IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 23 April 2024, accepted 17 May 2024, date of publication 23 May 2024, date of current version 31 July 2024.

*Digital Object Identifier 10.1109/ACCESS.2024.3404656*

RESEARCH ARTICLE

# BBAD: Blockchain-Backed Assault Detection for Cyber Physical Systems

**MASOOMA ANWAR[1], NOSHINA TARIQ[1], MUHAMMAD ASHRAF[2], SYED ATIF MOQURRAB[3], BAYAN ALABDULLAH[4], HATOON S. ALSAGRI[5], AND ABRAR ALMJALLY[6]**

[1]Department of Avionics Engineering, Air University, Islamabad 44000, Pakistan
[2]School of Electrical Engineering and Computer Science, National University of Sciences & Technology, Islamabad 44000, Pakistan
[3]School of Computing, Gachon University, Sujeong-gu, Seongnam-si 13120, South Korea
[4]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P. O. Box 88428, Riyadh 11671, Saudi Arabia
[5]Information Systems Department, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University, Riyadh 13318, Saudi Arabia
[6]Information Technology, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University, Riyadh 13318, Saudi Arabia

Corresponding author: Bayan Alabdullah (bialabdullah@pnu.edu.sa)

This work was supported by Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia, through the Researchers Supporting Project PNURSP2024R440.

**ABSTRACT** Cybersecurity challenges pose a significant threat to Healthcare Cyber Physical Systems (CPS) because they heavily rely on wireless communication. Particularly, jamming attacks can severely disrupt the integrity of these CPS networks. This research introduces a decentralized system to address this issue. Therefore, this paper suggested a system that leverages trust and blockchain technology to detect jamming attacks in healthcare CPS effectively. It proposes a layered model to improve CPS networks' lifetime and performance. In smart healthcare environments, it ensures secure and reliable communication between sensor nodes, wearable sensors, medical devices, and monitoring systems. Results show that the suggested approach outperforms the baseline model in identifying and minimizing jamming assaults, with an average percentage difference of 15.71% more detection rate, 20.21% less packet loss rates, 16.65% less node-level energy consumption, reduced network latency of 8.29%, and 9.63% more network throughput.

**INDEX TERMS** Smart healthcare, cyber-physical systems, jamming attacks, sensor nodes, trust.

## I. INTRODUCTION

The world of technology has seen a major transformation with the rise of Cyber Physical Systems (CPS), affecting various sectors through the merger of mobile tech, wireless innovations, and the blending of physical and digital operations. [1]. These systems unite tangible objects with digital communication, creating a dynamic network. The physical parts of CPS, such as sensors and actuators, gather and act on data from the environment. At the same time, the cyber aspect involves computing tools that process this data for instant analysis and decision-making [2]. This integration allows real-world objects to translate vast amounts of data into actionable insights, aiming for seamless interaction between the physical and digital realms to foster continuous integration and smart decision-making [3], [4].

The associate editor coordinating the review of this manuscript and approving it for publication was Binit Lukose.

This breakthrough is set to revolutionize industries including energy, healthcare, and business, particularly impacting healthcare due to the critical nature of patient data reliant on continuous health monitoring via sensors [2]. It is critical to assure trust in data with various sensors interacting and communicating the system [5]. With CPS handling significant sensitive data, establishing strong security measures is essential to safeguard data integrity, confidentiality, and availability from cyber threats [2].

As the reliance on CPS grows, especially in healthcare for remote care and quick diagnostics, ensuring top-notch security for data transfer becomes imperative due to the sensitive information involved. However, many CPS devices are vulnerable to unauthorized access and data breaches [2], [6]. This paper proposes a blockchain solution to counteract jamming attacks in healthcare CPS, offering a robust alternative to traditional security methods and showing promise over other technologies like Deep Learning (DL), AI,

and Federated Learning (FL). In this perspective, blockchain implementation is particularly designed to defend against these challenges.

In contrast to the traditional Machine Learning (ML) approaches with inflexible and non-scalable systems in emerging healthcare environments [7], blockchain technology provides high reliability due to the decentralized design and is compliant against jamming attacks. Furthermore, with a static and immutable ledger, the transactions over it can undoubtedly have even higher security than the present DL and FL ways. That is, where FL may fall short in maintaining privacy and reliability of the data across distributed networks [8], blockchain offers cryptographic mechanisms to ensure data confidentiality and reliability. The smart contract technology coming under blockchain technology provides immediate and automatic responses to any kind of attack. It means the level of flexibility and efficiency that the user would conventionally not have been able to secure from using AI methods. Unsurpassed by any AI model in operation with the help of huge training data and enormous computing power, blockchain smart contracts provide quick, efficient decision-making [9]. This means that the effects of jamming attacks on healthcare operations are lessened. This research centers on bolstering the security and dependability of healthcare systems by integrating blockchain and smart contract technologies to secure data and evaluate trust. The paper's significant contributions include:

1) The introduction of a sophisticated Trust-based layered framework for healthcare CPS, supported by a blockchain-empowered fog layer, aiming to enhance trust and security in these systems.
2) Achieving a superior detection rate and a reduction in packet loss, surpassing current leading methods.

The remaining paper is structured as follows: Section II presents a complete background of CPS and its applications. Section III contributes a detailed related work, whereas Section IV describes the research gap of the study. Section V provides a scenario based on a reactive jamming attack. Section VI illustrates the proposed plan. Section VII demonstrates the experimentation and results. Section VIII presents the discussion on the acquired results of the study. Finally, Section IX delves into the conclusion of the paper along with its possible future directions.

## II. BACKGROUND

This section details the background of CPS, and a functionality-based blockchain is proposed to be implemented.

### A. APPLICATIONS OF CYBER PHYSICAL SYSTEMS

CPS finds applications in various fields, including the following:

1) **Smart Grids**: Integration of CPS into smart grid management enables the monitoring and optimization of power generation, distribution, and consumption. This technology facilitates integrating renewable energy sources, grid stability management, and responsive demand strategies, fostering a reliable and sustainable power grid infrastructure [10].
2) **Smart Transport Systems**: CPS significantly improves transportation systems through real-time monitoring, data analytics, and informed decision-making. Notable CPS-driven applications include smart transportation infrastructure, autonomous vehicles, vehicle-to-vehicle communication, and smart traffic flow solutions, all contributing to reduced congestion and improved road safety [11].
3) **Healthcare and Telemedicine**: By integrating sensors, wearable technology, and data analytics for remote patient monitoring, individualized treatment, and efficient healthcare delivery, CPS has valuable applications in healthcare. These CPS applications improve patient care standards and facilitate early disease detection [12].
4) **Industrial Automation and Production**: CPS enables smart automation and optimization of manufacturing processes, resulting in increased productivity, consistency, and adaptability. CPS technologies streamline supply chain management, smart factory operations, and digital twin simulations, reducing downtime and increasing productivity [13].
5) **Smart Cities**: CPS plays a crucial role in developing smart cities that enhance the quality of life for their citizens. Applications include waste management, environmental surveillance, automated transportation, energy efficiency, and infrastructure management. Through resource optimization, CPS and data-driven decision-making contribute to sustainable and livable urban environments [1].

### B. CPS AND BLOCKCHAIN

The convergence of blockchain and CPS can revolutionize numerous sectors, which include transportation, healthcare, manufacturing, and smart cities. Blockchain provides a decentralized database and cryptography techniques for storing and accessing the associated database [14]. With its secure and distributed ledger for tamper-proof records of transactions and sensor data, not only improves CPS security and dependability but also streamlines data sharing in CPS networks by facilitating direct communication via smart contracts and decentralized consensus mechanisms [15]. This integration improves identity management in CPS by enabling secure, decentralized authorization and verification processes that effectively reduce the risks associated with unauthorized access and data breaches [16]. Blockchain has become a key element in reorganizing CPS systems for greater security and effectiveness, as shown in Fig. 1.

This comprehensive integration redefines CPS systems, thereby improving their security and efficacy. IoT devices also play a vital role by contributing private data to shared blockchain transactions that ensure transparency, accountability, and dispute prevention for all parties involved [17]. In line

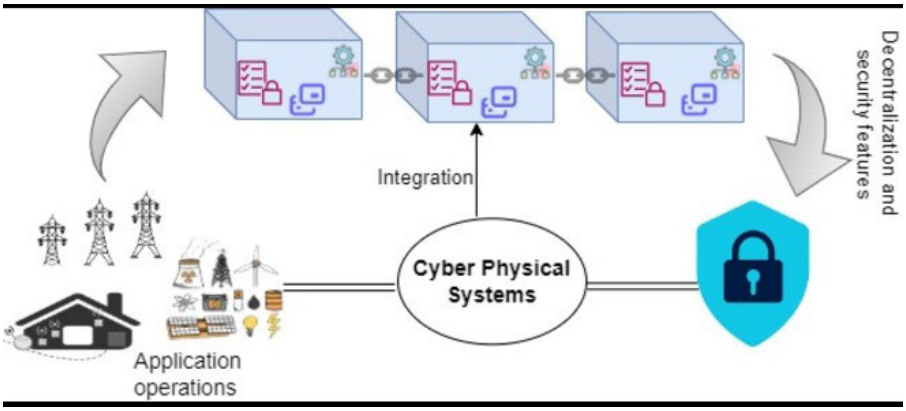


**FIGURE 1.** CPS and Blockchain.

with these transformative possibilities, the research conducted here involves evaluating existing cyber physical security measures, developing strategies to ensure uninterrupted CPS functionality, investigating advanced data transmission techniques, and implementing a blockchain-based security mechanism that ensures scalability, fault tolerance, and resilience. In addition to preventing single-point failures, this mechanism creates a decentralized, tamper-resistant CPS environment [18].

### C. CPS AND CYBER SECURITY

Cyber Physical Systems represent an industry-transforming convergence of physical components, computational intelligence, and networked communication [19]. However, this integration heightens the importance of cybersecurity. CPS combines the advantages of the physical and digital domains, thereby optimizing functionality and efficiency. However, it also introduces vulnerabilities that could be exploited by malicious actors, resulting in severe repercussions [20]. Critical infrastructures, manufacturing processes, healthcare systems, and transportation infrastructures are exposed to various cyber threats due to the interconnected nature of CPS [19]. The cyber threats that pose attacks on CPS are numerous and widespread. To procure unauthorized access to CPS networks, attackers could exploit system weaknesses like inadequate access controls or outdated software [21].

Prohibited access to CPS networks can cause operational disruption, loss of control, and possibly physical loss. Exploiting sensors' data or signals could compromise the accuracy and reliability of CPS functions, leading to decision-making mistakes. Additionally, Denial-of-Service (DoS) attacks could saturate CPS networks, disrupting services and diminishing crucial processes [21]. CPS systems can be taken captive by ransomware attacks that require payment to restore control. Because CPS relies on real-time communication, any interference with the correspondence channels could affect the integrity of the system and allow attackers to insert vicious commands or steal vulnerable information [21], [22]. The ever-changing nature of cyber-related threats underscores the necessity for extensive security measures to assure

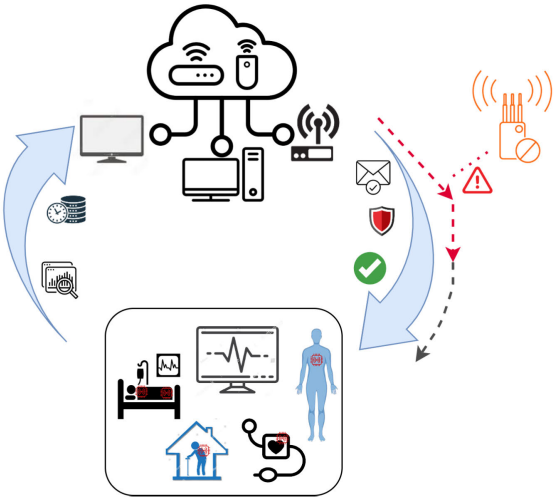

**FIGURE 2.** Reactive Jamming Attack.

CPS's security and safety and its reliability across different sectors [19].

### D. JAMMING ATTACKS

Jamming attacks are launched in wireless infrastructure by intentionally intruding with signals sent between nodes. These attacks manipulate weaknesses in wireless channels, hindering the usual activity of communications systems [23]. The consequences of the jamming attack are severe and can make crucial systems unavailable, damage the transmission of connected devices, and reduce the efficiency of the targeted network. These attacks increase interference or noise in the wireless communication range, impeding authorized devices' transmission or reception of data. This interference causes packet loss, signal quality degradation, and increased latency [24]. Jamming attacks can be executed using different methods, including jamming transmitters, software-based techniques, and software-defined radio manipulation.

One method is reactive jamming, which involves monitoring the communication channel and transmitting interference only when legitimate communication is detected, making it harder to detect and mitigate [25]. Such attacks have

**TABLE 1.** Various Attacks Impact.

| Attack | Attack Type | Network Performance |
|---|---|---|
| Malware | Internal | Compromised device functionality, data leakage |
| DoS | External | Service unavailability, degraded system responsiveness |
| Spoofing | External | Impersonation of authorized users, unauthorized access |
| Jamming | External | Disruption of wireless communication, increased latency |
| Ransomware | Internal | System lockdown, disruption of healthcare services |
| Wormhole | External | Fake shorter paths between network nodes, routing manipulation |
| Sybil | External | Creation of multiple fake identities to compromise network trust |
| Sniffing | External | Unauthorized interception of network traffic, data theft |
| Black Hole | External | Discards all received packets, disrupts communication |
| Sinkhole | External | Misdirects network traffic to a malicious entity, data interception |

far-reaching repercussions, affecting IoT devices, wireless networks, vital infrastructure, and military communications. Jamming attacks can compromise transportation, healthcare, emergency communication systems, and wireless network security and privacy [26].

### E. REACTIVE JAMMING ATTACK

A reactive jamming attack is a sophisticated cybersecurity threat that exploits vulnerabilities in wireless communication networks. Unlike Continuous Wave (CW) jamming, which involves continuous interference transmission across a range of frequencies, reactive jamming strategically disrupts communication only when it detects legitimate transmissions [27]. This approach makes the attack more challenging to detect and counteract. In a reactive jamming attack scenario, the attacker monitors the wireless communication channel, awaiting the transmission of legitimate signals by authorized devices.

Once such signals are detected, the attacker rapidly responds by transmitting interference or noise over the channel. This interference overwhelms legitimate signals, rendering them unreadable or causing them to be misinterpreted by receiving devices [28]. Reactive jamming attacks often leverage the dynamic nature of wireless networks, where the attacker can effectively identify communication patterns, frequencies, and timing to disrupt transmissions [29]. Figure 2 illustrates the reactive jamming attack, whereas Table 1 showcases the impact of various attacks in CPS.

## III. RELATED WORK

This review delves into the complex world of cybersecurity threats, focusing on jamming attacks targeting Healthcare CPS. It discusses the DAE-TRUST DL model, extensively reviewed in the work of [30], which capitalizes on Cognitive Radio (CR) technology to detect and neutralize jamming sources in IoT frameworks. Despite its innovative approach, misleading IoT devices could compromise the model's effectiveness, leading to potentially flawed spectrum allocation by Fusion Centers (FC). Moreover, Reference [31] proposes an Edge-AI-based (EAB) detection strategy for jamming, promising enhanced defense in IoT wireless networks. This method integrates sophisticated AI algorithms and immediate data processing at the network's edge. However, this Edge-AI methodology has challenges, such as being dependent on predefined features for detection and having very high resource demands; therefore, it is unfriendly to CPS settings with resource constraints.

Reference [40] follows a blockchain-based solution for the security of data. The authors proposed that data has to be selected using a combination of RSA hashing and Differential Evolution. However, many issues could be associated with this approach, such as reducing computational costs and the dependence on large data for training. The proposed blockchain model focused on decentralized consensus mechanisms and designed smart contracts. This method increases security and protection against threats while reducing computational demands. The importance of AI techniques, such as DL, FL, and ML, to safeguard the security of the CPS is described in [41]. Although the AI approach provides speedy ways of assessing the incidents, its generalization, accuracy, coverage, and variations in noise are some of the problems it faces. Few blockchain-based models also propose smart capabilities for increasing accuracy by overcoming the problematic issues related to different kinds of bandwidth limitations and deviations in noise. It reduces the bandwidth requirements by using another optimized execution consensus algorithm and uses cryptographic hashing for data integrity to lessen the impact of noise fluctuations.

The model in [42] shows how the PatternProof Malware Validation (PoPMV) algorithm can be implemented in Blockchain technology in Industry Cyber Physical Systems (ICPS). In combination, those two advanced methods of DL (specifically, Long Short-Term Memory (LSTM)) and reinforcement learning aim to increase both the security of ICPS and the speed of its processing. However, despite its benefits, the algorithm faces some challenges. For instance, when workflow tasks fail on various computing nodes, the algorithm experiences increased computation time. Moreover, existing methods may struggle to efficiently detect known and unknown attacks in distributed fog cloud microservices, particularly in healthcare applications. The proposed blockchain model incorporates decentralized consensus mechanisms to uphold data integrity and employs smart contracts for automated security enforcement. By utilizing the unalterable ledger of the blockchain, the model guarantees transparent record-keeping, enabling swift incident response. Moreover, the model includes dynamic microservice allocation and comprehensive attack detection algorithms, enhancing security and resilience.

**TABLE 2.** Comparison Among State-of-the-Art.

| Ref. | Attack | Characteristics/Features | Limitations |
|---|---|---|---|
| [28] | Reactive Jamming | Frequency hopping, random time intervals | Limited effectiveness |
| [32] | Continuous Wave Jamming | Continuous interference signal, signal strength modulation | Continuous interference signal hinders detection |
| [33] | Reactive Jamming | Dynamic power levels, spread spectrum modulation | Real-time detection challenges |
| [34] | Sweep Jamming | Wideband jamming, frequency agility | Sweep jamming across frequencies is hard to detect. |
| [35] | Reactive Jamming | Bursty transmission, adaptive jamming patterns | Rapid changes in attack patterns complicate defenses. |
| [36] | Randomized Jamming | Randomized frequency hopping, variable jamming intervals | Unpredictable attack patterns make defense difficult. |
| [37] | Reactive Jamming | Bitrate adaptation, adaptive waveform shaping | Rapid adaptation to network conditions complicates detection. |
| [38] | smart Jamming | ML-based jamming, energy-efficient attacks | Energy consumption, Adversarial intelligence adapts to countermeasures. |
| [39] | Reactive Jamming | Multi-dimensional parameter space, dynamic attack profiles | Only uses one parameter for mitigating attacks that may result in misleading trust results |

Reference [43] presented a method that uses DL to improve the security of anomaly detection in healthcare CPS. Their research uses neural networks to identify abnormal actions and potential risks in real-time. However, DL techniques face challenges in terms of scalability and interpretability, especially in complex healthcare CPS settings. Whereas the proposed blockchain-based approach enhances the trustworthiness and integrity of the data while also complementing the anomaly detection capabilities of DL models. Reference [44] presents a blockchain-based two-factor authentication system for the LoRaWAN join process. In a different context, Reference [45] explores the security performance of wireless blockchain networks against malicious jamming, utilizing the RAFT consensus mechanism. Reference [46] proposes a pursuing-evasion game among jammers and authorized nodes as a defense strategy against jamming attacks. This approach involves device nodes retreating from jammer locations to restore communication.

Reference [47] put forward a Bayesian game-theoretic mitigation strategy. Reference [48] introduces a reinforcement learning-based technique for addressing jamming attacks. Similarly, [49] proposes a 2-D mobile communication scheme using a deep Q-network approach with deep convolutional neural networks and macro-action techniques to expedite learning in dynamic scenarios. While proactive defense strategies hold promise, many mechanisms are centralized, limiting their applicability in highly mobile networks. In this context, [48] presents an FL-based mutable jamming attack defense strategy incorporating an on-device federated jamming detection process and a model-free Q-learning process with an adaptive exploration-exploitation epsilon-greedy policy. Table 2 presents the comparison among different state-of-the-art and Table 3 provides state-of-the-art details.

## IV. RESEARCH GAP

Based on comprehensive analysis, key areas of research gap and limitations have been identified in the cybersecurity frameworks for healthcare CPS. The existing models, like anomaly detection based on DL and resilience enhancement through fog computing, often encounter limitations in scalability and performance when applied to large-scale healthcare CPS deployments. These models struggle to handle the volume and complexity of data generated by interconnected healthcare devices and systems. Numerous current solutions concentrate on particular elements of cybersecurity, such as identifying anomalies or safeguarding data through encryption, without considering the wider demands for interoperability and integration in healthcare CPS environments. This absence of interoperability could impede the smooth transmission and examination of healthcare data among different systems and devices.

Moreover, many existing solutions rely on centralized security measures, such as intrusion detection systems and encryption techniques, which can introduce single points of failure and vulnerabilities. It can often bring along an intrinsic lack of transparency and result in security incidents. The proposed framework uses blockchain technology to overcome such constraints by rendering a decentralized approach to lightweight consensus and improved data structures tailor-made for healthcare CPS. It, therefore, enhances the scalability and performance of blockchain technology, enabling a better healthcare environment for cybersecurity. This strategy includes distributed security features that include decentralized consensus and an indestructible ledger that eliminates vulnerable areas and increases the security and integrity of information.

## V. SCENARIO: REACTIVE JAMMING ATTACK IN HEALTHCARE CPS

The following scenario is helpful in the healthcare CPS discussion of issues with reactive jamming and its implications.

### A. BACKGROUND

The CPS in smart healthcare centers monitors patients' vital signs in real time. The CPS includes various sensors, wearable

**TABLE 3.** State-of-the-art Details.

| Ref. | Trust model | Trust parameters | Simulator | Nodes | Time | Result |
|---|---|---|---|---|---|---|
| [50] | Intelligence-based | Packet loss rate | NS-3 | 150 | 1000 s | PLR < 27% |
| [51] | Behavior Analysis | Node Behavior, Node density | COOJA | 200 | 800 s | Node Density > 45% |
| [52] | Fuzzy | Energy consumption | COOJA | 120 | 900 s | Energy < 50% |
| [53] | ML | Feature selection, PLR | TensorFlow | 250 | 2000 s | PLR < 18% |
| [54] | Hybrid | PDR, Node Density | OMNeT++ | 200 | 500s | PDR > 85% |
| [55] | Game Theory | Packet Loss | MATLAB | 50 | 2000s | PLR < 15% |
| [56] | Trust-based | Packet loss | COOJA | 75 | 800s | NM < 18% |
| [57] | Fuzzy | Energy | COOJA | 50 | 1500s | Energy < 28% |
| [58] | Bayesian Inference | PLR | NS-3 | 300 | 1500s | PLR < 20% |
| [59] | Fuzzy | Energy | OMNeT++ | 300 | 1500s | Energy > 45% |

gadgets, and an overall monitoring approach. Patients depend on this system to favor continuous monitoring of their health. Any disturbance or alteration to the information could result in serious negative consequences.

### B. SCENARIO DESCRIPTION

- **Network Configuration:**
  - The Healthcare CPS network consists of 100 sensor nodes ($N = 100$) distributed throughout the facility.
  - These sensor nodes continuously collect and transmit vital sign data (e.g., heart rate, blood pressure, temperature) to the central monitoring system.
  - Communication between sensor nodes and the central system occurs wirelessly, making the network susceptible to jamming attacks.
- **Attack Initiation ($P_t$):**
  - At a specific time step ($t$), an attacker initiates a reactive jamming attack ($P_t = 0.05$).
  - The attacker aims to disrupt the communication between sensor nodes and the central monitoring system.
- **Node Detection and Confirmation:**
  - Upon the initiation of the attack, affected sensor nodes ($N_a$) detect the sudden disruption in data transmission based on trust assessment ($P_{\text{detect}}$).
  - These nodes flag the anomaly as a potential attack.
  - Neighboring nodes utilize trust-based information to validate the attack ($P_{\text{validate}}$).
- **Alert Generation and Countermeasures:**
  - Affected nodes ($N_a$) generate alerts ($P_{\text{alert}}$) to inform the central system and administrators about the attack.
  - The central system receives the alerts and immediately investigates and mitigates the attack.
  - Some affected nodes attempt to implement trust-based countermeasures ($P_{\text{countermeasure}}$) to bypass the jamming interference, such as switching communication frequencies or adjusting transmission power.
- **Network Resilience and Unaffected Nodes:**
  - Despite the attack, a portion of the sensor nodes ($N_u$) remains unaffected ($N_u = 80$).
  - Unaffected nodes continue to transmit accurate data to the central system.
  - Unaffected nodes refrain from generating false alerts ($P_{\text{no\_alert}}$) to avoid unnecessary disruptions.
- **Challenges and Consequences:**
  - The reactive jamming attack disrupts the healthcare CPS network, leading to temporary data loss and delays in vital sign monitoring.
  - The central system's response time is crucial in mitigating the attack and resuming normal operations.
  - Countermeasures implemented by affected nodes may or may not be successful ($P_{\text{no\_countermeasure}}$) in overcoming the jamming interference.
  - Administrators must analyze the attack patterns and trust data to enhance the system's security and adapt to evolving threats.

*Theorem 1:* In the presence of a reactive jamming attack ($P_t > 0$), the sensor nodes ($N$) in the healthcare CPS network experience disruptions in data transmission.

*Proof:* The reactive jamming attack initiated by the attacker ($P_t > 0$) interferes with wireless communication between sensor nodes ($N$) and the central monitoring system, resulting in disruptions in data transmission. Thus, the theorem is proven.

*Lemma 1:* Affected sensor nodes ($N_a$) detecting the attack based on trust assessment ($P_{\text{detect}} > 0$) correctly flag the anomaly as a potential attack.

*Proof:* When the reactive jamming attack occurs ($P_{\text{detect}} > 0$), sensor nodes with trust-based anomaly detection capabilities correctly identify the sudden disruption in data transmission as a potential attack. Thus, the lemma is proven.

*Proposition 1:* Utilizing trust-based information, neighboring nodes can effectively validate the legitimacy of a reactive jamming attack ($P_{\text{validate}} > 0$).

*Proof:* Neighboring nodes collaborate and utilize trust-based information to validate the legitimacy of a reactive jamming attack. This trust-based approach is an effective method to confirm the presence of an attack. Thus, the proposition is proven.

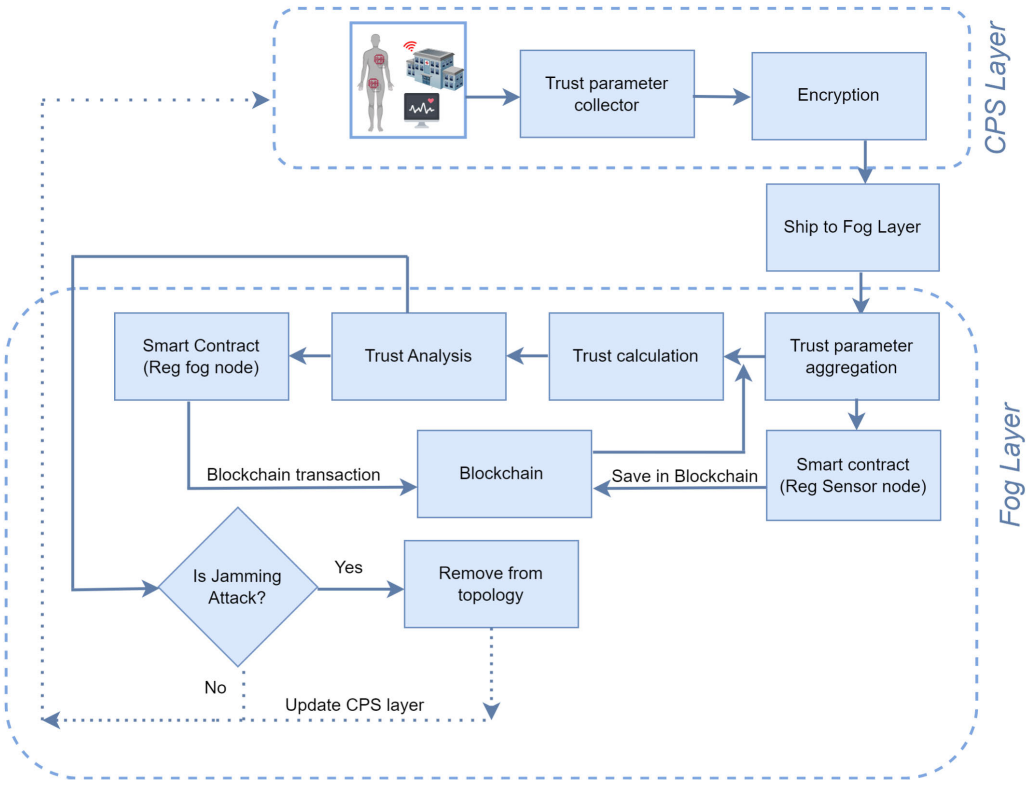


**FIGURE 3.** The proposed model architecture.

## VI. PROPOSED WORK: BLOCKCHAIN-BACKED ASSAULT DETECTION IN HEALTHCARE CYBER PHYSICAL SYSTEMS

This section presents a framework for detecting cyber attacks, specifically jamming attacks, on Healthcare CPS using blockchain technology based on our previous work [8]. It seeks to enhance the security and reliability of communication channels in smart healthcare infrastructures by addressing the disruptions caused by these malicious jamming attacks. By integrating blockchain into both the Fog and CPS layers, the approach significantly strengthens the defense mechanism of the smart healthcare system.

As shown in Fig. 3, the research blueprint advocates for a dual-layered architecture: the CPS device layer and the Fog Layer, each playing a pivotal role in ensuring the uninterrupted and secure exchange of information across the healthcare system. This framework is dedicated to mitigating the impact of jamming attacks on Healthcare CPS, promising a more secure, dependable, and trustworthy smart healthcare environment through the strategic application of blockchain technology across critical layers.

### A. FOG LAYER

This section describes how CPS can enable the Fog Layer, the CPS, and the device layer, which includes the communication of the sensor nodes employed in the CPS layer in the smart healthcare system. Sensor nodes are liable for gathering vital data and play an essential part in the system's operation. Attacks that block Healthcare CPS are tackled through these layers, which ensure communication safety and reliability in smart healthcare systems. Integrating blockchain technology into our structure increases health systems' security, reliability, and security with smart technology. Through encryption and further security approaches, the fog nodes are regarded as reputed service providers that ensure security. Fog layers make it simpler for the nodes of the CPS layer to exchange information and assess each other's trustworthiness. It consists of the following modules:

1) The Trust Parameter Aggregation Module: It collects and aggregates trust-related parameters derived through the CPS layer. The parameters include information relating to the authenticity of the source, the quality of the communication, and behavior patterns. Aggregation plays a crucial role in preparing data to aid in trust analysis and assessment. This module is created to warrant that the data is properly structured and formatted for successive analysis.
2) Smart Contracts Module: Integration of the Smart Contracts Modules inside this layer is vital since it allows the registration of the fog and sensor nodes to the blockchain. The system oversees the registration of sensor nodes in the blockchain, monitors their existence, and assigns an initial trust value. Furthermore, fog nodes are crucial in enabling registration in the blockchain network. The primary function of this module is to

guarantee the accurate registration and identification of sensor and fog nodes in the blockchain system, thereby augmenting the security and transparency of the network.

3) Blockchain Module: This module stores the trust-related data in the blockchain to ensure its transparency, immutability, and accessibility. The data is ready to be recorded on the blockchain after it has been collected and analyzed. It also registers the systems, sensor, and fog nodes through automated smart contract rules. Blockchain ensures that recorded data cannot be changed or deleted, which results in a reliable historical record of transactions in the CPS environment.
4) Trust Calculation Module: It uses a Hybrid model to calculate the trustworthiness of the nodes. It evaluates each node's trust using both behavior and reputation metrics. It calculates the overall trust scores before transmitting them for further analysis. This process is necessary to evaluate the node's reliability in the network.
5) Trust Analysis Module: This module analyzes the computed scores in real time to detect trust deviation patterns. Thus, it will monitor suspicious patterns from data sources and computed trust scores. From the historical trust data and predefined thresholds, it detects suspicious patterns related to the reactive jamming nodes. This module is a network security response that is initiated upon the discovery of any anomaly or attack.
6) Topology Update Module: It is very instrumental in keeping the integrity and security of the network by updating the data in the nodes and their levels of trust by identifying and deleting the malicious nodes from the topology.

### B. THE CPS LAYER

The CPS Layer has the following modules:

1) Trust Parameter Collector Module: This Module operates in the CPS layer and is essential in collecting sensor trust-related data. It collects information about the source's identity, communication quality, and behavior patterns. These parameters are vital for evaluating the dependability of nodes and, in particular, identifying the possibility of reactive jamming attacks. The Module's data collection provides input for trust analysis and evaluation.
2) Encryption Module: After acquiring trust data, the Encryption Modules charged with protecting it are then charged with encrypting it. They secure the data to safeguard its confidentiality and warrant its security throughout transmission. Healthcare settings insist on security to safeguard sensitive patient information. This module utilizes encryption methods to protect the trust parameters of the Fog layer for further processing.
3) Shift to Fog Layer Module: It is an intermediary element that connects CPS to the Fog Layer. CPS and the module's role is to transmit the encrypted parameters related to trust from the CPS layer to the Fog layer. The ease of processing trust-related data can be seen in the Fog layer, where trust analysis and evaluation occur.

**Algorithm 1 Description:** Algorithm 1 improves Healthcare CPS privacy and trust. First, it starts with a system of good trust and better security. Second, it introduces the CPS and Fog Layers background of the algorithm. Step 3 would be placing sensor nodes in the CPS Layer in a well-thought-out manner to enhance data collection. Finally, Step 4 would install Fog nodes in the Fog Layer to enhance proper data processing and transmission. Function: Step 5 is paramount and central because it aims to boost trust and security by gathering trust-related features from the Sensor Nodes, encrypting this information, and forwarding it to the Fog Layer for further processing. These improve private medical information protection and create an improved, secure network environment in the Healthcare CPS.

### C. METHODOLOGY FOR DETECTING REACTIVE JAMMING ATTACKS IN CPS USING A HYBRID TRUST MODEL AND BLOCKCHAIN

The proposed strategy is designed as a multilayer defense to counter such cyber threats robustly. It sets the reactive jamming attack detection technique and provides a comprehensive framework with functions as shown in the referenced algorithm. It covers the reactive jamming attack detection technique and introduces a comprehensive framework as depicted in the referenced Algorithm. 1.

#### 1) TRUST MODEL DESIGN

First, in the trust model, we define the key metrics to measure the trust of CPS nodes. It computes a Hybrid Trust Score ($\Theta_{TS}$) that is computed from a reputation score ($\rho$) based on historical actions and a Behavior Score ($\beta$) representing activities of the present. This dual score ensures a balanced trust evaluation, considering both past behaviors and present operations.

1) Define the trust assessment metrics: The metrics used are as follows:
   a) Reputation Score ($\rho$): This score is derived from the track record of data transmissions ($\Sigma_{TX}$) and detected attack incidents ($\Delta_{AT}$) in a specific timeframe, providing a historical perspective on trust, as shown in Eq. 1.

$$\rho = \frac{\Sigma_{TX}}{\Sigma_{TX} + \Delta_{AT}} \tag{1}$$

   b) Behavior Score ($\beta$): t assesses real-time metrics such as communication reliability ($C_{RT}$), responsiveness, ($RS_{Tm}$), and consistency of data ($D_{Cn}$) offering an up-to-the-minute trust evaluation.

$$\beta = \omega_1 \times C_{RT} + \omega_2 \times RS_{Tm} + \omega_3 \times D_{Cn} \tag{2}$$

   In Eq. 2, $\omega_1, \omega_2, \omega_3$ are weight factors representing the importance of each behavior metric.
   c) Hybrid Trust Score Calculation: This phase zeroes in on pinpointing reactive jamming attacks

**Algorithm 1** Reactive Jamming Attack Detection Algorithm

**Input:** Trust-related data, Sensor nodes, Fog nodes
**Output:** Enhanced security and trust in Healthcare CPS
**Initialization:**
**Function** `DefineLayers`:
  **Data:** None
  **Result:** CPSLayer, FogLayer
  CPSLayer ← `CreateCPSLayer()`;
  FogLayer ← `CreateFogLayer()`;
  **return** *CPSLayer, FogLayer*;
**Function** `CreateCPSLayer`:
  **Data:** None
  **Result:** SensorNodes
  **foreach** *sensor node s* **do**
    DeploySensorNode(*s*);
  **return** *SensorNodes*;
**Function** `CreateFogLayer`:
  **Data:** None
  **Result:** FogNodes
  **foreach** *fog node f* **do**
    DeployFogNode(*f*);
  **return** *FogNodes*;
**Set:**
**Function** `InitializeSensorNodes`:
  **Data:** None
  **Result:** Enhanced security and trust in Healthcare CPS
  **foreach** *sensor node s* **do**
    TrustParams ← CollectTrustParameters(*s*);
    EncryptedData ← EncryptTrustData(TrustParams);
    TransmitDataToFogLayer(EncryptedData);
**Do Process:**
**Function** `InitializeFogNodes`:
  **Data:** None
  **Result:** Enhanced security and trust in Healthcare CPS
  **foreach** *fog node f* **do**
    AggregatedTrustData ← AggregateTrustDataFromCPSLayer();
    InitializeSmartContracts(*f*);
    RegisterNodesInBlockchain(*f*, SensorNodes, FogNodes);
**Function** `CalculateTrustScores`:
  **Data:** None
  **Result:** Enhanced security and trust in Healthcare CPS
  **foreach** *fog node f* **do**
    TrustScores ← CalculateTrustScores(*f*);
    AnalyzeTrustScores(TrustScores);
    IdentifyAttacksAndDeviation(TrustScores);
    RespondToAttacksAndDeviation(TrustScores);
    InitializeSmartContracts(*t*);
    StoreTrustScoreToBlockchain(*t*, SensorNodes, TrustScore);
**Check:**
**Function** `UpdateTopology`:
  **Data:** None
  **Result:** Enhanced security and trust in Healthcare CPS
  **foreach** *sensor node s* **do**
    UpdateNodeStatusFromFogLayer(*s*);
    **if** *MaliciousNodeDetected(s)* **then**
      RemoveNodeFromTopology(*s*);

in CPS. Nodes actively monitor for red flags indicating possible jamming, like unexpected packet drops, signal fluctuations, or odd traffic flows. Upon suspecting a jamming attempt, a node flags it and initiates a trust verification process. It employs blockchain-enabled smart contracts to alert $\Theta_{TS}$ for cross-validation. These neighbors then corroborate the alert using the shared trust data on the blockchain, reaching a consensus via smart contracts. If the threat is confirmed by a sufficient number of peers, an alert is issued, prompting counteractions such as frequency or power adjustments.

$$\Theta_{TS} = \alpha \times \rho + (1 - \alpha) \times \beta \tag{3}$$

In Eq. 3, $\alpha$ is a weighting factor representing the relative importance of reputation-based trust assessment compared to behavior-based trust assessment, and its value ranges from 0 to 1.

d) Blockchain Integration:
Incorporating blockchain into the CPS enhances data security and trustworthiness. It secures trust scores and behavior logs in an immutable blockchain ledger, accessible to authorized network nodes. Smart contracts on the blockchain streamline the trust assessment and verification, executing algorithms and consensus protocols to authenticate trust scores network-wide. This setup ensures secure data exchange regarding detected threats and countermeasures among nodes and fortifies overall communication security in the smart healthcare CPS.

i) Storing Data with Blockchain Technology: By leveraging blockchain technology, a secure and unalterable system for storing critical data is established, including trust scores and historical behavior records of nodes. This strategy empowers the network with a robust mechanism for maintaining data integrity and historical accuracy, which are essential for evaluating the trustworthiness of each node.

ii) Automated Registration with Smart Contracts: smart contracts are utilized in the blockchain framework to register various network components, such as systems, sensor nodes, and fog nodes. These smart contracts are ingeniously designed to execute the registration process automatically, providing secure, tamper-proof, and transparent documentation of all network participants. This implementation simplifies the registration process and significantly boosts the network's security posture by offering an immutable and transparent record of all entities involved.

Algorithm 2 defines the process for registering a system in the CPS layer using a blockchain.

**Algorithm 2** System Registration in CPS Layer

**Input :** System ID (*sysID*), Gateway ID (*gatewayID*), Blockchain (*blockchain*)
**Output :** Registration Result (*registrationResult*)

```
Initialization Steps:
Function RegisterSystem(sysID, gatewayID, blockchain):
    while condition do
        if SystemExists(sysID, gatewayID, blockchain) == False then
            register_SID(sysID, blockchain);
            concerned_gateway(gatewayID, sysID, blockchain);
            return "System registered successfully";
        else
            return "System ID already registered";
```

The method begins with an initialization stage in which it checks if the system registration database contains the given System ID (*sysID*), Gateway ID (*gatewayID*), and Blockchain (*blockchain*). The algorithm then performs a registration check in Step 2, and if the system cannot be located (based on the result of Step 1), it proceeds with the system registration procedure. The process of registering the System ID (*sysID*) with the designated Blockchain (*blockchain*) is covered in Step 3. Step 4 requires notifying the relevant Gateway (textitgatewayID) about the newly registered system and relaying critical details such as the System ID (textitsysID) and Blockchain (textitblockchain). The algorithm finally completes its execution in Step 5 by returning the result, which is usually "System registered successfully." On the other hand, if in Step 1 the condition will return True, that is, the system is already registered, then it will jump to Step 2 to Step 4 and go to Step 5, where it has to return "System ID already registered." It is a significant method of effective management and monitoring of the system in such a way that the identity and registration of the system are assured in a CPS environment.

Algorithm 3 observes the rules of sensor node registration in the blockchain-based system. It is a part of the core algorithm started by the first step (the "RegisterNode" function), and its result is repeated running. Step two: if the node has already been captured in the blockchain, the algorithm has to decide. It goes on to the third step of extending an error in the

**Algorithm 3** Sensor Node Registration Rules

**Input :** Node address (*node.address*), Blockchain (*blockchain*)

```
Initialization:
Function register_node(node.address, blockchain):
    while condition do
        if node_exists(node.address, blockchain) == true then
            error();
        else
            register_node(node.address, blockchain);
```

case of finding already existing nodes. If the node is not found on the blockchain, then the fourth step follows, which is the invocation of the "RegisterNode" function. After that, the node gets registered on the blockchain. For this, it is imperative to maintain the integrity and authenticity of all sensor nodes registered in the blockchain system since they will allow the management of information securely and systematically.

**Algorithm 4** Fog Node Registration Smart Contract

**Input :** Node address (*node.address*), Blockchain (*blockchain*)
**Output :** Registration result

```
Initialization:
Set:
while condition do
    if node_exists(node.address, blockchain) == true then
        return error();
    else
        register_fog_node(node.address, blockchain);
        return "Fog node registered successfully";
```

Algorithm 4 is essential for facilitating fog node registration in a blockchain application. The initial step is to establish the rules. The method needs two critical inputs to function, namely the address of the node and the target blockchain, to produce a registration result. There are no particular steps involved in the initialization phase of Step 2. The third crucial step ensures that fog nodes remain unique by having the program verify if the node address entered is already registered in the designated blockchain. The algorithm moves on to Step 4 and quickly responds

with an error to preserve the integrity of the system if an existing node is detected, as indicated by the blockchain check. Step 5 is triggered, effectively registering the node if it is not on the blockchain. By sending the result message "Fog node registered successfully," the algorithm comes to an end in Step 6, guaranteeing the safe and efficient administration of fog node registrations inside the blockchain-based system.

**Algorithm 5** Blockchain Integration for Trust Data and Secure Communication

**Input:** Monitoring status
**Output:** None
1 **Set:**;
2 **while** *monitoring* **do**
3 *collected_data* ← Data_Collection_from_CPS_Layer();
4 *encrypted_data* ← EncryptWithPKI(*collected_data*, *recipient_public_key*);
5 *trust_scores* ← calculate_trust_scores(*collected_data*);
6 store_trust_data(*trust_scores*);
7 **while** *trust_scores* **do**
8 create_transaction(type =′ *trust_data*′, data = *trust_scores*);
9 add_transaction_to_blockchain(transaction);
10 **end**
11 **if** *detect_jamming_attack*(*trust_scores*) **then**
12 generate_alert();
13 adjust_transmission_settings();
14 **end**
15 secure_communication(*encrypted_data*);
16 wait(*data_collection_interval*);
17 **end**

Algorithm 5 is intended to improve data trust and security in a CPS environment. Step 1 starts ongoing monitoring during the "Set" phase. Data is gathered in Step 2 from the CPS layer, and in Step 3, Public Key Infrastructure (PKI) is used to encrypt the data using the public key of the recipient. In order to promote data integrity and trustworthiness, Step 4 computes trust ratings based on the gathered data and stores them using a trust data storage method. Step 5 creates transactions with corresponding trust scores in a nested loop. Step 6 adds these transactions to a blockchain, creating an unchangeable and safe ledger for trust data. If an attack is detected, Step 8 notifies the system operators by generating alerts, and Step 9 modifies the transmission settings to lessen the impact of the attack. Lastly, Step 10 transmits the encrypted data to ensure secure communication, and Step 11 adds a waiting period to help with systematic data gathering at predetermined intervals.

### D. REACTIVE JAMMING ATTACK DETECTION

The steps in a reactive jamming attack are as under:

a) Observation and Initial Detection by Nodes: Every node in our system constantly monitors the communication channels for signs of a reactive jamming attack. They are looking for red flags like unexpected packet loss, odd signal strength fluctuations, and traffic flow anomalies.
b) Detection of Potential Attacks: Upon spotting patterns that might indicate a jamming attempt, a node raises an alarm and starts a verification process rooted in trust. It uses the blockchain's smart contracts to alert its neighbors about the suspected jamming, sharing$\Theta_{TS}$ for further scrutiny.
c) Verification Through Collective Trust: The neighboring nodes, upon receiving this alert, dive into the blockchain data to examine the claim's validity. Leveraging smart contracts and a system of consensus among themselves, they assess whether the suspected attack is genuine, using trust scores and observed behaviors as their guide.
d) Alert Generation and Reaction: If enough neighbors concur that an attack is underway, the node that spotted the trouble sounds the alarm and initiates counteractions. These might involve tweaking the communication frequencies, adjusting the power levels of transmissions, or even rerouting traffic to dodge the jamming.

2) Adapting and Keeping the System Up-to-Date:
The strategy does not stop at detection and response. It involves ongoing adjustments and enhancements to stay ahead of attackers:

a) Dynamic Model Adaptation: Our hybrid trust model is not static but designed to evolve with the network's environment. It continually refreshes trust scores and adjusts its parameters, like the trust metric weight factors ($\omega_1, \omega_2, \omega_3$) and $\alpha$ and the balance between reputation and behavior assessments, based on live data from the blockchain and observed attack patterns.
b) Record-keeping and Analysis for Improvement: Nodes log every detected attack, trust scores, and the responses onto the blockchain. This rich trove of data serves as a foundation for system administrators to analyze trends, fine-tune the model for better accuracy, and enhance the system's resilience.

## VII. EXPERIMENTATION AND RESULTS

The experiment used a high-performance Intel Core i7 processor with 16GB of RAM and an SSD to ensure

**TABLE 4.** Simulation Environment and Details.

| Network Simulation | |
|---|---|
| Simulation Tool | Cooja |
| Number of Nodes | 50 CPS Node, 10 Fog Nodes |
| Initial Energy | 100 J |
| Number of Malicious Nodes | 5 |
| Simulation Time | 60 mins |
| Number of Simulations | 10 |
| **Blockchain Components & Library** | |
| For SN development | Contiki-NG OS |
| For blockchain interaction | web3.js |
| **Tools** | |
| Ethereum emulator | Ganache |
| For SN development | Node.js |
| For communication with the blockchain | JsonRPC |
| IDE for smart contract development | Remix |
| For smart contract development | Solidity |
| For smart contract compilation and deployment | Truffle Suite |
| **Energy Consumption Model** | |
| Node Initial Energy | 100 J |
| Standby Power | 0.708 mJ/s |
| Erx | 0.0009 mJ/bit |
| Etx | 0.0010875 mJ/bit |

quick data retrieval. We used Cooja for our simulation environment, deploying 50 CPS nodes and 10 fog nodes to create a realistic CPS scenario. We included five attacking nodes to simulate attack conditions. The simulations ran for a full hour, allowing us to gather ample data for our analysis. We crafted a virtual IoT network in Cooja, portraying IoT devices as nodes, and utilized it to pilot our trust-based jamming attack detection mechanism. The integration of essential blockchain components was achieved on the Contiki-NG OS, with the web3.js library facilitating core blockchain operations, including the creation of blocks and processing transactions. Further, we ventured into developing Ethereum smart contracts using Solidity, which were then deployed on a simulated Ethereum blockchain to actualize our concepts. The Ethereum framework supported our implementation of blockchain-based data storage and the execution of smart contracts. To develop these smart contracts, we employed Remix, an intuitive web-based IDE designed specifically for Ethereum smart contract creation. To simulate blockchain behaviors accurately in our experiment, we chose the BlockchainSim simulator. This combination of hardware configuration and simulation tools created a reliable and effective environment for testing our proposed blockchain-based attack detection mechanism for CPS environments.Table 4 provides a summary of the experimentation setup.

### A. EVALUATION PARAMETERS

In order to detect reactive jamming attacks in a smart healthcare system, key parameters must be monitored to identify potential disruptions. The packet loss rate is an essential metric in which the interference caused by an attacker during an attack results in packet loss rates that exceed a predefined threshold. Signal-to-Noise Ratio (SNR) is also monitored; a higher SNR indicates signal transmission with minimal interference. During an attack, the interference introduced by the attacker reduces the SNR below a predetermined threshold. The transmission delay, or the time it takes for data packets to travel between nodes, is crucial. Due to channel interference, normal operations feature low transmission delays, whereas reactive jamming attacks introduce transmission delays. These parameters reveal the presence of a reactive jamming attack, allowing for timely detection and response.

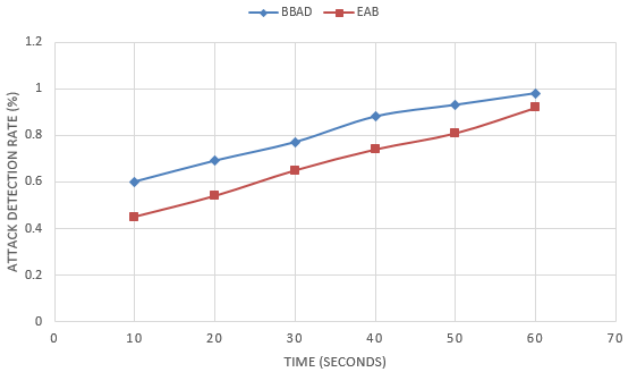


**FIGURE 4.** Attack Detection Rate.

#### 1) ATTACK DETECTION RATE

In our context, The attack detection rate refers to a system's ability to identify and respond to reactive jamming attacks effectively. Figure 4 illustrates the detection rate of reactive jamming attacks for the BBAD approach compared to the baseline approach EAB [31]. At simulation time 10, BBAD achieves a detection rate of 0.60 (i.e., 60%), notably higher than the EAB detection rate of 0.45(45%). At simulation time 30, BBAD reaches 0.77 (i.e., 77% ) while Base is 0.64 (i.e., 64%). Finally, at 60, BBAD has a 98% detection rate while Base has 92%. The percentage difference between

both approaches is approximately 15.71%, indicating that the BBAD approach has an average detection rate of around 15.71% compared to the EAB approach. The advanced hybrid trust model, which uses specific parameters like SNR, packet loss rate, and transmission delay, improves the detection of reactive jamming attacks.

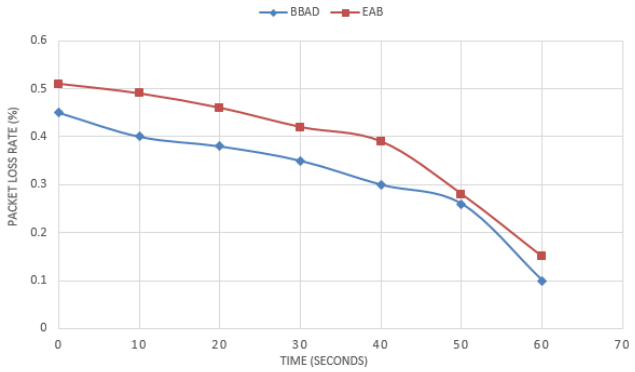


**FIGURE 5.** Packet Loss Rate.

### 2) PACKET LOSS RATE

Figure 5 defines packet loss rate as the proportion of data packets in a network that fail to reach their intended destination. The BBAD approach begins the simulation (at time 0) with a packet loss rate of 0.45 (i.e., 45%), while the EAB approach begins with 0.51 (i.e., 51%). A gradual reduction in packet loss rates for both approaches is observed as the simulation progresses. The BBAD approach achieves a significantly lower packet loss rate of 0.1 at simulation time 60 than the EAB approach, which reaches 0.15. The BBAD approach consistently outperforms EAB across all simulation times in terms of packet loss rate. The percentage difference in the average packet loss rates between the two approaches is calculated as 20.21%, highlighting the BBAD approach's improved performance. Due to the trust model's capacity to identify and isolate potential malicious nodes, disruptions and interferences in the transmission of data packets are prevented.

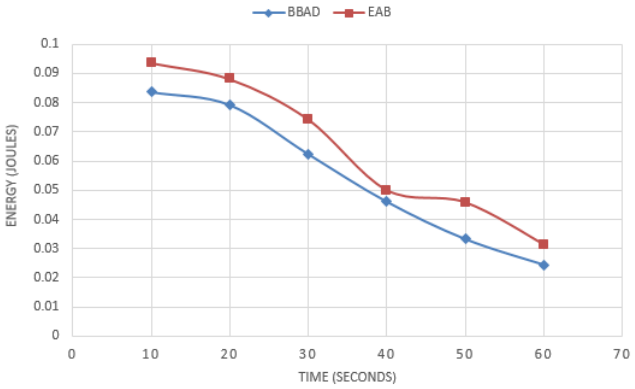


**FIGURE 6.** Energy Consumption.

### 3) ENERGY CONSUMPTION

Figure 6 In the context of our analysis, energy consumption refers to the energy usage in the network during the simulation of reactive jamming attacks. At the initial simulation time of 10, the BBAD approach consumes 8.36% of energy, while the EAB approach consumes 9.36%. It signifies better energy utilization by the BBAD approach. As the simulation advances to time 20, the BBAD approach demonstrates a consumption of 7.92%, outperforming the EAB approach, which consumes 8.81%. By the time the simulation reaches 60, the BBAD approach achieves an energy consumption rate of 2.45%, while the EAB approach consumes 3.15%. It reflects a significant improvement in energy efficiency for the BBAD approach throughout the simulation. The percentage difference for the BBAD approach is approximately 16.65% lower than that of the EAB approach. It indicates that the BBAD method is more energy-efficient in the context of reactive jamming attack detection. This is due to the integration of a fog computing layer, which enhances energy efficiency. The fog layer reduces the need for extensive data transmission by bringing processing and decision-making closer to the data source.

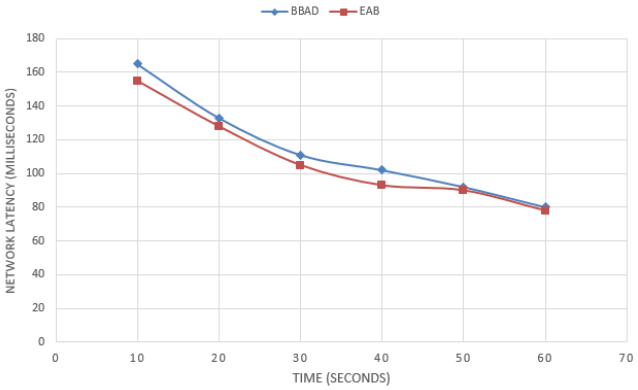


**FIGURE 7.** Network Latency.

### 4) NETWORK LATENCY

Figure 7 Network latency refers to the time delay experienced by data packets as they traverse the network. The BBAD approach has a latency of 165 units at an initial simulation time of 10, whereas the EAB approach has a latency of 155. As the simulation progresses, the network latency values for both approaches decrease gradually. At simulation time 60, the BBAD approach reaches 80 units of latency, whereas the EAB approach reaches 78 units. The percentage difference is 8.29%, indicating that the BBAD approach has a slightly higher average network latency than the EAB approach. This difference may be due to the BBAD strategy's enhanced security measures and real-time monitoring. While the advanced trust model and mechanisms of the BBAD approach provide increased protection against attacks, the additional layers of security and verification processes may slightly increase network latency. Nevertheless, this trade-off between enhanced security and slightly increased latency is frequently deemed acceptable, as it ensures the integrity and dependability of data transmission in the network.

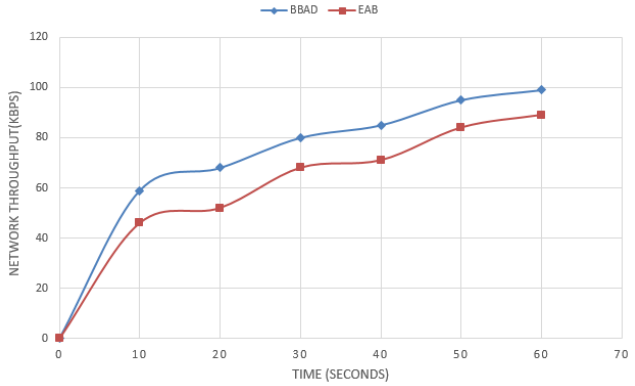


**FIGURE 8.** Network Throughput.

#### 5) NETWORK THROUGHPUT

Network latency is the time required for data packets to travel from their source to their destination in a network. Figure 8 represents no network latency at the beginning of the simulation (time 0) because no data is being transmitted. At simulation time 30, the network latency for the BBAD approach is 80 units, whereas the Base approach experiences a latency of 68 units. It indicates that the BBAD approach has a slightly higher network latency. As the simulation time reaches 60, the network latency values for both methods decrease. The BBAD approach experiences a network latency of 99 units, while the Base approach has a latency of 89 units. The percentage difference is 9.63%, indicating that the BBAD approach maintains a lower average network throughput than the EAB approach.

## VIII. DISCUSSION

Using a hybrid trust model in the proposed healthcare CPS systems augments the effectiveness of detection approaches. The hybrid model integrates two fundamental trust evaluation techniques: reputation-based and behavior-based. Reputation-based trust refers to the process through which nodes in a system create and uphold their reputations via prior interactions. It effectively enables the system to differentiate between trustworthy and suspicious nodes. In contrast, assessing trust based on behavior involves continuously monitoring nodes' actions in real-time, considering their patterns of packet forwarding and communication. All these combined form a substantial ratio of increased ability for the system to detect potential threats, especially active jamming attacks. This way, the network's trustworthiness could be determined not only from its reputation built in the past but also from the behavior of the current one.

Another way is how blockchain technology would enhance the evaluation of trust. It acts as a strong and secure kind of ledger, made precisely to check the recorded trust and reliability of every single node. Authenticity in the trust information is a prime concern against being exploited by an adversary. Furthermore, with the help of blockchain technology, smart contracts can also be formulated, which can further bring in an even higher level of efficiency in the system for assessing and confirming the trust process. The rules can trigger, in case the defined condition is met, a response to the potential threat instantly, so they enhance the system in its capability to fight the attempts of being blocked. Implication: ''The hybrid trust model for CPS-based networks with blockchain technology'' implies robust and scalable security for protecting the CPS-based network from an ever-growing cyberattack vector.

### A. FUTURE DIRECTION

In demand to tackle the ever-changing role of cybersecurity in healthcare CPS, it is essential to define precise paths to future research and enhancements. Scalability and processing speed should be improved due to the blockchain infrastructure's use of more sophisticated algorithms for consensus. It can completely alter CPS security and be applied to other areas of vital importance, such as smart cities, industrial automation, and smart buildings, thereby making the world a more secure and efficient interconnected environment. Identifying areas of future research and improvement in advancing cybersecurity measures and protecting the security of CPS networks are listed below:

1) Scalability enhancement: Strategies to boost the capacity of our framework built on blockchain are being investigated to ensure that it can manage the growing amount of health data in addition to network members. This could mean analyzing ways to improve the size of blocks and consensus algorithms–network throughput to enable large-scale implementations without sacrificing speed.
2) Use of Emerging technologies: Such AI might be useful in future applications, and it is possible only when some limitations are solved. There are challenges such as scalability, data privacy, and integrity, or other problems that need to be solved in order to be able to utilize AI in the cybersecurity framework. Future research should focus on developing algorithms and methodologies that can resolve the scalability problems; then, AI-based solutions will also operate effectively with vast data and changes in surroundings. Also, it is necessary to increase the possibilities of solutions that protect privacy and data encryption. These dimensions are vital to protecting sensitive information and ensuring the confidentiality of Artificial Intelligence (AI)-powered systems.
3) Usability enhancement: The primary goal will be to increase the user-friendliness of the suggested system, making it more straightforward to implement, manage, and maintain in real-world healthcare settings. It could mean developing interfaces that are easy to use and streamlined configuration processes and supplying intuitive management tools that allow healthcare professionals and administrators to maximize the system's capabilities.
4) Adapting to Changing Threats: Monitor and continuously adjust the cybersecurity framework to deal with new security threats and vulnerabilities for healthcare environments using CPS. It includes staying

current with changing cybersecurity threats, performing regular reviews of the security risks, and implementing proactive security measures, such as using threat intelligence to detect irregularities and automating the incident response.

## IX. CONCLUSION

This paper introduces a hybrid trust model that includes blockchain technology and smart contracts to find possibilities for jamming attacks across CPS networks. The proposed framework shall deploy a unique set of trust assessment techniques, rather than on the reputation and behavior of the nodes, to warrant an accurate and intensive evaluation of the latter's reliability. For example, blockchain technology is very resilient in nature, offering a permanent way of data storage since it always assures that the integrity of data is highly regarded for maintaining safety from unauthorized changes. In addition, smart contracts, systems, sensor nodes, and fog nodes. Smart contracts automatize and secure the registration process to assure all network entities that the records are safe and transparent. The proposed integrated approach, while ensuring scalability and flexibility, provides a resilient way to protect CPS networks from jamming attacks. This method allows for real-time response and continuously improves the network's security. Further, the design addressed the requirements concerning the technology devices that can guarantee reliable and secure communication in the healthcare environment, such as the Internet of Things. The loss of packets is greatly minimized, and thus, the detection rate from the blockchain application technology is higher than that of the reference paper. This study shows that the system distinguished and removed instances of interference very well and, therefore, helped improve the safety and efficiency of the healthcare services in the network of the CPS. In future, we aim to expand the suggested method and evaluating its effectiveness across real life healthcare test-bed and network configurations. Additionally, we also aim to use cutting-edge AI and ML techniques to increase the trust evaluation process to identify a wide range of other attacks.

## REFERENCES

[1] A. Mishra, A. V. Jha, B. Appasani, A. K. Ray, D. K. Gupta, and A. N. Ghazali, "Emerging technologies and design aspects of next generation cyber physical system with a smart city application perspective," *Int. J. Syst. Assurance Eng. Manage.*, vol. 14, no. S3, pp. 699–721, Jul. 2023.

[2] N. Tariq, M. Asim, F. A. Khan, T. Baker, U. Khalid, and A. Derhab, "A blockchain-based multi-mobile code-driven trust mechanism for detecting internal attacks in Internet of Things," *Sensors*, vol. 21, no. 1, p. 23, Dec. 2020.

[3] B. A. Salau, A. Rawal, and D. B. Rawat, "Recent advances in artificial intelligence for wireless Internet of Things and cyber–physical systems: A comprehensive survey," *IEEE Internet Things J.*, vol. 9, no. 15, pp. 12916–12930, Aug. 2022.

[4] S. A. Moqurrab, A. Anjum, N. Tariq, and G. Srivastava, "An efficient framework for semantically-correlated term detection and sanitization in clinical documents," *Comput. Electr. Eng.*, vol. 100, May 2022, Art. no. 107985.

[5] D. Patel, C. K. Sahu, and R. Rai, "Security in modern manufacturing systems: Integrating blockchain in artificial intelligence-assisted manufacturing," *Int. J. Prod. Res.*, vol. 62, no. 3, pp. 1041–1071, Feb. 2024.

[6] M. Hammoudeh, G. Epiphaniou, and P. Pinto, "Cyber-physical systems: Security threats and countermeasures," *J. Sensor Actuator Netw.*, vol. 12, no. 1, p. 18, Feb. 2023.

[7] W. Li, Y. Chai, F. Khan, S. R. U. Jan, S. Verma, V. G. Menon, F. Kavita, and X. Li, "A comprehensive survey on machine learning-based big data analytics for IoT-enabled smart healthcare system," *Mobile Netw. Appl.*, vol. 26, no. 1, pp. 234–252, Feb. 2021.

[8] L. Javed, A. Anjum, B. M. Yakubu, M. Iqbal, S. A. Moqurrab, and G. Srivastava, "ShareChain: Blockchain-enabled model for sharing patient data using federated learning and differential privacy," *Expert Syst.*, vol. 40, no. 5, Jun. 2023, Art. no. e13131.

[9] S. Baker and W. Xiang, "Artificial intelligence of things for smarter healthcare: A survey of advancements, challenges, and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1261–1293, Mar. 2023.

[10] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electric Power Syst. Res.*, vol. 215, Feb. 2023, Art. no. 108975.

[11] D. K. Jain, S. Neelakandan, T. Veeramani, S. Bhatia, and F. H. Memon, "Design of fuzzy logic based energy management and traffic predictive model for cyber physical systems," *Comput. Electr. Eng.*, vol. 102, Sep. 2022, Art. no. 108135.

[12] M. Karatas, L. Eriskin, M. Deveci, D. Pamucar, and H. Garg, "Big data for healthcare Industry 4.0: Applications, challenges and future perspectives," *Expert Syst. Appl.*, vol. 200, Aug. 2022, Art. no. 116912.

[13] M. Kumari, M. Singh, A. Grover, A. Sheetal, C. Goel, and Suvidhi, "The cyber physical systems and industrial Internet of Things (IIoT)," in *Security and Resilience of Cyber Physical Systems*. Boca Raton, FL, USA: CRC Press, 2022, pp. 1–12.

[14] E. U. Haque, M. S. Baig, A. Ahmed, A. Ahmad, M. Alajmi, Y. Y. Ghadi, H. K. Alkahtani, and A. Akhmediyarova, "Scalable EdgeIoT blockchain framework using EOSIO," *IEEE Access*, vol. 12, pp. 41763–41772, 2024.

[15] A. A. Khalil, J. Franco, I. Parvez, S. Uluagac, H. Shahriar, and M. A. Rahman, "A literature review on blockchain-enabled security and operation of cyber-physical systems," in *Proc. IEEE 46th Annu. Comput., Softw., Appl. Conf. (COMPSAC)*, Jun. 2022, pp. 1774–1779.

[16] H. Rathore, A. Mohamed, and M. Guizani, "A survey of blockchain enabled cyber-physical systems," *Sensors*, vol. 20, no. 1, p. 282, Jan. 2020.

[17] D. Wang, B. Song, Y. Liu, and M. Wang, "Secure and reliable computation offloading in blockchain-assisted cyber-physical IoT systems," *Digit. Commun. Netw.*, vol. 8, no. 5, pp. 625–635, Oct. 2022.

[18] J. Wang, J. Chen, Y. Ren, P. K. Sharma, O. Alfarraj, and A. Tolba, "Data security storage mechanism based on blockchain industrial Internet of Things," *Comput. Ind. Eng.*, vol. 164, Feb. 2022, Art. no. 107903.

[19] S. Walker-Roberts, M. Hammoudeh, O. Aldabbas, M. Aydin, and A. Dehghantanha, "Threats on the horizon: Understanding security threats in the era of cyber-physical systems," *J. Supercomput.*, vol. 76, no. 4, pp. 2643–2664, Apr. 2020.

[20] S. A. Moqurrab, A. Anjum, N. Tariq, and G. Srivastava, "Instant_Anonymity: A lightweight semantic privacy guarantee for 5G-enabled IIoT," *IEEE Trans. Ind. Informat.*, vol. 19, no. 1, pp. 951–959, Jan. 2023.

[21] J. Zhang, L. Pan, Q.-L. Han, C. Chen, S. Wen, and Y. Xiang, "Deep learning based attack detection for cyber-physical system cybersecurity: A survey," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 3, pp. 377–391, Mar. 2022.

[22] N. Tariq, M. Asim, Z. Maamar, M. Z. Farooqi, N. Faci, and T. Baker, "A mobile code-driven trust mechanism for detecting internal attacks in sensor node-powered IoT," *J. Parallel Distrib. Comput.*, vol. 134, pp. 198–206, Dec. 2019.

[23] M. K. Hanawal, D. N. Nguyen, and M. Krunz, "Cognitive networks with in-band full-duplex radios: Jamming attacks and countermeasures," *IEEE Trans. Cognit. Commun. Netw.*, vol. 6, no. 1, pp. 296–309, Mar. 2020.

[24] M. Riahi Manesh and N. Kaabouch, "Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions," *Comput. Secur.*, vol. 85, pp. 386–401, Aug. 2019.

[25] S. Bagali and R. Sundaraguru, "Efficient channel access model for detecting reactive jamming for underwater wireless sensor network," in *Proc. Int. Conf. Wireless Commun. Signal Process. Netw. (WiSPNET)*, Mar. 2019, pp. 196–200.

[26] P. Zhou, Q. Yan, K. Wang, Z. Xu, S. Ji, and K. Bian, "Jamsa: A utility optimal contextual online learning framework for anti-jamming wireless scheduling under reactive jamming attack," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 3, pp. 1862–1878, Jul. 2020.

[27] U. Altun, A. Kaplan, G. K. Kurt, I. Altunbas, D. Kucukyavuz, M. Kesal, and E. Basar, "Reactive jammer detection in OFDM with index modulation," *Phys. Commun.*, vol. 55, Dec. 2022, Art. no. 101909.

[28] G. Chen and W. Dong, "Reactive jamming and attack mitigation over cross-technology communication links," *ACM Trans. Sensor Netw.*, vol. 17, no. 1, pp. 1–25, Feb. 2021.

[29] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 767–809, 2nd Quart., 2022.

[30] M. S. Abdalzaher, M. Elwekeil, T. Wang, and S. Zhang, "A deep autoencoder trust model for mitigating jamming attack in IoT assisted by cognitive radio," *IEEE Syst. J.*, vol. 16, no. 3, pp. 3635–3645, Sep. 2022.

[31] A. Hussain, N. Abughanam, J. Qadir, and A. Mohamed, "Jamming detection in IoT wireless networks: An edge-AI based approach," in *Proc. 12th Int. Conf. Internet Things*, Nov. 2022, pp. 57–64.

[32] E. Bout and V. Loscrí, "An adaptable module for designing jamming attacks in WiFi networks for ns-3," in *Proc. Int. Conf. Model. Anal. Simul. Wireless Mobile Syst. Int. Conf. Model. Anal. Simul. Wireless Mobile Syst.*, Oct. 2022, pp. 121–124.

[33] A. A. Fadele, M. Othman, I. A. T. Hashem, I. Yaqoob, M. Imran, and M. Shoaib, "A novel countermeasure technique for reactive jamming attack in Internet of Things," *Multimedia Tools Appl.*, vol. 78, no. 21, pp. 29899–29920, Nov. 2019.

[34] A. Pourranjbar, G. Kaddoum, and W. Saad, "Jamming pattern recognition over multi-channel networks: A deep learning approach," in *Proc. 55th Asilomar Conf. Signals, Syst., Comput.*, Oct. 2021, pp. 305–308.

[35] F. t. Zahra, Y. S. Bostanci, and M. Soyturk, "Real-time jamming detection in wireless IoT networks," *IEEE Access*, vol. 11, pp. 70425–70442, 2023.

[36] B. A. Aldawsari and J. H. Jafarian, "A jamming-resilient and scalable broadcasting algorithm for multiple access channel networks," *Appl. Sci.*, vol. 11, no. 3, p. 1156, Jan. 2021.

[37] S. Sciancalepore and R. D. Pietro, "Bittransfer: Mitigating reactive jamming in electronic warfare scenarios," *IEEE Access*, vol. 7, pp. 156175–156190, 2019.

[38] H. B. Salameh, S. Otoum, M. Aloqaily, R. Derbas, I. A. Ridhawi, and Y. Jararweh, "Intelligent jamming-aware routing in multi-hop IoT-based opportunistic cognitive radio networks," *Ad Hoc Netw.*, vol. 98, Mar. 2020, Art. no. 102035.

[39] M. Hachimi, G. Kaddoum, G. Gagnon, and P. Illy, "Multi-stage jamming attacks detection using deep learning combined with kernelized support vector machine in 5G cloud radio access networks," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Oct. 2020, pp. 1–5.

[40] A. Aljabri, F. Jemili, and O. Korbaa, "Intrusion detection in cyber-physical system using rsa blockchain technology," *Multimedia Tools Appl.*, vol. 83, no. 16, pp. 48119–48140, Nov. 2023.

[41] K. Girdhar, C. Singh, and Y. Kumar, "AI and blockchain for cybersecurity in cyber-physical systems: Challenges and future research agenda," in *Advances in Information Security*. Cham, Switzerland: Springer, 2023, pp. 185–213.

[42] M. A. Mohammed, A. Lakhan, D. A. Zebari, M. K. A. Ghani, H. A. Marhoon, K. H. Abdulkareem, J. Nedoma, and R. Martinek, "Securing healthcare data in industrial cyber-physical systems using combining deep learning and blockchain technology," *Eng. Appl. Artif. Intell.*, vol. 129, Mar. 2024, Art. no. 107612.

[43] Y. Luo, Y. Xiao, L. Cheng, G. Peng, and D. Yao, "Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities," *ACM Comput. Surveys*, vol. 54, no. 5, pp. 1–36, Jun. 2022.

[44] S. M. Danish, M. Lestas, W. Asif, H. K. Qureshi, and M. Rajarajan, "A lightweight blockchain based two factor authentication mechanism for LoRaWAN join procedure," in *Proc. IEEE Int. Conf. Commun. Workshops*, May 2019, pp. 1–6.

[45] H. Xu, L. Zhang, Y. Liu, and B. Cao, "RAFT based wireless blockchain networks in the presence of malicious jamming," *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 817–821, Jun. 2020.

[46] A. Eldosouky, A. Ferdowsi, and W. Saad, "Drones in distress: A game-theoretic countermeasure for protecting UAVs against GPS spoofing," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2840–2854, Apr. 2020.

[47] X. Wang, M. Cenk Gursoy, T. Erpek, and Y. E. Sagduyu, "Jamming-resilient path planning for multiple UAVs via deep reinforcement learning," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2021, pp. 1–6.

[48] L. Xiao, Y. Ding, J. Huang, S. Liu, Y. Tang, and H. Dai, "UAV anti-jamming video transmissions with QoE guarantee: A reinforcement learning-based approach," *IEEE Trans. Commun.*, vol. 69, no. 9, pp. 5933–5947, Sep. 2021.

[49] Y. Xu, M. Lei, M. Li, M. Zhao, and B. Hu, "A new anti-jamming strategy based on deep reinforcement learning for MANET," in *Proc. IEEE 89th Veh. Technol. Conf. (VTC-Spring)*, Apr. 2019, pp. 1–5.

[50] B. Seyedi and R. Fotohi, "NIASHPT: A novel intelligent agent-based strategy using hello packet table (HPT) function for trust Internet of Things," *J. Supercomput.*, vol. 76, no. 9, pp. 6917–6940, Sep. 2020.

[51] M. Jeyaselvi, M. Sathya, S. Suchitra, S. Jafar Ali Ibrahim, and N. S. Kalyan Chakravarthy, "SVM-based cloning and jamming attack detection in IoT sensor networks," in *Advances in Information Communication Technology and Computing*. Cham, Switzerland: Springer, 2022, pp. 461–471.

[52] M. A. Jasim and T. S. Atia, "An IoT-Fuzzy-Based jamming detection and recovery system in wireless video surveillance system," *Int. J. Comput. Intell. Appl.*, vol. 22, no. 2, Jun. 2023, Art. no. 2350004.

[53] L. Xue, B. Ma, J. Liu, and Y. Yu, "Jamming attack against remote state estimation over multiple wireless channels: A reinforcement learning based game theoretical approach," *ISA Trans.*, vol. 130, pp. 1–9, Nov. 2022.

[54] M. Wang, Y. Geng, J. Wang, K. Liu, X. Che, and Q. Wei, "$H_\infty$ control for ICPS with hybrid-triggered mechanism encountering stealthy DoS jamming attacks," *Actuators*, vol. 11, no. 7, p. 193, Jul. 2022.

[55] M. Jeyaselvi, S. Suchitra, M. Sathya, and R. Mekala, "Energy efficient witness based clone and jamming attack detection in wsn," *J. Green Eng.*, vol. 11, no. 2, pp. 1525–1548, 2021.

[56] B. Mbarek, M. Ge, and T. Pitner, "An adaptive anti-jamming system in hyperledger-based wireless sensor networks," *Wireless Netw.*, vol. 28, no. 2, pp. 691–703, Feb. 2022.

[57] K. P. Vijayakumar, K. Pradeep Mohan Kumar, K. Kottilingam, T. Karthick, P. Vijayakumar, and P. Ganeshkumar, "An adaptive neuro-fuzzy logic based jamming detection system in WSN," *Soft Comput.*, vol. 23, no. 8, pp. 2655–2667, Apr. 2019.

[58] N. Nishanth and A. Mujeeb, "Modeling and detection of flooding-based denial-of-service attack in wireless ad hoc network using Bayesian inference," *IEEE Syst. J.*, vol. 15, no. 1, pp. 17–26, Mar. 2021.

[59] K. P. Vijayakumar, P. Ganeshkumar, M. Anandaraj, K. Selvaraj, and P. Sivakumar, "Fuzzy logic–based jamming detection algorithm for cluster-based wireless sensor network," *Int. J. Commun. Syst.*, vol. 31, no. 10, p. e3567, Jul. 2018.

**MASOOMA ANWAR** received the bachelor's degree in information systems from the University of Bahrain, Bahrain, a foundational step that equipped her with a comprehensive understanding of information technology and the master's degree in information security from Air University, Islamabad. Her academic journey reflects her diverse interests, encompassing information security, blockchain technology, sensors, cyber-attacks, and networking. Her passion for exploring the intricate domains of information systems and security positions her at the forefront of cutting-edge developments in these fields. Driven by a commitment to excellence, she stands poised to make significant contributions to the ever-evolving landscape of cybersecurity.

**NOSHINA TARIQ** received the M.S. and Ph.D. degrees in computer science from the FAST—National University of Computer and Emerging Sciences, Islamabad, Pakistan. She is currently an Accomplished Researcher in computer science and cybersecurity. She is also an Assistant Professor with the Department of Avionics Engineering and Information Security, Air University, Islamabad. Her research interests include various aspects of cybersecurity, such as network security, the Internet of Things (IoT), wireless sensor networks (WSN), fog and cloud computing, blockchain, and AI. She is also an active research community member, serving as a peer reviewer for many high-repute research journals. With her passion for research and dedication to the field, she is poised to contribute further to advancing cybersecurity and computer science.

**MUHAMMAD ASHRAF** received the bachelor's degree in avionics engineering from the College of Aeronautical Engineering, Risalpur, National University of Sciences and Technology (NUST), Pakistan, the M.S. degree in information security from NUST, Pakistan, and the Ph.D. degree in cryptography from Middle East Technical University, Ankara, Turkey, in 2013. He was the Chair Avionics Engineering Department and the General Director of the Institute of Avionics and Aeronautics, Air University, Islamabad. He is also a Faculty Member of the School of Electrical Engineering and Computer Science, NUST. His research interests include but are not limited to post quantum cryptography, public key cryptography, efficient computation over finite fields, stream ciphers, elliptic curve-based cryptography, random number generation, and information security.

**SYED ATIF MOQURRAB** received the master's degree from the National University of Computer and Emerging Sciences and the Ph.D. degree from the COMSATS Institute of Information Technology. He is currently a Distinguished Academic, an Educator, and a Researcher, has made significant contributions to the fields of computer science and artificial intelligence. His research interest includes critical aspects of privacy and security in various domains. As a Research Assistant Professor with Gachon University, South Korea, and formerly an Assistant Professor with Air University, Pakistan, he has showcased expertise in a broad spectrum of subjects. His extensive publication record features innovative solutions for preserving privacy, advanced data analytics, and deep learning models.

**BAYAN ALABDULLAH** received the Ph.D. degree in informatics from the University of Sussex, Brighton, U.K., in May 2022. She was an Assistant Professor with the Department of Information System, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University. She teaches several courses with the Information System Department, such as data governance, system security, and database systems. Her research interests include ML, data science, and privacy and security.

**HATOON S. ALSAGRI** received the master's and Ph.D. degrees in information systems from the Department of Information Systems, College of Computer and Information Sciences, King Saud University. During her graduate studies, she has had the opportunity to participate in various conferences and has published various journal articles. She is currently an Assistant Professor with the Department of Information Systems, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University. Her main research interests include the field of data mining, information diffusion, and social analysis.

**ABRAR ALMJALLY** is currently an Assistant Professor with the Department of Information Systems, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University. Her main research interests include the field of artificial intelligence, information diffusion, and cyber security.