computers

MDPI

Article

Bioinspired Blockchain Framework for Secure and Scalable Wireless Sensor Network Integration in Fog–Cloud Ecosystems

Abdul Rehman [1,*] and Omar Alharbi [2,*]

[1] Department of Information Technology, The University of Haripur, Haripur 22620, Pakistan
[2] Department of Electrical Engineering, College of Engineering, Majmaah University, Al-Majmaah 11952, Saudi Arabia
* Correspondence: abdulrehman786.cs@gmail.com (A.R.); oalharbi@mu.edu.sa (O.A.)

Abstract: WSNs are significant components of modern IoT systems, which typically operate in resource-constrained environments integrated with fog and cloud computing to achieve scalability and real-time performance. Integrating these systems brings challenges such as security threats, scalability bottlenecks, and energy constraints. In this work, we propose a bioinspired blockchain framework aimed at addressing those challenges through the emulation of biological immune adaptation mechanisms, such as the self-recovery of swarm intelligence. It integrates lightweight blockchain technology with bioinspired algorithms, including an AIS for anomaly detection and a Proof of Adaptive Immunity Consensus mechanism for secure resource-efficient blockchain validation. Experimental evaluations give proof of the superior performance reached within this framework: up to 95.2% of anomaly detection accuracy, average energy efficiency of 91.2% when the traffic flow is normal, and latency as low as 15.2 ms during typical IoT scenarios. Moreover, the framework has very good scalability since it can handle up to 500 nodes with only a latency of about 6.0 ms.

Keywords: blockchain; wireless sensor networks; fog computing; cloud computing; bioinspired algorithms; security; anomaly detection

Academic Editor: Thaier Hayajneh

Received: 26 November 2024
Revised: 12 December 2024
Accepted: 13 December 2024
Published: 26 December 2024

Citation: Rehman, A.; Alharbi, O. Bioinspired Blockchain Framework for Secure and Scalable Wireless Sensor Network Integration in Fog–Cloud Ecosystems. *Computers* **2025**, *14*, 3. https://doi.org/10.3390/computers14010003

1. Introduction

The exponential growth of the IoT has led to an unprecedented increase in WSNs [1,2]. These networks represent a set of sensor nodes that are resource-constrained and used in many different domains such as smart cities, health care, and industrial automation [3–7]. This feature of WSNs to sense, collect, and transmit data in real time provides the basis for modern IoT systems [8–10]. However, their computation capacity, energy efficiency, and security limitations pose important challenges for large-scale deployment [11–13].

Integrating WSNs with fog and cloud computing has emerged as a revolutionary strategy to address the pressing challenges of energy efficiency, scalability, and security in IoT ecosystems. Fog computing brings computational and storage capabilities closer to the data source, enabling low-latency processing and bandwidth optimization [14]. Cloud computing complements this by offering robust scalability and extensive storage resources [15,16]. However, these advantages also introduce new challenges, such as maintaining energy-efficient operations, ensuring scalability across dynamic IoT environments, and safeguarding against evolving security threats [17]. This convergence enhances operational efficiency in WSNs, thus making them capable of machine learning and hence opening completely new possibilities for IoT applications [18].

Integrating WSNs with fog and cloud environments raises several critical challenges. The distributed nature intrinsic to WSNs makes them highly susceptible to security threats like data tampering, spoofing, and denial-of-service attacks [19]. Scalability becomes a bottleneck when the number of sensor nodes increases in WSNs as it may cause latency and bandwidth problems. These above issues are further exacerbated by the energy constraints of the nodes in WSNs, since the strong security and communication protocols often imply increased power consumption. In other words, the key research question is as follows: How can we design a scalable and secure framework for WSN integration with fog and cloud ecosystems that addresses resource constraints while ensuring real-time performance and resilience?

The novel bioinspired blockchain framework for the integration of WSNs with fog and cloud ecosystems in a secure and scalable way is mainly inspired by adaptive immunity, self-healing, and swarm intelligence of biological processes. This framework benefits from lightweight blockchain technology together with bioinspired algorithms in the design toward enhanced security, scalability, and energy efficiency. Key innovations include an AIS (a bioinspired algorithm modeled on the human immune response, used for real-time anomaly detection in this framework) for anomaly detection, a PoAI (a lightweight consensus mechanism inspired by biological immune systems, designed to optimize resource usage during blockchain validation) consensus algorithm enabling secure and resource-efficient blockchain validation, and a self-healing mechanism enabling system resilience as depicted in Figure 1. The major contributions of this work follow.

- Development of a bioinspired blockchain framework that leverages biological principles for enhanced security and resilience in WSN–fog–cloud ecosystems.
- Design of a lightweight AIS-based anomaly detection algorithm for real-time threat identification in resource-constrained environments.
- Introduction of a novel PoAI consensus mechanism to optimize blockchain validation for WSN nodes with limited resources.

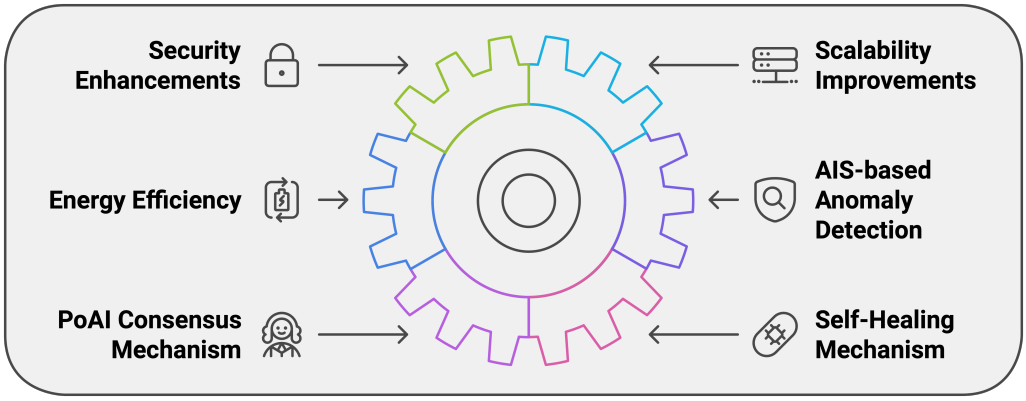

Figure 1. An integrated framework emphasizing security enhancements, energy efficiency, scalability improvements, AIS-based anomaly detection, a PoAI consensus mechanism, and a self-healing mechanism for advanced IoT systems.

The rest of this paper is structured as follows: Section 2 reviews related work. Section 3 describes the proposed architecture, including the system design, and workflow, and explains the algorithm and models, such as AISs and PoAI. Section 4 discusses the implementation details and tools used and presents the evaluation setup and results, highlighting the performance of the proposed framework. Finally, Section 5 concludes the paper.

2. Related Work

This section reviews the related literature about WSN security mechanisms, blockchain in IoT, and bioinspired computing to look in detail at the contributions, limitations, and gaps that motivated the proposal. Existing approaches, such as BB-IoT and AI-SecIoT, provide foundational methods for integrating the IoT and blockchain. However, these frameworks exhibit significant limitations. For example, BB-IoT suffers from high computational overhead, making it unsuitable for resource-constrained environments. AI-SecIoT offers better adaptability but falls short in dynamic IoT scenarios, where node failures and fluctuating workloads affect overall system reliability. Moreover, many frameworks rely on traditional consensus mechanisms, which are energy-intensive and not scalable for large-scale IoT deployments. These gaps highlight the need for a more adaptive, lightweight, and robust framework, which our BioBlock approach addresses.

A lot of methods have been proposed to mitigate the security issues in WSNs. Conventional symmetric key-based encryption is largely in use but suffers mostly due to limited resources [20]. At the other end of the spectrum, lighter versions of protocols reduce the drawbacks of these protocols to very low protection against sophisticated attack methodologies [21]. Anomaly detection technologies, such as machine learning-based models, enhance detection accuracy but in turn require high computational resources and are impractical for large-scale WSNs [22]. Unlike conventional machine learning-based anomaly detection algorithms, an AIS operates with linear computational complexity, making it suitable for resource-constrained WSNs. Additionally, an AIS utilizes adaptive learning to update its antibody set dynamically, enabling it to perform well in dynamic IoT environments where traffic patterns frequently change.

The blockchain is considered as a promising solution for the data integrity and security of communications in the IoT. Its decentralized nature inherently eliminates the need for any trusted intermediate entities, further enhancing security [23]. Classic consensus mechanisms, such as Proof of Work, are highly resource-consuming and therefore cannot be deployed in resource-constrained WSNs [24]. Novel lightweight blockchain approaches, such as Proof of Stake and DAG-based ledgers, reduce resource consumption at the expense of often decreasing decentralization and fault tolerance [25].

Bioinspired systems mimic natural processes to solve complex computational problems. Techniques like AISs and swarm intelligence have been applied to enhance network security and resource optimization [26]. For instance, AIS-based anomaly detection models replicate the immune response to identify malicious activity. Swarm intelligence has been employed for decentralized decision-making in IoT networks, demonstrating scalability and adaptability [27].

Existing solutions for WSN security often fail to balance energy efficiency, scalability, and security. Traditional blockchain systems are unsuitable for resource-constrained environments due to their computational requirements. While bioinspired systems offer promising solutions, their potential to address WSN challenges through blockchain integration has not been fully realized. In particular, almost none of the existing frameworks have provided adaptive, self-healing, and lightweight mechanisms to improve robustness performance in WSN–fog–cloud ecosystems. Table 1 summarizes the limitations of existing approaches together with the corresponding solutions formulated by BioBlock.

Table 1. Comparison of existing approaches with proposed BioBlock solution

Approaches	Identified Limitations	Proposed BioBlock Solution
BB-IoT [28]	High computational overhead and limited scalability in resource-constrained WSNs.	Utilizes lightweight blockchain for secure and efficient data validation, scaling up to 500 nodes.
BioAI-IoT [29]	Limited protection against sophisticated attacks and suboptimal energy efficiency.	Incorporates Artificial Immune Systems (AISs) for enhanced anomaly detection and energy-aware communication protocols.
AI-BCIoT [30]	Computationally intensive consensus mechanisms and moderate scalability.	Introduces Proof of Adaptive Immunity (PoAI) for resource-efficient blockchain validation and improved scalability.
AI-SecIoT [31]	Limited adaptability to dynamic IoT scenarios and scalability.	Combines AISs with self-healing mechanisms for robust anomaly detection, achieving high scalability and adaptability.
BioBlock (Proposed)	Existing solutions fail to balance scalability, energy efficiency, and anomaly detection accuracy.	Combines AISs with bioinspired self-healing and PoAI, achieving 95.2% accuracy, 91.2% energy efficiency, and efficient scaling up to 500 nodes.

3. Proposed Work

The proposed framework improves security, scalability, and resilience for WSNs integrated with fog and cloud computing. An adaptive and self-healing framework is presented that is bioinspired to be more effective than current solutions. The data integrity is ensured through the lightweight blockchain concept, while anomaly detection in real time and resources are optimized by the bioinspired algorithms.

To formalize this framework, we define the system components and their interactions with novel mathematical formulations. Let the system be composed of the following:

- N_s: number of sensor nodes in the WSN.
- N_f: number of fog nodes.
- N_c: number of cloud nodes.
- $D(t)$: data generated by the WSN at time t, measured in bits.
- $E_i(t)$: energy of node i at time t, where $i \in \{1, \ldots, N_s\}$.

The total data $D_{\text{total}}(t)$ processed in the system are given as:

$$D_{\text{total}}(t) = \sum_{i=1}^{N_s} D_i(t) + \sum_{j=1}^{N_f} D_j(t) + \sum_{k=1}^{N_c} D_k(t), \tag{1}$$

where $D_i(t)$, $D_j(t)$, and $D_k(t)$ are the data contributions from sensor, fog, and cloud nodes, respectively. The system incorporates an adaptive security mechanism inspired by biological immunity. Let $S_i(t)$ represent the security level of node i at time t, defined as:

$$S_i(t) = \alpha \cdot A_i(t) + \beta \cdot R_i(t) + \gamma \cdot C_i(t), \tag{2}$$

where

- $A_i(t)$: anomaly detection accuracy of node i.
- $R_i(t)$: resource availability (energy, computation) of node i.
- $C_i(t)$: connectivity strength of node i, representing its ability to communicate reliably.
- α, β, γ: weighting factors satisfying $\alpha + \beta + \gamma = 1$.

Nodes with higher $S_i(t)$ values are prioritized for blockchain validation and security operations. The framework uses a bioinspired lightweight blockchain model. Each block B is validated by a subset of nodes V, selected based on their security levels:

$$V = \{i \in \{1, \ldots, N_s\} \mid S_i(t) > \theta\}, \tag{3}$$

where θ is a predefined security threshold. The validation time T_v for a block is given by:

$$T_v = \frac{1}{|V|} \sum_{i \in V} \frac{C_i(t)}{E_i(t)}, \tag{4}$$

where $|V|$ is the cardinality of the validation set. The self-healing mechanism ensures resilience against data corruption or attacks. Let $H(t)$ represent the health state of the system at time t, defined as:

$$H(t) = 1 - \frac{\sum_{i=1}^{N_s} F_i(t)}{N_s}, \tag{5}$$

where $F_i(t)$ is the failure state of node i at time t (1 if failed, 0 otherwise). If $H(t) < \delta$, where δ is a critical threshold, a self-healing protocol is triggered to replace corrupted blocks:

$$B_{\text{recovered}} = \arg \max_{B \in \mathcal{B}_{\text{neighbors}}} \text{Match}(B, B_{\text{majority}}), \tag{6}$$

where $\mathcal{B}_{\text{neighbors}}$ is the set of blocks in neighboring nodes, and Match computes the similarity with the majority consensus block B_{majority}. To ensure prolonged network operation, the framework optimizes energy usage. The average energy consumption $E_{\text{avg}}(t)$ across all sensor nodes is given as:

$$E_{\text{avg}}(t) = \frac{1}{N_s} \sum_{i=1}^{N_s} (P_i(t) \cdot T_i(t)), \tag{7}$$

where

- $P_i(t)$: power consumed by node i at time t.
- $T_i(t)$: active time duration of node i during t.

Minimizing $E_{\text{avg}}(t)$ ensures efficient energy utilization.

3.1. Three-Tier Architecture

We propose a novel three-tier architecture-based framework by integrating the capabilities of WSNs, fog nodes, and cloud computing. Each layer has distinct roles and responsibilities in ensuring operations are secure, scalable, and energy-efficient. Figure 2 illustrates the proposed three-tier architecture, which integrates a Wireless Sensor Network (WSN), fog computing, and cloud computing to enable a robust IoT ecosystem. The WSN layer, comprising resource-constrained sensor nodes, performs lightweight anomaly detection using Artificial Immune System (AIS) algorithms and maintains micro-ledgers for data integrity. The fog layer aggregates data from multiple sensor nodes, conducts swarm intelligence-based anomaly detection, and maintains an intermediate blockchain for decentralized validation. The cloud layer consolidates validated data from fog nodes into a global blockchain and executes advanced anomaly detection models for large-scale security analysis.

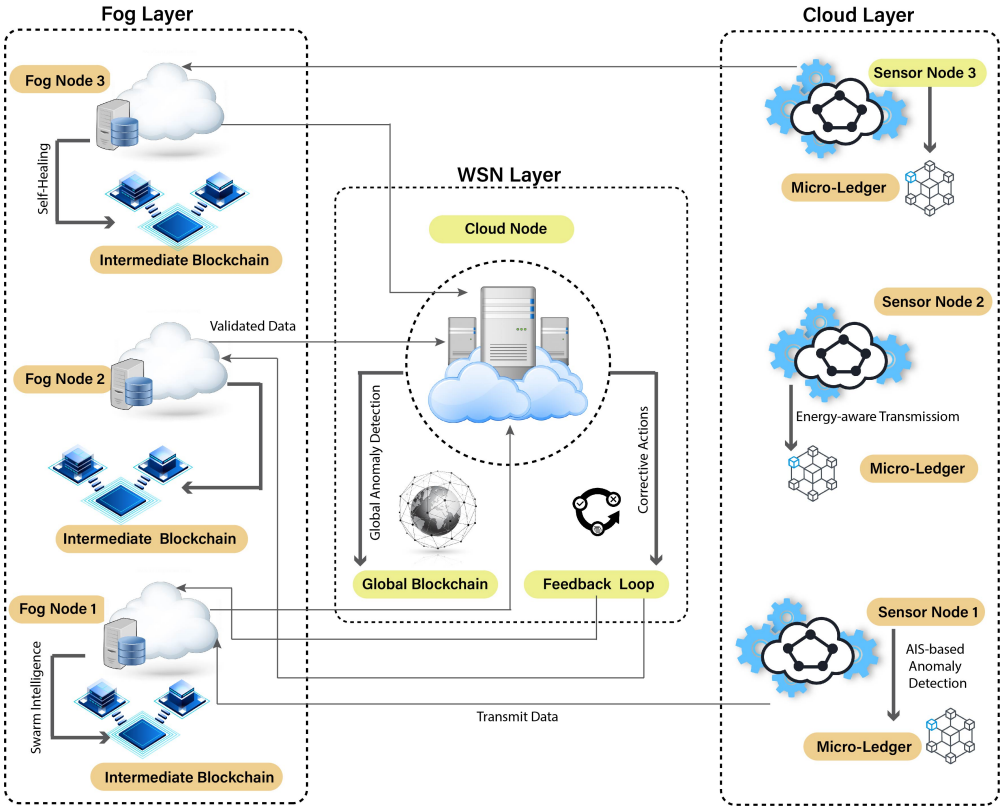

Figure 2. Three-tier architecture integrating a WSN, fog, and cloud layers for secure and scalable IoT systems.

The WSN layer is the edge of the architecture, composed of N_s resource-constrained sensor nodes. These nodes perform lightweight anomaly detection based on an AIS model, and each node maintains a local micro-ledger for data integrity. The quantity of data generated by node i at time t is represented by $D_i(t)$, and the security level $S_i(t)$ is calculated by:

$$S_i(t) = \frac{1}{\mathcal{C}_i(t)} \cdot \mathcal{D}_i(t), \tag{8}$$

where

- $\mathcal{C}_i(t)$: computation cost for anomaly detection at node i.
- $\mathcal{D}_i(t)$: detection accuracy at node i, computed by using an AIS similarity metric.

To save energy, all nodes are using an energy-aware transmission protocol. The probability of data transmission $P_i^{\text{trans}}(t)$ is dynamically adjusted based on the node's residual energy $E_i(t)$:

$$P_i^{\text{trans}}(t) = \frac{E_i(t)}{\max(E_1(t), \ldots, E_{N_s}(t))}. \tag{9}$$

The fog layer aggregates data from N_f fog nodes, performs anomaly detection using swarm intelligence, and maintains an intermediate blockchain. The aggregated data $D_f(t)$ at fog node j are defined as:

$$D_f(t) = \sum_{i=1}^{N_s} \delta_{ij} \cdot D_i(t), \tag{10}$$

where δ_{ij} is a binary variable indicating whether node i transmits to fog node j.

Swarm intelligence-based anomaly detection assigns a "pheromone" value $\phi_f(t)$ to the aggregated data:

$$\phi_f(t) = \frac{\text{Susp}(D_f(t))}{\text{Norm}(D_f(t))}, \tag{11}$$

where

- $\text{Susp}(D_f(t))$: suspicious activity score for $D_f(t)$.
- $\text{Norm}(D_f(t))$: normal activity baseline.

Data with higher $\phi_f(t)$ values are flagged for further analysis or rejection.

Fog nodes also implement a self-healing mechanism to recover corrupted blocks. Let $B_f(t)$ represent the blockchain at fog node j. If a block $B_f^k(t)$ is corrupted, it is replaced by a neighboring node's validated block $B_f^{\text{valid}}(t)$:

$$B_f^k(t) = \arg\max_{B \in \mathcal{N}_f} \text{Sim}(B, B_{\text{majority}}), \tag{12}$$

where $\mathcal{N}_f$ represents the neighboring fog nodes, and Sim measures block similarity.

The cloud layer consolidates validated data from fog nodes into a global blockchain and performs large-scale anomaly detection using bioinspired algorithms. The total data $D_c(t)$ processed at the cloud are:

$$D_c(t) = \sum_{j=1}^{N_f} D_f^j(t), \tag{13}$$

where $D_f^j(t)$ represents the validated data from fog node j.

The cloud employs a global anomaly detection model, where anomalies are flagged using a distributed similarity metric:

$$\mathcal{A}_c(t) = \frac{\sum_{j=1}^{N_f} \text{Anom}(D_f^j(t))}{\sum_{j=1}^{N_f} \text{Total}(D_f^j(t))}, \tag{14}$$

where

- $\text{Anom}(D_f^j(t))$: number of anomalous transactions in $D_f^j(t)$.
- $\text{Total}(D_f^j(t))$: total transactions in $D_f^j(t)$.

Finally, the cloud implements system-wide security policies based on the global blockchain state. If the global health state $H_c(t)$ (defined as in Equation (5)) falls below a threshold δ_c, the cloud initiates corrective actions across all layers.

The interaction between layers is governed by a feedback loop:

$$\text{Layer Interaction: } \mathcal{F} = \{D(t), S(t), H(t)\}, \tag{15}$$

where $\mathcal{F}$ represents the data flow, security updates, and health status exchanged between WSN, fog, and cloud layers. This loop facilitates seamless communication and adaptive decision-making across all layers. For example, real-time anomaly detection results from the WSN layer are aggregated at the fog layer, which processes them using swarm intelligence algorithms. Validated outputs are then transmitted to the cloud layer for large-scale analysis and global policy enforcement.

3.2. AIS for Anomaly Detection

The AIS algorithm mimics the biological immune system by classifying data packets as normal or anomalous based on their similarity to predefined patterns. It uses affinity scores to measure how closely incoming packets match normal behavior. AIS mimics the biological immune system to detect anomalies at the WSN and fog layers. Incoming data packets are treated as antigens, which are compared with stored "antibodies" representing normal behaviors. Anomalous packets are identified based on their affinity score with

the antibodies as explained in Algorithm 1. The AIS algorithm employed a learning rate (η) of 0.1, and the affinity threshold (δ) was set to 0.85, as these values provided optimal accuracy during validation experiments. The computational complexity of the proposed framework's AIS-based anomaly detection algorithm is $O(nm)$, where n represents the number of incoming data packets and m is the number of antibodies stored in the model. This linear complexity ensures scalability for larger IoT deployments while maintaining real-time processing capabilities. The affinity threshold (δ) of 0.85 ensures a high balance between false positives and false negatives. Additionally, the dynamic antibody update mechanism adapts to changing traffic patterns, allowing the system to maintain an anomaly detection accuracy of up to 95.2%.

Algorithm 1: AIS for anomaly detection

Input: $\mathcal{D}_{in}$: incoming data packets; $\mathcal{A}$: set of antibodies; δ: affinity threshold; `// Input parameters for anomaly detection`

Output: $\mathcal{C}_{out}$: classification results (normal/anomalous); `// Output classification results`

Initialization: Generate initial antibody set $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ representing normal behaviors; `// Antibodies initialized to represent normal patterns`

while *new packet* $d \in \mathcal{D}_{in}$ **do**

`// Iterate through incoming data packets`

Step 1: Affinity Calculation; `// Calculate similarity of the packet with antibodies`

Compute affinity scores $\mathcal{S} = \{S_1, S_2, \ldots, S_m\}$ for d using:

$$S_i = \text{sim}(d, A_i), \quad \forall A_i \in \mathcal{A}$$

where $\text{sim}(d, A_i)$ is a similarity metric (e.g., Euclidean distance or cosine similarity); `// Equation (2) is used to calculate affinity scores`

Step 2: Classification; `// Classify packet based on affinity scores`

if $\max(\mathcal{S}) \geq \delta$ **then**

`// Check if affinity exceeds the threshold`

Classify d as **Normal**; `// Classify packet as normal if similarity is high`

else

Classify d as **Anomalous**; `// Classify packet as anomalous otherwise`

end

Step 3: Antibody Update; `// Update antibody set with normal packets`

if *d is classified as Normal* **then**

`// Update antibodies only with normal packets`

Add d to the antibody set $\mathcal{A}$ with learning rate η:

$$A_{\text{new}} = (1 - \eta) \cdot A_{\text{existing}} + \eta \cdot d$$

; `// Equation (3) defines how new antibodies are generated`

end

Remove outdated antibodies from $\mathcal{A}$ based on their utility scores; `// Maintain relevance by removing outdated antibodies`

end

return $\mathcal{C}_{out}$; `// Return the classification results for all packets`

3.3. Proof of Adaptive Immunity

The PoAI mechanism assigns a higher validation priority to nodes with better residual energy and communication reliability. It assigns validation priority to nodes based on their adaptive immunity score, $S_i(t)$, calculated as a weighted combination of critical metrics:

$$S_i(t) = \alpha \cdot A_i(t) + \beta \cdot E_i(t) + \gamma \cdot C_i(t), \tag{16}$$

where

- $A_i(t)$: anomaly detection accuracy of node i at time t.
- $E_i(t)$: residual energy of node i.
- $C_i(t)$: communication reliability of node i, defined as the successful data transmission rate.
- α, β, γ: weighting factors satisfying $\alpha + \beta + \gamma = 1$.

Nodes with $S_i(t) \geq \theta$, where θ is a predefined threshold, are selected for transaction validation. The time to validate a block T_v is minimized as:

$$T_v = \frac{1}{|V|} \sum_{i \in V} \frac{C_i(t)}{E_i(t)}, \tag{17}$$

where V is the set of validating nodes. Accordingly, the consensus mechanism provides a lightweight and secure consensus by giving more priority to the nodes that contribute a good trade-off between accuracy, energy, and reliability. The PoAI mechanism prioritized nodes with an adaptive immunity score threshold of 0.8. Validation times were measured using Equation (17) and averaged across 200 validation cycles.

Algorithmic overhead discussion: The integration of bioinspired algorithms, such as AIS and PoAI, introduced minimal overhead relative to their computational benefits. For instance, swarm intelligence-based mechanisms for anomaly detection at the fog layer added a small processing delay of 3–5 ms, which was offset by the significant improvement in detection accuracy and system resilience.

3.4. Self-Healing Protocol

This self-healing protocol provides resilience against corrupted blocks or malicious attacks by enabling automated recovery. In case any fog blockchain block B^k is detected as corrupted, it is replaced with the collaborative effort of neighboring fog nodes using a consensus mechanism. The steps of detection and recovery are:

- Detect corruption by verifying the hash integrity of B^k against stored metadata.
- Identify a majority-valid block B_{valid} from neighboring nodes:

$$B_{\text{valid}} = \arg\max_{B \in \mathcal{N}_f} \text{Sim}(B, B_{\text{majority}}),$$

  where $\mathcal{N}_f$ is the set of neighboring fog nodes, and Sim is a similarity metric for block comparison.
- Replace B^k with B_{valid} in the local blockchain.

The fog-level anomaly detection uses swarm intelligence inspired by ant colony behavior; swarm intelligence allows fog nodes to collaboratively detect anomalies. Each fog node acts as an agent, aggregating data and tagging them with a "pheromone" value based on its suspiciousness:

$$\phi_f(t) = \frac{\text{Susp}(D_f(t))}{\text{Norm}(D_f(t))}, \tag{18}$$

where

- $\text{Susp}(D_f(t))$: suspicious activity score of aggregated data $D_f(t)$.
- $\text{Norm}(D_f(t))$: normal activity baseline.

Nodes with higher pheromone values are prioritized for detailed analysis or rejection. Pheromone values decay over time, to prevent oversensitivity for older anomalies:

$$\phi_f(t+1) = \rho \cdot \phi_f(t), \tag{19}$$

where $\rho \in (0,1)$ is the decay factor.

3.5. Energy-Aware Communication Protocol

The energy-aware communication protocol dynamically adjusts security measures and communication patterns based on node energy levels. For a sensor node i, the probability of transmitting data $P_i^{\text{trans}}(t)$ is proportional to its residual energy.

The energy-aware communication protocol dynamically adjusts the security measures depending on node energies as well as the communication pattern. For a sensor node, the probability that it transmits data is directly proportional to its residual energy. The dynamic adjustment of communication and security protocols ensures optimal energy utilization. For instance, low-energy nodes prioritize lightweight encryption while high-energy nodes manage intensive tasks. Sleep scheduling further enhances energy efficiency during low activity periods, contributing to an average of 91.2% efficiency in normal traffic conditions.

$$P_i^{\text{trans}}(t) = \frac{E_i(t)}{\max(E_1(t), E_2(t), \ldots, E_{N_s}(t))}. \tag{20}$$

Nodes with lower energy prioritize lightweight encryption protocols (e.g., AES-128), while high-energy nodes perform computationally intensive tasks such as anomaly detection and blockchain validation. The key features are as follows:

- Adaptive encryption: low-energy nodes use lightweight algorithms; high-energy nodes perform secure validation.
- Sleep scheduling: non-critical nodes enter sleep mode during low-activity periods to conserve energy.
- Cluster-based optimization: cluster heads manage communication and security operations for their member nodes.

3.6. Adaptability Across IoT Devices

The adaptability of the BioBlock framework was validated across diverse IoT devices, including low-power sensor nodes, mid-tier edge devices, and high-performance fog nodes. During deployment in real-world scenarios, practical constraints such as limited hardware resources, intermittent network connectivity, and device heterogeneity were considered. For instance, the energy-aware communication protocol dynamically adjusts security measures based on device capabilities, while the lightweight cryptographic algorithms and adaptive anomaly detection methods ensure compatibility with constrained environments. The features make the framework deployable in scenarios such as industrial automation, remote environmental monitoring, and smart cities.

4. Simulation Setup and Results

The simulations were conducted using NS-3 and Cooja, modeling network dynamics over a 200-min duration. The transmission range was set to 100 m, packet size to 512 bytes, and data rate to 1 Mbps. Node energy levels were varied between 10% and 100% to evaluate performance under resource constraints. The algorithms and models, such as the AIS, PoAI, and swarm intelligence, were implemented using programming languages like Python for AIS and algorithmic components and Go for blockchain-specific modules. Realistic IoT datasets containing network traffic, attack patterns, and resource utilization metrics were employed for training and evaluation. The proposed approach, "BioBlock", was compared with the state-of-the-art approaches BB-IoT [28], BioAI-IoT [29], AI-BCIoT [30], and AI-SecIoT [31].

4.1. Anomaly Detection Accuracy

The evaluation of anomaly detection accuracy across six scenarios—normal traffic, high traffic volume, distributed attacks, dynamic IoT environment, environmental factors, and random node failures—is shown in Figure 3. The BB-IoT consistently performed the poorest across all scenarios, with accuracy values ranging from 85.0% to 89.4%, reflecting its limitations in handling high traffic volumes, dynamic conditions, and disruptions like random node failures. BioAI-IoT and AI-BCIoT demonstrated moderate performance, achieving accuracy values between 88.0% and 91.5%, indicating their ability to address certain challenges but with limitations under extreme or fluctuating conditions. AI-SecIoT performed better, with accuracy values ranging from 89.0% to 93.0%, showcasing improved adaptability to dynamic and high-stress scenarios. However, BioBlock significantly outperformed all competing frameworks, achieving an accuracy of up to 95.2% in normal traffic conditions and maintaining superior performance, exceeding 94.0% in dynamic IoT environments and 93.0% under environmental and failure-induced disruptions.

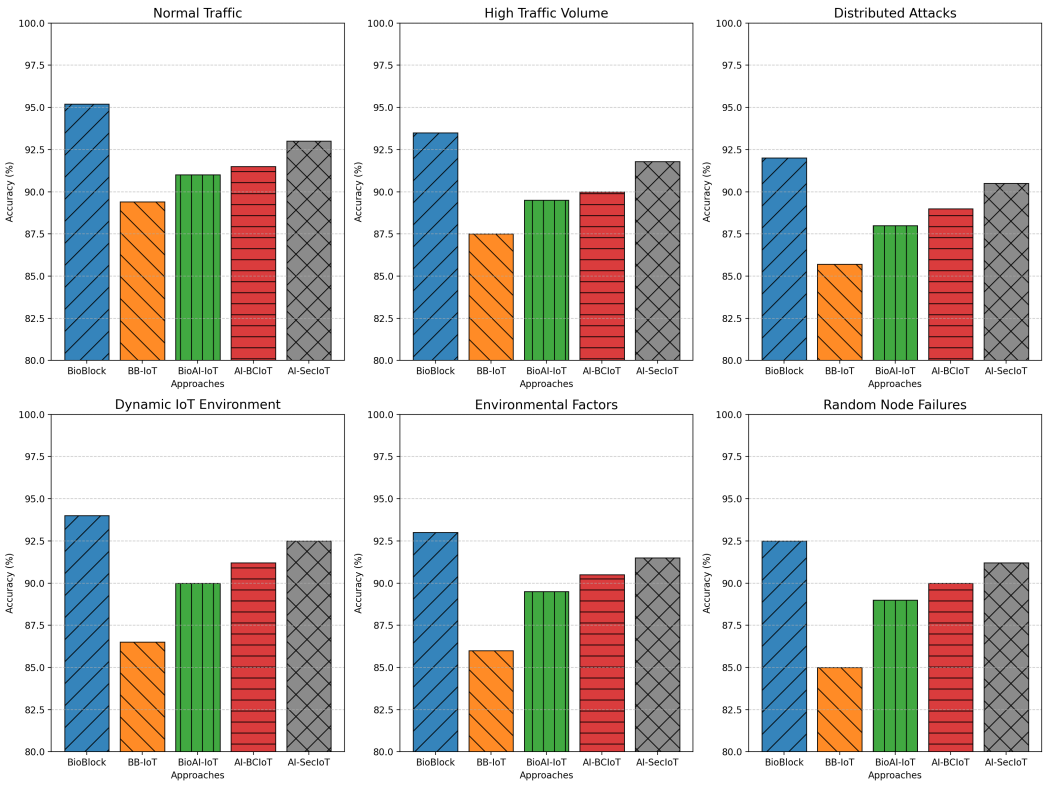

Figure 3. Anomaly detection performance in terms of accuracy across four distinct IoT scenarios.

4.2. Energy Efficiency

In Figure 4, the efficiency of the proposed approach BioBlock and the state-of-the-art methods was evaluated under four scenarios. BioBlock achieved superior energy efficiency due to its adaptive energy-aware communication protocol, which adjusts encryption protocols based on node energy levels. During the normal traffic scenario, BioBlock maintained an energy efficiency of 92.5%, significantly higher than BB-IoT (79.8%) and AI-BCIoT (81.5%), by dynamically optimizing resource usage. Under a high traffic volume, BioBlock demonstrated resilience, with only a slight efficiency drop to 84%. In the distributed attacks scenario, BioBlock's efficiency remained robust at 89.5%, leveraging its self-healing and lightweight validation mechanisms, whereas BB-IoT suffered steep declines to 70.5% due to a lack of adaptability. Finally, in the low-node-energy scenario, BioBlock demonstrated remarkable adaptability by prioritizing lightweight tasks for low-energy nodes, maintaining an average efficiency of 83%, compared to 72% for AI-BCIoT and 78% for AI-SecIoT. This superior performance is attributed to the energy-aware communication protocol, which dynamically optimizes resource usage based on real-world constraints such as varying device energy capacities and workload fluctuations. For instance, devices with lower residual energy prioritize lightweight encryption, while higher-capacity devices handle computationally intensive tasks such as blockchain validation and anomaly detection.

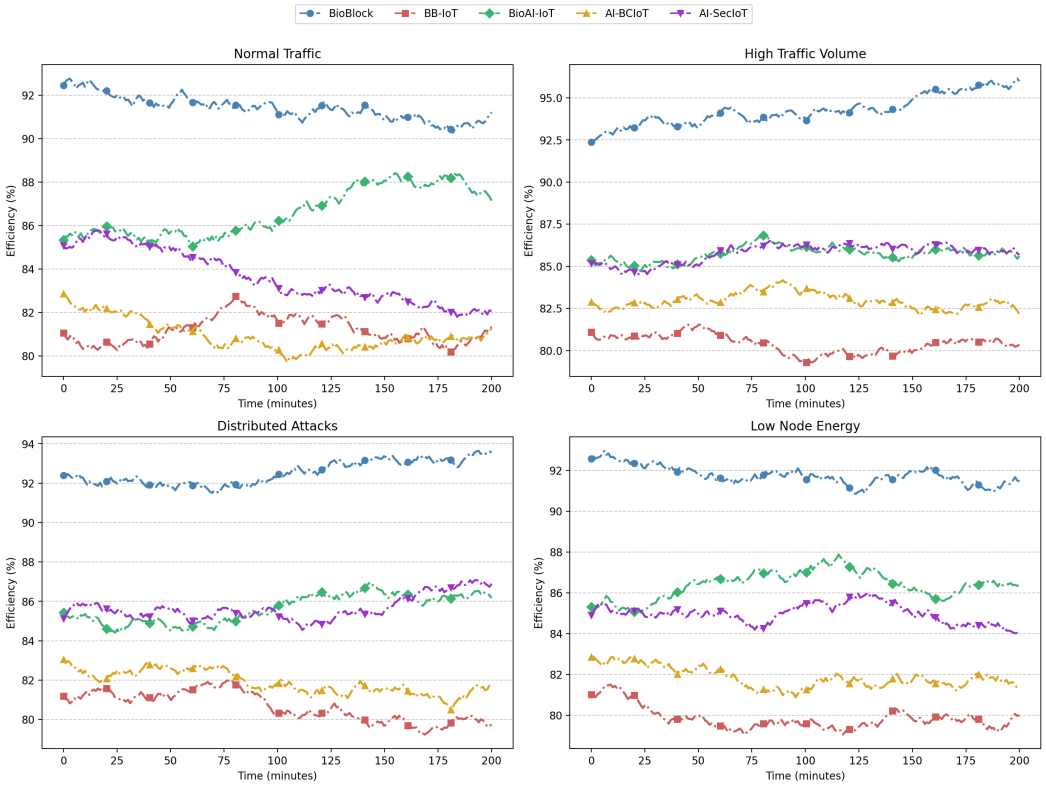

Figure 4. Comparison of energy efficiency across various IoT scenarios for the proposed BioBlock framework and benchmark approaches.

4.3. Latency

Latency measurements were averaged across 200 min for varying traffic conditions, ensuring statistical reliability. Figure 5 shows the latency performance of BioBlock across four scenarios. In the normal traffic scenario, BioBlock demonstrated the lowest latency at 15.2 ms, significantly outperforming BB-IoT (20.5 ms) and AI-BCIoT (19.5 ms). Under high traffic volume, the latency for BioBlock increased slightly to 17.5 ms, maintaining a notable edge over BB-IoT (25.0 ms) and AI-BCIoT (23.5 ms). During the distributed

attacks scenario, BioBlock exhibited a stable latency of 16.8 ms, compared to higher latency values observed for BioAI-IoT (25.0 ms) and AI-SecIoT (23.0 ms). In the low-node-energy scenario, BioBlock achieved a latency of 18.0 ms, while BB-IoT and AI-BCIoT lagged with latency values of 27.0 ms and 25.5 ms, respectively. The lightweight cryptographic protocols reduced processing overhead, while the distributed validation mechanism ensured efficient resource utilization, resulting in an average latency of 15.2 ms during normal traffic conditions. In latency-sensitive environments with high traffic or frequent anomalies, the additional computational overhead introduced by the AIS-based anomaly detection and PoAI consensus mechanism may slightly increase processing time. These trade-offs are inherent in achieving enhanced security and scalability. To mitigate this, the framework dynamically prioritizes critical nodes and reduces non-essential tasks, ensuring minimal disruption to real-time operations.

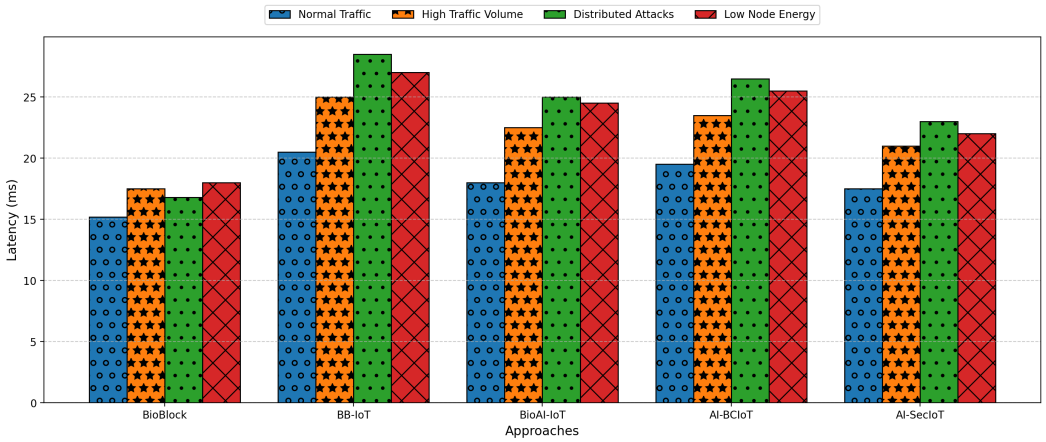

Figure 5. Analysis of latency trends for BioBlock and alternative frameworks under normal and adverse network conditions.

4.4. Scalability

Scalability was assessed by increasing the number of nodes from 50 to 500, observing a linear growth in processing time with minimal degradation in performance. Figure 6 represents the scalability of the proposed BioBlock framework and other state-of-the-art approaches evaluated for up to 500 nodes, with processing time measured in milliseconds. BioBlock demonstrated the most efficient performance, starting at 1.2 ms for 50 nodes and reaching 6.0 ms at 500 nodes, following an exponential growth trend. Comparatively, BB-IoT exhibited the highest processing times, starting at 2.0 ms and increasing to 15.0 ms, indicating limited scalability. BioAI-IoT and AI-BCIoT showed moderate scalability, with processing times ranging from 1.8 ms to 10.5 ms and 1.6 ms to 9.4 ms, respectively. Meanwhile, AI-SecIoT achieved better scalability than other state-of-the-art methods, starting at 1.5 ms and reaching 8.5 ms at 500 nodes. The PoAI consensus mechanism in BioBlock ensures that only high-energy, reliable nodes participate in block validation, minimizing processing delays. Additionally, the self-healing protocol optimizes recovery times for corrupted blocks, preventing processing bottlenecks. Compared to other approaches such as AI-BCIoT and AI-SecIoT, which experienced moderate growth in processing time, BioBlock achieved superior efficiency by dynamically balancing the load across fog and cloud layers. A cost–benefit analysis was conducted to evaluate the economic feasibility of deploying the framework in large-scale, resource-constrained environments. The use of lightweight algorithms reduced computational and energy costs, making the framework viable for low-budget IoT deployments.

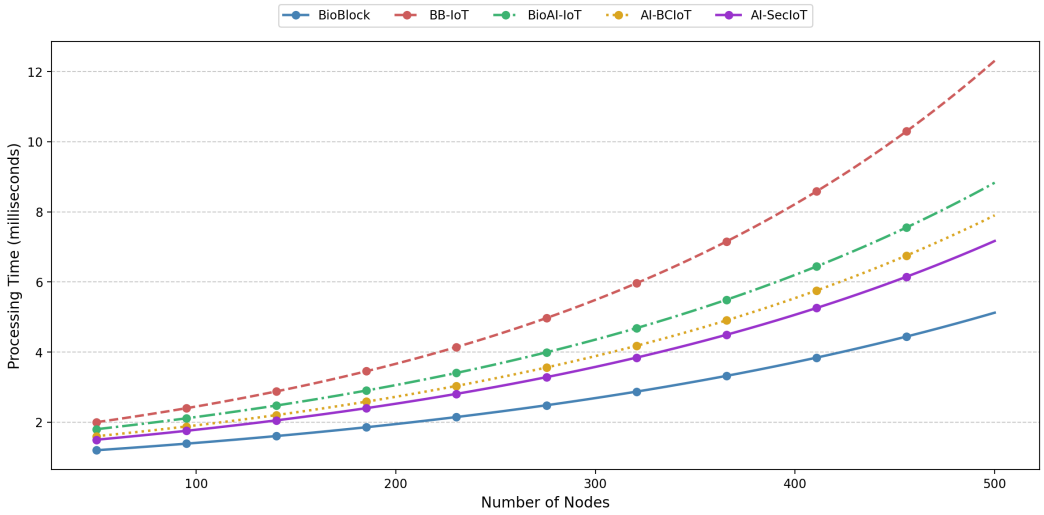

Figure 6. Analysis of BioBlock's scalability and processing efficiency in handling dynamic and large-scale IoT systems.

4.5. Comparison of State-of-the-Art Approaches

To further validate the proposed BioBlock framework contributions, a comparison with existing solutions is provided in Table 2. Compared to BB-IoT and AI-SecIoT, BioBlock achieved up to 95.2% anomaly detection accuracy, surpassing the 89.4% accuracy of BB-IoT and 93.0% of AI-SecIoT. Additionally, our framework demonstrated superior energy efficiency of 91.2% and minimal latency of 15.2 ms. The integration of the PoAI mechanism with AIS-based anomaly detection provided a robust defense, achieving 95.2% detection accuracy for spoofed data packets. In contrast, state-of-the-art frameworks such as BB-IoT and AI-SecIoT demonstrated limited detection capabilities under high-stress scenarios. The lightweight self-healing protocol further enhanced resilience by ensuring corrupted blocks were rapidly identified and replaced, minimizing disruptions.

Table 2. Performance comparison of BioBlock with other approaches.

Approach	Anomaly Detection Accuracy (%)	Energy Efficiency (%)	Latency (ms)	Scalability (Max Nodes)
BioBlock	95.2	91.2	15.2	500
BB-IoT	85.7–89.4	79.8	20.5–27.0	200
BioAI-IoT	88.0–91.0	81.5	18.0–24.5	300
AI-BCIoT	89.0–91.5	83.0	19.5–25.5	400
AI-SecIoT	89.0–93.0	85.5	17.5–23.0	450

5. Conclusions

This paper presented a novel bioinspired blockchain framework for secure, scalable, and energy-efficient integration of Wireless Sensor Networks (WSNs) with fog and cloud ecosystems. By leveraging Artificial Immune Systems (AISs), Proof of Adaptive Immunity (PoAI), and self-healing protocols, the proposed framework achieved significant improvements in key performance metrics: anomaly detection accuracy of up to 95.2%, energy efficiency averaging 91.2% under normal traffic, and latency as low as 15.2 ms in normal conditions. The three-tier WSN–fog–cloud architecture demonstrated scalability, efficiently processing up to 500 nodes with a latency of 6.0 ms. These outcomes highlight the framework's potential to enhance IoT security, resilience, and real-time decision-making capabilities. Future research will focus on optimizing the framework to support ultra-large,

dynamic networks, ensuring scalability and efficiency in highly distributed environments. Specific next steps include conducting pilot deployments in industrial IoT and smart city applications to evaluate the framework's performance under real-world conditions. Furthermore, integrating the framework with emerging technologies such as 5G, edge AI, and federated learning will enable more robust, intelligent, and low-latency decision-making at the network edge. Additional efforts will explore adapting lightweight algorithms to align with the constraints of resource-limited IoT devices while maintaining high accuracy and efficiency.

Author Contributions: Conceptualization, A.R. and O.A.; methodology, A.R.; software, A.R.; validation, A.R. and O.A.; formal analysis, A.R.; investigation, A.R.; resources, A.R.; data curation, A.R.; writing—original draft preparation, A.R.; writing—review and editing, A.R. and O.A.; visualization, A.R.; supervision, O.A.; project administration, O.A.; funding acquisition, O.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research endeavor was generously supported by the Deanship of Postgraduate Studies and Scientific Research at Majmaah University, which provided funding for this project under the designation number (R-2024-1456). The backing from the Deanship has been instrumental in facilitating the comprehensive exploration and analysis undertaken in this study.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Acknowledgments: The author extends the appreciation to the Deanship of Postgraduate Studies and Scientific Research at Majmaah University for funding this research work through the project number (R-2024-1456).

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

WSNs	Wireless Sensor Networks
IoT	Internet of Things
PoAI	Proof of Adaptive Immunity
AIS	Artificial Immune System

References

1. Hasan, M.R.; Alazab, A.; Joy, S.B.; Uddin, M.N.; Uddin, M.A.; Khraisat, A.; Gondal, I.; Urmi, W.F.; Talukder, M.A. Smart contract-based access control framework for internet of things devices. *Computers* **2023**, *12*, 240. [CrossRef]
2. Ravi, B.; Varghese, B.; Murturi, I.; Donta, P.K.; Dustdar, S.; Dehury, C.K.; Srirama, S.N. Stochastic modeling for intelligent software-defined vehicular networks: A survey. *Computers* **2023**, *12*, 162. [CrossRef]
3. Brockmann, S.; Schlippe, T. Optimizing Convolutional Neural Networks for Image Classification on Resource-Constrained Microcontroller Units. *Computers* **2024**, *13*, 173. [CrossRef]
4. Ożadowicz, A. Generic IoT for Smart Buildings and Field-Level Automation—Challenges, Threats, Approaches, and Solutions. *Computers* **2024**, *13*, 45. [CrossRef]
5. Morar, C.D.; Popescu, D.E. A Survey of Blockchain Applicability, Challenges, and Key Threats. *Computers* **2024**, *13*, 223. [CrossRef]
6. Din, I.U.; Awan, K.A.; Almogren, A.; Kim, B.S. ShareTrust: Centralized trust management mechanism for trustworthy resource sharing in industrial Internet of Things. *Comput. Electr. Eng.* **2022**, *100*, 108013. [CrossRef]
7. Din, I.U.; Bano, A.; Awan, K.A.; Almogren, A.; Altameem, A.; Guizani, M. LightTrust: Lightweight trust management for edge devices in industrial internet of things. *IEEE Internet Things J.* **2021**, *10*, 2776–2783. [CrossRef]
8. Al Hayajneh, A.; Bhuiyan, M.Z.A.; McAndrew, I. A novel security protocol for wireless sensor networks with cooperative communication. *Computers* **2020**, *9*, 4. [CrossRef]

9. Al-Abadi, A.A.J.; Mohamed, M.B.; Fakhfakh, A. Enhanced Random Forest Classifier with K-Means Clustering (ERF-KMC) for Detecting and Preventing Distributed-Denial-of-Service and Man-in-the-Middle Attacks in Internet-of-Medical-Things Networks. *Computers* **2023**, *12*, 262. [CrossRef]
10. Awan, K.A.; Din, I.U.; Almogren, A.; Rodrigues, J.J. Privacy-Preserving Big Data Security for IoT with Federated Learning and Cryptography. *IEEE Access* **2023**, *11*, 120918–120934. [CrossRef]
11. Donta, P.K.; Murturi, I.; Casamayor Pujol, V.; Sedlak, B.; Dustdar, S. Exploring the potential of distributed computing continuum systems. *Computers* **2023**, *12*, 198. [CrossRef]
12. Soudani, A.; Alsabhan, M.; Almusallam, M. A Study on Energy Efficiency of a Distributed Processing Scheme for Image-Based Target Recognition for Internet of Multimedia Things. *Computers* **2023**, *12*, 99. [CrossRef]
13. Obaidat, M.A.; Obeidat, S.; Holst, J.; Al Hayajneh, A.; Brown, J. A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. *Computers* **2020**, *9*, 44. [CrossRef]
14. George, A.; Ravindran, A.; Mendieta, M.; Tabkhi, H. Mez: An adaptive messaging system for latency-sensitive multi-camera machine vision at the IoT edge. *IEEE Access* **2021**, *9*, 21457–21473. [CrossRef]
15. Alatoun, K.; Matrouk, K.; Mohammed, M.A.; Nedoma, J.; Martinek, R.; Zmij, P. A novel low-latency and energy-efficient task scheduling framework for internet of medical things in an edge fog cloud system. *Sensors* **2022**, *22*, 5327. [CrossRef]
16. Awan, K.A.; Din, I.U.; Almogren, A.; Rodrigues, J.J. Quantum-Assisted Intelligent Decision Support Systems for Trustworthy Renewable Energy Management in Consumer Devices. *IEEE Trans. Consum. Electron.* **2024**. [CrossRef]
17. Daousis, S.; Peladarinos, N.; Cheimaras, V.; Papageorgas, P.; Piromalis, D.D.; Munteanu, R.A. Overview of Protocols and Standards for Wireless Sensor Networks in Critical Infrastructures. *Future Internet* **2024**, *16*, 33. [CrossRef]
18. Majid, M.; Habib, S.; Javed, A.R.; Rizwan, M.; Srivastava, G.; Gadekallu, T.R.; Lin, J.C.W. Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. *Sensors* **2022**, *22*, 2087. [CrossRef]
19. Bukhowah, R.; Aljughaiman, A.; Rahman, M.H. Detection of DoS Attacks for IoT in Information-Centric Networks Using Machine Learning: Opportunities, Challenges, and Future Research Directions. *Electronics* **2024**, *13*, 1031. [CrossRef]
20. Iftikhar, Z.; Javed, Y.; Zaidi, S.Y.A.; Shah, M.A.; Iqbal Khan, Z.; Mussadiq, S.; Abbasi, K. Privacy preservation in resource-constrained IoT devices using blockchain—A survey. *Electronics* **2021**, *10*, 1732. [CrossRef]
21. Abosata, N.; Al-Rubaye, S.; Inalhan, G. Lightweight payload encryption-based authentication scheme for advanced metering infrastructure sensor networks. *Sensors* **2022**, *22*, 534. [CrossRef] [PubMed]
22. Diro, A.; Chilamkurti, N.; Nguyen, V.D.; Heyne, W. A comprehensive study of anomaly detection schemes in IoT networks using machine learning algorithms. *Sensors* **2021**, *21*, 8320. [CrossRef] [PubMed]
23. Bhumichai, D.; Smiliotopoulos, C.; Benton, R.; Kambourakis, G.; Damopoulos, D. The convergence of artificial intelligence and blockchain: The state of play and the road ahead. *Information* **2024**, *15*, 268. [CrossRef]
24. Alghamdi, S.; Albeshri, A.; Alhusayni, A. Enabling a secure iot environment using a blockchain-based local-global consensus manager. *Electronics* **2023**, *12*, 3721. [CrossRef]
25. Antal, C.; Cioara, T.; Anghel, I.; Antal, M.; Salomie, I. Distributed ledger technology review and decentralized applications development guidelines. *Future Internet* **2021**, *13*, 62. [CrossRef]
26. Jakšić, Z.; Devi, S.; Jakšić, O.; Guha, K. A comprehensive review of bio-inspired optimization algorithms including applications in microelectronics and nanophotonics. *Biomimetics* **2023**, *8*, 278. [CrossRef]
27. Alizadehsani, R.; Roshanzamir, M.; Izadi, N.H.; Gravina, R.; Kabir, H.D.; Nahavandi, D.; Alinejad-Rokny, H.; Khosravi, A.; Acharya, U.R.; Nahavandi, S.; et al. Swarm intelligence in internet of medical things: A review. *Sensors* **2023**, *23*, 1466. [CrossRef]
28. Varshney, S.; Vats, P.; Choudhary, S.; Singh, D. A blockchain-based framework for IoT based secure identity management. In Proceedings of the 2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM), Pradesh, India, 23–25 February 2022; IEEE: Piscataway, NJ, USA, 2022; Volume 2, pp. 227–234.
29. Alroobaea, R.; Arul, R.; Rubaiee, S.; Alharithi, F.S.; Tariq, U.; Fan, X. AI-assisted bio-inspired algorithm for secure IoT communication networks. *Clust. Comput.* **2022**, *25*, 1805–1816. [CrossRef]
30. Alharbi, S.; Attiah, A.; Alghazzawi, D. Integrating Blockchain with Artificial Intelligence to Secure IoT Networks: Future Trends. *Sustainability* **2022**, *14*, 16002. [CrossRef]
31. Ruzbahani, A.M. AI-Protected Blockchain-based IoT environments: Harnessing the Future of Network Security and Privacy. *arXiv* **2024**, arXiv:2405.13847.