthcare professionals [1].

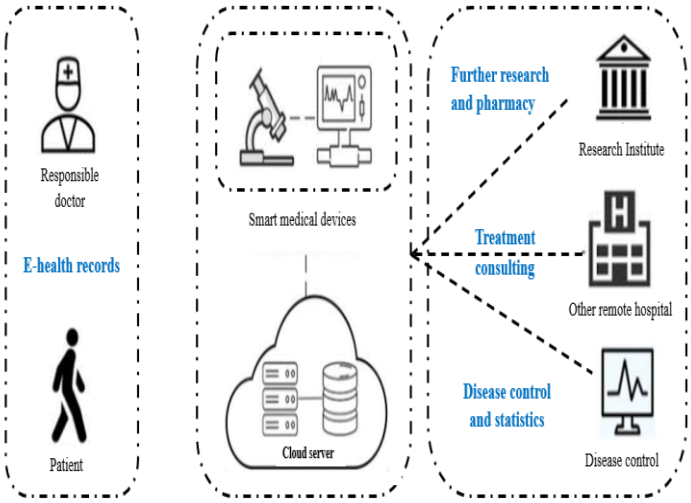

Figure 1. Medical cyber-physical system overview.

Due to advancements in wireless sensor network technology, cloud computing, and medical sensors, cyber-physical systems (CPS), as depicted in **Figure 1**, have gained the capability to be applied in healthcare, specifically for remote patient care and swift response to medical emergencies. A medical cyber-physical system (MCPS) is the integration of a network that brings together medical equipment and cyber-physical systems commonly found in essential healthcare facilities. Within the MCPS framework, important roles are played by medical sensors, implantable devices, and wearable gadgets, which monitor a patient's physiological data efficiently. This data is then transmitted to healthcare providers for treatment [2]. Wearable devices are tasked with monitoring various health parameters for enhancing the patient's quality of life. However, the medical data collected by these sensors and transmitted through network connections like Bluetooth, ZigBee, or Wi-Fi are susceptible to security risks, including data breaches, theft, tampering, as well as security breaches like man-in-the-middle attacks, falsified data injection, and SQL injection [3]. As MCPS generates a significant amount of medical data in a short period, which is stored on cloud servers, stringent security measures become essential. Existing literature has proposed numerous solutions to reinforce security and privacy, such as fog computing [4], mobile edge computing [5] and alternative strategies. Current MCPS implementations primarily rely on cryptographic techniques to protect medical data [6]. However, accessing this data through the cloud presents challenges, including increased latency, limitations in network bandwidth, scalability difficulties, data volume management, and the preservation of medical data confidentiality [7].

The main motivation behind developing MCPS system is, it empowers healthcare professionals to remotely oversee patients' well-being and conduct medical procedures from a distance. MCPS plays an important role in generating, sensing, analyzing, and transmitting extensive volumes of medical data. Given the sensitive nature of medical information, stringent privacy measures must be upheld. However, real-world situations bring their own set of challenges, as they reveal potential weaknesses in networks that may result in unauthorized data access or the creation of counterfeit data, such as data exfiltration [8]. As a result, a range of crypblocktographic encryption techniques[9] have been implemented to protect this data, with attribute-based encryption (ABE) and symmetric encryption (SE) being commonly utilized methods. In addition, recent

research has integrated machine learning and statistical algorithms to enhance proactive security measures. Nonetheless, a notable limitation of current models is their inability to adjust to the continually changing landscape of cyberattacks, mainly due to their predetermined and predefined security protocols. To achieve this adaptability, there's a need to develop a cognitive, human-like behavioural framework capable of recognizing emerging attack patterns and dynamically adjusting security policies.

We aim to illuminate the driving force behind our research, to emphasize the importance of safeguarding confidential information within cyber-physical systems and to showcase the innovative potential of consortium blockchain as a privacy solution. Our study holds promise in enhancing the security of CPS by providing practical techniques to safeguard secrets against evolving cyber threats and ensuring the reliability of these critical systems. Furthermore, this work has the potential to advance CPS security.

CPS secrets can be stored, shared, and accessed with the utmost security, restricted to authorized entities only, due to the use of blockchain's unchangeable and distributed ledger technology. This effectively reduces the likelihood of data breaches and internal threats. The suggested privacy approach has the potential to revolutionize the way CPSs manage confidential data by providing:

- Enhanced security: A consortium blockchain addresses worries about data breaches and unauthorized access by providing a secure and unchangeable platform for storing sensitive information.
- Privacy preservation: The consortium blockchain's emphasis on privacy ensures that confidential information remains secure and can only be retrieved by authorized entities, thereby bolstering the confidentiality of secrets within CPSs.
- Increased trust and accountability: The trustworthiness of blockchain technology is bolstered by its transparent and verifiable characteristics, which empower participants to confirm and authenticate the security of stored information.
- Interoperability and scalability: A consortium blockchain has the potential to enable smooth integration and compatibility among various CPS components, thereby facilitating the effective sharing and administration of confidential information. Moreover, its ability to expand makes certain that the system can adapt to the increasing data demands of CPSs.

1.1. Cyber-Physical System: Blockchain

As processors have become increasingly ubiquitous in recent decades, there has been a transition from primarily relying on paper-based records to the generation and management of digital versions on computers. This evolution represents just one of the many digital challenges that processors have enabled. Although these records are now generated and stored electronically, data entry still requires manual input. It can be argued that human beings continue to be the primary source of data collection in these applications, especially in cases like financial transactions, medical records, and insurance records. Nonetheless, the progression of IoT and the evolution of sensor technologies over the recent years have led to sensors taking on a more significant role in data collection for numerous organizations.

Cyber-physical systems, commonly known as these systems, amalgamate physical processes, software, and data to create a cohesive system with the ability to perform design, analysis, and abstraction. This field encompasses various disciplines and is fundamentally rooted in dynamic analysis.

Financial transactions on the blockchain have undergone comprehensive analysis and documentation. The direct transfer of funds to authorized individuals has become possible due to technological advancements, all without relying on a centralized authority[10]. By integrating smart contracts into the blockchain, the probability of experiencing delays, disruptions, or external influences is significantly diminished. This system remains invulnerable to breaches, guaranteeing comprehensive financial stability and upholding a clear and transparent record of contract conditions. Moreover, online identity tracking and management become more convenient when utilizing blockchain technology. Additionally, as discussed in by Mounir and Maleh[11], blockchain serves

as an economical notary system, preventing different types of fraud by generating unique certificates that are easy to verify.

1.2. Key highlights

This research work aims to establish an efficient security system for mobile payment and communication systems (MPCS) by using deep learning and blockchain technology. The following objectives were pursued:

- Development of effective blockchain and deep learning integrated system for medical CPS.
- Improve the security of the medical side with advanced blockchain techniques i.e., smart contract.
- With the inbuilt high cryptic analysis, each medical record is been covered from outside potential attacks.
- With the novelty, the usage of a deep learning classifier which is LSTM (long short-term memory), has the capability to give a secure layer and is also possible to detect anomalies with a stack of Recurrent Neural Networks (RNNs).
- Experimental results indicate that the suggested system surpasses existing state-of-the-art models.

Organization of the paper: In our earlier discussion, section 1 discussed the connection between blockchain and medical cyber-physical systems (CPS). Section 2 provides a summary of existing research, section 3 delineates the methodology employed, section 4 presents a performance analysis, and section 5 serves as the conclusion of the paper.

2. Literature review

Al-Ghuraybi et al.[12] investigate the integration of blockchain technology, physical unclonable function (PUF), and machine learning within the domain of cyber-physical systems (CPS). Their primary objective is to enhance the performance and security aspects of CPS, particularly in thwarting external threats. The study provides a comprehensive examination of recent research findings that highlight the efficacy of blockchain in improving CPS performance while maintaining robust security measures. Additionally, the paper discusses the synergistic use of blockchain and machine learning methods to strengthen CPS security. Furthermore, it assesses the potential of combining blockchain with physically unclonable functions to significantly enhance the effectiveness of physical device authentication.

In Kanagala's [13] study, they proposed an efficient cybersecurity system for safeguarding optical data in healthcare applications by employing a deep learning approach within the framework of cyber-physical systems (CPS). This approach was designed to process IoT-generated data while enhancing data security. By utilizing a deep learning model, an algorithm was employed to handle and convert raw IoT data into actionable knowledge. Furthermore, this system employs a policy-based access control mechanism to secure the data against potential attacks such as denial of service (DoS) and distributed denial-of-service (DDoS). Through performance analysis, this approach is shown to facilitate effective data classification and ensure the reliability of data storage. It also provides real-time protection against DoS and DDoS attacks on IoT data within the realm of cyber-physical systems.

Alzahrani et al.[14] embarked on a comprehensive three-year research endeavor. Their study, titled "Leveraging machine learning for enhanced wireless medical cyber-physical systems (EWMCPS)," introduces a novel framework encompassing multiple components and subsystems. The authors painstakingly crafted the blueprint for this EWMCPS architecture, which they illustrate through a scenario exemplifying its practical applications in the medical domain. In the realm of healthcare, cyber-physical systems play an important role in ensuring the security of critically important health data. They possess a high level of contextual awareness and are essential for protecting vital life-related information from potential data breaches and cyber threats. The field of medical cyber-physical systems research faces several pressing challenges, including issues related to reliability, confidence, security, and transparency. To confront these formidable challenges, the authors advocate for the adoption of an improved wireless medical cyber-physical system (EWMCPS) grounded in the

principles of machine learning. Given the array of devices seamlessly integrated into these systems, including mobile devices and body sensor nodes, they become susceptible to various types of cyber-attacks. As a result, it is important to establish resilient security measures within this environment by using deep neural networks for the detection and categorization of attacks.

Akbarfam et al.[15] introduced DLACB, an innovative solution for decentralized access control. DLACB, an acronym denoting deep learning-based access control using blockchain, harnesses the capabilities of blockchain technology to provide transparency, traceability, and dependability across multiple domains like healthcare, finance, and government. It harnesses deep learning's capabilities to obviate the necessity for predefined access control policies, ultimately automating the entire process. By seamlessly integrating blockchain and deep learning, DLACB introduces a flexible framework that can be applied to diverse domains, ensuring the transparent and trustworthy recording of all transactions. With every piece of data stored on the blockchain, it becomes feasible to detect and pinpoint malicious activities. To accelerate the detection procedure, a storage system keeps a record of malevolent actions and employs a verification algorithm to check them against the blockchain. Additionally, the authors perform evaluations and comparisons of the processing time between the smart contracts in the access control system they've implemented, contrasting it with conventional access control techniques while evaluating the resultant time-related performance impact.

Vignesh Saravanan et al.[16] explain about several key aspects. They examine the characteristics of cyber-physical systems (CPS), conduct an analysis of the current state of CPS, identify security threats that CPS face, and propose solutions to mitigate these threats. Furthermore, their work includes discussions on the utilization of blockchain techniques to bolster the security mechanisms in CPS. The fusion of blockchain technology and cyber-physical systems holds the promise of transforming operations in various sectors. Specifically, blockchain enables the transfer of data or information to private blockchain ledgers, which can be incorporated into shared transactions, ultimately bolstering the efficacy of security applications through improved generalization capabilities.

Ali et al.[17] presented a novel healthcare system framework that harnesses blockchain technology to enhance scalability and security. This innovative system utilizes hybrid deep learning models and operates based on a permissions-oriented approach. The main objective of this framework is to restrict unauthorized access and changes to confidential health information, ensuring the privacy of patients, while also promoting the easy exchange of data and collaboration among healthcare professionals. Furthermore, the incorporation of hybrid deep learning models enables real-time analysis of extensive healthcare data, which supports prompt diagnoses, treatment suggestions, and disease predictions. The combination of blockchain technology and hybrid deep learning provides several advantages, including increased scalability, enhanced security measures, improved compatibility, and more informed decision-making in healthcare systems. Nevertheless, the successful implementation of this approach requires addressing challenges like computational complexity, adherence to regulatory standards, and ethical considerations.

Chakraborty et al.[18] introduced a specialized cybersecurity detection system tailored for the healthcare sector. This system utilizes a combination of centralized and federated transfer learning techniques to enhance the efficiency of data transmission between healthcare domains and the cloud. The facilitator of this process is the edge of things (EoT) framework they have introduced. Their approach centers around the centralized with multi-source transfer learning (CMTL) algorithm, meticulously designed to identify and categorize a broad spectrum of security threats, including activities like information gathering, DoS/DDoS attacks, malware intrusions, injection attacks, and man in middle attacks. The authors assessed the framework's performance by conducting evaluations with a variety of datasets, including EMNIST (extended modified national institute of standards and technology database), X-IIoTID, and federated TON_IoT. Their findings demonstrated that their framework outperforms other algorithms in terms of speed of execution, all the while maintaining a high level of accuracy.

Myrzashova et al.[19] presented a paper titled "Blockchain integration with federated learning in healthcare: An in-depth examination of advantages and constraints". They conducted a content analysis to investigate the advantages and drawbacks of merging these two technologies. The authors highlight three primary research domains that have been systematically identified through an examination of the application of blockchain technology in (i) the Internet of medical things (IoMT), (ii) the administration of electronic health records (EHR) and electronic medical records (EMR), and (iii) the secure notification systems employed in digital healthcare systems with internal consortia. Additionally, they introduced a novel conceptual framework for implementing Federated Learning using blockchain in the context of digital healthcare. To conclude, the paper sheds light on the challenges and future trajectories for the amalgamation of blockchain and Federated Learning within the realm of healthcare applications.

3. Proposed methodology

Blockchain-based platform to assess patient health condition, emphasizing simultaneous implementation and AI in healthcare networks, as well as the suggested methodology. The suggested method has been assessed, as well as simulated, healthcare systems. It analyzes the patient's overall condition, diagnosis, and recovery system and looks into the pertinent surgical interventions by simultaneous operations and clinical decision-making computational studies to assess the quality of care for patients and the feasibility of diagnosis.

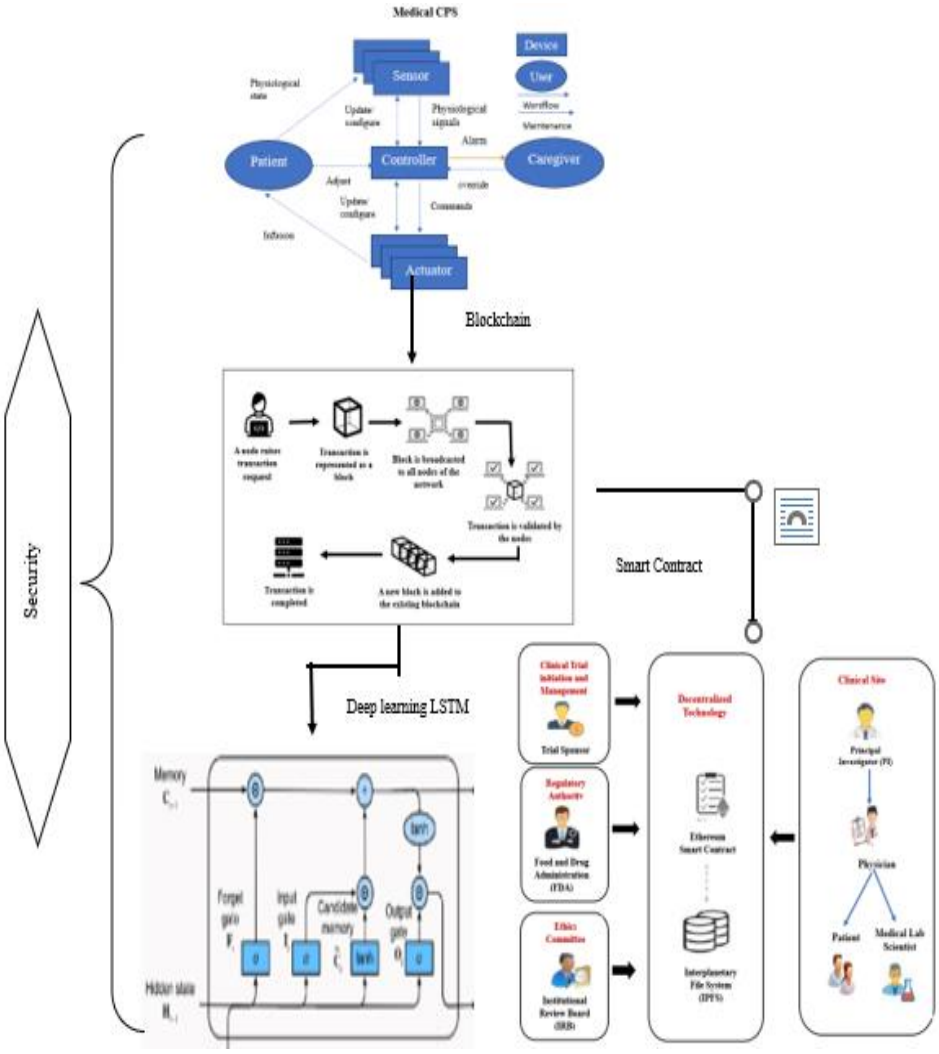

Figure 2. Our proposed network.

Blockchain is a relatively new and rising technology with creative uses in its effective application to the healthcare industry. Efficient and seamless data transfer and exchange across all of the major players in the

network and healthcare providers helps to develop affordable and advanced treatments for a wide range of illnesses. This will spur the healthcare industry's expansion in the upcoming years. The benefits of blockchain technology for the healthcare sector are demonstrated by the recently disclosed prospects it provides the logistics sector. This is one of the first areas where digital transformation innovates and improves since it immediately impacts living quality. Blockchain technology is also becoming more widely used, mostly in the financial industry. Here, **Figure 2** depicts the configuration of the system being proposed, and further elaboration on each phase will be presented in the following sections.

3.1. Blockchain modules

The medical cyber-physical system (MCPS) comprises several essential components, including a medical sensor, an IoT gateway, a decision support system, and an actuator [20]. Within the MCPS, devices are categorized into two distinct groups based on their specific roles: monitoring or sensing devices, which gather patient data and monitor vital signs like heart rate and oxygen levels, and transportation devices, such as infusion pumps, ventilators, and pacemakers, which deliver treatments to modify the patient's physiological condition [21]. **Figure 2** illustrates the architectural diagram of the MCPS, and below, you'll find a comprehensive explanation of each entity within the MCPS.

- Central server: Within this module, the server logs in by utilizing a valid username and password. Once the login is successful, various operations become accessible, including authorizing doctors, authorizing sensor patients, generating clinical reports, viewing patient details, processing access control requests, handling encryption key requests, monitoring key transactions, and viewing results presented in a chart format.
- View and authorize users: Within this module, administrators have the ability to access a roster of registered users. This functionality enables administrators to review and manage user details, including their usernames, email addresses, and physical addresses, while also granting or revoking user authorizations.
- Sensor patient: In this module, there are several patient sensors, and it is essential for the owner to undergo a registration procedure before gaining access to any features. After a patient's registration is successfully completed, their information is safely stored in the database. Subsequently, the owner must log in using their authorized username and password. Once logged in, the owner gains access to a variety of functions, including the ability to view profiles, input patient data, retrieve patient records, monitor authorization requests, and review clinical reports.
- Doctor: In this module, you'll find several patient sensors. To use any of its features, the owner must first go through a registration process. Upon completing the patient registration process, the information is recorded in the database. Subsequently, the owner is required to log in using a valid username and password. After successfully logging in, they gain access to a range of functions, such as viewing profiles, inputting patient information, retrieving patient records, reviewing critical requests, and examining clinical reports, among other tasks.
- Decision support system (DDS): The DSS is tasked with scrutinizing the gathered data, leading to the creation of alerts for medical emergencies and the transmission of directives to the actuator.

Transporting device or actuator:

The actuator holds a crucial position in carrying out the instructions given by the decision support system in the intelligent medical device, enabling the provision of healthcare services through equipment like dialysis machines, infusion pumps, oxygen concentrators, and similar devices.

The integrity, security, and traceability of transactions within the network are assured by the permissioned blockchain module [22]. In a permissioned AP2chain, data is shared only following a rigorous authentication procedure. Within this framework, two essential components exist: the cluster head and the data accessor. The

operational model is dependent on two separate operational modules, specifically the electronic health record (EHR) generation and storage unit, as well as the EHR access unit.

3.2. Operation block: Cluster head

An EHR is created by gathering patient data and securely recording it on a blockchain [23]. To facilitate data storage, the process involves choosing a cluster head, and the role and responsibilities of this cluster head are elaborated upon below:

Cluster head selection: The designated leader within this permissioned blockchain acts as the overseer, responsible for overseeing all transaction executions. The process of selecting the cluster head in this permissioned blockchain involves transaction mining within the network[24]. Unlike the bitcoin network, where cluster head selection differs, in this case, the miner of the block takes on the role of the cluster head. Their responsibilities include managing all transactions and keeping the ledger, which is divided into two categories: one for successful transactions and another for unsuccessful ones. In this context, a successful transaction refers to a genuine exchange between valid participants. Participants are rewarded for successful transactions while incurring penalties for unsuccessful ones. In the reward system, a miner earns one point for every successful transaction while losing one point for each unsuccessful one. This mechanism safeguards the trustworthiness and operational effectiveness of the permissioned blockchain.

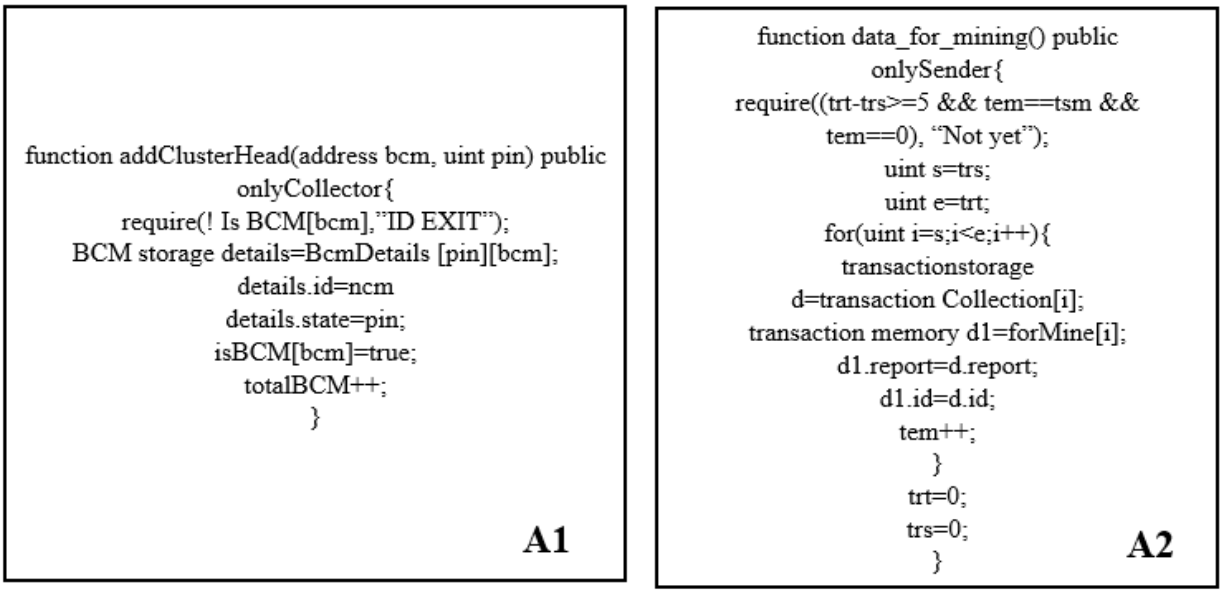

Figure 3. Cluster head selection process.

Functions linked to the proposed framework: Within this framework proposal, several functions are connected to the Algorithm 1. The following section elaborates on the description of these functions.

- addCluster Head(): In **Figure 3**, block A1 provides a detailed explanation of how the cluster head selection process works in the proposed scheme. This selection method is based on the location, where the nodes are asked to provide certain parameters like their ID and address pin. Following this, the cluster head is determined by a consensus reached among the majority of participating nodes.
- data for mining(): **Figure 3**'s block A2 provides an explanation of how blocks are added and validated within the proposed scheme.
- addNewPatient(): The purpose of this function is to integrate a new patient into the blockchain network by collecting a range of information from the patient, including their name, Aadhar details, and postal code. Subsequently, the cluster head will authenticate this information and incorporate the patient into the blockchain network.

- addHospitals(): The main goal of this function is to integrate newly established hospitals into the blockchain. To achieve this, it will seek essential information about the hospital, such as its name and the corresponding PIN code. Following that, a cluster leader will assess and then integrate this information into the blockchain network.

Algorithm 1 Selection head

Input for the procedure includes: Consensus, Patient Data (PD), Hospital Data (HD), and Doctor Data (DD)
Output: Identifying a cluster head for the blockchain network
Algorithm
1. Begin
2. While iterating from i to n,
2.1 Mine(Block)
2.2 Collect patient data (DataP)
2.3 Collect hospital data (DataH)
2.4 Collect doctor data (DataD)
2.5 Execute Consensus
2.6 Mine the block
2.7 Add data to the blockchain
3. End the loop
4. End the procedure

3.3. Accessing block

Within this section, an electronic health record (EHR) is created, and a medical data access system will be established. The data access system will initiate requests for data retrieval, and authentication will be conducted before sharing the data with the access system [25]. A comprehensive description of this section is provided below as Algorithm 2.

Algorithm 2 Registration of healthcare

Input: Hospital Data (HD), Patient Data (PD), Doctor Data (DD))
Output: Registration ID (R id) and password (R pw) for hospitals, patients, and doctors
1. *Begin*
2. *While true*
2.1 *Execute function add(new registration(N R))*
2.2 *Perform Add()*
2.3 *Provide (HD, PD, DD)*
2.4 *Verify (HD, PD, DD)*
2.5 *Execute Verify()*
2.6 *The cluster head will verify*
2.7 *If verification is successful*
2.7.1 *Then add()*
2.8 *Else remove*
3. *End if*
4. *End function*
5. *End the loop*
6. *Provide (Registration ID, Password)*
7. *End the process*

Data accessor: A data user, such as a hospital, patient, or doctor, seeks to obtain information from the blockchain. To access data within this blockchain network, certain rules have been established. Integration into this blockchain network necessitates that data users undergo verification by the cluster leader. The verification procedure hinges on the identification and password provided by the cluster leader for new participants in the network[26]. Once authentication is successfully completed, the data will be made accessible to the data user. A detailed explanation for this process is explained in Algorithm 3.

Algorithm 3 Accessing block

Input: Login ID, Password
Output: Released data
Algorithm

1. *Start*
2. *While iterating from i to n*
   - *2.1 Send a request to Cluster Head (ID, Password)*
   - *2.2 Execute function validate(verification)*
   - *2.3 Execute function Verify(ID, Password)*
   - *2.4 If it equals the data supplied by the Cluster Head*
   - *2.5 If yes*
     - *2.5.1 Success*
   - *2.6 Else rejected*
3. *End if*
4. *End function*
5. *End function*
6. *End while*

3.4. Smart contract: Blockchain

We utilize Ethereum's smart contracts to establish intelligent renditions of existing medical records, which are distributed across individual network nodes[27]. These contracts are crafted to incorporate information concerning record ownership, access authorizations, and data integrity. In our system, blockchain transactions carry instructions that are cryptographically signed to facilitate the management of these attributes. The state-transition functions of the contracts ensure that policies are enforced exclusively through legitimate transactions, preserving the integrity of the data. These rules can be customized to uphold a broad spectrum of regulations related to specific medical records, as long as they can be represented computationally. For instance, one such regulation might require separate consent transactions from both patients and healthcare professionals before granting third-party viewing access. We've developed a system that utilizes blockchain smart contracts to oversee intricate healthcare workflows. These smart contracts are customized for various medical processes and are responsible for governing data access permissions among different entities within the healthcare ecosystem [28].

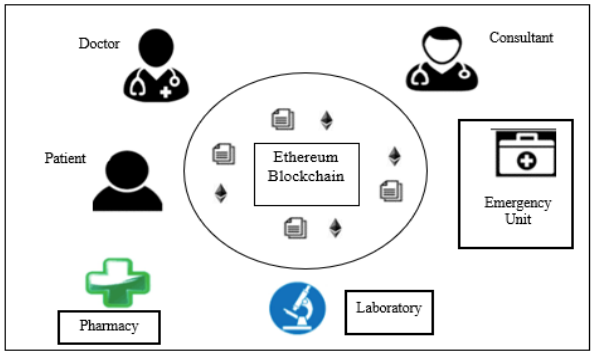

Figure 4. Smart contract: Blockchain for MCPS.

A blockchain-based smart contract has the capacity to be structured to cover a wide range of scenarios, including the management of diverse permissions and data access, as depicted in **Figure 4**. It is evident that multiple stakeholders participate in this framework, each engaged in distinct activities. This innovation will enhance the interaction between healthcare professionals and patients. The smart contracts contain rules for authorizing data access and enable the comprehensive tracking of activities through unique identifiers, spanning from their initiation to conclusion[29]. Multiple scenarios have been devised and elucidated, seamlessly integrating all pertinent functions and processes into smart contracts. This eradicates the necessity for a central overseeing entity to monitor and approve operations, resulting in a significant reduction in

administrative costs. Medical record data is stored in a local database to guarantee effective performance and cost-effectiveness, with the data's hash serving as an essential component in the blockchain's committed block.

The procedure entails the utilization of an individual's private key, whether they are a patient or a doctor, to sign data transactions. In the system, the content of each block is employed to indicate data ownership and shared viewing authorizations within a peer-to-peer private network[30]. Utilizing blockchain technology, we harness smart contracts that enable the automation and monitoring of specific state transitions, including changes in viewing rights or the creation of new system records. To ensure the integrity of patient-provider relationships, we utilize smart contracts on the Ethereum blockchain, connecting medical records with viewing permissions and data retrieval instructions, effectively serving as benchmarks for execution on external servers. To thwart unauthorized alterations, a cryptographic hash of the record is appended to the blockchain. Both providers and patients can engage with the system. Providers have the ability to append new records for particular patients, whereas patients can grant access for sharing their records with providers. In both scenarios, automated notifications are sent to the recipient of the new information, allowing them to review the proposed record before accepting or declining it. This process guarantees that all parties involved are well-informed and actively participate in the management of their records. The system's focus on user-friendliness is further emphasized by the inclusion of a dedicated contract that consolidates references to all of a user's patient-provider relationships. This acts as a central hub for checking updates to their medical history. To handle identity verification, we employ public key cryptography and a Domain Name System (DNS)-like approach to map widely accepted forms of identification, such as names or social security numbers, to the user's Ethereum address [31]. The procedure involves cross-referencing the blockchain with our database authentication server to confirm permissions and a synchronization algorithm is responsible for managing the exchange of "off-chain" data between a patient database and a provider database.

3.5. Deep learning: Bi-LSTM

We employ LSTM models for the purpose of forecasting future values based on historical data[32]. LSTMs use the notion of gates to simplify and efficiently perform calculations for both long term memory (LTM) and short-term memory (STM).

- Forget gate: When an LTM enters this mode, useless data is forgotten.
- Learn gate: STM and event (current input) are combined so that the current input can use the essential knowledge that we have recently acquired via STM.
- Remember gate: This serves as an updated LTM by combining STM and event data with LTM information that we haven't forgotten.
- Utilize gate: This gate functions as an updated STM by predicting the output of the current event using LTM, STM, and event.

Breaking down the architecture of LSTM:

1) Learn gate: Takes event (E_t) and previous short-term memory (STM_{t-1}) as input and keeps only relevant information for prediction.
    - Previous short-term memory STM_{t-1} and current event vector E_t are joined together [STM_{t-1}, E_t] and multiplied with the weight matrix W_n having some bias which is then passed to tanh (hyperbolic tangent) function to introduce non-linearity to it, and finally creates a matrix N_t.
    - For ignoring insignificant information, we calculate one Ignore Factor it, for which we join short term memory STM_{t-1} and current event vector E_t and multiply with weight matrix W_i and passed through sigmoid activation function with some bias.
    - Learn matrix N_t and ignore factor it is multiplied together to produce learn gate result.
2) The forget gate: Takes previous long-term memory (LTM_{t-1}) as input and decides on which information should be kept and which to forget.

- Previous short-term memory STM_{t-1} and current event vector E_t are joined together [STM_{t-1}, E_t] and multiplied with the weight matrix W_f and passed through the Sigmoid activation function with some bias to form forget factor f_t.
- Forget factor f_t is then multiplied with the previous long-term memory (LTM_{t-1}) to produce forget gate output.

3) The remember gate: Combine previous short-term memory (STM_{t-1}) and current event (E_t) to produce output.
   - The output of forget gate and learn gate are added together to produce an output of remember gate which would be LTM for the next cell.
4) The use gate: Combine important information from previous long-term memory and previous short-term memory to create STM for next and cell and produce output for the current event.
   - Previous long-term memory (LTM_{t-1}) is passed through Tangent activation function with some bias to produce U_t.
   - Previous short-term memory (STM_{t-1}) and current event (E_t)are joined together and passed through sigmoid activation function with some bias to produce V_t.
   - Output U_t and V_t are then multiplied together to produce the output of the use gate which also works as STM for the next cell.

As depicted in **Figure 5**, a time window of past data can be represented as $W\text{past} = (St, St+1, \ldots, St+k)$, where *St* represents a sensor reading at time *t*, and the time window has a size of *k*. Subsequently, this sequence is utilized to predict a future time-window sequence $W\text{future} = St+k+1, St+k+1, St+k+2, \ldots, St+k+m$, with the time window size being *m*. In this particular experiment, we are forecasting a single future value, namely $W\text{future} = St+k+1$, where $m = 1$. The value of *k* is set to 60. A step (or distance) can be defined between *W*past and *W*past + 1. If the starting point of *W*past is *St*, the starting point of *W*past + 1 is *St* + step. We have set the step to be 1. As demonstrated in **Figure 5**, for the neural model, we employ a single LSTM layer and a dense layer to construct a basic model. We can fine-tune the LSTM layer's unit count to enhance its performance. The units in the dense layer are set to match the size of the *W*future window (i.e., m). The model is designed to predict values within the future time window $W\hat{}future$.

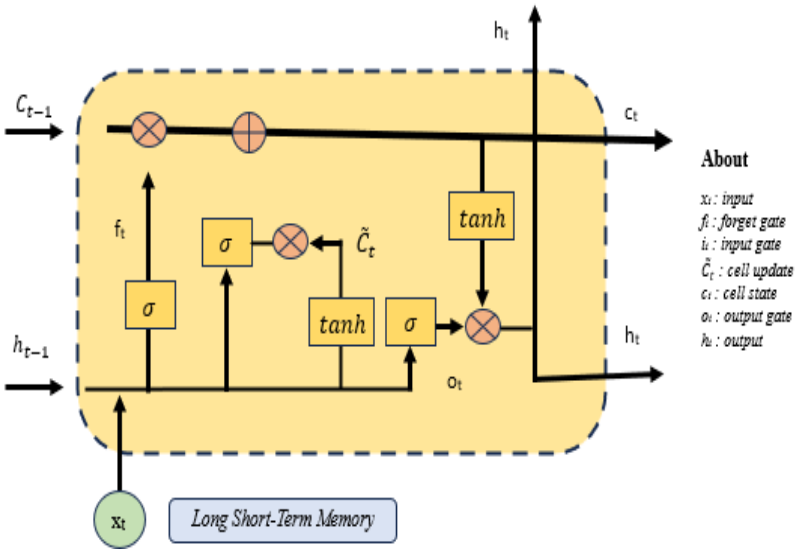

Figure 5. LSTM unit schema representation.

Anomaly scores:

We use prediction errors to determine anomaly scores, with a focus on having the model calculate and reduce the mean squared error (MSE) between the observed *W*future and the predicted $W\hat{}future$. During the

training phase, the model acquires knowledge about the characteristics of normal data. In the testing phase, anomalies are identified when prediction errors exceed a predefined threshold. To build and validate the model, we employ 80% of the dataset for training and allocate 20% for validation.

Detection process:

The neural model's hyperparameters encompass factors such as the number of layers, batch size, epochs, learning rate, and the units within each layer, including LSTM and Dense layers. These hyperparameters are contingent on the specific learning task and the data's characteristics. Researchers must experimentally determine the most effective hyperparameter combinations. In our case, we established the batch size at 100, the learning rate at 0.001, and set the LSTM units to 30, as shown in **Figure 6**.

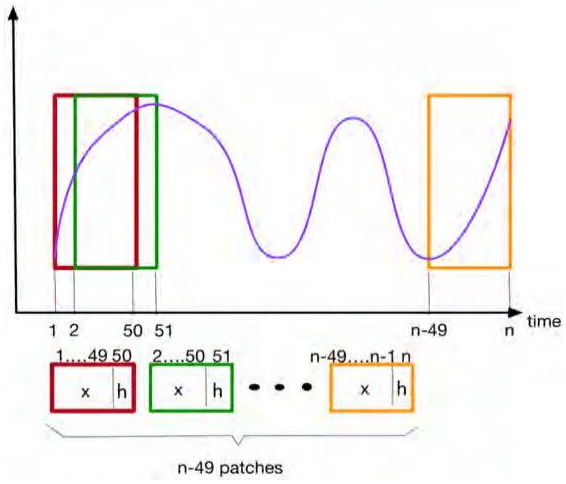

Figure 6. Sliding window showcase of LSTM unit.

4. Performance analysis

The proposed approach has been implemented on a range of hardware resources, including the GTX NV graphics card, a 1 TB hard drive, and the Windows 10 operating system. The software components employed in this implementation consist of Python, an open-source library for creating machine learning frameworks, and Google Colab, an open-source environment for constructing machine learning and deep learning models. The experimental analysis involves evaluating various metrics, including accuracy, sensitivity, specificity, precision, recall, F1-score, detection rate, true positive rate (TPR), false positive rate (FPR), throughput, security, and complexity. **Table 1** presents a comparative analysis between the proposed system, known as SLSTM-MCPS, and other cutting-edge models labelled as "L". SLSTM-MCPS outperforms other models with its models being trained and tested, which takes advantage of its intricate structure (**Figure 7**).

Table 1. Comparison analysis of accuracy, sensitivity, specificity.

Models	Accuracy	Sensitivity	Specificity
L1	76	85	88
L2	84	87	89
L3	86	81	86
L4	83	79	80
L5	88	92	89
SLSTM-MCPS	96	97	97

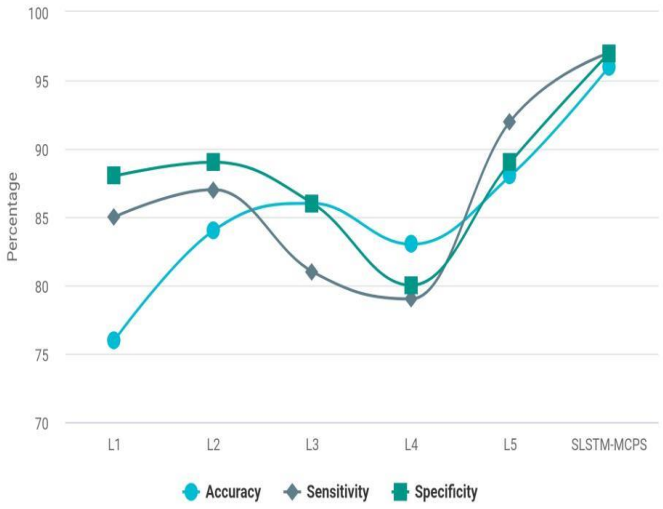

Figure 7. Models vs. accuracy, sensitivity, specificity.

Table 2. Comparison analysis of precision, recall, F1-score.

Models	Precision	Recall	F1-score
L1	72	77	83
L2	76	82	82
L3	83	84	85
L4	85	84	86
L5	81	86	89
SLSTM-MCPS	86	90	92

Table 2 illustrates a contrast in precision, recall, and F1-score among different models, underscoring the exceptional performance of the suggested system. This superiority can be attributed to the effectiveness of the deep learning model LSTM, which was implemented on a series of RNN layers. By multiple stacks of RNN, the complex structure will try to learn each parameter which is coming from a smart contract and able to process each unit and thereby efficacy of the classifier increased than expected (**Figure 8**).

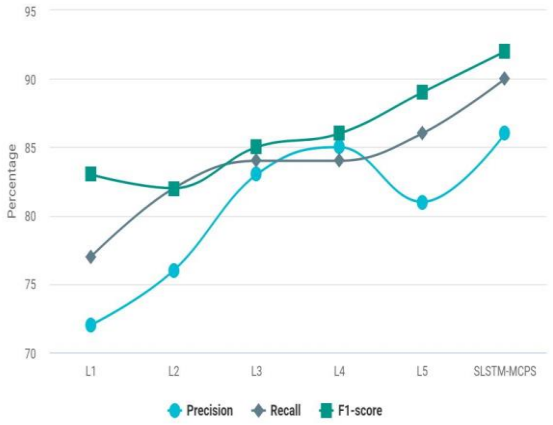

Figure 8. Models vs. precision, recall, F1-score.

Table 3 shows the comparison analysis of the proposed system over detection rate, true positive rate (TPR), and false positive rate (FPR). The proposed system outperforms as it overcomes the issue of usage of less complex blockchain systems and is able to train the classifier with its own capabilities. The system was able to train under greater parameters and also with quality processed inputs (**Figure 9**).

Table 3. Comparison analysis: Detection rate, TPR, FPR.

Models	Detection rate	TPR	FPR
L1	75	77	23
L2	72	75	25
L3	82	86	14
L4	85	82	18
L5	88	87	13
SLSTM-MCPS	94	90	10

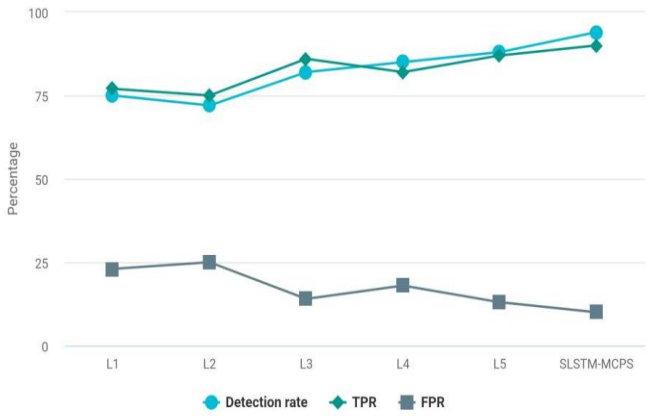

Figure 9. Models vs. detection rate, TPR, FPR.

Table 4. Models vs. throughput, security, complexity.

Models	Throughput	Security	Complexity
L1	✕	✕	✕
L2	✕	✓	✕
L3	✕	✕	✕
L4	✓	✕	✕
L5	✕	✕	✕
SLSTM-MCPS	✓	✓	✓

Table 4 shows the overall system improvement in giving a finalized better performance which is mainly security. It's clearly understood that other state-of-the-art models have fewer checks compared to our proposed model.

In the last, we found interesting research done by Meghna et al.[33] and Tyagi et al. [34] in their research articles regarding blockchain and its integration/ use in several sectors in today's scenarios.

5. Conclusion

In summary, the fusion of deep learning with smart contract-based blockchain technology has marked a significant breakthrough in the domain of medical cyber-physical systems (CPS). This innovative approach not only achieved an outstanding 96% accuracy rate in medical data analysis but also enhanced the security of these systems to unprecedented levels. By merging the data processing and analysis capabilities of deep learning with the inherent security attributes of blockchain, we have laid the groundwork for a more resilient, efficient, and trustworthy ecosystem for medical CPS. The promising outcomes of this research hold immense potential for reshaping healthcare, ensuring the privacy and authenticity of patient information, and ultimately enhancing patient outcomes. As we continue to refine and expand upon this integration, the future of medical

CPS appears brighter than ever.

Blockchain technology has the potential to revolutionize the field of medical cyber-physical systems, providing a secure, transparent, and efficient framework for managing healthcare data and devices. Looking ahead, the incorporation of blockchain technology into medical cyber-physical systems holds the potential to tackle vital healthcare challenges, including issues related to data security, interoperability, and the provision of patient-centred care. One of the primary benefits of blockchain in medical cyber-physical systems is data security. Medical data, including patient records, diagnostic information, and treatment plans, are highly sensitive and need to be protected from unauthorized access and tampering. Blockchain's decentralized and immutable ledger ensures that once data is recorded, it cannot be altered without consensus from the network. This guarantees the integrity and confidentiality of healthcare information, reducing the risk of data breaches and ensuring patients' privacy.

Moreover, blockchain enhances interoperability, a longstanding issue in healthcare. Different medical devices and systems often use incompatible data formats and protocols, making it challenging to exchange information seamlessly. Blockchain's standardized data structure and smart contracts can facilitate the interoperability of medical devices and systems, streamlining communication between various components of the healthcare ecosystem. Blockchain's patient-centric approach is another important aspect of its potential in medical cyber-physical systems. Patients can have greater control over their health data, deciding who can access it and for what purpose. This empowers individuals to actively participate in their healthcare decisions and research collaborations, fostering a more patient-centric and transparent healthcare system. In addition, blockchain can streamline the supply chain management of pharmaceuticals and medical devices, reducing counterfeit drugs and ensuring the authenticity and quality of products. This can save lives and resources by preventing the distribution of substandard or fake medications.

Author contributions

Conceptualization, BFB; methodology, KT and ST; software, KT and ST; validation, SMJS; formal analysis, SMJS; investigation, AKT; resources, AKT; data curation, AKT; writing—original draft preparation, AKT; writing—review and editing, AKT; visualization, AKT; supervision, AKT; project administration, AKT; funding acquisition, AKT. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. Norouzi M, Arshaghi A, Ashourian M. An Approach to Integrate Wireless Sensor Networks with Cloud Computing Technology in Medical Context. Majlesi Journal of Telecommunication Devices. 2023; 12(2).
2. Čuljak I. Method for analysis of sleep parameters based on ultra-wideband communication channel impulse response measurement [PhD thesis]. University of Zagreb. 2023.
3. Hernandez-Jaimes ML, Martinez-Cruz A, Ramírez-Gutiérrez KA, et al. Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud-Fog-Edge architectures. Internet of Things. 2023; 23: 100887. doi: 10.1016/j.iot.2023.100887
4. Bonomi F, Milito R, Natarajan P, Zhu J. Fog Computing: A Platform for Internet of Things and Analytics. In: Big Data and Internet of Things: A Roadmap for Smart Environments; Studies in Computational Intelligence; Springer: Cham, Switzerland, 2014; Volume 546, pp. 169-186.
5. Abbas F, Ke Y, Yu R, et al. Volatile terpenoids: multiple functions, biosynthesis, modulation and manipulation by genetic engineering. Planta. 2017; 246(5): 803-816. doi: 10.1007/s00425-017-2749-x
6. Vellela SS, Venkateswara Reddy B, Chaitanya KK, et al. An Integrated Approach to Improve E-Healthcare System using Dynamic Cloud Computing Platform. 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT). Published online January 23, 2023. doi: 10.1109/icssit55814.2023.10060945
7. Kumar R, Agrawal N. Analysis of multi-dimensional Industrial IoT (IIoT) data in Edge–Fog–Cloud based architectural frameworks : A survey on current state and research challenges. Journal of Industrial Information

Integration. 2023; 35: 100504. doi: 10.1016/j.jii.2023.100504
8. Aslam MM, Tufail A, Kim KH, et al. A Comprehensive Study on Cyber Attacks in Communication Networks in Water Purification and Distribution Plants: Challenges, Vulnerabilities, and Future Prospects. Sensors. 2023; 23(18): 7999. doi: 10.3390/s23187999
9. Biais B, Capponi A, Cong LW, et al. Advances in Blockchain and Crypto Economics. Management Science. 2023; 69(11): 6417-6426. doi: 10.1287/mnsc.2023.intro.v69.n11
10. Srilatha D, Nadesan T. Blockchain for Cyber-Physical Systems. Blockchain Applications - Transforming Industries, Enhancing Security, and Addressing Ethical Considerations. Published online July 26, 2023. doi: 10.5772/intechopen.110394
11. Mounir S, Maleh Y. Cybersecurity Management in Cyber-Physical Systems Using Blockchain. Computational Intelligence for Cybersecurity Management and Applications. Published online March 14, 2023: 209-234. doi: 10.1201/9781003319917-14
12. Al-Ghuraybi HA, AlZain MA, Soh B. Exploring the integration of blockchain technology, physical unclonable function, and machine learning for authentication in cyber-physical systems. Multimedia Tools and Applications. Published online September 29, 2023. doi: 10.1007/s11042-023-16979-2
13. Kanagala P. Effective cyber security system to secure optical data based on deep learning approach for healthcare application. Optik. 2023; 272: 170315. doi: 10.1016/j.ijleo.2022.170315
14. Alzahrani A, Alshehri M, AlGhamdi R, et al. Improved Wireless Medical Cyber-Physical System (IWMCPS) Based on Machine Learning. Healthcare. 2023; 11(3): 384. doi: 10.3390/healthcare11030384
15. Akbarfam AJ, Barazandeh S, Maleki H, Gupta D. Deep learning meets blockchain for automated and secure access control.
16. Vignesh Saravanan K, Thilaga PJ, Kavipriya S, Vijayalakshmi K. Data Protection and Security Enhancement in Cyber-Physical Systems Using AI and Blockchain. In: AI Models for Blockchain-Based Intelligent Networks in IoT Systems: Concepts, Methodologies, Tools, and Applications. Cham: Springer International Publishing; 2023. pp. 285-325.
17. Ali A, Ali H, Saeed A, et al. Blockchain-Powered Healthcare Systems: Enhancing Scalability and Security with Hybrid Deep Learning. Sensors. 2023; 23(18): 7740. doi: 10.3390/s23187740
18. Chakraborty C, Nagarajan SM, Devarajan GG, et al. Intelligent AI-based Healthcare Cyber Security System using Multi-Source Transfer Learning Method. ACM Transactions on Sensor Networks. Published online May 15, 2023. doi: 10.1145/3597210
19. Myrzashova R, Alsamhi SH, Shvetsov AV, et al. Blockchain Meets Federated Learning in Healthcare: A Systematic Review with Challenges and Opportunities. IEEE Internet of Things Journal. 2023; 10(16): 14418-14437. doi: 10.1109/jiot.2023.3263598
20. Kumar A, Chatterjee K. A lightweight blockchain-based framework for medical cyber-physical system. The Journal of Supercomputing. 2023; 79(11): 12013-12041. doi: 10.1007/s11227-023-05133-2
21. Meghna Manoj Nair, Amit Kumar Tyagi, Chapter 11 - AI, IoT, blockchain, and cloud computing: The necessity of the future, Editor(s): Rajiv Pandey, Sam Goundar, Shahnaz Fatima, Distributed Computing to Blockchain, Academic Press, 2023, Pages 189-206, ISBN 9780323961462, https://doi.org/10.1016/B978-0-323-96146-2.00001-2.
22. Pelekoudas-Oikonomou F, Ribeiro JC, Mantas G, et al. Prototyping a Hyperledger Fabric-Based Security Architecture for IoMT-Based Health Monitoring Systems. Future Internet. 2023; 15(9): 308. doi: 10.3390/fi15090308
23. Rai BK. PcBEHR: patient-controlled blockchain enabled electronic health records for healthcare 4.0. Health Services and Outcomes Research Methodology. Published online June 7, 2022. doi: 10.1007/s10742-022-00279-7
24. Paulraj D, R L, Jayasudha T, et al. Blockchain-based Wireless Sensor Network Security Through Authentication and Cluster Head Selection. 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS). Published online February 24, 2023. doi: 10.1109/icicacs57338.2023.10099593
25. Duggineni S. Impact of Controls on Data Integrity and Information Systems. Science and Technology. 2023; 13(2): 29-35.
26. Wang J, Chen J, Xiong N, et al. S-BDS: An Effective Blockchain-based Data Storage Scheme in Zero-Trust IoT. ACM Transactions on Internet Technology. 2023; 23(3): 1-23. doi: 10.1145/3511902
27. Al Amin M, Altarawneh A, Ray I. Informed Consent as Patient Driven Policy for Clinical Diagnosis and Treatment: A Smart Contract Based Approach. Proceedings of the 20th International Conference on Security and Cryptography. Published online 2023. doi: 10.5220/0012090600003555
28. Cerchione R, Centobelli P, Riccio E, et al. Blockchain's coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem. Technovation. 2023; 120: 102480. doi: 10.1016/j.technovation.2022.102480
29. Taherdoost H. Smart Contracts in Blockchain Technology: A Critical Review. Information. 2023; 14(2): 117. doi: 10.3390/info14020117
30. Zhang W, Huo X, Bao Z. An alliance chain-based incentive mechanism for PSG data sharing. Peer-to-Peer Networking and Applications. Published online October 21, 2023. doi: 10.1007/s12083-023-01571-0
31. Wang H, Li H, Smahi A, et al. MIS: A Multi-Identifier Management and Resolution System in the Metaverse.

ACM Transactions on Multimedia Computing, Communications, and Applications. Published online May 26, 2023. doi: 10.1145/3597641
32. Bilgili M, Pinar E. Gross electricity consumption forecasting using LSTM and SARIMA approaches: A case study of Türkiye. Energy. 2023; 284: 128575. doi: 10.1016/j.energy.2023.128575
33. Meghna Manoj Nair and Amit Kumar Tyagi, "Blockchain technology for next-generation society: current trends and future opportunities for smart era", in the book: Blockchain Technology for Secure Social Media Computing, 2023. DOI: 10.1049/PBSE019E_ch11.
34. Tyagi AK, Dananjayan S, Agarwal D, Thariq Ahmed HF. Blockchain—Internet of Things Applications: Opportunities and Challenges for Industry 4.0 and Society 5.0. Sensors. 2023; 23(2):947. https://doi.org/10.3390/s23020947