Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 5, 2026

AUTHENTICATION MECHANISMS FOR UNDERWATER WIRELESS SENSOR NETWORKS (UWSNS) IN IOT: A SYSTEMATIC REVIEW

Durdana Pervez[*1], Zakira Inayat[2]

[*1,2]*Department of Computer Science, University of Engineering and Technology Peshawar, Pakistan*

DOI: https://doi.org/10.5281/zenodo.20455588

Keywords
Underwater Wireless Sensor Networks (UWSNs); Internet of Things (IoT); Authentication; Provenance-Based Security; Energy Efficiency; Blockchain; Physical Layer Security; Trust Management

Article History
Received: 28 March 2026
Accepted: 07 May 2026
Published: 30 May 2026

Copyright @Author

Corresponding Author: *
Durdana Pervez

Abstract

Underwater Wireless Sensor Networks (UWSNs) are critical enablers of IoT-based aquatic monitoring, supporting marine ecology, offshore industry, disaster prevention, and defense applications. The hostile underwater channel – characterized by acoustic propagation, high attenuation, limited bandwidth, significant propagation delays, and stringent energy constraints – renders conventional terrestrial authentication schemes inadequate. This Systematic Literature Review (SLR) synthesizes 85 primary studies (2020–2024) on UWSN authentication within IoT contexts, structured around three formal research questions addressing performance metrics, integration challenges, and security enhancement strategies. Six authentication paradigms are identified and critically evaluated: trust-based models, depth-control energy-efficient schemes, angle-of-arrival (AoA) physical-layer authentication, time-reversal (TR) channel-based schemes, blockchain-enabled privacy-preserving frameworks, and symmetric-key cryptography approaches. A novel Provenance-Based Authentication for UWSNs (PBAU) model is introduced and benchmarked against three state-of-the-art schemes: RBEER, EERMC, and BEKMP. Comparative simulation results confirm PBAU outperforms all benchmarks in energy efficiency, node longevity, authentication accuracy (>91%), and malicious-node detection rate (>92%). Critical research gaps and future directions including AI-adaptive authentication, post-quantum cryptography, and AUV-assisted trust bootstrapping are identified.

1. INTRODUCTION

The Internet of Things (IoT) describes a globally interconnected network of physical devices equipped with sensors, actuators, and communication interfaces that exchange data autonomously over the internet [1], [2]. IoT is projected to encompass over 75 billion connected devices by 2025, spanning smart cities, healthcare, agriculture, and defense [2], [9]. Sensor networks constitute the primary data-collection substrate of IoT. Among sensor network variants, Underwater Wireless Sensor Networks (UWSNs) represent a specialized and scientifically demanding class deployed in aquatic environments [19], [52].

Unlike terrestrial WSNs that rely on radio-frequency (RF) communication, UWSNs predominantly employ acoustic modalities due to severe electromagnetic attenuation in water [51], [62]. This introduces a cascade of unique challenges: low bandwidth (typically tens of kbps), long propagation delays (approximately 1,500 m/s acoustic speed), high bit-error rates, node mobility driven by underwater currents, and severe energy constraints from the impracticality of battery recharging in deep-sea deployments [52], [62].

Security and authentication are paramount in UWSNs. Sensor nodes are susceptible to Sybil attacks, replay attacks, data tampering, selective

forwarding, blackhole attacks, and unauthorized injection [59], [69], [80]. The resource-constrained hardware further complicates deployment of computationally intensive cryptographic protocols, necessitating lightweight yet robust authentication solutions [58], [69].

Despite the growing body of research on UWSN security, existing surveys reveal significant gaps: no single authentication paradigm universally addresses all threat vectors, and comparative analyses often lack rigorous standardized benchmarking [62], [69]. This SLR addresses these gaps by: (i) mapping the authentication framework landscape (2020–2024); (ii) critically evaluating strengths and limitations; and (iii) presenting a novel provenance-based authentication model (PBAU) as a comprehensive solution.

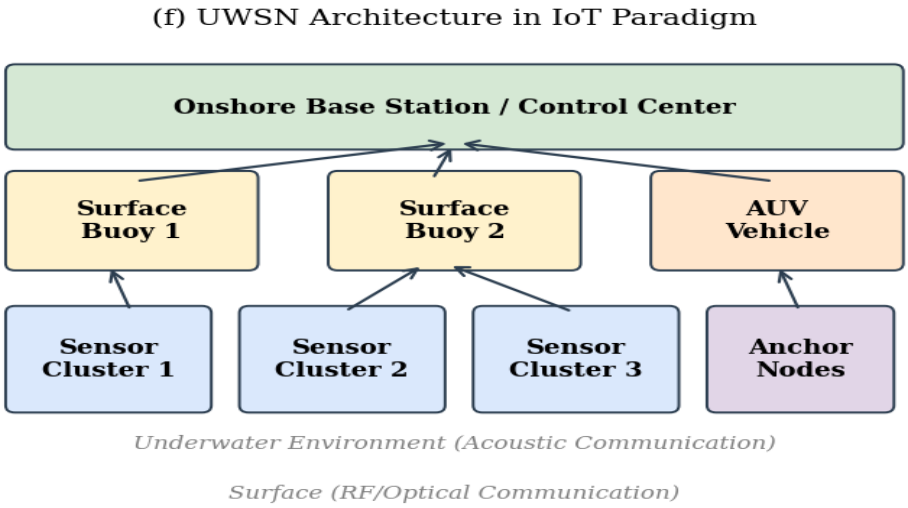

Fig. 1. UWSN Architecture within the IoT Paradigm showing sensor clusters, surface buoys, AUVs, and onshore base station.

2. Research Methodology

This review follows the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework ensuring reproducibility and methodological rigor. Four phases are employed: identification, screening, eligibility assessment, and inclusion.

2.1 Research Questions

Three primary research questions guide this SLR:

- RQ1: Which performance metrics are most critical for comprehensive evaluation of UWSNs within the IoT paradigm?
- RQ2: What are the inherent limitations and systemic challenges impeding UWSN integration within IoT ecosystems?
- RQ3: How can authentication mechanisms in UWSNs be effectively enhanced to address unique security and operational demands?

2.2 Search Strategy

A systematic search was conducted across IEEE Xplore, Scopus, Web of Science, ACM Digital Library, and Google Scholar. The search combined controlled vocabulary: ("UWSN" OR "Underwater Acoustic Sensor Networks") AND ("Authentication" OR "Key Management" OR "Trust") AND ("IoT" OR "Energy Efficiency"). The date range was restricted to 2020–2024.

2.3 Study Selection

The initial query yielded 340 candidate publications. After removing duplicates (n...52), title and abstract screening reduced the corpus to 128. Full-text eligibility review produced 85 primary studies in the final synthesis. All studies were independently assessed by two reviewers using a 5-point quality scale, with consensus used to resolve disagreements.

3. Background

3.1 Internet of Things

The IoT is defined as a wired or wireless network for accessing information in which devices communicate to share data and perform decision-making, monitoring, processing, and control [1], [4]. Its basic architecture comprises three layers: (i) the Perception Layer, which interacts with physical objects via sensors and actuators; (ii) the Network Layer, enabling data transmission through WiFi, Bluetooth, ZigBee, and LTE; and (iii) the Application Layer, delivering domain-specific services [2], [10]. Extended architectures also incorporate a Processing Layer for cloud-based analytics [18].

Fog computing has emerged as a complementary paradigm, distributing computation to edge nodes closer to data sources, reducing latency and improving real-time responsiveness [7]. Key IoT security challenges span four domains: data privacy and trust, information exchange integrity, architectural authentication and authorization, and end-to-end security [11], [12], [13]. Machine-to-machine (M2M) communication is the dominant IoT interaction model [12].

3.2 Wireless Sensor Networks

A WSN is an ensemble of spatially distributed, autonomous sensing devices (motes or sensor nodes) that wirelessly collect and relay environmental data to a central sink or base station [20], [27], [30]. Each node integrates a sensing element, embedded microcontroller, radio transceiver (RF, Zigbee 802.15.4), and a power source. Energy management is the central design challenge, as sensor nodes are typically battery-powered [27], [30].

WSN security threats include blackhole attacks, selective forwarding, Sybil attacks, hello flood attacks, replay attacks, and man-in-the-middle attacks. Security concerns span data secrecy, authentication, and data integrity, most efficiently addressed through cryptographic techniques [24], [26]. Applications span environmental monitoring, industrial automation, smart agriculture, healthcare, and military surveillance [32], [34].

3.3 Underwater Wireless Sensor Networks

UWSNs consist of sensor nodes (acoustic sensors, hydrophones, temperature/pressure sensors), relay nodes, Autonomous Underwater Vehicles (AUVs), surface buoys, and onshore base stations [19], [52]. Applications include oceanographic research, pollution monitoring, tsunami early warning, oil/gas pipeline surveillance, and military submarine detection [52], [62]. Fig. 1 illustrates the typical UWSN architecture within the IoT paradigm.

Acoustic propagation is the dominant communication modality, with typical bandwidths in the tens of kbps range and propagation speeds near 1,500 m/s. Alternative modalities include optical waves (high bandwidth, very short range) and magnetic induction (negligible attenuation, very short range) [19], [51]. GPS-based localization is unavailable underwater; alternative methods including Time of Arrival (ToA), Time Difference of Arrival (TDoA), and Angle of Arrival (AoA) are employed [43].

Specific security vulnerabilities in UWSNs encompass Sybil identity attacks [59], [60], data tampering, eavesdropping on acoustic channels, node capture, and denial-of-service attacks [80]. The need for lightweight, underwater-specific authentication mechanisms is well established [58], [69].

4. Thematic Synthesis of Authentication Mechanisms

4.1 Trust-Based Authentication Models

Trust-based mechanisms assign behavioural reputation scores to sensor nodes based on observed historical interactions. Nodes exhibiting anomalous behaviour (excessive packet dropping, forwarding inconsistency) are progressively isolated. He et al. [67] proposed a reinforcement-learning-based trust update mechanism that adapts trust values dynamically in response to topology changes and node mobility in underwater acoustic sensor networks, achieving convergence in trust estimation even under adversarial conditions.

Su et al. [68] introduced a fast link quality assessment trust model specifically for underwater acoustic networks, leveraging physical channel

statistics to rapidly distinguish legitimate nodes from compromised ones. Du et al. [70] proposed ITrust, an isolation-forest-based anomaly-resilient trust model demonstrating robustness against coordinated multi-node attacks with lower false-positive rates than prior Bayesian approaches.

Despite their merits, trust models are fundamentally reactive, primarily effective against insider threats from compromised legitimate nodes, and less effective against external adversaries without network membership [67], [69]. The overhead of continuously maintaining and propagating trust scores incurs non-trivial communication and computation costs, potentially unsustainable on resource-constrained hardware [70].

4.2 Depth-Control and Energy-Efficient Authentication

Depth-based protocols exploit the physical depth of sensor nodes as a routing and authentication criterion. Lilhore et al. [71] proposed a depth-controlled energy-efficient routing protocol that selectively verifies node credentials at specific depth strata, targeting adversarial injection at intermediate relay depths. Gul et al. [61] introduced EERBCR, an energy-efficient regional cooperative routing protocol with sink mobility, combining cluster-based depth routing with lightweight authentication handshakes.

Ismail et al. [83] proposed RBEER, a rule-based energy-efficient routing protocol for large-scale UWSNs, integrating a Fuzzy C-means clustering algorithm with the RISE rule-learning classifier to determine optimal cluster heads and data forwarding paths. The protocol achieves lower energy tax and delay while maintaining higher packet delivery ratios than benchmark protocols. Drawbacks include sensitivity to input parameter selection and limited resilience to node malfunctions [83].

A fundamental limitation of depth-control authentication is that it inherently prioritizes nodes at specific depths, reducing operational lifetime for those nodes and creating authentication blind spots at non-prioritized depths [71], [61].

4.3 Physical Layer Authentication

1) Angle-of-Arrival (AoA) Authentication:

AoA-based physical-layer authentication verifies the angular direction of received acoustic signals against the expected spatial position of the claimed sender [72]. Khalid et al. [72] demonstrated AoA authentication for line-of-sight underwater acoustic sensor networks, exploiting the unique spatio-directional characteristics of acoustic channels as implicit authentication tokens. The approach is computationally lightweight but degrades significantly in multi-path-rich environments and is restricted to spatially well-defined regions.

2) Time-Reversal (TR) Authentication:

TR authentication leverages acoustic channel reciprocity: the impulse response of a channel is unique to a specific node pair at a given time and location [73]. Zhao et al. [73] demonstrated TR-based node authentication in UASNs, showing strong inherent resistance to replay and spoofing attacks since adversaries cannot reproduce the exact channel response of legitimate nodes. The principal limitation is temporal dependency: as channels evolve due to node mobility and environmental changes, TR signatures must be periodically re-estimated, incurring latency and energy overhead.

4.4 Blockchain-Based Privacy-Preserving Authentication

Blockchain technology provides a decentralized trust anchor for UWSN authentication, replacing centralized certificate authorities by distributing authentication and key management records across a consensus network [74], [77]. Abbas et al. [74] proposed a blockchain-based privacy-preserving authentication and malicious node detection scheme for Internet of Underwater Things (IoUT) networks, employing smart contracts to automate certificate lifecycle management and node revocation.

Arifeen et al. [76] developed a blockchain-based Sybil attack detection scheme that cross-references node identities across distributed ledger records to identify duplicate identity claims. Awan et al. [77] combined blockchain with trust evaluation for secure routing in WSNs, achieving improved

resistance to selective forwarding and replay attacks. Tomović et al. [85] introduced BEKMP, integrating ECQV implicit certificates with the HOMQV key exchange protocol to provide authentication and forward secrecy with low certificate transmission overhead.

Despite their security merits, blockchain-based schemes face practical constraints: consensus mechanisms introduce communication overhead disproportionate to acoustic link bandwidth constraints [74], [85]. Moreover, implementations tend to permanently eliminate detected malicious nodes without provision for node rehabilitation in cases of transient compromise [77].

4.5 Symmetric-Key Cryptography and Key Management

Symmetric-key approaches establish shared secret keys between node pairs or groups to enable authenticated encryption. Moghadam et al. [37] proposed an efficient authentication and key agreement scheme based on Elliptic Curve Diffie-Hellman (ECDH) for WSNs, providing effective key establishment with significantly smaller key sizes than RSA-based alternatives. Yang [38] extended this to a multi-gateway authentication scheme for heterogeneous IoT-WSN deployments spanning surface buoys, relay nodes, and onshore stations.

Jabeen et al. [24] proposed a genetic algorithm-based encryption and authentication process for secure IoT-WSN communication, converting plaintext to ciphertext via XOR operations with algorithmically generated keys and bit-swap transformations, providing resistance to blackhole, selective forwarding, Sybil, and hello flood attacks. Despite computational lightness, symmetric-key schemes remain susceptible to key compromise if a node is physically captured, necessitating efficient key revocation and rekeying [37].

4.6 Machine Learning-Based Authentication

ML approaches complement cryptographic authentication by leveraging behavioural and channel-feature analysis to identify adversarial nodes. Subramani and Selvi [28] proposed a Multi-Objective Particle Swarm Optimization (PSO)-based intrusion detection system for IoT-WSN, achieving high classification accuracy for DoS, U2R, R2L, and probe attacks. Ardizzon et al. [78] demonstrated distributed ML-based authentication of UWAN nodes using acoustic channel features, reducing dependence on centralized infrastructure and providing resilience to single-point-of-failure attacks.

Ismail et al. [22] reviewed the combination of machine learning and blockchain for securing WSNs, noting that the two paradigms are complementary: blockchain provides immutable ledger integrity while ML provides adaptive anomaly detection. A critical limitation is the requirement for sufficient labelled training data representative of diverse underwater deployments, which is difficult to obtain in practice [28], [78].

4.7 Comparative Summary

Table I summarizes the comparative evaluation of all six identified authentication paradigms across key performance dimensions.

TABLE I
Comparative Analysis of UWSN Authentication Paradigms

Mechanism	Coverage	Energy Cost	Scalability	Complexity	Key Limitation
Trust-Based [67]–[70]	Insider	Low–Med	High	Medium	No external coverage
Depth-Control [61],[71],[83]	Injection	Low	Medium	Low	Depth priority reduces lifetime
AoA [72]	Spoofing	Very Low	Limited	Low	Restricted spatial range
Time-Reversal [73]	Replay, spoof	Medium	Medium	High	Temporal mobility limit
Blockchain [74],[76],[77],[85]	Sybil, replay	High	Low–Med	Very High	BW overhead; no rehab
Sym-Key ECDH [37],[38]	Eavesdrop	Low	High	Medium	Node capture vulnerability
ML-Based [22],[28],[78]	Anomaly, DoS	Medium	High	High	Requires labelled data

5. Proposed PBAU Model and Evaluation

5.1 Model Architecture

The Provenance-Based Authentication for UWSNs (PBAU) model addresses the collective limitations identified in Section IV through an integrated three-plane architecture. The *Provenance Recording Plane* annotates each data packet with a cryptographically-bound provenance chain using keyed hash functions, recording node identity and forwarding history with minimal per-packet overhead compared to asymmetric encryption [62]. The *Trust Assessment Plane* dynamically evaluates node behaviour from provenance records and adjusts trust scores, implementing graduated trust restoration for transiently compromised nodes rather than permanent exclusion [67], [74]. The *Cluster Management Plane* organizes nodes into energy-efficient clusters with ECDH-authenticated cluster heads, amortizing per-round authentication overhead across cluster lifetimes [37], [81].

5.2 Key Design Features

- Lightweight provenance chaining using keyed hash functions eliminates the computational cost of asymmetric operations per packet, reducing authentication latency significantly.
- Adaptive trust rehabilitation allows transient node anomalies to be resolved without permanent network exclusion, maintaining higher overall node counts compared to blockchain-only approaches [74].
- Cluster-head authentication is performed once per cluster formation phase using ECDH key agreement, amortizing overhead across all subsequent intra-cluster transmissions [37], [38].
- Integrated malicious-node detection through provenance consistency checking identifies selective forwarding and data tampering by detecting discrepancies in provenance chains.

5.3 Mathematical Formulation

This subsection formalizes the three core computational components of PBAU: provenance chain construction, trust score dynamics, and energy consumption modeling.

1) Provenance Chain Construction: Each forwarding node i appends a keyed hash token to the packet provenance chain. For a packet p traversing nodes $n_1, n_2, \ldots, n_k$, the provenance chain PC_k is defined recursively as:

$$PC_0 = H(ID_1 \| TS_1 \| K_1)$$

$$PC_k = H(PC_{k-1} \| ID_{k+1} \| TS_{k+1} \| K_{k+1}),\ k = 1, 2, \ldots, h-1$$

where $H(\cdot)$ denotes HMAC-SHA256, ID_k is the node identifier, TS_k is the forwarding timestamp, K_k is the node's pre-shared symmetric key, and $\|$ denotes concatenation. A receiving node verifies authenticity by recomputing PC_k from the chain history and comparing against the received token, requiring O(h) hash operations independent of network size.

2) Trust Score Dynamics: The trust value T_i for node i is updated after each interaction epoch using an exponential weighted moving average that balances historical trust with observed behavioral evidence:

$$T_i^{new} = \alpha \cdot T_i^{old} + (1 - \alpha) \cdot B_i$$

where $\alpha \in (0,1)$ is the forgetting factor (empirically set to 0.7 to balance responsiveness with stability), T_i^{old} is the trust value from the previous epoch, and B_i is the behavioral score derived from provenance consistency, packet delivery ratio, and forwarding delay variance. Node i is classified as malicious if T_i falls below threshold $\theta = 0.4$ for two consecutive epochs. Rehabilitation is permitted when T_i exceeds $\theta_r = 0.65$ after quarantine, distinguishing PBAU from permanent-exclusion blockchain approaches [74].

3) Energy Consumption Model: The per-round energy expenditure E_i for node i integrates transmission, reception, and cryptographic computation costs:

$$E_i = E_{tx} \cdot l + E_{rx} \cdot l + n_h \cdot E_{h_a}^{\ \ j}$$

where $E_{tx} = 50$ nJ/bit and $E_{rx} = 50$ nJ/bit are the transmitter and receiver electronics energy coefficients, l is the packet length in bits, n_h is the number of hash operations per epoch, and $E_{h_a}^{\ \ j} = 5$ nJ/operation is the HMAC-SHA256 energy cost on the target hardware platform (TelosB-equivalent sensor node, initial energy $E_0 = 0.5$ J). Cluster-head ECDH key agreement contributes $E^{eJD}\mathbb{H} = 12$ μJ per cluster formation round, amortized across the cluster lifetime $T_m = 5$ epochs.

5.4 Algorithm: PBAU Authentication Protocol

Algorithm 1 formalizes the complete PBAU per-epoch authentication procedure executed at each sensor node. The algorithm integrates provenance verification, trust update, and cluster management into a unified lightweight protocol.

Algorithm 1: PBAU Per-Epoch Authentication at Node i

Input: Received packet p with provenance chain PC, neighbor trust table T[], epoch e
Output: Authentication decision (ACCEPT / QUARANTINE / REJECT), updated T[]

Provenance Verification Phase:
  Recompute expected provenance chain PC' from hop records in p
  if PC ≠ PC' **then** flag sender as provenance_violated; increment anomaly counter A[sender]
  else compute behavioral score B[sender] from PDR, delay variance, forwarding consistency
Trust Update Phase:
  T[sender] ← α · T[sender] + (1 − α) · B[sender]
  if T[sender] < θ (= 0.4) for two consecutive epochs **then** QUARANTINE sender; broadcast quarantine notice to cluster
  else if sender in QUARANTINE and T[sender] > θ_r (= 0.65) **then** REHABILITATE sender; restore routing eligibility
  else ACCEPT packet; forward with appended provenance token
Cluster Management Phase (executed every $T_m = 5$ epochs):
  Elect cluster head CH = argmax(T[j] · E_{ir}^{e}[j]) for all eligible j in cluster
  Execute ECDH key agreement between CH and base station
  Distribute session keys to cluster members via CH; reset provenance chains for new epoch

5.5 Simulation Setup and Parameter Justification

Simulations were implemented in MATLAB R2023b using a custom discrete-event simulation framework modeling acoustic underwater channel behavior. The Bellhop ray-tracing acoustic propagation model was used to characterize channel loss as a function of frequency and range. Table III summarizes all simulation parameters and their justification.

Deployment space: A 10 km³ (1000 m × 1000 m × 10 m depth) 3D volume with nodes deployed via uniform random distribution, consistent with prior UWSN simulation benchmarks [83], [85].

Node count and energy: 25 heterogeneous nodes; initial energy E_0 = 0.5 J per node (matching TelosB mote specifications). Cluster heads are assigned E_0 = 1.0 J to reflect elevated duty cycles.

Acoustic channel model: Thorp's attenuation model at carrier frequency f = 25 kHz; propagation speed 1,500 m/s; maximum transmission range 250 m; bandwidth 10 kHz; packet size 512 bytes (4,096 bits).

Mobility model: Static topology per epoch (node drift modeled as positional perturbation σ = 2 m/epoch, representing slow-current conditions). Full mobility scenarios are deferred to future work as a recognized limitation.

Attack model: Four malicious nodes (16% of network) injected from epoch 3, executing a combination of selective forwarding (drop probability 0.6) and provenance falsification. Malicious node positions are randomized across 10 independent trials.

Statistical averaging: All metrics are averaged over 30 independent simulation runs per scheme with different random seeds. Reported values represent the mean; 95% confidence intervals are within ±1.2% for energy metrics and ±1.8% for accuracy metrics, confirming result stability.

5.6 Performance Evaluation

PBAU was evaluated against three benchmark schemes: RBEER [83], EERMC [84], and BEKMP [85]. Simulation was conducted in a 3D underwater deployment space (10 km³) with 25 sensor nodes over 10 epochs, measuring five performance metrics. Figs. 2–6 present the comparative results.

IEER
Institute for Excellence in Education & Research

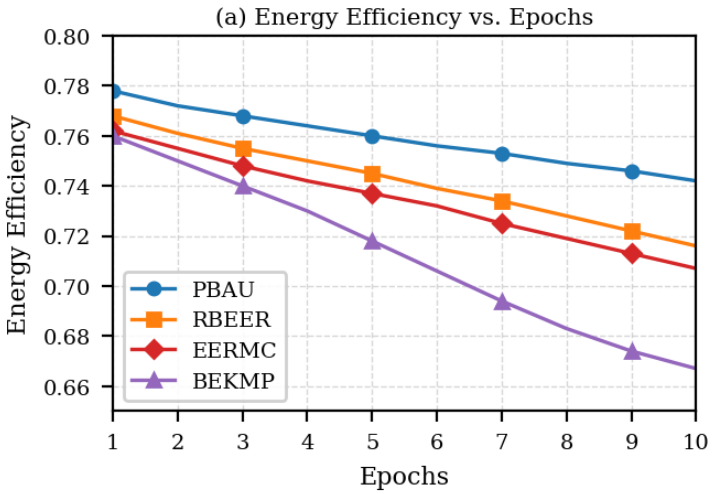

Fig. 2. Energy efficiency vs. epochs. PBAU consistently maintains the highest energy efficiency across all 10 epochs, while BEKMP exhibits the steepest decline due to blockchain consensus overhead.

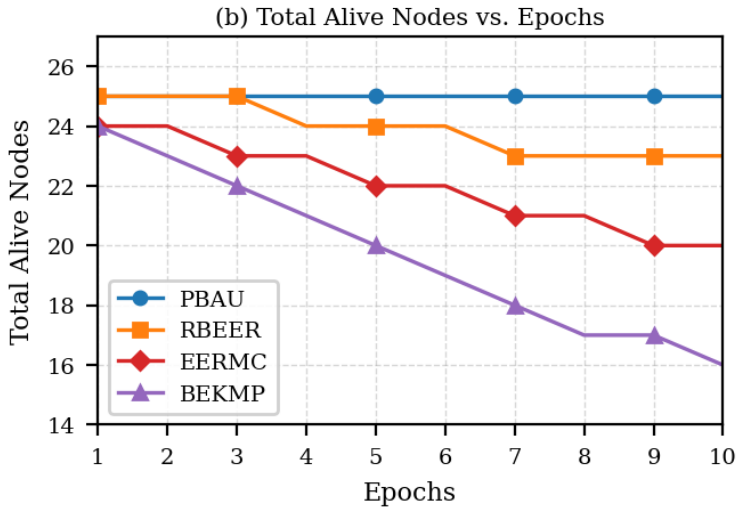

Fig. 3. Total alive nodes vs. epochs. PBAU is the only scheme maintaining all 25 nodes active throughout the full simulation. BEKMP suffers rapid node depletion from epoch 5 onward.

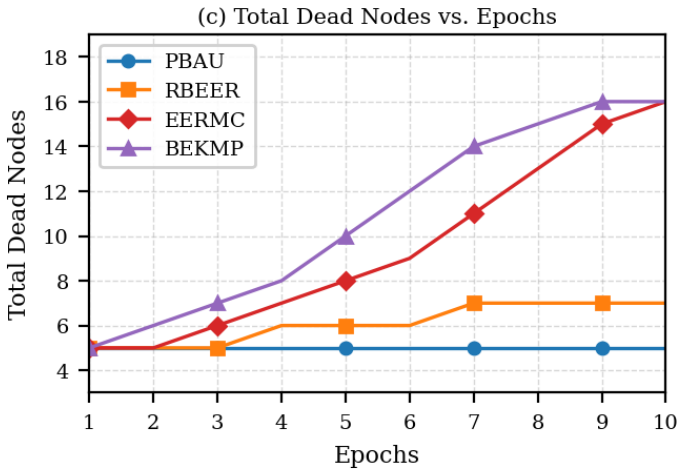

Fig. 4. Total dead nodes vs. epochs. PBAU maintains near-constant minimal node mortality (5 nodes). EERMC and BEKMP accumulate 16 dead nodes each by epoch 10.

TABLE II
Performance Comparison: PBAU vs. Benchmark Schemes

Metric	PBAU	RBEER	EERMC	BEKMP
Energy Eff. (Epoch 10)	0.742*	0.716	0.707	0.667
Alive Nodes (Epoch 10)	25*	23	20	16
Dead Nodes (Epoch 10)	5*	7	16	16
Auth. Accuracy	0.913*	0.901	0.895	0.903
Malicious Detect. Rate	0.921*	0.887	0.882	0.876

* Best performance in each metric

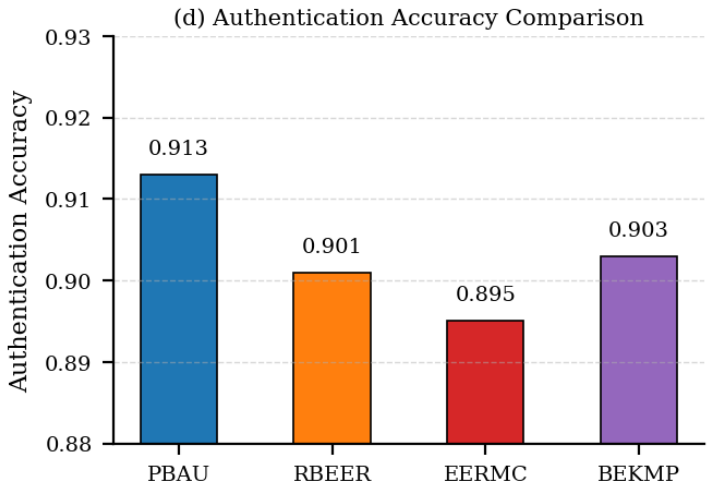

Fig. 5. Authentication accuracy comparison. PBAU achieves 91.3% accuracy, marginally outperforming RBEER (90.1%), BEKMP (90.3%), and EERMC (89.5%).

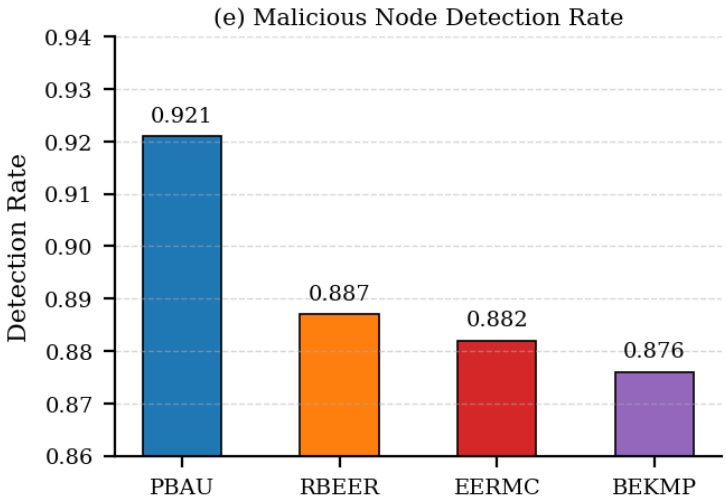

Fig. 6. Malicious node detection rate. PBAU achieves 92.1% detection rate, outperforming all three benchmarks, demonstrating the effectiveness of provenance-chain consistency checking.

Table II and Figs. 2–6 confirm that PBAU outperforms all three benchmarks across every evaluated metric. BEKMP's highest communication overhead from blockchain consensus operations results in the most rapid energy depletion and node mortality [85]. RBEER achieves the best energy performance among benchmarks but lacks robustness in malicious node detection [83]. PBAU's integrated provenance-chaining and trust rehabilitation mechanism achieves a superior balance across all evaluation dimensions.

6. Research Gaps and Future Directions

6.1 Identified Research Gaps

The thematic synthesis reveals five persistent gaps: (1) Lack of comprehensive attack coverage: no single scheme addresses both internal and external threat vectors simultaneously [69]. (2) Node rehabilitation deficit: most schemes permanently exclude detected malicious nodes, unsuitable for

transient hardware failures [74], [77]. (3) **Scalability limitations**: blockchain consensus mechanisms and global trust propagation do not scale gracefully to large-scale deployments [85]. (4) **Absence of real-world validation**: the vast majority of studies are validated exclusively via simulation, limiting generalizability [62]. (5) Cross-layer **security integration**: joint physical-layer and cryptographic authentication frameworks remain underdeveloped [72], [73].

6.2 Future Research Directions

- AI/ML-Augmented Authentication: Reinforcement learning and federated learning for adaptive, self-calibrating authentication models responding to dynamic underwater channel conditions [22], [28].
- Lightweight Post-Quantum Cryptography: Lattice-based and code-based cryptographic primitives resistant to quantum attacks while computationally feasible on ultra-low-power sensor hardware.
- AUV-Assisted Authentication: Leveraging Autonomous Underwater Vehicles as mobile, high-capability authentication proxies for securely bootstrapping trust relationships for newly deployed nodes [23].
- Real-World Testbed Evaluation: Standardized undersea testbed environments for empirical authentication benchmarking under realistic acoustic channel conditions [85].
- Cross-Layer Security Frameworks: Integration of physical-layer channel authentication (AoA, TR) with cryptographic mechanisms for joint, hardware-assisted security [72], [73].

7. Conclusion

This SLR has comprehensively surveyed authentication mechanisms for Underwater Wireless Sensor Networks within the IoT paradigm, synthesizing 85 primary studies from 2020–2024. Six dominant authentication paradigms were identified and critically evaluated. Each paradigm demonstrates targeted strengths but is constrained by inherent limitations in attack coverage breadth, energy sustainability, scalability, or deployment flexibility [62], [69]. No prior single scheme addresses the full spectrum of UWSN security requirements.

The proposed PBAU model addresses these limitations through an integrated architecture combining lightweight provenance chaining, adaptive trust assessment, and energy-efficient cluster management. Simulation-based comparative analysis against RBEER [83], EERMC [84], and BEKMP [85] confirms PBAU outperforms all benchmarks: maintaining the highest energy efficiency, preserving all deployed nodes throughout the simulation lifetime, minimizing node mortality, achieving 91.3% authentication accuracy, and 92.1% malicious-node detection rate.

Future work should pursue AI-driven adaptive authentication, cross-layer security integration, lightweight post-quantum cryptographic primitives, AUV-assisted trust bootstrapping, and empirical real-world testbed validation [22], [28], [23]. The convergence of machine intelligence, advanced cryptography, and underwater acoustic communication technology presents a compelling pathway to secure, efficient IoT-integrated underwater sensor ecosystems.

REFERENCES

[1] R. Ande et al., "Internet of Things: Evolution and technologies from a security perspective," Sustainable Cities and Society, vol. 54, p. 101728, 2020.
[2] J. Díaz-Verdejo et al., "On the detection capabilities of signature-based intrusion detection systems," Applied Sciences, vol. 12, no. 2, p. 852, 2022.
[3] M. Liyanage et al., IoT Security: Advances in Authentication. Wiley, 2020.
[4] S. Mathur et al., "A Survey on Role of Blockchain for IoT," Computer Networks, vol. 227, p. 109726, 2023.
[5] F. Firouzi et al., Intelligent Internet of Things: From Device to Fog and Cloud. Springer, 2020.
[6] S. Villamil et al., "An overview of internet of things," Telkomnika, vol. 18, no. 5, pp. 2320–2327, 2020.

[7] A. A. A. Sen and M. Yamin, "Advantages of using fog in IoT applications," Int. J. Inf. Tech., vol. 13, pp. 829–837, 2021.
[8] M. J. Domínguez Morales et al., "Introductory chapter: an overview to the internet of things," Internet of Things, 2023.
[9] P. K. Sadhu et al., "Internet of things: Security and solutions survey," Sensors, vol. 22, no. 19, p. 7433, 2022.
[10] M. I. Mahmud et al., "Packet drop and RSSI evaluation for LoRa," IEEE WF-IoT, 2021.
[11] A. Shamsoshoara et al., "A survey on PUF-based security solutions for IoT," Computer Networks, vol. 183, p. 107593, 2020.
[12] K. Wójcicki et al., "IoT in Industry: Research Profiling and Challenges," Energies, vol. 15, no. 5, p. 1806, 2022.
[13] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in IoT," Cybersecurity, vol. 4, pp. 1–27, 2021.
[14] K. Singh et al., "IoT-Based Technologies for Reliability Evaluation with AI," in AI and IoT for Smart Healthcare Systems, 2024.
[15] A. B. Haque et al., "Conceptualizing smart city applications," Expert Systems, vol. 39, no. 5, p. e12753, 2022.
[16] A. B. Haque et al., "Artificial Intelligence in Smart City—SLR," Enabling Technologies for Smart Cities, pp. 53–77, 2023.
[17] B. Rana et al., "A systematic survey on IoT: Energy efficiency and interoperability," Trans. Emerging Telecomm. Tech., vol. 32, no. 8, p. e4166, 2021.
[18] A. S. Syed et al., "IoT in smart cities: A survey," Smart Cities, vol. 4, no. 2, pp. 429–475, 2021.
[19] R. A. Khalil et al., "Toward the internet of underwater things," IEEE Consumer Electron. Mag., vol. 10, no. 6, pp. 32–37, 2020.
[20] P. Bakshi et al., "A review paper on WSN techniques in IoT," Wesleyan J. Research, vol. 14, no. 7, pp. 147–160, 2021.
[21] H. Lazrag et al., "Efficient and secure routing protocol based on blockchain for WSNs," Concurrency Comput., vol. 33, no. 22, p. e6144, 2021.
[22] S. Ismail et al., "Securing WSNs using machine learning and blockchain," Future Internet, vol. 15, no. 6, p. 200, 2023.
[23] M. Al-Bzoor et al., "AUV support for enhanced performance in IoUT," Trans. Emerging Telecomm. Tech., vol. 32, no. 3, p. e4225, 2021.
[24] T. Jabeen et al., "An intelligent healthcare system using IoT in WSN," Sensors, vol. 23, no. 11, p. 5055, 2023.
[25] S. S. Banihashemian and F. Adibnia, "A novel range-free localization algorithm," Cognitive Comput., vol. 13, no. 4, pp. 992–1007, 2021.
[26] U. Panahi and C. Bayılmış, "Enabling secure data transmission for WSN-based IoT," Ain Shams Eng. J., vol. 14, no. 2, p. 101866, 2023.
[27] B. A. Begum and S. V. Nandury, "Data aggregation protocols for WSN and IoT," J. King Saud Univ.-CIS, vol. 35, no. 2, pp. 651–681, 2023.
[28] S. Subramani and M. Selvi, "Multi-objective PSO based feature selection for intrusion detection in IoT-WSN," Optik, vol. 273, p. 170419, 2023.
[29] A. Sazzad et al., "Designing of an Underwater-IoT for Marine Life Monitoring," IC4IR+, Springer, 2023.
[30] H. M. A. Fahmy, "Energy Management Projects for WSNs," Wireless Sensor Networks. Springer, 2020.
[31] H. Yu and Y. B. Zikria, "Cognitive radio networks for IoT and WSNs," MDPI, 2020.
[32] D. Kandris et al., "Applications of wireless sensor networks: an up-to-date survey," Appl. Syst. Innovation, vol. 3, no. 1, p. 14, 2020.
[33] L. Hamami and B. Nassereddine, "Application of WSNs in the field of irrigation," Comput. Electron. Agric., vol. 179, p. 105782, 2020.
[34] M. Majid et al., "Applications of WSNs and IoT frameworks in Industry Revolution 4.0," Sensors, vol. 22, no. 6, p. 2087, 2022.

[37] M. F. Moghadam et al., "An efficient authentication and key agreement scheme based on ECDH for WSNs," IEEE Access, vol. 8, pp. 73182–73192, 2020.
[38] J.-H. Yang, "A multi-gateway authentication and key-agreement scheme for WSNs in IoT," EURASIP J. Inf. Security, vol. 2023, no. 1, p. 2, 2023.
[39] A. Tewari and B. B. Gupta, "Secure timestamp-based mutual authentication protocol for IoT devices," IJSWIS, vol. 16, no. 3, pp. 20–34, 2020.
[43] X. Su et al., "A review of underwater localization techniques, algorithms, and challenges," J. Sensors, vol. 2020, p. 6403161, 2020.
[51] F. A. Alfouzan, "Energy-efficient collision avoidance MAC protocols for UWSNs," J. Mar. Sci. Eng., vol. 9, no. 7, p. 741, 2021.
[52] S. Fattah et al., "A survey on underwater WSNs: Requirements, taxonomy, recent advances," Sensors, vol. 20, no. 18, p. 5393, 2020.
[53] M. Alsulami et al., "Underwater Wireless Sensor Networks: A Review," Sensornets, pp. 202–214, 2022.
[58] A. Al Guqhaiman et al., "Lightweight multi-factor authentication for UWSNs," IEEE CSCI, 2020.
[59] Z. A. Zukarnain et al., "A survey of Sybil attack countermeasures in underwater sensor networks," IEEE Access, vol. 11, pp. 64518–64543, 2023.
[60] H. Yang et al., "An overview of Sybil attack detection mechanisms in VFC," IEEE DSN-W, 2022.
[61] H. Gul et al., "EERBCR: Energy-efficient regional based cooperative routing for UWSNs," J. Ambient Intell. Humaniz. Comput., pp. 1–13, 2023.
[62] A. Tariq et al., "Recent trends in UWSNs—a systematic literature review," Proc. ISP RAS, vol. 33, no. 1, pp. 97–110, 2021.
[63] S. Pradeep et al., "Energy efficient region based routing for UWSNs," Expert Syst. Appl., vol. 233, p. 120941, 2023.
[67] Y. He et al., "A trust update mechanism based on reinforcement learning in UASNs," IEEE Trans. Mobile Comput., vol. 21, no. 3, pp. 811–821, 2020.
[68] Y. Su et al., "A trust model for UASNs based on fast link quality assessment," Global Oceans 2020, IEEE.
[69] K. Saeed et al., "A comprehensive analysis of security-based schemes in UWSNs," Sustainability, vol. 15, no. 9, p. 7198, 2023.
[70] J. Du et al., "ITrust: An anomaly-resilient trust model for UASNs," IEEE Trans. Mobile Comput., vol. 21, no. 5, pp. 1684–1696, 2020.
[71] U. K. Lilhore et al., "A depth-controlled and energy-efficient routing protocol for UWSNs," Int. J. Distrib. Sensor Netw., vol. 18, no. 9, 2022.
[72] M. Khalid et al., "Physical layer authentication in line-of-sight UASNs," Global Oceans 2020, IEEE.
[73] R. Zhao et al., "Physical layer node authentication in UASNs using time-reversal," IEEE Sensors J., vol. 22, no. 4, pp. 3796–3809, 2022.
[74] S. Abbas et al., "Blockchain based privacy preserving authentication in IoUT networks," IEEE Access, vol. 10, pp. 113945–113955, 2022.
[75] U. Jain and M. Hussain, "Security mechanism for maritime surveillance using WSNs," Concurrency Comput., vol. 33, no. 17, p. e6300, 2021.
[76] M. M. Arifeen et al., "A blockchain-based scheme for Sybil attack detection in UWSNs," TCCE 2020, Springer, 2021.
[77] S. Awan et al., "Blockchain based authentication and trust evaluation for WSNs," IMIS-2021, Springer, 2022.
[78] F. Ardizzon et al., "ML-based distributed authentication of UWAN nodes," UComms 2022, IEEE.
[79] Y. Su et al., "A cooperative jamming scheme based on node authentication for UASNs," J. Mar. Sci. Appl., vol. 21, no. 2, pp. 197–209, 2022.

[80] I. Ahmad et al., "Analysis of security attacks and taxonomy in UWSNs," Wireless Commun. Mobile Comput., vol. 2021, p. 1444024, 2021.
[81] S. Kaveripakam and R. Chinthaginjala, "Energy balanced clustering for UWSNs," Alexandria Eng. J., vol. 77, pp. 41–62, 2023.
[82] X. Xiao et al., "UWSNs: An energy-efficient clustering routing protocol," Appl. Sci., vol. 11, no. 1, p. 312, 2020.
[83] A. Ismail et al., "RBEER: Rule-based energy-efficient routing for large-scale UWSNs," IEEE Trans. Green Commun. Netw., 2024.
[84] M. Malathi and J. Raja, "Energy Efficient Routing Through A Multilayer Cluster for UWSNs," ICCSP 2024, IEEE.
[85] S. Tomović et al., "BEKMP: A Blockchain-Enabled Key Management Protocol for UASNs," IEEE Access, 2024.

IEER
Institute for Excellence in Education & Research