IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 31 July 2022, accepted 7 September 2022, date of publication 25 October 2022, date of current version 4 November 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3216850

RESEARCH ARTICLE

Blockchain Based Privacy Preserving Authentication and Malicious Node Detection in Internet of Underwater Things (IoUT) Networks

SHAHID ABBAS[1], (Member, IEEE), HINA NASIR[2], AHMAD ALMOGREN[3], (Senior Member, IEEE), AYMAN ALTAMEEM[4], AND NADEEM JAVAID[1], (Senior Member, IEEE)

[1]Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan
[2]Department of Computer Science, Air University, Islamabad 44000, Pakistan
[3]Chair of Cyber Security, Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11633, Saudi Arabia
[4]Department of Natural and Engineering Sciences, College of Applied Studies and Community Services, King Saud University, Riyadh 11543, Saudi Arabia

Corresponding authors: Ahmad Almogren (ahalmogren@ksu.edu.sa) and Nadeem Javaid (nadeemjavaidqau@gmail.com)

This work was supported by the Deanship of Scientific Research at King Saud University, Riyadh, Saudi Arabia, through the Vice Deanship of Scientific Research Chairs: Chair of Cyber Security.

ABSTRACT The usage of Internet of Underwater Things (IoUT) Networks allows for the detection of a variety of aquatic factors like temperature, pressure, pollution, etc. They are also used to forecast the ocean's weather to collect information about natural disasters. However, they are easily compromised by attackers due to deployment in unattended environments. To overcome these issues, security is required in IoUT networks to avoid unauthorized access and ensure network credibility. This work proposes an authentication and a malicious node detection mechanism to restrict the unauthorized external nodes from accessing the network and the internal nodes from acting maliciously, respectively. Moreover, blockchain stores the hashes of sensor nodes' credentials during the registration process to make the system secure and traceable. Meanwhile, for data aggregation and malicious nodes' detection, a weighted trust evaluation mechanism is introduced. Moreover, an additive increase multiplicative decrease algorithm puts malicious nodes in an intensive observation queue to verify the data of malicious nodes before aggregating. Moreover, weights are assigned to sensor nodes based on their behaviour. If the weight of a sensor node becomes zero, it is revoked by the blockchain. Besides, the proposed malicious node detection mechanism's enhanced efficiency is proved via extensive simulations.

INDEX TERMS Authentication, blockchain, Internet of Underwater Things, malicious node detection, privacy preservation.

I. INTRODUCTION

Since water covers 70% of the earth's surface, underwater research has become very popular in recent years [1]. It is essential for the oil industry, natural disaster's predictions, study of marine life, etc. Moreover, underwater networks are envisioned to automate the underwater traffic. In order to increase the effectiveness of ocean monitoring, underwater exploration has attracted the attention of numerous researchers. The development of several security methods to provide safe and reliable communication in the Internet of Underwater Things (IoUT) Networks has benefited from the previous few decades.

Additionally, compared with the terrestrial Internet of Things (IoT), IoUT networks are deployed in an unattended environment. Therefore, they face uncertain conditions, which cause security issues like existence of unauthenticated and malicious nodes, privacy leakage, data tampering, etc., [2]. Moreover, in the unattended underwater networks, terrestrial protocols are inefficient because they are designed

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

TABLE 1. List of abbreviations and acronyms.

Abbreviation	Description
AIMD	Additive Increase Multiplicative Decrease
BAM	Blockchain based privacy preserving Authentication and Malicious node detection
BS	Base Station
BTM	Blockchain based Trust Model
DoS	Denial of Service
IoT	Internet of Things
IoUT	Internet of Underwater Things
MA	Manufacturing Authority
SN	Sink Node
TCP	Transmission Control Protocol
WSNs	Wireless Sensor Networks
WTE	Weighted Trust Evaluation
A	Aggregation Result
B	Blockchain
D_n	Data of Ordinary Node
dec	Decryption
enc	Encryption
ID_O	ID of Owner
ID_S	ID of Sensor Node
L_{BS}	Location of BS
L_S	Location of Sensor Node
N	Number of Sensor Nodes
$w(t)$	Data Rate
W_n	Weight of Sensor Node

especially for the terrestrial sensor networks. Also, these protocols pose an extra computational burden on the underwater network nodes. Therefore, these protocols are not recommended for the underwater networks. Moreover, the diverse nature of IoUT networks causes issues like high propagation delay, narrow bandwidth and multi-path effect, which affect the efficiency of a network and cause above mentioned security issues.

Authentication of nodes is an essential feature for protecting network communication from external nodes [3]. In authentication process, usually Base Stations (BSs) check the legitimacy of sensor nodes before allowing them to enter the network. The authors in [4] propose an authentication scheme in which the credentials of sensor nodes are stored in a nearby BS. However, BSs are physically accessible by attackers, which can steal or alter the stored credentials. The underwater sensor nodes have very sensitive credentials, such as locations and identities; so, an attacker can reveal the sensor node's location to physically access the node. In addition, the Identifications (IDs) of the sensor nodes are used in different encryption-decryption schemes. Therefore, the sensor nodes' credentials require a secure storage mechanism to preserve their privacy. The lack of privacy can disturb the deployment of sensor nodes because attackers can steal the location for accessing the particular node [5], [6]. To deal with this issue, the researchers propose distributed blockchain based authentication schemes in different domains, i.e., vehicular networks [7], [8], IoTs [9], [10], energy trading [11], etc. She et al. [12] propose a malicious node detection and a secure routing mechanism for the Wireless Sensor Network (WSN). However, they do not propose a method for restriction of the entry of unauthenticated external nodes. Moreover, in malicious node detection mechanism, the system revokes the malicious nodes completely from the network. However, sometimes sensor nodes may also have technical faults like destructive interference effects that can be resolved automatically or by the relevant authority. So, the complete revocation of sensor nodes is not an effective solution. Furthermore, Kim et al. discuss in [13] the reputation[1] of the sensor nodes to collect the data by the highly reputed nodes. However, they do not discuss the recovery of sensor nodes' reputation when any sensor node gets reinstated from a malicious state.

In this paper, a blockchain based privacy preserving authentication mechanism is proposed for IoUT networks. This mechanism registers the sensor nodes by storing their credentials' hash in blockchain to achieve anonymity [14]. Besides, the issue of detection and partial revocation of the suspected malicious nodes is addressed by integrating the Weighted Trust Evaluation (WTE) mechanism [15] with the Additive Increase Multiplicative Decrease (AIMD) mechanism [16]. WTE is used to evaluate nodes through data aggregation enabled weights while AIMD is used to control the transmission rate of the suspected node. The aggregation of data causes low bandwidth consumption during data transmission because redundant data is removed. Similarly, AIMD enabled communication control mechanism reduces the bandwidth consumption by controlling the communication rate of the suspected sensor node.

A. BLOCKCHAIN

The traditional centralized architectures have many issues like lack of immutable data storage, single point of failure, a bandwidth bottleneck occurs in case of high traffic, etc. Therefore, blockchain technology is used to store the data distributively, which is generated during registration process. A copy of an immutable ledger is stored on each node of the blockchain, which is a distributed platform for data storage [17], [18]. If the attacker wants to alter the block's data, it must change all hashes in the blockchain. Therefore, it is almost impossible for the attacker to alter the whole blockchain because the distributed ledger is stored in a peer-to-peer network [19].

B. LIST OF CONTRIBUTIONS

The proposed work comes with five-fold contributions: noitemsep

- a privacy preserving authentication mechanism is proposed for IoUT networks,
- a WTE mechanism is used to detect malicious nodes in IoUT networks,
- an AIMD algorithm is implemented for data rate control of sensor nodes in case of malicious behaviour,
- weight recovery mechanism is introduced to enable the re-entrance of the revoked sensor node in the network and

[1] Reputation and weight are used synonymously.

- an attacker model is used to check the credibility of the proposed Blockchain based privacy preserving Authentication and Malicious node detection model (BAM).

The remaining sections of the manuscript are structured as follows. A survey of the literature on blockchain and underwater WSNs is presented in Section II. The proposed system model is covered in Section III. The simulation settings, performance metrics, and performance assessment of the system model are presented in Section IV. The attacker model and security analysis are highlighted in Sections V and VI, respectively. The conclusion of this manuscript and suggestions for future research are presented in Section VII.

II. LITERATURE REVIEW

IoUT networks are affected by the different types of attacks, similar to the terrestrial IoT. However, the underwater environment is more complex and dynamic as there are more constraints than the terrestrial IoTs. In this section, the literature review of the existing schemes is discussed and categorized into two types: centralized and distributed architectures. The underwater environment is more prone to security concerns due to the hostile and unattended environment. Therefore, the authentication protocols for terrestrial WSNs are not suitable for underwater WSNs due to the need of additional computational requirements.

Goyal et al. propose a secure authentication and data aggregation protocol that enables the network to run smoothly in a harsh underwater environment [20]. However, this protocol relies only on a centralized authority as a gateway that is vulnerable to a single point of failure. Zhang et al. [21] apply chaotic maps for remote user authentication. This scheme consists of a lightweight one-way hash function for the underwater acoustic network. The security scheme is certified through a random oracle model. However, a single point of failure and other related issues arise due to the utilization of a centralized registration center. Moreover, mutual authentication is challenging due to lack of trust factor and usage of different protocols for communication, which are not understandable by cross-vendor devices. Authors in [22] propose an attack resistant trust model based on multidimensional trust metrics to track and revoke the malicious activities in the underwater WSNs. This model consists of link trust, which is achieved through considering the unreliability metrics and ocean's diverse environment. In [23], the authors propose a mutual authentication scheme in the underwater sensor network. The sensors are deployed at the front of the underwater vehicles. If the sensor node detects the movement of another underwater vehicle, it fetches the credentials from BS to perform mutual authentication. However, BSs are centralized authorities that are easily accessible in the underwater environment. Therefore, the storage of nodes' sensitive credentials is risky for BSs. In [24], a trust aware selection criteria for cluster heads and sensor node is proposed by Vani et al. Firstly, nodes are authenticated using a lightweight XOR encryption scheme. Secondly, the nodes are selected based on the trust values calculated by fuzzy parameters, such as distance, relative mobility and energy. Moreover, the security of the nodes is checked by the trust manager. However, the XOR function is lightweight that can easily be guessed by the attackers. In addition, selecting the cluster head as a trust manager seems unreliable due to its short life span. In [25], authors state that an unreliable environment causes high packet drop that affects the communication rate. Therefore, they propose a trust strategy based on a dynamic Bayesian game to address the existing problems. Baye's rule helps the nodes to update their trust values. In addition, regular nodes are always monitored to evaluate the neighbour nodes' trust. The proposed model is better than the existing schemes because it proposes an efficient cooperation strategy between the nodes. In [26], Ahmad et al. propose an intrusion detection mechanism using the dataset of nodes' previous communication history. The dataset is categorized into different types of attacks. Moreover, terrestrial based WSN protocol is used in the low energy-aware cluster hierarchy protocol in the underwater environment. However, the authors only focus on detecting a Denial of Service (DoS) attack while other cyber attacks are neglected, which are more harmful to the network like wormhole attack, sybil attack, etc.

The centralized nature of the aforementioned protocols makes them susceptible to various security risks, such as single point of failure, privacy leakage, lack of immutability, etc. Uddin et al. [27] propose a lightweight routing protocol that requires few control messages to forward packets. The routing protocol uses a bloom filter to achieve privacy and secure the credentials of end nodes. This protocol is multi layered that is based on blockchain in which fog and cloud nodes are used to store the data securely. In [28], authors state that data sharing in marine IoT is not efficient because edge devices are prone to trust issues. In marine IoT, edge devices are increasing day by day; therefore, chances of their privacy leakage are increasing. Existing centralized architectures are still having some flaws related to trust. Therefore, they propose a secure data sharing mechanism that consists of blockchain and federated learning. Moreover, the authors propose a reputation mechanism for selecting federated learning.

Furthermore, many authors use blockchain technology in other fields of research to ensure security, i.e., vehicular based trust management system [29], [30], secure energy trading [31], [32], supply chain management [33], and secure medical data storage [34].

III. SYSTEM MODEL

In this section, a detailed discussion of our proposed system model is presented. Firstly, fundamental network assumptions and the network model are discussed. Secondly, the initialization and description of the proposed system model are provided. Then, the steps of the proposed system model, such as registration, weighted trust evolution of sensor nodes, malicious node detection, communication control and weight recovery are discussed in detail.

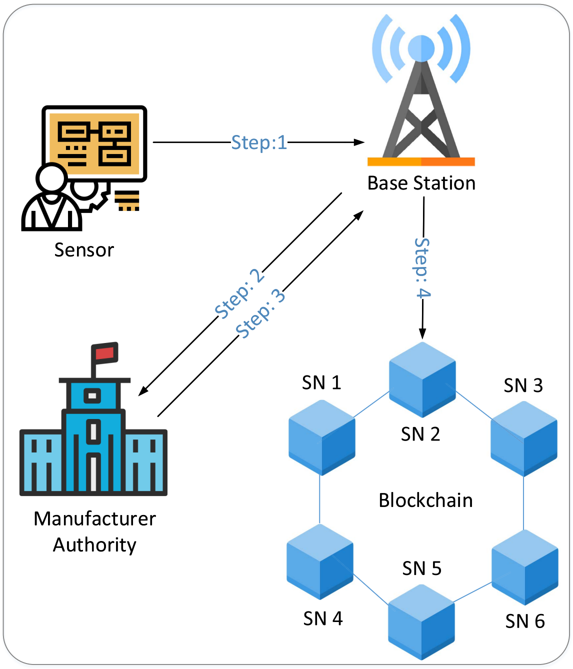


FIGURE 1. Proposed authentication model.

A. INITIALIZATION OF NETWORK

In the initialization phase, sensor nodes are deployed randomly and statically in the given field to achieve accurate results. Also, sensor nodes are considered homogeneous. Moreover, the distance between the sensor nodes and BSs is calculated using the Euclidean distance formula [35]. This distance remains the same due to static deployment. Sink Nodes (SNs) and BSs are deployed statically at the ocean's surface and in the ocean, respectively. Therefore, it is assumed that they have no energy and computational constraints [36] and blockchain is deployed on them to efficiently perform the mining task. SNs are used to provide a connection between the underwater environment and the Internet. BSs are working as data collectors, aggregators and forwarders for the underwater network. Sensor nodes send data to SNs through BSs because they are not directly connected to SNs. Moreover, there is a multi-hop communication between BSs (BAM has two layers of BS) and SNs in which every sensor node is directly connected with BS. Moreover, SNs and BSs are assumed to be legitimate nodes and they tend to communicate safely. Furthermore, a Manufacturing Authority (MA) manufactures and assigns every sensor node to its respective owner for secure and efficient operations. MA is assumed to be the external, off-chain and independent authority. It contains every sensor node's unique ID, which is stored with the corresponding owner's ID.

B. SYSTEM MODEL DESCRIPTION

To make a network secure, registration and authentication are done through the blockchain, which stores the data distributively to avoid single point of failure issue. The proposed authentication mechanism for the sensor nodes is motivated from [37]. The step-wise authentication process is shown in Fig. 1.

1) REGISTRATION AND AUTHENTICATION

Algorithm 1 is proposed to register the sensor nodes and the step-wise process is discussed below. *Step 1:* An interested sensor node encloses its identity ID_S, corresponding location L_S and its owner's ID ID_O into one packet and encrypts it with the public key of BS BS_{enc}, as given in Eq. 1. The sensor node then sends the registration request to BS.

$$Reg_{req\rightarrow BS} = BS_{enc}(ID_S, L_S, ID_O). \tag{1}$$

Step 2: BS receives this request, decrypts it with its private key BS_{dec}, adds its location L_{BS} and again encrypts it with MA's public key MA_{enc}. BS requests MA for verification of sensor nodes, as given in Eq. 2.

$$Reg_{req\rightarrow MA} = MA_{enc}(ID_S, L_S, ID_O, L_{BS}). \tag{2}$$

Step 3: MA decrypts the Reg_{req} with its private key BS_{dec} and checks the presence of a sensor node's credentials in its database. If credentials are found, it sends a lightweight *true* message to BS and vice versa.

Note: MA already has records of the sensor nodes along with the relevant owners' IDs. This mapping of the sensor nodes' ownership is only stored in MA's database because MA manufactures the sensor nodes. As blockchain is deployed on BSs and MA is an off-chain entity, MA first sends the data to BS, which then appends it to the chain.

Step 4: Now, BS generates the hash of sensor node's credentials using SHA-256 and stores it in the blockchain B, as given in Eq. 3.

$$B = ((ID_S)_{hash}, (L_S)_{hash}, (ID_O)_{hash}, (L_{BS})_{hash}). \tag{3}$$

In case of any sensor node's malicious behaviour, blockchain is used to track the malicious node by comparing the malicious node's L_S hash with already stored hash.

Step 5: When any registered sensor node wants to log in to the network, the first stage is its verification from the blockchain network through BS. BS generates a hash of the corresponding sensor node's credentials and performs the comparison between the already stored hashes and the newly generated hashes in the blockchain. If match is found, the sensor node is allowed to communicate in the network. Otherwise, it will not be allowed to communicate in the network.

2) WEIGHTED TRUST EVALUATION OF SENSOR NODES

In [15], the detection of malicious nodes is performed via WTE. In our work, we use it for IoUT networks, which are divided into groups based on the ocean's depth and the distance of nodes from SN, as shown in Fig. 2.

The sensor nodes send data to their corresponding BSs for aggregation. After aggregation, BSs evaluate the sensor nodes

Algorithm 1 Registration Process of Sensor Nodes

```
Initialization;
Send to BS $BS_{enc}(ID_S, L_S, ID_O)$;
if $BS_{PK}$ belongs to BS then
    $BS_{dec}(ID_S, L_S, ID_O)$;
    Add $BS_{coordinates}$;
    Send to MA $MA_{enc}(ID_S, L_S, ID_O, L_{BS})$;
    if Match of $ID_S$ and $ID_O$ is Found then
        Recommend for Registration;
        Store Hashes in Blockchain
        $(ID_S)_{hash}, (L_S)_{hash}, (ID_O)_{hash}, (L_{BS})_{hash}$;
    else
        Rejected;
    end
else
    Rejected;
end
```

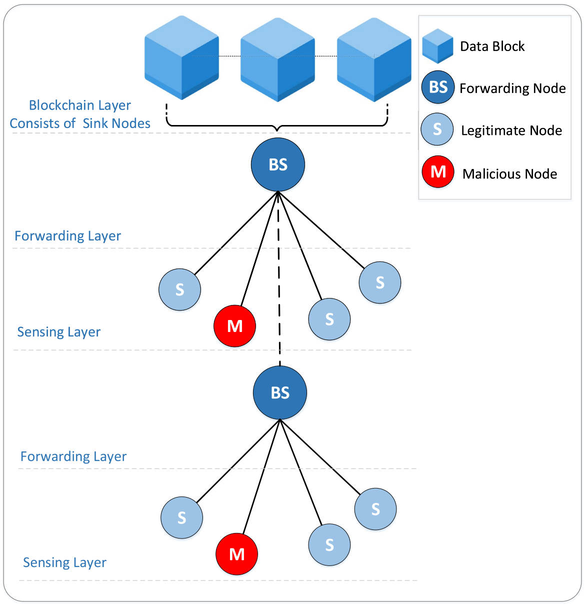


FIGURE 2. Layered architecture for malicious node detection.

based on their generated data. BS aggregates the data using updated weights of sensor nodes stored in the blockchain database, according to Eq. 4 [15]. Initially, the weight of every sensor node is 0.5, which is an already defined threshold for taking part in the network. If the sent data of the sensor node is equal to the aggregated data of the whole network, the weight of the sensor node is increased by 0.1. Similarly, if the data is not equal to the aggregated data, the nodes are suspected as malicious and their weight is decreased by 0.1. If the weight becomes less than the defined threshold, the contribution of the sensor nodes in aggregated data becomes less. In contrast, if the weight gets increased, the sensor node's contribution will become high. The contribution of the sensor node in aggregated data is directly proportional to its weight. Moreover, if the sensor node's weight becomes zero, its contribution will also be zero.

$$A = \sum_{n=1}^{N} W_n \times D_n. \tag{4}$$

where, A is the aggregated result of the data, which is calculated by BS. W_n is the weight of a sensor node where its value ranges from $(0 \rightarrow 1)$. N is the total number of sensor nodes, which are taking part in the network and D_n is the data generated by the sensor node.

3) MALICIOUS NODE DETECTION

For the detection and removal of the malicious nodes from the sensor networks, numerous studies have been performed [12], [13]. However, there are chances of technical faults in sensor nodes due to destructive interference effects in IoUT networks, which cause nodes malicious behaviour. These technical faults can be resolved automatically or by the relevant authority. In BAM, a sensor node is not completely revoked from the network. Also, its communication rate is reduced in order to check the correctness of its data parallelly. In this way, the transmission of the network is controlled. If the sensor node's technical fault gets resolved, it can increase the communication rate additively. However, if a sensor node keeps sending false data for a long time, the system revokes the suspected sensor node completely from the network, as discussed in Subsection III-B4 and shown in Fig. 3. There are three steps to detect malicious nodes.

Step 1: BS checks the correctness of the sensor node's data by comparing the data with aggregated data. If both the data are not similar, the sensor node is declared as a malicious node.

Step 2: When any sensor node is detected as malicious, its weight is decreased by 0.1. Also, it is added to the intensive observation queue.

Step 3: Once the weight of a malicious node is reduced to zero by continuously sending false data, it is completely revoked by deleting its registration from the blockchain.

4) COMMUNICATION CONTROL

In BAM, AIMD algorithm is used in Transmission Control Protocol (TCP) to control the data rate when a malicious node is detected in the network [16]. AIMD decreases the data rate of the malicious node multiplicatively. After decreasing the data rate, it continuously monitors the data traffic. If the sensor node gets stable, the network allows it to start sending the packets again with an additive increment, which will be increasing up to the standard data rate, as given in Eq. 5 [38]. Moreover, pseudo-code is given in Algorithm 2 and the pictorial representation of the mechanism is shown in Fig. 3.

$$w(t+1) = \begin{cases} w(t) + a & \text{if transmission is getting stable,} \\ w(t) \times b & \text{if malicious transmission is detected.} \end{cases} \tag{5}$$

Algorithm 2 Assigning Weights to Sensor Nodes

```
Initialization;
Initial Weight = 1;
for Number of Sensor Nodes do
    Send Data to BS (True or False);
    if (Aggregated Value == True) then
        if (Sensor Gives True Value) then
            Weight is Increased by 0.1;
        else
            Weight is Decreased by 0.1;
        end
    else
        if (Sensor Gives False Value) then
            Weight is Increased by 0.1;
        else
            Weight is Decreased by 0.1;
        end
    end
end
```

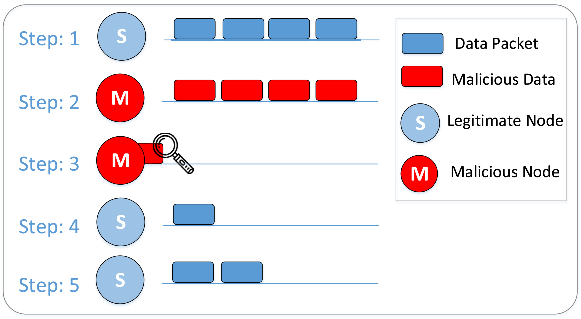


FIGURE 3. Proposed model for traffic control.

where, $w(t)$ is data rate with respect to time and a and b are the increase and decrease rate, respectively. Also, the values of a and b are $a = 1$ and $b = 0.5$.

5) WEIGHT RECOVERY

Initially, a weight is assigned to every sensor node to take part in the communication system. However, when a sensor node is detected as malicious, its weight is reduced and it is placed in an intensive observation queue. Algorithm 3 checks whether the data of the sensor node is equal to the aggregated data or not. If so, it increases the sensor node's data rate additively. Otherwise, the data rate is decreased multiplicatively because malicious node's data affects the aggregated result. Therefore, resources are not highly consumed. Besides, when a suspected malicious node acts normally, its data rate reaches the standard uploading threshold. Algorithm 3 sets its weight back to the initial value and declares it as a normal node.

Algorithm 3 AIMD Based Weight Recovery

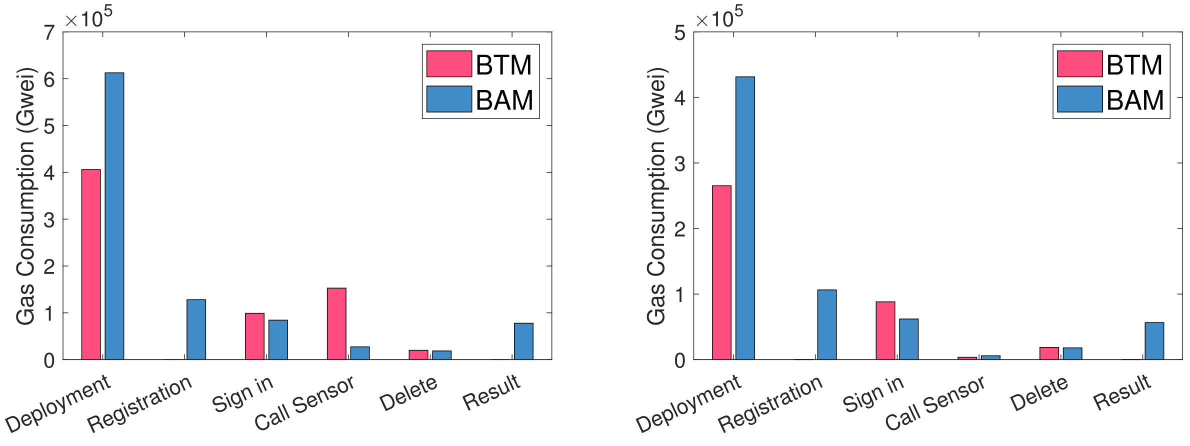
```
Initialization;
Initial Weight = 1;
for No. of Communication Rounds do
    for No. of Sensor Nodes do
        Require ($1 > Weight > 0$);
        Put Suspected Malicious Node in Intensive
          Observation Queue;
        if (Sensor Node's Value == Aggregated) then
            $w(t) + a$;
        else
            $w(t) \times b$;
            No. of Tries for Recovery;
        end
        if (Threshold Value == Standard Threshold)
          then
            Weight of Sensor Node = Initial Weight;
        end
    end
end
```

TABLE 2. Simulation parameters.

Parameters	Value
Sensing Area	$500 \times 500\ m^2$
No. of sensor nodes	225
No. of BSs	20
No. of SNs	5
Wireless Range of Sensor Nodes	250 m
Hashing Scheme	SHA-256
Initial Energy of Sensor Nodes	0.5J
Initial Energy of BSs	No Energy Constraint
Network Topology	Random Distribution

IV. PERFORMANCE EVALUATION

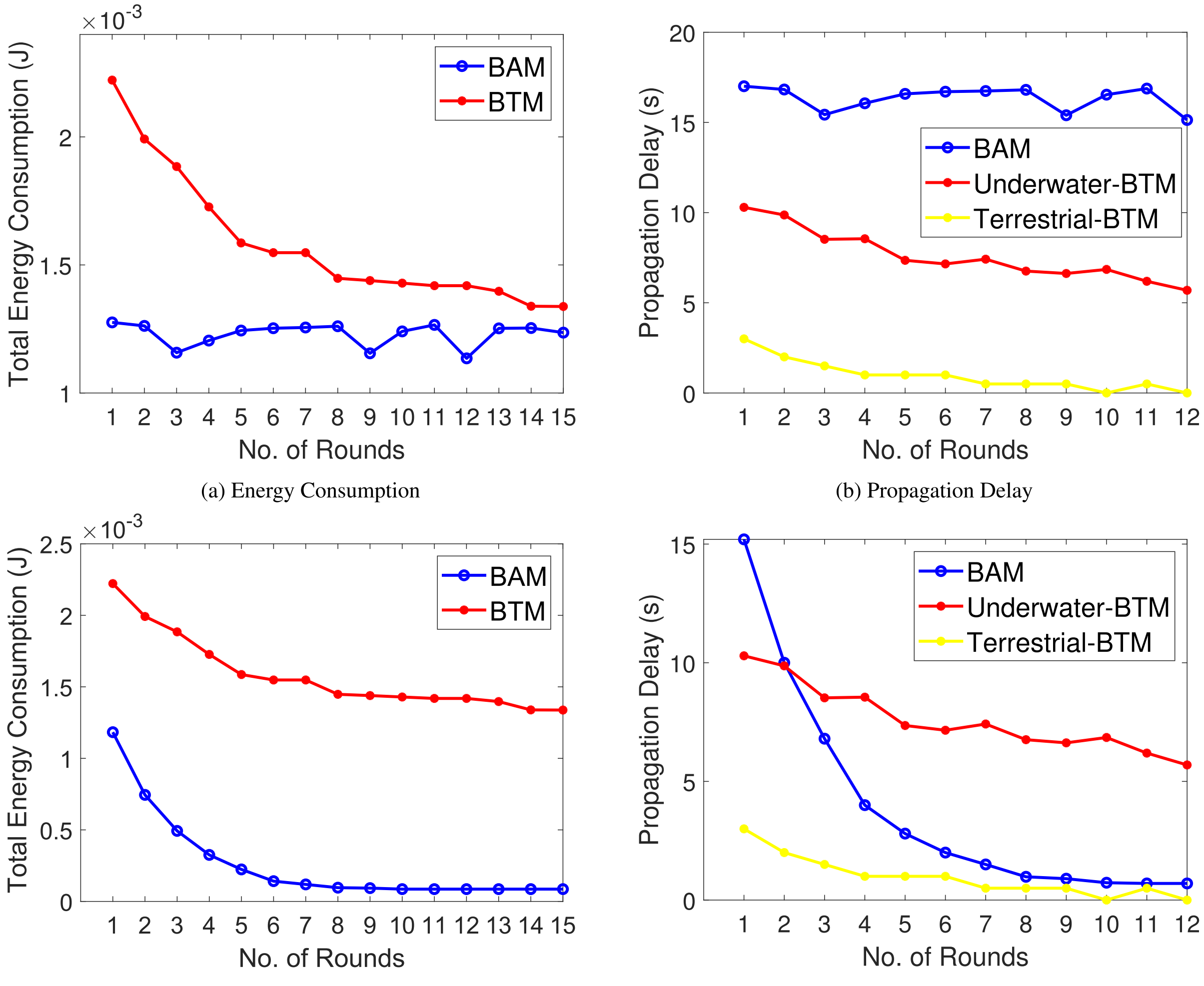
In this section, simulation results of the proposed BAM are discussed and compared with BTM [12] to evaluate the feasibility of the proposed scheme. BTM is designed for the terrestrial sensor networks while we have implemented it in IoUT networks because according to our knowledge, no scheme works with blockchain in underwater scenarios. It is used in our work according to IoUT network's requirements to evaluate BAM's working. Also, BTM is simulated for the terrestrial network. Moreover, in BTM, the malicious nodes are detected and revoked based on their performance metrics. In contrast, in our model, suspected malicious nodes are allowed to communicate even after being detected as malicious. However, the communication is controlled with AIMD. Additionally, the implementation of BTM in IoUT networks needs to change the basic parameters for compatibility. The blockchain model is simulated using Remix IDE, MetaMask



(a) Transaction Cost

(b) Execution Cost

FIGURE 4. **Gas consumption.**



(a) Energy Consumption

(b) Propagation Delay

(c) Energy Consumption

(d) Propagation Delay

FIGURE 5. **(a), (b) Complete revocation - (c), (d) Partial revocation.**

and Ganache. The Solidity programming language is used to write smart contracts. Besides, malicious node detection and revocation, AIMD, weighted recovery mechanism and attacker model are implemented in MATLAB. All the simulations are performed on a core i5, 7th generation machine comprising 2.3 GHz processor and 8 GB RAM. For a given

TABLE 3. Consumption of Gas.

Cost Name	Scheme	C1	C2	C3	C4	C5	C6
Transaction Cost	BTM	405984	-	99023	152764	19991	-
	BAM	612622	128111	84373	27387	18602	77797
Execution Cost	BTM	265312	-	88237	3651	18709	-
	BAM	431442	106455	62013	5923	18001	56525

Note: C1, C2, C3, C4, C5 and C6 denote Deployment, Registration, Sign in, Call sensor, Delete and Results, respectively.

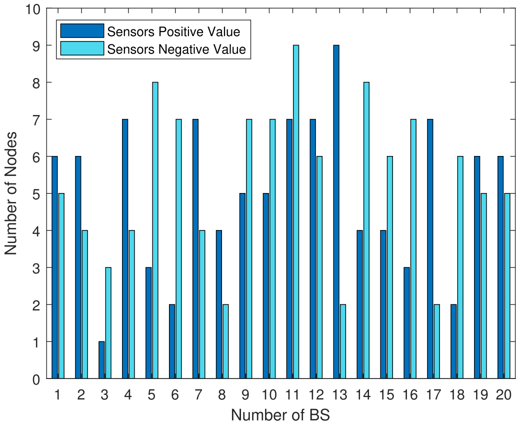


FIGURE 6. Ratio of legitimate and malicious nodes.

scenario, 225 sensor nodes, 20 BSs and 5 SNs are deployed in the field of 500 × 500 m^2. BSs and SNs are deployed at fixed positions while sensor nodes are deployed randomly. Sensor nodes are associated with BSs based on the communication range. The energy of each sensor node is 0.5 J while SNs and BSs have no energy constraints.

Figs. 4a and 4b depict the transaction and execution costs of BAM and BTM. The gas incurred for the deployment of the smart contract in BAM is more than that incurred in BTM. While, the gas consumption of Sign In, Call Sensor and Delete functions is more in BTM than in BAM. From the figures, it is visualized that the gas consumption of Registration and Result is zero in BTM. The reason is that these two functions are not involved in BTM.

Furthermore, the execution and transaction costs in terms of gas consumption are given in Table 3. The transaction and execution costs for C2 (registration) and C6 (results) are not considered for BTM because BTM does not have these mechanisms. Moreover, the gas consumption for C2 is higher because in the registration process, registration data is collected and stored, which consumes high resources. While the cost of C3 (Sign in) is low. It is because in Sign in only the comparison of hashes with the already stored hashes is performed. If the hashes match, the node is allowed to access the system. Similarly, in C4 (Call sensor) and C5(Delete), transaction and execution cost are less because in these functions, simple operations of calling a sensor and deleting the data are performed, respectively. In C6, the results are being displayed and analyzed, if required. Therefore, the cost is high. Furthermore, the malicious node detection is performed by directly comparing the data packets of nodes with the aggregated result.

Fig. 5a shows the total energy consumption for each round for both BAM and BTM. The uncertainty of the blue line shows that AIMD algorithm revokes the malicious nodes. In BAM, less energy is consumed at the third, ninth and twelfth rounds. It is because malicious nodes' energy consumption is not included. Moreover, in the rounds following the aforementioned rounds, some sensor nodes are reinstated and again allowed to communicate; therefore, the total energy consumption is increased. While in BTM, the red line shows continuous decreasing behaviour due to the permanent revocation of malicious nodes in every iteration. In Fig. 5a, the total propagation delay of the network is shown. In the third communication round, a sudden drop in the blue line is observed because many malicious nodes are detected. Similarly, sudden drops are observed at ninth and twelfth rounds. Whereas, from the fourth to sixth round, a stable blue line is observed due to the stability of the majority of sensor nodes. During this interval, the sensors provide correct data to BS. However, both underwater and terrestrial BTM schemes' red lines show that the malicious nodes are revoked continuously. Moreover, the propagation delay of BAM is higher than BTM because in BAM, when the node is reinstated in its normal state after some time, its propagation delay is re-added to the total propagation delay. Therefore, the total propagation delay of the network remains almost the same even after detecting malicious nodes.

Fig. 5c shows the energy consumption of the whole network while performing a partial revocation of malicious nodes by deleting their credentials from the blockchain in both schemes (BAM and BTM). This process of deleting the credentials is executed for many communication rounds to acquire the total energy consumption of all sensor nodes. Fig. 5d shows the propagation delay for the partial revocation of malicious nodes. The total delay of the malicious nodes is decreased at each communication round for BAM. The results are shown for 15 communication rounds in Figs. 5a and 5c, and for 12 communication rounds in Figs. 5b and 5d to show the effectiveness of BAM as compared to BTM in a better way.

TABLE 4. Feature comparison.

Ref No.	F1	F2	F3	F4	F5
[12]	×	×	✓	×	×
[13]	×	×	✓	×	×
BAM	✓	✓	✓	✓	✓

Note: F1, F2, F3, F4 and F5 denote Authentication, Privacy, Malicious Node Detection, Weight Recovery and Traffic Rate, respectively.

Fig. 6 shows the ratio of malicious and legitimate nodes for different rounds of communication against every BS. Table 4 shows a feature comparison of BAM with different benchmark trust models. In the first column, references are mentioned while the following columns consist of different features, labeled from F1-F5, where F1-F5 represents Authentication, Privacy, Malicious Node detection, Weight Recovery and Traffic Rate, respectively.

V. ATTACKER MODEL: DENIAL OF SERVICE

A DoS attack occurs by sending data packets to the destination in order to limit the response capability. In terrestrial WSNs, the DoS attack is widespread because many sensor nodes are deployed in very harsh and unattended environments and can easily be compromised by attackers. While an IoUT network operates in even more unattended environment. Therefore, attackers can perform this attack easily [27]. However, as discussed in Subsection III-B3, the proposed system detects the malicious nodes based on aggregated data. It detects the DoS attack in 5-10 data packets. The system then revokes the sensor node partially in the first stage. Moreover, AIMD mechanism reduces the data rate multiplicatively, as discussed in Subsection III-B4. The data rate of the node does not increase if it keeps on showing malicious behaviour. When the sensor node continuously shows malicious behaviour, its weight is further decreased and is completely revoked from the network.

VI. INFORMAL SECURITY ANALYSIS

To analyze the proposed BAM mechanism, three security concerns are analyzed.

A. LEMMA 1: THE PRIVACY IS PRESERVED; SO, IMPERSONATION ATTACK AND SYBIL ATTACK ARE NOT POSSIBLE

1) PROOF

Privacy leakage is one of the main issues in network communication. Therefore, we analyze our architecture critically to show whether it preserves privacy or not. In Subsection III-B1, it is discussed that how the credentials of sensor nodes are stored in the blockchain while simultaneously maintaining their privacy. The sensor node encrypts its credentials with BS_{enc} and sends the encrypted data to BS as Reg_{req}. BS receives Reg_{req} and decrypts it with BS_{dec}. Then, BS adds L_{BS} and encrypts it with the MA_{enc}. MA decrypts this cipher text with MA_{dec}. MA checks the authenticity of the sensor node by comparing these credentials with already stored data in its database. In this way, MA verifies the sensor node's existence along with adopting the hash format for storing the credentials on the blockchain. Hence, sensor nodes' privacy is preserved during the authentication process. So, impersonation and sybil attacks are not possible as credentials of nodes are encrypted and hashed. Moreover, the data is aggregated through WTE mechanism; so, it does not contain any particular information about the source node. Hence, during communication, privacy is preserved.

B. LEMMA 2: SNs AND BSs ARE SECURE AGAINST THE ATTACKS

1) PROOF

BSs and SNs are sensitive nodes in WSNs because they perform different duties in the network, such as aggregation of data, localization and reputation calculation. Therefore, attackers are more intended to attack these nodes. In our network, the blockchain is deployed on SNs to provide a privacy preserving authentication mechanism in which the credentials of sensor nodes are stored in hashed form. Therefore, attackers are unable to misuse the transparency feature of the blockchain. They misuse transparency by retrieving the location of nodes to physically access them. So, sybil and impersonation attacks are challenging to perform. Moreover, blockchain is tamper resistant because blocks are chained through hashes. Therefore, the attackers have to perform a 51% attack to compromise the blockchain, which is almost impossible in real-time scenarios. However, due to the unattended environment, managing the bandwidth for the network is challenging. BAM tackles the excessive bandwidth consumption problem through AIMD algorithm.

C. LEMMA 3: DATA CREDIBILITY IS ACHIEVED

1) PROOF

Data credibility is usually compromised in multi-hop communication because data is more likely to be attacked by the man in the middle. Whereas, in BAM, sensor nodes are directly connected to BS and the data is collected at BSs. To alter the data stored in blockchain is almost impossible because of its distributed nature. Moreover, the data submitted to the blockchain is aggregated. It is ensured by WTE that aggregated data, which is provided the majority nodes. Therefore, it is impossible to misguide the network with the wrong data. Hence, BAM ensures the credibility of data.

VII. CONCLUSION

To achieve privacy enabled authentication in IoUT networks, the blockchain technology is deployed in the underlying work. The registration of sensor nodes is performed for authentication and their credentials are hashed to store in blockchain anonymously. These stored records are used for the revocation of the malicious nodes upon their detection. However, there are chances that a sensor node sends incorrect data due to some technical faults like destructive interference effects. So, BAM revokes the sensor node partially and allows it to communicate under intensive observation. WTE algorithm checks the data packets of the sensor node and compares them with the aggregated data. If the sensor node behaves normally, its data rate increases additively. Otherwise, the data rate decreases multiplicatively using AIMD. In case of normal behaviour, the system recovers the sensor node's weight using the weight recovery algorithm. The simulation results show that our scheme achieves the objective of partial revocation. Moreover, gas consumption of BAM is higher than BTM because it has multiple functions to achieve authentication. Moreover, total propagation delay and total energy consumption is analyzed to evaluate the effectiveness of our model. In the future, we plan to enhance the efficiency of malicious node detection mechanism by using machine learning techniques. The expensive data storage issue is significant enough to be tackled in the sensor networks. Moreover, we will work on the location based storage mechanism.

REFERENCES

[1] C. Nunez. Find Out About the World's Ocean Habitats and More. Environment. National Geographic. Accessed: Oct. 5, 2021. [Online]. Available: https://www.nationalgeographic.com/environment/article/ocean

[2] S. Jiang, "On securing underwater acoustic networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 729–752, 1st Quart., 2019.

[3] Q. Fan, J. Chen, L. J. Deborah, and M. Luo, "A secure and efficient authentication and data sharing scheme for Internet of Things based on blockchain," *J. Syst. Archit.*, vol. 117, Aug. 2021, Art. no. 102112, doi: 10.1016/j.sysarc.2021.102112.

[4] A. K. Das, "A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks," *Peer-to-Peer Netw. Appl.*, vol. 9, no. 1, pp. 223–244, Jan. 2016.

[5] H. Xu, X. Qiu, W. Zhang, K. Liu, S. Liu, and W. Chen, "Privacy-preserving incentive mechanism for multi-leader multi-follower IoT-edge computing market: A reinforcement learning approach," *J. Syst. Archit.*, vol. 114, Mar. 2021, Art. no. 101932, doi: 10.1016/j.sysarc.2020.101932.

[6] P. Kumar, G. P. Gupta, and R. Tripathi, "TP2SF: A trustworthy privacy-preserving secured framework for sustainable smart cities by leveraging blockchain and machine learning," *J. Syst. Archit.*, vol. 115, May 2021, Art. no. 101954, doi: 10.1016/j.sysarc.2020.101954.

[7] K. Li, W. F. Lau, M. H. Au, I. W.-H. Ho, and Y. Wang, "Efficient message authentication with revocation transparency using blockchain for vehicular networks," *Comput. Electr. Eng.*, vol. 86, Sep. 2020, Art. no. 106721, doi: 10.1016/j.compeleceng.2020.106721.

[8] O. Samuel, N. Javaid, A. Almogren, M. U. Javed, U. Qasim, and A. Radwan, "A secure energy trading system for electric vehicles in smart communities using blockchain," *Sustain. Cities Soc.*, vol. 79, Apr. 2022, Art. no. 103678.

[9] S. S. Panda, D. Jena, B. K. Mohanta, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, "Authentication and key management in distributed IoT using blockchain technology," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12947–12954, Aug. 2021, doi: 10.1109/JIOT.2021.3063806.

[10] Z. Abubaker, N. Javaid, A. Almogren, M. Akbar, M. Zuair, and J. Ben-Othman, "Blockchained service provisioning and malicious node detection via federated learning in scalable Internet of Sensor things networks," *Comput. Netw.*, vol. 204, Feb. 2022, Art. no. 108691.

[11] A. S. Yahaya, N. Javaid, M. U. Javed, A. Almogren, and A. Radwan, "Blockchain-based secure energy trading with mutual verifiable fairness in a smart community," *IEEE Trans. Ind. Informat.*, vol. 18, no. 11, pp. 7412–7422, Nov. 2022.

[12] W. She, Q. Liu, Z. Tian, J.-S. Chen, B. Wang, and W. Liu, "Blockchain trust model for malicious node detection in wireless sensor networks," *IEEE Access*, vol. 7, pp. 38947–38956, 2019.

[13] T.-H. Kim, R. Goyat, M. K. Rai, G. Kumar, W. J. Buchanan, R. Saha, and R. Thomas, "A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks," *IEEE Access*, vol. 7, pp. 184133–184144, 2019.

[14] J. Li, S. Hu, Y. Shi, and C. Zhang, "A blockchain-based trustable framework for IoT data storage and access," in *Proc. Int. Conf. Blockchain Trustworthy Syst.* Singapore: Springer, 2019, pp. 336–349.

[15] H. Hu, Y. Chen, W.-S. Ku, Z. Su, and C.-H. J. Chen, "Weighted trust evaluation-based malicious node detection for wireless sensor networks," *Int. J. Inf. Comput. Secur.*, vol. 3, no. 2, 2009, pp. 132–149.

[16] Y. R. Yang and S. S. Lam, "General AIMD congestion control," in *Proc. Int. Conf. Netw. Protocols*, 2000, pp. 187–198, doi: 10.1109/ICNP.2000.896303.

[17] A. Berentsen, *Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto* (21st Century Economics). Cham, Switzerland: Springer, 2019, pp. 7–8.

[18] M. U. Javed, N. Javaid, M. W. Malik, M. Akbar, O. Samuel, A. S. Yahaya, and J. B. Othman, "Blockchain based secure, efficient and coordinated energy trading and data sharing between electric vehicles," *Cluster Comput.*, vol. 25, no. 3, pp. 1839–1867, Jun. 2022.

[19] S. Abbas, N. Javaid, A. Almogren, S. M. Gulfam, A. Ahmed, and A. Radwan, "Securing genetic algorithm enabled SDN routing for blockchain based Internet of Things," *IEEE Access*, vol. 9, pp. 139739–139754, 2021.

[20] N. Goyal, M. Dave, and A. K. Verma, "SAPDA: Secure authentication with protected data aggregation scheme for improving QoS in scalable and survivable UWSNs," *Wireless Pers. Commun.*, vol. 113, no. 1, pp. 1–15, Jul. 2020, doi: 10.1007/s11277-020-07175-8.

[21] S. Zhang, X. Du, and X. Liu, "A secure remote mutual authentication scheme based on chaotic map for underwater acoustic networks," *IEEE Access*, vol. 8, pp. 48285–48298, 2020.

[22] H. Guangjie, J. Jiang, L. Shu, and M. Guizani, "An attack-resistant trust model based on multidimensional trust metrics in underwater acoustic sensor network," *IEEE Trans. Mobile Comput.*, vol. 14, no. 12, pp. 2447–2459, Dec. 2015.

[23] U. Jain and M. Hussain, "Security mechanism for maritime territory and frontier surveillance in naval operations using wireless sensor networks," *Concurrency Comput., Pract. Exper.*, vol. 33, no. 17, p. e6300, 2021.

[24] K. Vani and S. S. Manvi, "Trusted node selection in clusters for underwater wireless acoustic sensor networks using fuzzy logic," *Phys. Commun.*, vol. 47, Aug. 2021, Art. no. 101388, doi: 10.1016/j.phycom.2021.101388.

[25] R. Muthukkumar and D. Manimegalai, "Secured transmission using trust strategy-based dynamic Bayesian game in underwater acoustic sensor networks," *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 2, pp. 2585–2600, 2021.

[26] B. Ahmad, W. Jian, R. N. Enam, and A. Abbas, "Classification of DoS attacks in smart underwater wireless sensor network," *Wireless Pers. Commun.*, vol. 116, no. 2, pp. 1055–1069, 2021.

[27] Md. A. Uddin, A. Stranieri, I. Gondal, and V. Balasurbramanian, "A lightweight blockchain based framework for underwater IoT," *Electronics*, vol. 8, no. 12, p. 1552, 2019, doi: 10.3390/s19040970.

[28] Q. Zhenquan, J. Ye, J. Meng, B. Lu, and L. Wang, "Privacy-preserving blockchain-based federated learning for marine Internet of Things," *IEEE Trans. Computat. Social Syst.*, vol. 9, no. 1, pp. 159–173, Feb. 2021, doi: 10.1109/TCSS.2021.3100258.

[29] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, Jun. 2019.

[30] U. Javaid, M. N. Aman, and B. Sikdar, "A scalable protocol for driving trust management in Internet of Vehicles with blockchain," *IEEE Internet Things J.*, vol. 7, no. 12, pp. 11815–11829, Dec. 2020, doi: 10.1109/JIOT.2020.3002711.

[31] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2017.

[32] J. Anish, G. S. Aujla, N. Kumar, and M. Villari, "GUARDIAN: Blockchain-based secure demand response management in smart grid system," *IEEE Trans. Services Comput.*, vol. 13, no. 4, pp. 613–624, Jul. 2019.

[33] A. Shahid, A. Almogren, N. Javaid, F. A. Al-Zahrani, M. Zuair, and M. Alam, "Blockchain-based agri-food supply chain: A complete solution," *IEEE Access*, vol. 8, pp. 69230–69243, 2020.

[34] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-based medical records secure storage and medical service framework," *J. Med. Syst.*, vol. 43, no. 1, pp. 1–9, Jan. 2019, doi: 10.1007/s10916-018-1121-4.

[35] T. Sait and J.-I. Toriwaki, "New algorithms for Euclidean distance transformation of an N-dimensional digitized picture with applications," *Pattern Recognit.*, vol. 27, no. 11, pp. 1551–1565, 1994.

[36] G. Wang, T. Wang, W. Jia, M. Guo, H.-H. Chen, and M. Guizani, "Local update-based routing protocol in wireless sensor networks with mobile sinks," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2007, pp. 3094–3099, doi: 10.1109/ICC.2007.514.

[37] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A traceable blockchain-based access authentication system with privacy preservation in VANETs," *IEEE Access*, vol. 7, pp. 117716–117726, 2019, doi: 10.1109/ACCESS.2019.2936575.

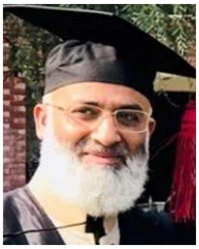
[38] D.-M. Chiu and R. Jain, "Analysis of the increase and decrease algorithms for congestion avoidance in computer networks," *Comput. Netw. ISDN Syst.*, vol. 17, no. 1, pp. 1–14, Jun. 1989, doi: 10.1016/0169-7552(89)90019-6.

SHAHID ABBAS (Member, IEEE) received the bachelor's degree in telecommunication and networking from the COMSATS Institute of Information and Technology, Attock Campus, in 2017, and the M.S. degree in computer science from the Communication Over Sensors (ComSens) Research Laboratory under the supervision of Prof. Nadeem Javaid. His research interests include blockchain in the Internet of Things, the Internet of Vehicular Networks, and wireless sensor networks.

HINA NASIR received the bachelor's degree in information and communication systems engineering from the NUST School of Electrical Engineering and Computer Science (SEECS), in 2008, the M.S. degree in computer science from the International Islamic University (IIUI), in 2015, and the Ph.D. degree in computer science under the supervision of Prof. Nadeem Javaid. She is currently serving as an Assistant Professor with the Department of Computer Science, Air University, Islamabad. Her research interests include wireless sensor networks, underwater wireless sensor networks, cooperative communication, cooperative routing, buffer-aided cooperative communication, energy harvesting in wireless networks, 5G networks, and the Internet of Things.

AHMAD ALMOGREN (Senior Member, IEEE) received the Ph.D. degree in computer science from Southern Methodist University, Dallas, TX, USA, in 2002. He is currently a Professor with the Computer Science Department, College of Computer and Information Sciences (CCIS), King Saud University (KSU), Riyadh, Saudi Arabia, where he is also the Director of the Cyber Security Chair, CCIS. Previously, he worked as the Vice Dean of the Development and Quality at CCIS. He also worked as the Dean of the College of Computer and Information Sciences and the Head of the Academic Accreditation Council, Al Yamamah University. His research interests include mobile-pervasive computing and cyber security. He served as the General Chair for the IEEE Smart World Symposium and a Technical Program Committee Member of numerous international conferences/workshops, such as IEEE CCNC, ACM BodyNets, and IEEE HPCC.

AYMAN ALTAMEEM received the Ph.D. degree in information technology from the University of Bradford, U.K., and the M.Sc. degree in information systems from London South Bank University, U.K. He is currently an Associate Professor with the College of Applied Studies, King Saud University, Riyadh, Saudi Arabia. His research interests include the Internet of Things, cloud computing, and artificial intelligence.



NADEEM JAVAID (Senior Member, IEEE) received the bachelor's degree in computer science from Gomal University, Dera Ismail Khan, Pakistan, in 1995, the master's degree in electronics from Quaid-i-Azam University, Islamabad, Pakistan, in 1999, and the Ph.D. degree from the University of Paris-Est, France, in 2010. He is currently working as a Professor and the Founding Director of the Communications Over Sensors (ComSens) Research Laboratory, Department of Computer Science, COMSATS University Islamabad, Islamabad Campus. He is also working as a Visiting Professor with the School of Computer Science, University of Technology Sydney, Australia. He has supervised 158 master's and 30 Ph.D. theses. He has authored over 900 articles in technical journals and international conferences along with three edited books. His research interests include energy optimization in smart/microgrids and in wireless sensor networks using data analytics and blockchain. He was a recipient of the Best University Teacher Award (BUTA'16) from the Higher Education Commission (HEC) of Pakistan, in 2016, and the Research Productivity Award (RPA'17) from the Pakistan Council for Science and Technology (PCST), in 2017. He is an Associate Editor of IEEE Access and an Editor of Sustainable Cities and Society journals.