Received: 2024-11-13
Accepted: 2025-01-02
Published Online: 2025-01-30
DOI: 10.70454/JRICST.2025.20109

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

Internet of Underwater things (IoUT): A Systematic Review Research

Pawan Kumar[1*], **Shashank Jha**[2], **Prashant**[3], **Ritik Kumar Singh**[4]

[1,2,3,4] Assistant Professor, COER University, Roorkee, Uttarakhand, India

***Corresponding Author Email**: Pawan0871@gmail.com

Abstract

The development of intelligent systems for the monitoring, exploration, and administration of underwater environments is made possible by the Internet of Underwater Things (IoUT), which is a revolutionary development in marine and environmental research.This thorough research examines the advancements, challenges, and promise of IoUT with a focus on its applications in domains such as resource extraction, the science of oceanography underwater tracking, and tracking the environment. IoUT systems require customised approaches in processing information, conservation of energy, connectivity, and sensor that is being tested design because to the particular difficulties of underwater settings. The new protocols and methods designed for underwater applications—such as acoustic, optical, and electromagnetic communications—as well as the incorporation of artificial intelligence (AI) and machine learning (ML) technologies for improved data processing and taking decisions are covered in this study.Furthermore, we draw attention to the urgent issues surrounding data security, environmentally friendly interaction, and installation expenses while providing suggestions for future lines of inquiry and technical advancements.

Keywords: IoT, Sensors, Underwater, Security, Water Sensing, IoUT.

1. INTRODUCTION

The ocean is covered by water on around 71% of its surface. A global network of intelligent, linked underwater objects known as the "Internet of Underwater Things" (IoUT) enables the monitoring of extraordinarily sizable, unknown ocean areas[1].The Internet of Underwater Things (IoUT) is a network of smart devices used underwater, such as sensor nodes, with specific communication and networking protocols. This framework combines different marine communication technologies, including acoustics waves, radio waves, optical waves, and magnetic induction [2]. In recent times, smart cities have been gaining popularity, and one of the essential technologies for this is the Internet of Things (IoT), which refers to the infrastructure of the information society. The concept of IoT was introduced back in 1985, and in 2012, the concept of Internet of Underwater Things

(IoUT) was introduced. IoUT involves connecting and controlling smart underwater objects, like sensors, Autonomous Underwater Vehicles (AUVs), buoys, and ships. IoUT represents a new category of IoT and plays a significant role in the evolution of smart cities [3]. The study investigates the potential of IoUT for monitoring our planet's large and uncharted water bodies. It provides a thorough architectural framework for IoUT and highlights the key distinctions between it and IoT. The report also discusses the main obstacles associated with those applications and showcases a variety of IoUT uses. A network of networked sensors and smart devices submerged to monitor and gather data from water bodies is known as the Internet of Underwater Things (IoUT). Marine monitoring, coastal area surveillance, marine life exploration, oil rig maintenance, and defence are only a few of its uses [4].

Energy-related issues at the networking and physical layer are a significant element influencing the Quality of Service (QoS) in underwater communication networks for IoUT. The routing protocol and network layout have a big impact on how much power IoUT nodes and cars use. In both deep and shallow waterways, acoustic waves are frequently employed for long-distance communications; however, in longer communication scenarios, they may be impacted by propagation delays [5]. The Multi-Router Traffic Graph (MRTG) is a commonly used tool for managing network traffic information. To manage large area networks effectively, a Network Management System (WSNMS) is suggested. Using radio channels, the sinks transmit the gathered data to a distant base station or monitoring centre on the coast. In UWSN systems, autonomous underwater vehicles (AUVs) can also be used for data collection and transmission. Numerous IoUT services are supported by UWSNs, including ecological monitoring, seismic monitoring, offshore gas and oil asset monitoring, disaster prevention, water quality monitoring, and marine animal tracking [6].

Two data collecting strategies are proposed to overcome IoUT challenges: the deployment of adaptable AUVs for data collection and the self-organization of IoUT nodes using a multi-hop transfer methodology. Tests of the suggested approach were conducted in a realistic system that included a computer, an intermediary device (gateway), and actual underwater equipment. ICMP (Internet Control Message Protocol) packets were used to monitor the system via the Internet. Although IoUT has several potential uses, issues with dependability, battery usage, and data collection in submerged conditions remain.

2. RELATED WORK

An overview of the Underwater Internet of Things (UIoT) is provided by the most recent paper by Qiu et al., which highlights challenges, unresolved research issues, applications, current developments, and future system architecture [19]. IoUTfocusses on combining powerful and modern technologies to reach the smart ocean, even if it is comparable to IoUT (Internet of Underwater Things) [19]. IoT protocols, hardware, networking, security issues, and solutions are all covered in another recent survey on IoT security by Mrabet et al. [20]. However, the unique challenges of IoUT are not covered in this work.

As far as we are aware, there doesn't seem to be a Systematic Literature Review (SLR) on the security issues that UWSNs face. Nonetheless, a number of survey and other research studies have been released that throw light on several UWSN security topics, which we will touch on in passing in this section. The latest survey on underwater wireless sensor network security issues is provided by Yang et al[13]The authors categorise the attacks and explain the challenges, restrictions, and attacks against UWSNs. The paper offers a current perspective on the field and can serve as a starting point for scholars who wish to comprehend the security issues and requirements of UWSN technology. Although it gives a general overview of security issues, it does not fully explain the dangers and solutions that we outline in this work. The authors of Reference [21] talk about possible attacks, secure localisation and routing techniques, and the security challenges of UWSNs.They highlight open research concerns as well as particular methods and security measures. They claimed that network performance needs to be assessed in real-world scenarios and that many research projects only provide simulated results utilizing localisation and routing algorithms. They don't address the entire spectrum of problems, attacks, and security solutions; they only focus on localization and routing. In 2017, Dargahi et al. introduced a distributed method for identifying and thwarting routing attacks on UWSNs. It offers background information on the unique problems of UWSNs and routing assaults, as well as local monitoring methods, while not being a survey article. Only routing attacks are the subject of Reference 22 [22].A survey of the current UWSN Medium Access Control (MAC) mechanisms was carried out by Yunus et al. [23]. They highlighted a few of the challenges that affect the design of underwater protocols, including propagation delay, noise, multipath, and transmission loss. However, UWSN attacks and defences are not covered.

Every study mentioned above provides information about security issues, dangers, and possible methods for detection, prevention, and mitigation. Nonetheless, some of them are very new, while others concentrate on a particular topic, like access control, localisation, or routing. As a developing technology, new methods and protocols are being created to enhance IoUT and UWSN security features. In order to support future research, it is imperative that a current review of recent research articles pertaining to the security of UWSNs be provided.

3. IoUT ARCHITECTURE

Communication and sensor components make up the Internet of Things. These entities are commonly referred to as sinks and nodes:

A. Endpoint nodes include things like radio or acoustic tags, cameras, hydrophones, sensors, and actuators.

B. Mid-layer nodes include things like relays, repeaters, gateways, and modems.

C. Satellites, land-based base stations, ships, and buoys all have sink nodes. Implementing a flexible, layered system is essential because IoUT systems are typically made up of several different components. Each layer has different characteristics in terms of operation and scalability.

D. In the architecture of the IoUT system, the perception layer is the lowest layer. It is made up of gadgets such as GPS sensors, surface links, monitoring stations, Unmanned Aerial Vehicles (UAVs), and energy harvesting components. The main purposes of sensors and actuators are data collection and actuation initiation. Retrieving water parameters, keeping an eye on water quality, and gathering data about aquatic life or objects are the main tasks of this layer.Network layerreceives and processes data from the perception layer. It is built on wired and wireless connections, remotely controlled stations, a cloud platform, and the internet. It handles bidirectional data packets using internet protocols and data routing.

E. The application layer is responsible for data analysis through the use of front-end services with graphical user interfaces. Identifying sensors- including their position, ID, amount, and typeis its main objective. Sensing, tracking, storing, and transferring data are all part of data collection [18].

The Internet of Underwater Things (IoUT) ecosystem will require greater networking and communication amongst its increasingly intelligent components. However, it can be difficult to establish and sustain communication linkages in the underwater environment because of the low network density. For the IoUT, a strong communication infrastructure is therefore essential.Typically, an Underwater Device (UT) is made up of embedded systems with sensing and communication components.To survive harsh environments, these gadgets might be buried underground and shielded by waterproof and weatherproof enclosures. They use a variety of sensors, including as temperature and soil moisture sensors, to collect environmental data locally. IoUT uses a variety of communication techniques, including- satellite, cellular, subsurface, Bluetooth, ZigBee, NFC, Wi-Fi, Sigfox, LoRa, and LoRaWAN.

Communication ranges can range from 100 meters to considerably greater distances, depending on the technology being used. Sinks (found on buoys, ships, etc.), nodes (devices like sensors, cameras, etc.), and mid-layer devices (modems, repeaters, etc.) are some of the components that make up IoUT systems. Together, these gadgets convey data and build a multi-layered, adaptable system. In order to address security concerns, researchers have suggested cloud-based IoUT architectures that include AI and ML solutions for quality of service (QoS), safe data transfer, and object detection. In IoUT architectures, data is sensed, transferred, and processed using ML-assisted solutions. The overall goal of the IoUT design is to develop a dependable and effective communication system that will facilitate smooth data flow between underwater sensors and enhance a range of applications in environmental research, marine monitoring, and exploration.Figure 1 illustrates the communicationarchitecture of IoUT design.

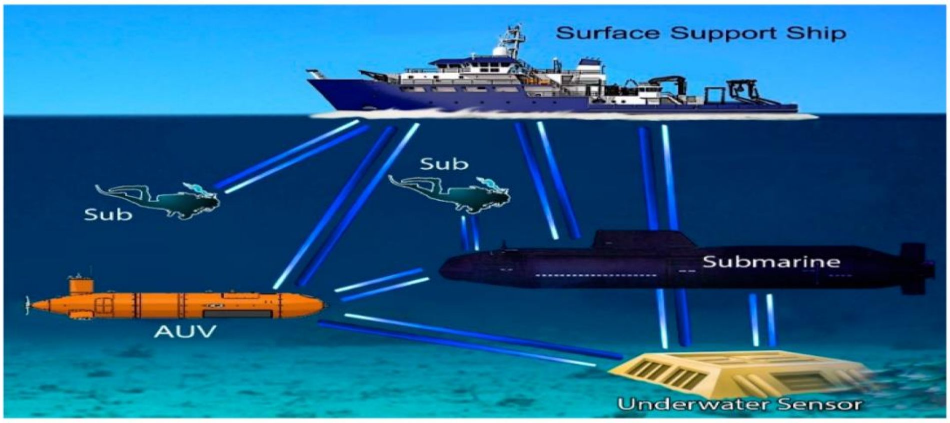


Fig.1 Architecture of Internet of Underwater Things

4. APPLICATIONS OF THE IoUTECOSYSTEM

One of the goals of the Internet of Underwater Things (IoUT) is to monitor, track, explore, and monitor the underwater ecology. A successful communication network is necessary to accomplish these objectives. In this section, we will discuss some applications that can be enhanced by establishing a robust communication network in the Internet of Things (IoT) [11].

Received: 2024-11-13
Accepted: 2025-01-02
Published Online: 2025-01-30
DOI: 10.70454/JRICST.2025.20109

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

A. **Marine Monitoring**: Numerous sensors on IoUT devices allow for continuous monitoring and data collection on environmental conditions, marine life, temperature, salinity, and water quality. This data can be transmitted in real time to monitoring centres or onshore base stations for analysis and decision-making thanks to an effective communication network.

B. **Underwater Tracking**: Underwater vehicles, marine animals, and other objects of interest can all be tracked with IoUT. Researchers and authorities can learn more about the behaviour and migration patterns of marine animals thanks to the communication network's ability to track and update locations in real time.

C. **Underwater Exploration**: By using IoUT devices for underwater exploration, researchers and scientists can find new underwater resources, geological features, and marine environments. Images and video feeds are among the exploration data that can be transmitted via the communication network for analysis and investigation.

D. **Underwater Surveillance:** Applications for underwater surveillance, including the monitoring of sensitive marine zones, undersea pipelines, and offshore oil and gas installations, heavily rely on IoUT. Fast responses to possible threats or abnormalities are made possible by the timely transmission of surveillance data, which is guaranteed by a dependable communication network.

E.**Environmental Research:** In order to perform environmental research in underwater areas, IoUT equipment are essential. The communication network facilitates the sharing of information about weather patterns, ocean currents, and how human activity affects marine ecosystems.

F.**Disaster Prevention:** Early warning systems and disaster prevention depend on an effective IoUT communication network. It makes it possible to transmit data in real time to track seismic activity, identify tsunamis, and forecast natural disasters, assisting coastal communities in better preparing for and responding to them.

G. **Underwater Infrastructure Maintenance**: Bridges, ports, and offshore sites are examples of undersea infrastructure that may be inspected and maintained with IoUT equipment. Timely assessments and repairs are made possible by the communication network's ability to relay video feeds and inspection data.

During these applications, text-based data, sensor readings, photos, videos, and other pertinent data may be sent and received between IoUT devices. Depending on the demands of the particular application, the communication network must be able to handle both real-time and non-real-time data transfer as well as intermittent or continuous connectivity requirements. The potential of IoUT may be fully utilised for environmental preservation, marine research, and other underwater applications with a well-planned and effective communication network.

5. COMMUNICATION TECHNOLOGIES OFIoUT

Seawater's harshness and turbidity can make it difficult for smart underwater items in the Internet of Underwater Things (IoUT) to communicate with one another. At the moment, IoUT communication is enabled via four primary technologies [28]:

A. **Acoustic Waves**: Due to their extended transmission range, acoustic waves are the most widely used communication method for underwater applications. In deep underwater conditions,

Received: 2024-11-13
Accepted: 2025-01-02
Published Online: 2025-01-30
DOI: 10.70454/JRICST.2025.20109

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

underwater acoustic networks can reach data speeds of up to 20 Kbps over distances of up to 1 km. Nevertheless, the data rate drops to 250–550 bps over longer distances, and higher latency is the price paid. Acoustic-based underwater communication systems have synchronization issues due to the significant delay.

B. **RF Waves**: There are two benefits to RF-based underwater communication networks. First, RF waves facilitate cross-border communication between terrestrial and underwater radio frequency networks by offering a seamless transition at interfaces such as air and water. Second, RF waves are able to withstand water turbidity and turbulence. However, at very low frequencies (30 Hz to 300 Hz), the main drawback of RF-based devices is their short transmission range under water. Large antennas are also necessary for underwater RF transmission networks, which raises the cost of design and energy usage.

C. **Optical Waves**: For IoUT, optical communication provides high data speeds and low latency, allowing multimedia applications and real-time underwater telephony. IoUT based on optical waves is an appealing technology due to the low cost and compact size of optical transceivers (photodiodes or laser diodes). However, the restricted underwater range of optical waves and the requirement for precise tracking and pointing between transmitters and receivers make the implementation of optical IoUT more difficult..

D. **Magnetic Induction (MI)**: For omnidirectional, short-range, average-speed underwater communications, magnetic induction is employed. When compared to the other communication methods, the MI channel's response is more consistent and reliable. MI waves can overcome latency problems sometimes brought on by acoustic waves by penetrating the lossy medium in the undersea environment at a speed roughly equivalent to the speed of light. MI communication is appropriate for a range of military and civilian applications since it uses tiny transmitter and receiver coils with non-visible and non-audible waves [29].

Every one of these communication technologies has advantages and disadvantages, and the particular needs and difficulties of the IoUT application determine which technology is best. It is anticipated that additional advancements and inventions will increase underwater communication capabilities in IoUT as technology develops.

6. SECURITY CHALLENGES

The Internet of Underwater Things (IoUT) has complex and unique security challenges due to the unique features of the underwater environment, which call for specialized methods for reliable, safe data processing and transmission. The following are some of the primary security issues with IoUT:

A. Communication Vulnerabilities:

The primary modalities of communication in underwater networks, acoustic and optical, are vulnerable to monitoring and manipulation by hostile actors because of their high latency and stringent frequency restrictions. Because underwater devices might be difficult to access and monitor, they are more susceptible to physical interference or damage from enemies, especially in unprotected or remote maritime locations.

B. Energy Constraints and Secure Protocols:

IoUT devices are mostly battery-powered and operate in a very energy-constrained environment. Rapid battery depletion brought on by the high power requirements involved in installing encryption and security measures may have a detrimental effect on device longevity and network availability. Because typical encryption processes can be excessively resource-intensive for IoUT nodes, it is vital to develop lightweight cryptographic algorithms that provide strong security without using a lot of energy.

C. **Data Integrity and Authenticity**:
Data from underwater devices must be safeguarded in order to preserve its secrecy. If detectors or hubs are compromised, attackers may change data, leading to potentially dangerous decisions or erroneous environmental assessments.Verifying the identity of devices connected to the network is crucial to preventing unauthorized access. However, this is challenging to guarantee because underwater equipment have limited energy and processing power.

D. **Network Security and Denial-of-Service (DoS) Attacks**:

Important surveillance and information gathering are made impossible by underwater networks' extreme susceptibility to denial-of-service (DoS) attacks, which can overload the few communication channels and disrupt network functionality.Because of their unique acoustic and optical properties, submarine broadcasts are susceptible to disruption. By obstructing or distorting transmission, illegal jamming techniques might jeopardize sensitive data.

E. **Privacy and Data Confidentiality**:

IoUT systems are commonly used to collect sensitive environmental data, such as resource finding, national security, and the marine environment. Maintaining the confidentiality of such data is challenging yet essential due to the limited encryption and storage capacities.To secure the whole communication chain, from underwater nodes to surface terminals, small yet effective cryptography that can protect data privacy without straining the limited IoUT infrastructure is required.

F. **Secure Deployment and Maintenance**:

When installed in harsh underwater environments, IoUT terminals are vulnerable to manipulation, environmental damage, and unauthorized physical access.Because submerged nodes are difficult to access, software upgrades are challenging. This limitation could make IoUT connections susceptible since nodes might not be updated to fend against new security attacks.

G. **Resilience Against Environmental Factors**:

In an underwater environment, a variety of uncontrollable factors, such as biological interference, temperature fluctuations, and pressure, might affect sensor performance and secure data transfer. In an uncertain environment, it is difficult to ensure safe and dependable information transmission; redundancy and trust models are required to validate the authenticity and dependability of the collected data. information transfer.

7. IoUT SECURITY OBJECTIVES

It falls into two categories: auxiliary security goals and fundamental security goals. All IoUT applications are expected to meet the three primary IoUT security goals of availability, confidentiality, and integrity. On the other hand, the IoUT's secondary security goals include safe localization, auditability, quality of service, privacy, synchronization, authenticity, and accountability. The different IoUT security goals are described here [30–32].

A. **Integrity:** To ensure the precision and reliability of undersea data, data integrity is essential in IoUT networks. Data integrity refers to the techniques used to ascertain whether the received data has been altered while transmission via an undersea channel. For example, the accuracy of received subsea data can be verified using a Message Integrity Check (MIC). Furthermore, an auto-integrity-checking technique can be applied in the context of IoUT to verify the accuracy of device software and log data.

B. **Availability:** In order to provide high-quality services such defending IoUT devices from hostile attacks, safeguarding harbor environments, protecting various life at risk, etc., data accessibility is crucial in IoUT networks. Self-healing, auto-recovery, and centralized data sharing characteristics are necessary to ensure availability in IoUT networks [30].

C. **Privacy:** In IoUT networks, privacy refers to the information or services that a certain user or device is able to access. Directly transferring existing privacy approaches to IoUT networks is difficult. Therefore, a robust privacy method needs to be transferred to IoUT in order to protect the data from hackers. The following categories comprise the several privacy techniques for IoUT.

D. **IoUT data privacy:** To protect secret messages from attackers, including enemy submarine attacks and secret message passing, data privacy is necessary in IoUT networks for naval applications.

E. **IoUT device privacy:**In IoUT networks, a device identity is usually used to track and send data to IoUT devices. The attackers can easily access the data because this identity can be followed. In this case, a robust identity protection approach is necessary to safeguard the device identifier from hostile nodes.

F. **IoUT location privacy**: Location information is necessary to track the mobility of IoUT devices in networks. The open location information is necessary for data flow between the nodes in the underwater environment. Furthermore, it is challenging to hide the positions of nodes when it is required. As a result, IoUT devices need to adopt a privacy-based location sharing technique.

G. **Authenticity:** In IoUT networks, authentication is the process of confirming the transmitter and recipient nodes. It is challenging to adapt the terrestrial authentication method to the IoUT environment. This makes it simpler for the attacker to cut the channel. For IoUT networks, a lightweight authentication method is therefore necessary.

H. **Auditability**: Analyzing the security activities and execution of security duties is necessary to provide high-quality services in IoUT networks. Therefore, it is possible to investigate an auto-auditing or self-auditing method for assessing security systems in the context of IoUT.

I. **Confidentiality:** An essential element of IoUT networks for safeguarding underwater data is confidentiality. A key sharing system is a suitable technique for protecting the data while it is being transmitted. To provide confidentiality in the IoUT environment, data retrieval and storage must also employ an auto-decision-making mechanism.

8. PASSIVE ATTACKS

Without changing the data, the unauthorized attacker tries to access the IoUT channel. Since silent carriers don't convey any signals, they are used in these attacks. A passive attack allows for node tampering, jamming, message distortion, and replaying while the attacker stays anonymous. Additionally, the attacker may be able to predict the idea of IoUT networks by identifying packet flow, monitoring packet exchange nodes, and predicting node position. One kind of passive attack is privacy-based attacks, which are also referred to as passive attacks. Examples of passive attacks are as follows:

Received: 2024-11-13
Accepted: 2025-01-02
Published Online: 2025-01-30
DOI: 10.70454/JRICST.2025.20109

A. **Eavesdropping and Monitoring**: Eavesdropping and monitoring are the most common types of data privacy threats in the context of IoUT. When there is a lot of network traffic, an attacker can get important information by tapping the network settings.
B. **Camouflage and Adversary**: In this scenario, an enemy node is injected into the IoUT network by the invisible attacker. By stealing packets, rerouting packets, and switching nodes, the attacker node can actually monitor and alter data in IoUT networks.
C. **Traffic Analysis:**By using the communication channel's pattern, the attacker infiltrates the IoUT networks in these attacks. The attacker has the ability to listen in on each node's location, routing path, behavior, and other details.

9. ACTIVE ATTACKS

Data on IoT networks can be altered, injected, deleted, or destroyed by unauthorized intruders. Both during and after transmission, the active attack might alter or remove data. There are five categories of active assaults in IoUT: DoS attacks, message distortion attacks, node manipulation, message replay attacks, and masquerade assaults are the first five types of attacks. Each tier of IoUT networks—the physical layer, data connection layer, network layer, transport layer, and application layer—is used to classify active attacks. Denial of service assaults, one of the most deadly active attacks, have the potential to do enormous damage. DoS attacks can be initiated at any IoUT network level. DoS attacks attempt to prevent valid nodes from accessing assets.The attacker tries to stop legitimate nodes from using the network's functions [33].

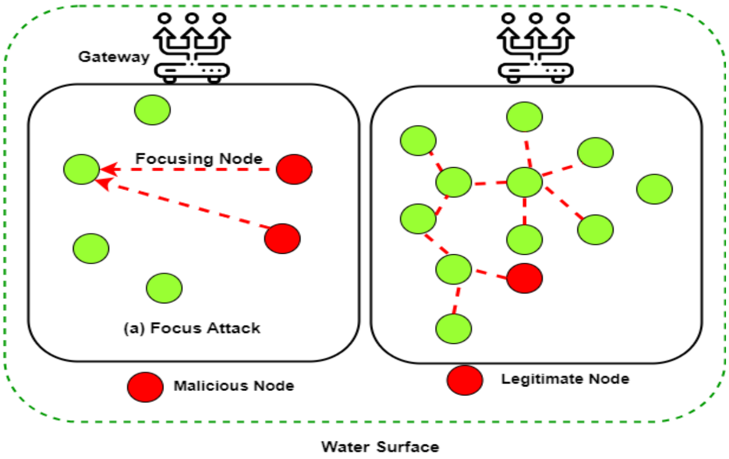


Fig.4. Types of DoS attacks in theIoUT environment.

A. **Node tampering:**IoUT nodes are physically made up of a controller, transmitter, receiver, and battery. Through node manipulation, the attacker can monitor and alter the software code of undersea nodes. The nodes in the IoUT ecosystem may suffer significant harm as a result of the hardware and software components becoming broken. Consequently, it results in data loss and a shorter network lifetime.
B. **Message Distortion:**In these attacks, the attacker has the ability to alter the data that is transmitted between IoUT nodes. For instance, message distortion in the naval application can compromise the security system in emergency IoUT applications. By giving end users inaccurate information, this could cause misunderstanding.

Received: 2024-11-13
Accepted: 2025-01-02
Published Online: 2025-01-30
DOI: 10.70454/JRICST.2025.20109

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

C. **Message Replay:**In these assaults, the attacker either intentionally halts data flow by hacking or poses as the source node and transmits identical data. Another name for a message replay assault is a play-back attack.

D. **Masquerade:**These attacks include the attacker pretending to be a legitimate node in order to obtain data from it. One kind of breach of privacy is a masquerade attack.

E. **Jamming attack:** In order to interfere with legitimate nodes in IoUT networks, the rogue nodes in these attacks frequently send out noise signals. Additionally, this attack can jam IoUT networks by compromising a few key nodes, like the root node, gateway, undersea cluster head, and so on. It essentially stops the gathering and transmission of data. A jamming attack is shown in Figure 7, where a malicious node attacks the root node frequently to stop it from communicating with the member node.

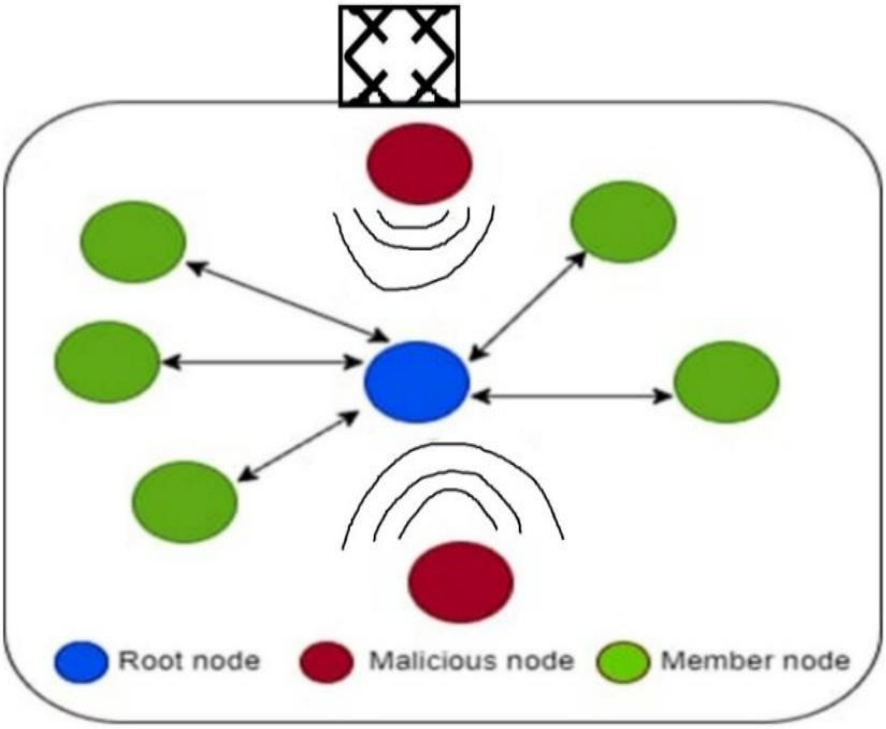


Fig. 5. Jamming attack in theIoUT environment.

F. **Collision attack:** The data-link layer of IoUT networks is where this assault takes place. When two underwater nodes deliver packets simultaneously, a collision happens. The data transmission rules, which stipulate that underwater nodes should not transmit data simultaneously, are followed by the underwater nodes in IoUT networks to prevent collisions. The attacker will break the restrictions and send the packets all at once in a collision attack, though.

G. Exhaustion attack/battery-oriented attack: Depleting the overall energy of underwater nodes in IoUT networks is the aim of this attack. An assault against IoUT networks focused on batteries is shown in Figure 6. In this instance, the rogue node sent node 0 a routing request (RREQ) message. In response, Node 0 sent the malicious node the routing response (RRES) message. Lastly, until node 0 dies, the rogue node will continue to deliver the distorted packets. It essentially reduces the lifespan of the network.

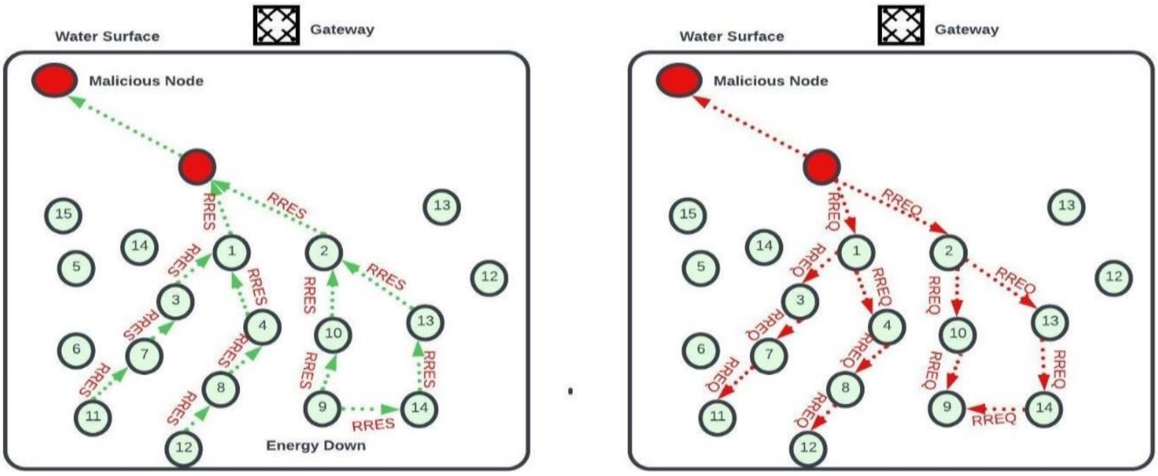
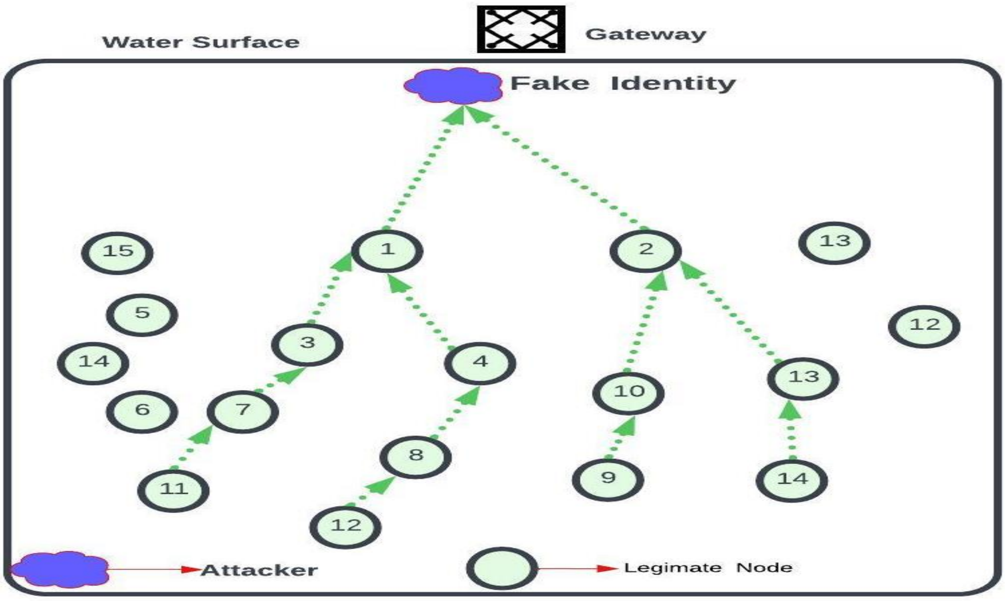


Fig 6. Battery-oriented attack.

H. Node Compromise Attack: To access or change data in memory, an attacker can take control over, damage, and compromise IoUT nodes. Furthermore, the compromised nodes can pose as trustworthy nodes in order to filter or interfere with the network, which could cause even more severe damage. By measuring and gathering the acoustic signal's strength, an attacker can find the network. Unfortunately, if there is no evidence of hack-confirmation equipment or other security measures, the attacker can surely breach and exploit them to view private data (such as the encryption algorithm, secret key, or trust value) and change it in the internal memory. In addition, it is possible to screen the hacked node or initiate persistent attacks by inserting it into the network as a real node.

I. Sybil Attack: The Sybil attack is a routing attack. In this instance, the attacker uses a false identity to steal the data. An attacker can be anywhere in IoUT networks and use many identities to trick routing, as shown in Figure 7. It causes transmission delay or packet loss.



Received: 2024-11-13
Accepted: 2025-01-02
Published Online: 2025-01-30
DOI: 10.70454/JRICST.2025.20109

Fig. 7. Sybil attack inIoUT environment.

J. **Wormhole Attack:** An attacker uses two malicious nodes to tunnel traffic over IoUT networks in a wormhole attack [34–37]. The two plotting nodes intercept packets at one end and block them at the other. Wormhole attacks offer the potential for an additional routing channel and can produce false neighbor connections. The process of a wormhole attack is shown in Figure 8, which results in a communication channel breach just because the wormhole node seems closer than authorized nodes.

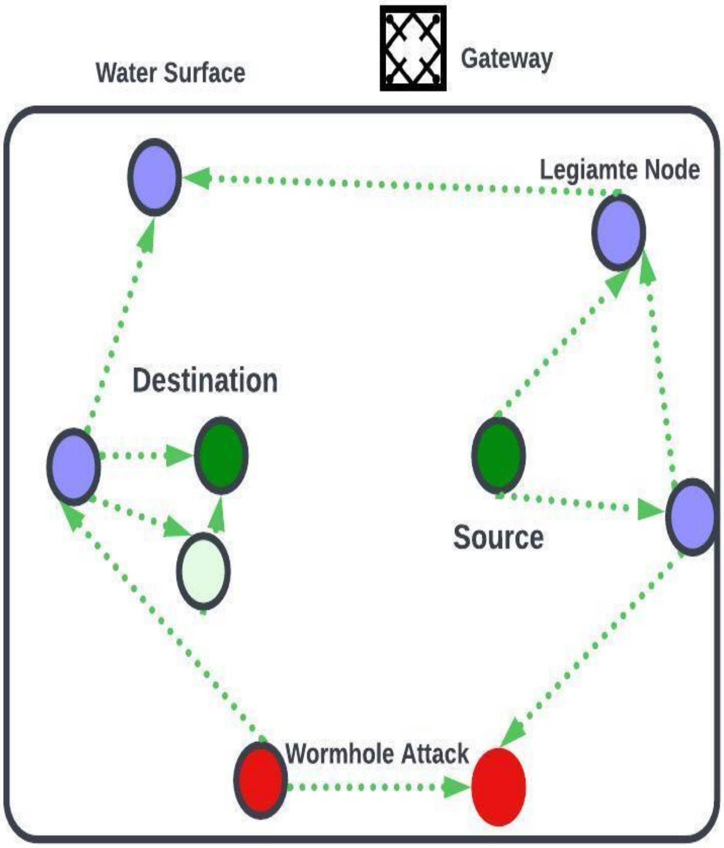


Fig. 8. Wormhole attack in theIoUT environment.

K. **Unfairness:**A denial-of-service attack is what this is. Rather than completely stopping data transfer, the attacker aims to disrupt legitimate nodes' functionality. In IoUT networks, it can really result in transmission delays.

L. **Hello Flooding Attack:**To identify its neighbour node, each node in an IoUT environment will emit HELLO packets. When an adversary node in an IoUT network repeatedly broadcasts HELLO packets to legitimate nodes in an attempt to drain their battery, this is known as a hello flooding attack. The attacker node will use a powerful signal to convince the legitimate node in this scenario. Consequently, the legitimate node will send data by posing as the hostile node. It effectively reduces the lifespan of the network and causes power failure. In order to attract legitimate nodes, the rogue node in IoUT networks sends strong signal intensity HELLO packets, as shown in Figure 9 [38].

Received: 2024-11-13
Accepted: 2025-01-02
Published Online: 2025-01-30
DOI: 10.70454/JRICST.2025.20109

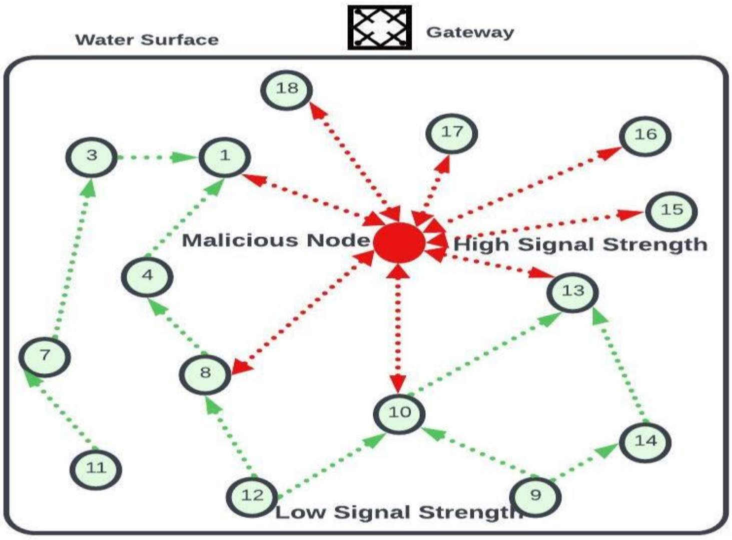


Fig. 9 Hello flooding attack in theIoUT environment.

M. Selective forwarding: In these attacks, the rogue node is placed close to the IoUT network gateway. The legitimate nodes will find a new path to the gateway to deliver the data once any packets are identified. Figure 10a illustrates how the rogue node might selectively drop some packets before arriving at the target in this attack. In IoUT networks, it causes packet loss.

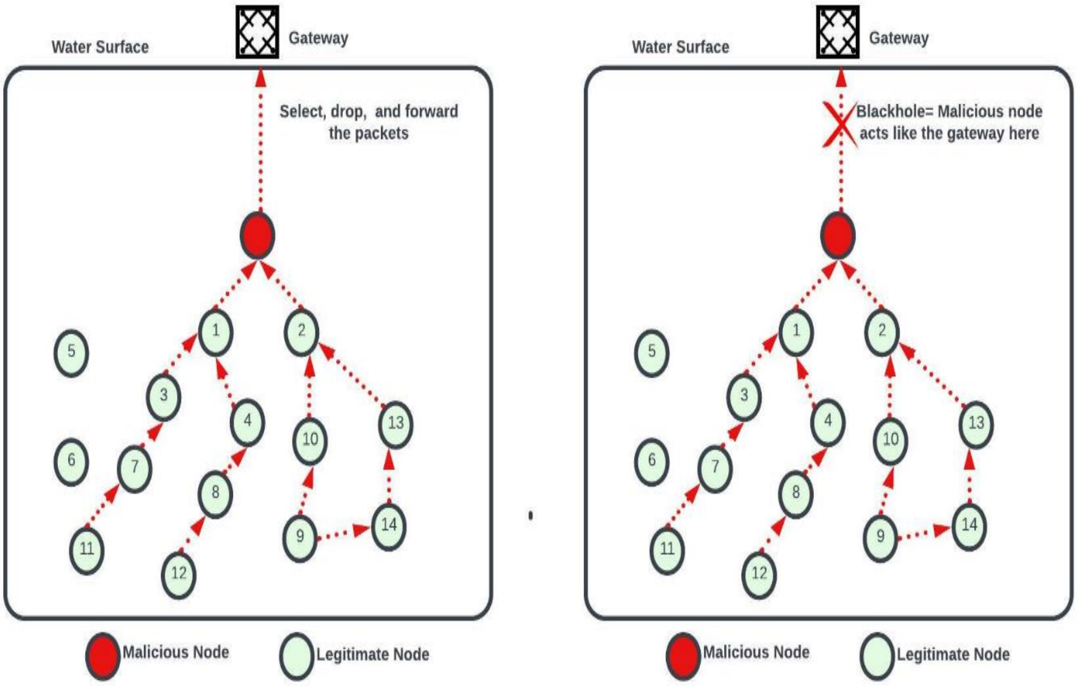


Fig.10. (**a**) Selective forwarding attack, (**b**) black hole attack in theIoUT environment.

N. **Blackhole attack:**In these attacks, packets are discarded during routing because the rogue node assumes the role of the cluster head or gateway. A rogue node can blackhole packets that are routed from regular nodes by changing or discarding them, as shown in Figure 10.b. Black hole attacks are the term used to describe lost packets in IoUT networks.

O. **Gateway block attack:**In this assault, all data sent from legitimate nodes to the gateway is blocked by the unauthorized network that is situated close to the gateway. In this case, all of the routing data that was sent to the gateway as the destination is successfully stolen by the attacker. In reality, it causes total packet loss. Therefore, a gateway block attack is the main danger in IoUTnetworks.

P. **Misdirection attack:** The infected node can be located anywhere in theIoUT network and track the routing path to change the route to the malicious node in this attack. This assault results in packet loss or data transmission delay.

Q. **Homing attack:**The malicious node attacks the most crucial nodes, like the cluster head and gateway, while keeping an eye on traffic on IoUT networks. These specific nodes can also be jammed or destroyed by this attacker via a denial-of-service attack.

R. **Desynchronization attack**: This attack breaks active connections between nodes in IoUT networks by sending bogus packets. In this case, the fraudulent packets will include fake sequence numbers to interfere with the synchronization of the underwater nodes. It affects how accurate IoUTnetworks are.

S. **Clock skewing attack**: In this type of attack, the attacker tries to obtain the timestamp data of an authentic node. This makes it possible to change the time stamp data in a lawful node. Consequently, it results in a problem with time synchronization in IoUTnetworks.

T. **Data aggregation attack:**In these assaults, the attacker tries to compile the privacy-based data from the genuine node in IoUT networks. Passwords and usernames can be obtained by the attacker [15].

8. IoUT SECURITY PROTOCOLS

The IoUT security protocol candidates are examined in this section.

A. **CCM-UW [3]:** It has been modified to utilise the CCM*1 operating mode in a UAC setting. Every stage has a different energy consumption and security level, and stage 6 is supported. Security at the MAC2 layer was created. Low bandwidth and signal loss prevented optimisation of the demonstration test result.

B. **UW-AKE [4]:** The protocol for key distribution and lightweight authentication. Members must be willing to provide a secret key and have proven themselves to be trustworthy. A separate key exchange method that integrates the authentication value to the authentication process is eliminated in order to reduce weight. The movement claims that network security was always the goal of the re-authentication mechanism's design. It has not undergone laboratory validation.

C. **SeFLOOD [5]:** This message exchange authentication technique is based underwater and is intended to guard against vulnerabilities like "Flooding," "Spoofing," and "DoS" because

IoUT is designed for fixed and reliable power supply performance devices, it is challenging to determine the appropriate security procedures, despite the existence of underwater security standards.

Table 1. Analysis of Underwater security protocols

Security Condition	CCM-UW	UW-AKE	SeFLOOD
Lightweight	Different by 6 step security level	Combine authentication key	Not affordable forIoUT
Low Power	Different by 6 step security level	Not consider	Not consider
Authentication & authorization	CBC-MAC[a]	Support	Support
Intrusion prevention	Frame counter by MAC	One Time Authentication(OTP)	Encrypted unicasting
Re-Authentication	Not Consider	Support but not efficient	Not Consider
Data Encryption	Different by security level	Combine encryption/decryption key	Conceptual

[a] Cipher Block Chaining-Message Authentication Code

9. Findings

The main conclusions from the selected original research publications are covered in this section. We provide an overview of the security field under investigation, together with the background and contributions made to each work under study. Three criteria are used to classify the primary studies [24]:

A. Security concerns: The majority of the papers in this part address the broad security concerns, limitations, and shortcomings of UWSNs.

B. Security attacks: articles that address security attacks and provide examples of attack methods are included in this section.

C. Attack detection and mitigation: This section contains papers that outline methods for spotting and stopping attacks on UWSNs.

Table 2. Focus Area

Focus area	Paper count
Security attacks	7
Security attacks	6
Authentication	4
Authentication	3

Trust management	3
Trust management	2
Data management	2

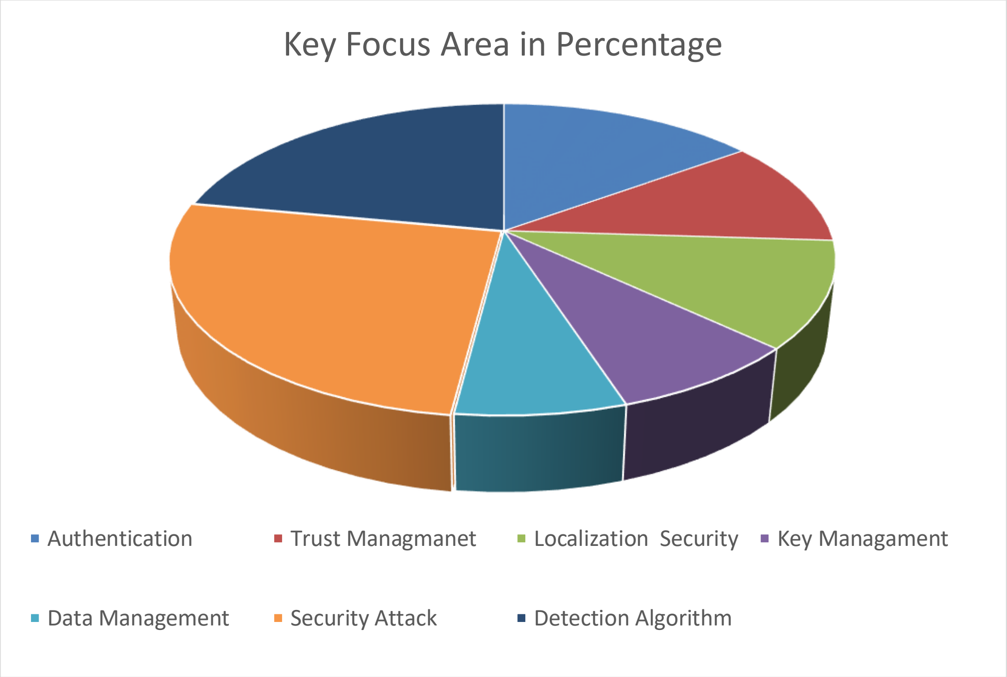


Fig. 11. Key Focus Area

10. Research Challenges and Scope

A thorough examination of a number of publications reveals that some aspects, including communication, energy, security, deployment, and maintenance, require improvement. Underwater signal transmission is challenging due to signal degradation, background noise, and interference that are frequent in aquatic environments. Although acoustic communication is frequently utilised, its operational range and bandwidth are limited.Energy-efficient design ideas must be given priority because underwater equipment frequently have limited battery capacity.The underwater environment poses significant obstacles for device deployment, recovery, and maintenance because of factors like pressure, corrosion, and severe weather. The need for strong encryption and comprehensive security measures is highlighted by the susceptibility of Internet of Underwater Things (IoUT) networks to cyberattacks, especially in military environments.

11. Conclusion

According to the aforementioned study, combining radio wave, optical, and acoustic communication techniques can increase data transfer speeds and efficiency. Developing techniques to power Internet of Underwater Things (IoUT) devices, including wave energy, sun energy (for surface elements), and temperature gradients. The use of collective behavioural techniques in Autonomous Underwater Vehicles (AUVs) to increase exploration and data collection efficiency is known as swarm intelligence applications. IncludingAI techniques for anomaly identification, predictive modelling, and data analysis in underwater environments.

combining acoustic, optical, and radio wave communications to improve the efficiency and speed of data transport. developing techniques including wave energy, solar energy (for surface components), and thermal gradients to power IoUT devices. using collective behaviour strategies to increase the efficiency of exploration and data collection in autonomous underwater vehicles. utilising AI techniques for data analysis, predictive modelling, and anomaly identification in underwater environments.

REFERENCES

[1] Domingo, M. C. (2012). An overview of the internet of underwater things. *Journal of Network and Computer Applications*, *35*(6), 1879-1890, https://doi.org/10.1016/j.jnca.2012.07.012.

[2] Khalil, R. A., Saeed, N., Babar, M. I., & Jan, T. (2020). Toward the internet of underwater things: Recent developments and future challenges. *IEEE Consumer Electronics Magazine*, *10*(6), 32-37, https://doi.org/10.1109/MCE.2020.2988441.

[3]Kao, C. C., Lin, Y. S., Wu, G. D., & Huang, C. J. (2017). A comprehensive study on the internet of underwater things: applications, challenges, and channel models. *Sensors*, *17*(7), 1477, https://doi.org/10.3390/s17071477.

[4] Bhattacharya, S., Victor, N., Chengoden, R., Ramalingam, M., Selvi, G. C., Maddikunta, P. K. R., &Gadekallu, T. R. (2022). Blockchain for internet of underwater things: State-of-the-art, applications, challenges, and future directions. *Sustainability*, *14*(23), 15659, https://doi.org/10.3390/su142315659.

[5] Ali, E. S., Saeed, R. A., Eltahir, I. K., &Khalifa, O. O. (2023). A systematic review on energy efficiency in the internet of underwater things (IoUT): Recent approaches and research gaps. *Journal of Network and Computer Applications*, *213*, 103594, https://doi.org/10.1016/j.jnca.2023.103594.

[6] K. M, D. R., Lee, J., Ko, E., Shin, S. Y., Namgung, J. I., Yum, S. H., & Park, S. H. (2020). Underwater network management system in internet of underwater things: open challenges, benefits, and feasible solution. *Electronics*, *9*(7), 1142, https://doi.org/10.3390/electronics9071142.

[7] Mohsan, S. A. H., Mazinani, A., Othman, N. Q. H., &Amjad, H. (2022). Towards the internet of underwater things: A comprehensive survey. *Earth Science Informatics*, *15*(2), 735-764, https://doi.org/10.1007/s12145-021-00762-8.

]8] Lima, F. H., Vieira, L. F., Vieira, M. A., Vieira, A. B., &Nacif, J. A. M. (2019). Water ping: ICMP for the internet of underwater things. *Computer Networks*, *152*, 54-63,https://doi.org/10.1016/j.comnet.2019.01.009

[9] Mohsan, S. A. H., Mazinani, A., Othman, N. Q. H., &Amjad, H. (2022). Towards the internet of underwater things: A comprehensive survey. *Earth Science Informatics*, *15*(2), 735-764, https://doi.org/10.1007/s12145-021-00762-8

[10] Bello, O., &Zeadally, S. (2022). Internet of underwater things communication: Architecture, technologies, research challenges and future opportunities. *Ad Hoc Networks*, *135*, 102933, https://doi.org/10.1016/j.adhoc.2022.102933.

11. Bello, O., &Zeadally, S. (2022). Internet of underwater things communication: Architecture, technologies, research challenges and future opportunities. *Ad Hoc Networks*, *135*, 102933, https://doi.org/10.1016/j.adhoc.2022.102933

[12] Razzaq, A., Mohsan, S. A. H., Li, Y., &Alsharif, M. H. (2023). Architectural framework for underwater iot: Forecasting system for analyzing oceanographic data and observing the environment. *Journal of Marine Science and Engineering*, *11*(2), 368, https://doi.org/10.3390/jmse11020368.

13. Vuran, M. C., Salam, A., Wong, R., & Irmak, S. (2018). Internet of underground things in precision agriculture: Architecture and technology aspects. *Ad Hoc Networks*, *81*, 160-173, https://doi.org/10.1016/j.adhoc.2018.07.017

[14] Mohsan, S. A. H., Li, Y., Sadiq, M., Liang, J., & Khan, M. A. (2023). Recent advances, future trends, applications and challenges of internet of underwater things (iout): A comprehensive review. *Journal of Marine Science and Engineering*, *11*(1), 124, https://doi.org/10.3390/jmse11010124.

[15] Mary, D. R. K., Ko, E., Kim, S. G., Yum, S. H., Shin, S. Y., & Park, S. H. (2021). A systematic review on recent trends, challenges, privacy and security issues of underwater internet of things. *Sensors*, *21*(24), 8262,https://doi.org/10.3390/s21248262.

[16] Yeom, S. H., Namgung, J. I., Shin, S. Y., & Park, S. H. (2017). Lightweight Security for Underwater IoT. In Advances in Computer Science and Ubiquitous Computing: CSA-CUTE2016 8 (pp. 774-778), https://doi.org/10.1007/978-981-10-3023-9_119.

[17] Khalil, R. A., Saeed, N., Babar, M. I., & Jan, T. (2020). Toward the internet of underwater things: Recent developments and future challenges. *IEEE Consumer Electronics Magazine*, *10*(6), 32-37, https://doi.org/10.1109/MCE.2020.2988441.

[18] Mohsan, S. A. H., Li, Y., Sadiq, M., Liang, J., & Khan, M. A. (2023). Recent advances, future trends, applications and challenges of internet of underwater things (iout): A comprehensive review. *Journal of Marine Science and Engineering*, *11*(1), 124, https://doi.org/10.3390/jmse11010124.

[19] Qiu T, Zhao Z, Zhang T, Chen C, Chen CLP. Underwater internet of things in smart ocean: system architecture and open issues. IEEE Trans Ind Inform. 2020;16(7):4297-4307. https://doi.org/10.1109/TII.2019.2946618.

[20] Mrabet, H., Belguith, S., Alhomoud, A., &Jemai, A. (2020). A survey of IoT security based on a layered architecture of sensing and data analysis. *Sensors*, *20*(13), 3625, https://doi.org/10.3390/s20133625.

[21] Shahapur, S. S., &Khanai, R. (2016, March). Localization, routing and its security in UWSN—A survey. In *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)* (pp. 1001-1006). IEEE, https://doi.org/10.1109/ICEEOT.2016.7754836.

[22] Dargahi, T., Javadi, H. H., &Shafiei, H. (2017). Securing underwater sensor networks against routing attacks. *Wireless Personal Communications*, *96*, 2585-2602, https://doi.org/10.1007/s11277-017-4313-1.

[23] Yunus, F., Ariffin, S. H., &Zahedi, Y. (2010, May). A survey of existing medium access control (MAC) for underwater wireless sensor network (UWSN). In *2010 Fourth Asia International Conference on Mathematical/Analytical Modelling and Computer Simulation* (pp. 544-549). IEEE, https://doi.org/10.1109/AMS.2010.110.

[24] Yisa, A. G., Dargahi, T., Belguith, S., &Hammoudeh, M. (2021). Security challenges of internet of underwater things: A systematic literature review. *Transactions on Emerging Telecommunications Technologies*, *32*(3), e4203, https://doi.org/10.1002/ett.4203.

[25] Singh, K. J., &Kapoor, D. S. (2017). Create your own Internet of things: A survey of IoT platforms. *IEEE Consumer Electronics Magazine*, *6*(2), 57-68, https://doi.org/10.1109/MCE.2016.2640718.

[26] Mohanty, S. P., Choppali, U., &Kougianos, E. (2016). Everything you wanted to know about smart cities: The Internet of things is the backbone. *IEEE consumer electronics magazine*, *5*(3), 60-70, https://doi.org/10.1109/MCE.2016.255687.

[27] Khalil, R. A., Saeed, N., Babar, M. I., & Jan, T. (2020). Toward the internet of underwater things: Recent developments and future challenges. IEEE Consumer Electronics Magazine, 10(6), 32-37, https://doi.org/10.1109/MCE.2020.2988441.

[28] Saeed, N., Celik, A., Al-Naffouri, T. Y., &Alouini, M. S. (2019). Underwater optical wireless communications, networking, and localization: A survey. *Ad hoc networks*, *94*, 101935, https://doi.org/10.1016/j.adhoc.2019.101935.

[29] Akyildiz, I. F., Wang, P., & Sun, Z. (2015). Realizing underwater communication through magnetic induction. *IEEE Communications Magazine*, *53*(11), 42-48, https://doi.org/10.1109/MCOM.2015.7321970.

[30] Dini, G., & Lo Duca, A. (2012). A secure communication suite for underwater acoustic sensor networks. *Sensors*, *12*(11), 15133-15158,https://doi.org/10.3390/s121115133.

[31] Khanam, S., Ahmedy, I. B., Idris, M. Y. I., Jaward, M. H., &Sabri, A. Q. B. M. (2020). A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things. *IEEE access*, *8*, 219709-219743, https://doi.org/10.1109/ACCESS.2020.3037359.

[32] Alsamani, B., &Lahza, H. (2018, March). A taxonomy of IoT: Security and privacy threats. In *2018 International Conference on Information and Computer Technologies (ICICT)* (pp. 72-77). IEEE, https://doi.org/10.1109/INFOCT.2018.8356843.

[33] Raymond, D. R., &Midkiff, S. F. (2008). Denial-of-service in wireless sensor networks: Attacks and defenses. *IEEE Pervasive Computing*, *7*(1), 74-81, https://doi.org/10.1109/MPRV.2008.6.

[34] Gorlatova, M.A.; Mason, P.C.; Wang, M.; Lamont, L.; Liscano, R. Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis. In Proceedings of the MILCOM 2006—2006 IEEE Military Communications Conference, Washington, DC, USA, 23–25 October 2006; pp. 1–7.

[35] Kong, J., Ji, Z., Wang, W., Gerla, M., Bagrodia, R., &Bhargava, B. (2004). On wormhole attacks in under-water sensor networks: A two-tier localization approach. *UCLA Computer Science Department Technical Report*, *4005*, https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=9d3775780ba92112cfcca6d3fb7d6dcc10a951f0.

[36] Jen, S. M., Laih, C. S., &Kuo, W. C. (2009). A hop-count analysis scheme for avoiding wormhole attacks in MANET. *Sensors*, *9*(6), 5022-5039, https://doi.org/10.3390/s90605022.

[37] Wang, W., Kong, J., Bhargava, B., &Gerla, M. (2008). Visualisation of wormholes in underwater sensor networks: a distributed approach. *International Journal of Security and Networks*, *3*(1), 10-23, https://doi.org/10.1504/IJSN.2008.016198.

[38] Kaur, P., &Gurm, J. S. (2016). Detect and prevent HELLO FLOOD attack using centralized technique in WSN. *Int. J. Comput. Sci. Eng. Technol*, *7*(8), 379-381,http://ijcset.com/docs/IJCSET16-07-08-023.pdf