IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received 8 February 2023, accepted 2 March 2023, date of publication 21 March 2023, date of current version 30 March 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3259982

RESEARCH ARTICLE

A Blockchain-Based Deep-Learning-Driven Architecture for Quality Routing in Wireless Sensor Networks

ZAHOOR ALI KHAN[1], (Senior Member, IEEE), SANA AMJAD[2], FARWA AHMED[3], ABDULLAH M. ALMASOUD[4], MUHAMMAD IMRAN[5], (Senior Member, IEEE), AND NADEEM JAVAID[2], (Senior Member, IEEE)

[1]Department of Computer Information Science, Higher Colleges of Technology, Fujairah, United Arab Emirates
[2]Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan
[3]Department of Aerospace, Mechanical and Electronics Engineering, South East Technical University, Waterford, X91 K0EK Ireland
[4]Department of Electrical Engineering, College of Engineering, Prince Sattam bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
[5]School of Engineering, Information Technology and Physical Sciences, Federation University, Brisbane, QLD 4000, Australia

Corresponding authors: Zahoor Ali Khan (zkhan1@hct.ac.ae) and Abdullah M. Almasoud (am.almasoud@psau.edu.sa)

This work was supported by the Deputyship for Research and Innovation, Ministry of Education, Saudi Arabia, under Project IF-PSAU-2021/01/19156.

ABSTRACT Over the past few years, great importance has been given to wireless sensor networks (WSNs) as they play a significant role in facilitating the world with daily life services like healthcare, military, social products, etc. However, heterogeneous nature of WSNs makes them prone to various attacks, which results in low throughput, and high network delay and high energy consumption. In the WSNs, routing is performed using different routing protocols like low-energy adaptive clustering hierarchy (LEACH), heterogeneous gateway-based energy-aware multi-hop routing (HMGEAR), etc. In such protocols, some nodes in the network may perform malicious activities. Therefore, four deep learning (DL) techniques and a real-time message content validation (RMCV) scheme based on blockchain are used in the proposed network for the detection of malicious nodes (MNs). Moreover, to analyse the routing data in the WSN, DL models are trained on a state-of-the-art dataset generated from LEACH, known as WSN-DS 2016. The WSN contains three types of nodes: sensor nodes, cluster heads (CHs) and the base station (BS). The CHs after aggregating the data received from the sensor nodes, send it towards the BS. Furthermore, to overcome the single point of failure issue, a decentralized blockchain is deployed on CHs and BS. Additionally, MNs are removed from the network using RMCV and DL techniques. Moreover, legitimate nodes (LNs) are registered in the blockchain network using proof-of-authority consensus protocol. The protocol outperforms proof-of-work in terms of computational cost. Later, routing is performed between the LNs using different routing protocols and the results are compared with original LEACH and HMGEAR protocols. The results show that the accuracy of GRU is 97%, LSTM is 96%, CNN is 92% and ANN is 90%. Throughput, delay and the death of the first node are computed for LEACH, LEACH with DL, LEACH with RMCV, HMGEAR, HMGEAR with DL and HMGEAR with RMCV. Moreover, Oyente is used to perform the formal security analysis of the designed smart contract. The analysis shows that blockchain network is resilient against vulnerabilities.

INDEX TERMS ANN, CNN, LSTM, GRU, HMGEAR, LEACH, malicious nodes' detection, blockchain.

I. INTRODUCTION

The wireless sensor networks (WSNs) play a key part in modern era [1], [2], [3]. They acquire data from the surrounding environment and use it for different purposes in different areas like healthcare, smart cities, military, etc. The sensor nodes send the data towards destination without any human involvement in the WSNs, after sensing it from the surrounding environment [4]. The data is sent using different communication protocols [5], [6], [7], [8]. Hence, in the

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

WSNs, the sensor nodes play a vital role [9]. However, they have limited storage space and are resource constrained devices [10]. Moreover, the sensor nodes do not generate energy on their own. Therefore, they easily get tampered by the attackers [11], [12].

Blockchain is a promising technology, which was introduced by Satoshi Nakamoto in 2008 [2]. This technology addresses the data security and third party involvement issues. The blockchain is not only used as a cryptocurrency, but it is also used in various other fields like healthcare [13], manufacturing, smart cities, etc., [14], [15]. It provides a distributed ledger in which records are added through consensus mechanism after performing the validation process. Moreover, it makes the records more secure without the need of a third party and resolves the issue of single point of failure. In addition, blockchain serves in the field of WSNs. The blockchain works as a storage mechanism and provides data security as the sensor nodes are resource constrained. It also works for ensuring nodes' privacy and authentication, non-repudiation as well as performing efficient and secure routing [16], [17].

In WSNs, nodes' communication is an important part for sending the data from source to destination. In some cases, the sensor nodes send the data to cluster heads (CHs) and CHs send it to the base station (BS). The CHs manage the sensed data which also work both as relaying nodes and sensor nodes. Due to the resource constrained nature of WSN, the network becomes prone to different types of attacks [18]. In [19], CHs send the data to a BS. However, no mechanism is used in the network for detecting the malevolent activities. Consequently, malicious activities can be performed by a malicious node (MN) that can easily enter the network and become a part of it. Moreover, in [20], the network consists of two types of nodes that are core nodes and edge nodes. In the Internet of things (IoT), devices send the transactions' request to the edge nodes. The edge nodes forward the request to the core nodes. The core nodes work as miners and use proof-of-work (PoW) during mining process. However, PoW incurs a lot of computational cost. Besides, 5G is integrated with blockchain in IoT applications for securing the industrial IoT applications [21], [22], [23].

The structuring of the remaining manuscript is done in the following manner. Section I presents introduction while the subject matter of Section II is the related work. Section III provides the problem statement while the discussion of the system model proposed in this work is given in Section IV. Moving ahead, the model's extensive evaluation is provided in Section V while the security analysis is the subject matter of Section VI. Finally, the paper is concluded in Section VII.

A. CONTRIBUTIONS

To address the mentioned problems, the following contributions are made in the proposed work.

- Deep learning (DL) models and real-time message content validation (RMCV) [24] are used for the detection of MNs in the network.
- The issue of high computational overhead of the network is solved using proof-of-authority (PoA) consensus mechanism.
- The model's robustness against different vulnerabilities is shown via security analysis performed using Oyente.

B. NOMENCLATURE

ANN	Artificial neural network
BS	Base station
CH	Cluster head
CNN	Convolutional neural network
DL	Deep learning
FPR	False-positive-rate
GRU	Gradient recurrent unit
HMGEAR	Heterogeneous gateway-based energy-aware multi-hop routing
ID	Identity
IoT	Internet of things
LEACH	Low-energy adaptive clustering hierarchy
LN	Legitimate node
LSTM	Long short term memory
MN	Malicious node
MND	Malicious nodes' detection
PoA	Proof-of-authority
PoW	Proof-of-work
RMCV	Real-time message content validation
SDN	Software defined networking
SPOF	Single point of failure
TPR	True-positive-rate
WSN	Wireless sensor network

II. RELATED WORK

In this section, the studies relevant to our proposed work are discussed. In [25], authors address the existence of MNs in WSNs. Machine learning and DL techniques are used to classify the nodes. Machine learning techniques are compared with DL model and a comparative analysis is performed. In [26], the authors address heterogeneity in IoT, which is prone to various kinds of cyber attacks. Also, the IoT nodes are resource constrained. To solve the security issue, the authors propose a software defined networking (SDN)-enabled DL architecture. The SDN controllers are trained based on the dataset, termed as CICDDoS2019, and are used to prevent intrusions from external attacks. The usage of DL techniques achieves high accuracy and minimum false-positive-rate (FPR). In [24], the authors address the issue of authentication protocols that are used for the verification of a message's origin. However, the authentication protocols fail to verify the integrity of messages. Therefore, a novel trust model is proposed, which verifies the message content, integrity, trustiness and the path a message follows from source to destination.

In [27], the authors address the issues that are caused when IoT devices are compromised through different cyber attacks. Besides, due to resource constrained nodes, centralized platforms are used for storage systems. However, the usage of the central authority causes a single point of failure (SPOF) issue. Therefore, the authors propose a blockchain based SDN architecture that controls the IoT devices and detects the cyber attacks being performed on the network. The blockchain solves the issue of SPOF and provides security as well as privacy against attacks.

In [28], the authors address data loss and data security issues in IoT environment. Moreover, the IoT applications used in different fields like healthcare, smart grid, transportation, etc., are merged with 5G technology to enhance the service quality. However, the data growth increases the concerns of data security and data loss. Therefore, a blockchain based DL technique is used, which is operated based on four layers: fog, cloud, user and edge. In [29], the blockchain is integrated with the SDN. Besides, the IoT ecosystems face various issues like increasing delay, lack of security, etc. Therefore, in this paper, authors propose a layered architecture of s smart network in which energy optimization, high throughput and minimum delay are achieved. Moreover, the routers and switches provide secure communication and optimal CH selection.

In [30], WSN is considered as an important part of the IoT network in which nodes send and receive services. Nodes' authentication is performed by the central authority due to which SPOF and trust issue arises. For that reason, an authentication mechanism is proposed that is based on hybrid blockchain. Also, the attacks' analysis is performed to check the network robustness. In [31], the localization of the network nodes is not performed and MNs give wrong locations. To tackle this issue, a trust management model is proposed that is based on blockchain. In this model, three types of trust are calculated, i.e., behavioral trust, feedback trust, and data trust. The behavioral trust is calculated based on the interactions between different nodes. Whereas, the data trust is evaluated directly and indirectly between beacon nodes. A threshold is set according to which ranges are decided for the nodes. The trusted nodes become the beacon nodes and find the location of unknown nodes. The blocks are created based on the nodes' ranking in the chain. The node having the highest trust value makes the genesis block. The trusted nodes in the network find the location of unknown nodes using trilaterational process.

In [32], no mechanism is proposed for identification of MNs in the WSN. Also, no traceability mechanism is proposed for MND. Therefore, authors propose a blockchain based trust model in which MND is performed. Also, the nodes' traceability is performed in the detection process. Three parameters, delayed transmission, response time and forwarding rate, are used to calculate the trust values of the nodes. The calculated values are stored in the blockchain, being deployed on the sink nodes. In the study, a quadrilateral measurement method is used to find unknown nodes' locations. This method finds the distance of unknown node from four known nodes. In this way, the nodes' locations are found and the information is broadcast in the network. Also, the neighbor nodes update their tables. Whereas, in [20], high latency, huge bandwidth and SPOF issues occur due to the increase in the number of nodes. Therefore, SDN based hybrid network architecture is proposed. In the study, the network has two types of nodes: core nodes and edge nodes. The SDN works as an interface between the core nodes and IoT nodes. All the SDNs working in the network make the edge network. To avoid the SPOF issue, a distributed network is used. To make the data secure, digital signatures are used and hashes are stored in the blockchain. Also, PoW is employed for the network security.

The dynamic behavior of sensors play an important role for the data collection. However, in [33], there exists a chance where an attack can be performed on the BS and the BS behaves maliciously in the key management process. Moreover, the clusters formed in the network are insecure. Therefore, a secure key management scheme based on blockchain is proposed in which the BS works as a key generator and distributes the keys to all the CHs. The CHs check the authenticity of the BS by its public key and signature. If it is verified, then it becomes a trusted entity. Otherwise, a message is broadcast that the BS is malicious. When the BS is verified successfully, then all the nodes' information is stored in the blockchain. Also, in clusters' formation, the CHs broadcast the message, and ordinary nodes join the CH based on their distances and signals. The ordinary nodes use the pairwise key generation mechanism when they select the CHs to join or leave the network.

In [34], the routing is performed by the sensor nodes. However, malicious nodes detection (MND) is not performed. Also, black hole attack may be performed in the network model. For that purpose, authors propose a secure reinforcement learning protocol based on the blockchain to select the secure route based on the number of successfully delivered data packets by a node. Also, Q-Learning is used to decide the forward routing nodes based on the number of maximum packets being delivered. The routing table of each node is stored and updated in the blockchain. It helps in removing MNs from the network that drop the packets. Moreover, a smart contract is used in the blockchain that removes the central authority issue. Moreover, in [35], the resource constrained sensing nodes are unable to perform the mining process in the blockchain. To eliminate the data storage issues, servers are used. Thus, data security may be compromised. Therefore, authors propose an information centric network for the decentralization of sensing nodes and for data security. The system model is composed of information centric plane and network plane. The sensor nodes forward the data gathered from the surrounding environment to the CHs that are on information centric plane. Moreover, CHs maintain cache for data storage. The blockchain is deployed on cloud,

TABLE 1. Related work.

Techniques	New achievements	Problems solved	Future problems
DL techniques [25]	Detection of different DoS attacks	Presence of MNs in WSNs	
SDN-enabled architecture leveraging hybrid DL [26]	Efficient detection of cyber threats and attacks	Resource constrained IoT devices	No storage mechanism, computationally expensive
Trust model [24]	Trustworthiness of messages	Authentication issue	Fail to verify message integrity
Blockchain-SDN based energy-aware architecture [27]	Energy saving, load balancing, increasing the network lifetime	Scalability, flexibility, complexity, monitoring, managing and collecting IoT data	N/A
Blockchain based security framework for intelligent 5G-enabled IoT [28]	Intelligent data analysis and data security	Breach and loss of sensitive data	Computational complexity
Layered architecture of smart network [29]	Energy optimization, high throughput, minimum delay	Inefficient communication and high end-to-end delay	Large scale integration not considered
Keccak hash function in a consortium blockchain based hybrid structure [30]	Energy consumption is analyzed	Node authentication, security issue, centralization	Validation of transactions in private blockchain
Trust management model [27]	Localization of network nodes	Wrong location information provided by MNs	Temporal complexity
Decentralized blockchain, public-key-infrastructure [32]	Reputation level of nodes	Security and privacy, consumption of energy	No proper evaluation parameters used
Blockchain key management scheme, pairwise key generation, key renewal mechanism [33]	Forward secrecy, backward secrecy, non repudiation attack	Untrusted behavior of nodes	N/A
Reinforcement learning protocol, Q-learning [34]	Selection of a secure route and forward routing nodes	Existence of MNs, improper detection of MNs	N/A
Information centric network [35]	Data security and decentralization of sensing nodes	Data storage, inefficient mining	Temporal complexity
Blockchain based routing protocol [36]	Packet delivery ratio, attacks (gray hole and black hole)	Ensured trust, mitigated effects of gray hole and black hole attacks	Not designed for temporary networks
Decentralized blockchain based authentication scheme [37]	Consumption of energy	Data privacy, untrusted nodes	N/A

where the mining is performed by the miners. The BS is used as a coordinator between the information centric plane and cloud. Furthermore, public key cryptography is used for both encryption and decryption.

In [36], a centralized authority is used for the authentication of IoT nodes. The grayhole and black hole attacks are possible in the IoT networks. Also, the routing overhead occurs due to the use of conventional routing protocols. Therefore, authors propose a blockchain based routing protocol in which routing nodes find the routes to reach the destination. The route establishment process is performed using the smart contract. Using the smart contract, each IoT node requests for the route discovery. The intermediary nodes listen to the request and offer the path towards destination. A token is used by the participating nodes to ensure packet forwarding. The request sender node accepts the offer and sends the packet to the intermediary nodes. The smart contract removes the route request and route reply packets, which overcome the routing overhead. The token process mitigates the grayhole and black hole attacks because if an MN drops a packet, it loses the tokens.

In [37], repudiation against the service provisioning problem occurs between a client and a service provider. For resolving the problem, an evidence storing mechanism is required. To overcome this issue, a secure non repudiation mechanism that is based on blockchain is proposed. The hash for a service is provided to the client through an on-chain mechanism while the service is provided through an off-chain mechanism. Also, the IoT client confirms the service that is provided by the blockchain. Moreover, a homomorphic hash function is used to generate hashes and provide them to the clients, which are further utilized to perform MND. The blockchain, as a whole, keeps records of all the clients to mitigate the repudiation.

III. PROBLEM STATEMENT

In the WSNs, sending data from source to destination via routing is considered an essential aspect. However, some nodes perform malicious activities by sending wrong information to the destination. Also, the network is prone to various types of attacks due to the distributed nature of the WSNs. In [19], CHs send the data towards BS. However, CHs do not use any mechanism for pointing out the malicious activities. Hence, any MN can enter the system. In [20], the network is presented that consists of two types of nodes: core nodes and edge nodes. The edge nodes receive transactions' request from IoT devices and send it to core nodes, who work as miners. PoW consensus mechanism is used for mining process. However, PoW consumes a lot of computational resources. Furthermore, for transferring the data between source and destination, a trusted routing path is required. However, in [30], the grayhole attack may be performed on the CHs, which deteriorates the CHs' performance.

IV. PROPOSED SYSTEM MODEL

This section describes the proposed system model and its components. Moreover, the dataset used for performing simulations is discussed. In the proposed model, RMCV and

DL models are used in the WSN for MND. Given dataset is based on WSN, and generated using the LEACH protocol. Moreover, both LEACH and heterogeneous gateway-based energy-aware multi-hop routing (HMGEAR) are used as benchmark techniques, which perform WSN routing and are not computationally expensive. Therefore, the proposed model accurately classifies all such nodes that depict the same behavior. The routing is performed both before and after MND using LEACH. Once MNs are detected and removed then routing is performed with both LEACH and HMGEAR protocols. Moreover, the computational overhead of the model is reduced using PoA consensus mechanism.

A. ASSUMPTIONS

In this section, the major assumption made in the system model is listed.

1) BS and CHs are LNs. These nodes are not able to perform maliciously.

B. PROPOSED ARCHITECTURE

We present a three-layered architecture, as shown in Fig 1. The middle layer is the blockchain enabled RMCV and DL network layer. Whereas, the first and the third are the WSN layers, comprising sensor nodes, CHs and BS. The BS and CHs are the nodes where blockchain is deployed. Moreover, ANN, CNN, long short term memory (LSTM), and gradient recurrent unit (GRU) are trained and tested on the LEACH protocol generated dataset, described in section IV-E. The nodes in the WSN perform routing using both LEACH and HMGEAR protocols. During routing, some nodes in the network may perform malicious activities. To minimize such activities in the network, the MNs are detected using the trained model and RMCV scheme. The nodes involved in the routing mechanism are classified using DL and RMCV techniques. Once classification is performed, the registration of LNs is done using PoA. While, routing is performed using LEACH and HMGEAR protocols after MND. The components of the proposed architecture are described in the following subsections.

1) BLOCKCHAIN NETWORK

The blockchain enabled RMCV and CNN detect the presence of MNs in the WSN. It is deployed on CHs and BS. After MND, the LNs are registered in the blockchain using the smart contract. The PoA consensus mechanism is used when LNs are registered in blockchain network.

2) WSN

The WSN is composed of N number of nodes that perform routing using LEACH and HMGEAR protocols. After data processing, the data is collected by the sensor nodes from the surrounding environment and sent towards the CHs for processing. Further data processing is performed by the CHs and the integrated data is sent towards BS. In the WSNs, some nodes may perform malicious activities and may send false messages to disturb the data traffic or drop the data packets. Therefore, MND is performed using RMCV and DL-driven architecture. RMCV calculates the nodes' trustworthiness, while on the other side, nodes' classification is performed by ANN, CNN, LSTM, and GRU. The MNs are removed from the network after being detected. While, routing is performed only between the LNs using LEACH and HMGEAR protocols.

C. ROUTING IN THE WSN

The routing in the WSNs, considered in this paper, is performed via LEACH protocol [39]. The sensor nodes send data to the CHs and CHs send aggregated data towards BS. In the WSNs, the nodes may perform malicious activities and may not send the data packets, drop the data packets or may perform an attack on the routing nodes. Therefore, the MNs are detected using RMCV and DL models. Furthermore, the LNs are registered in the blockchain and routing is performed again for the LNs using LEACH and HMGEAR protocols [38], [39]. The following steps present the detailed working of the proposed solution, also shown in Fig. 2.

1) *Network routing*: Initially, 100 number of nodes are deployed in the network comprising CHs and BS. The data is gathered by the sensor nodes from the surrounding environment and sent to the CHs for processing. To perform routing in the network, LEACH protocol is used. The CHs process the integrated data and send it towards the BS.
2) *MND*: In the WSNs, the MNs are detected using RMCV and DL models. The MNs are detected using both methods and is found that RMCV with LEACH and HMGEAR protocols perform better than DL. The network performance is checked both before and after the MND in terms of throughput, energy consumption and delay.
3) *RMCV*: The RMCV scheme detects the MNs in the WSNs. In the WSNs, the victim nodes may find the adversary messages sent by adversary nodes. The messages are evaluated based on their trustworthiness and integrity parameters, which are calculated by satisfying the following three conditions: message path, message conflict and message similarity. Each message contains a trust value and based on that trust value, the trust of each node is calculated. The nodes that send the maximum number of trusted messages are considered legitimate and trusted. While the nodes that send the minimum number of trusted messages are considered malicious and untrusted.
4) *Deep learning models*: The ANN, CNN, LSTM, and GRU are trained on a given dataset, WSN-DS 2016. ANN gives 90%, CNN gives 92%, LSTM gives 96%, and GRU gives 97% accuracy. The CNN model extracts the best features, which are used for classification. It is a multi layered architecture where the layers work well for feature extraction and classification purposes.

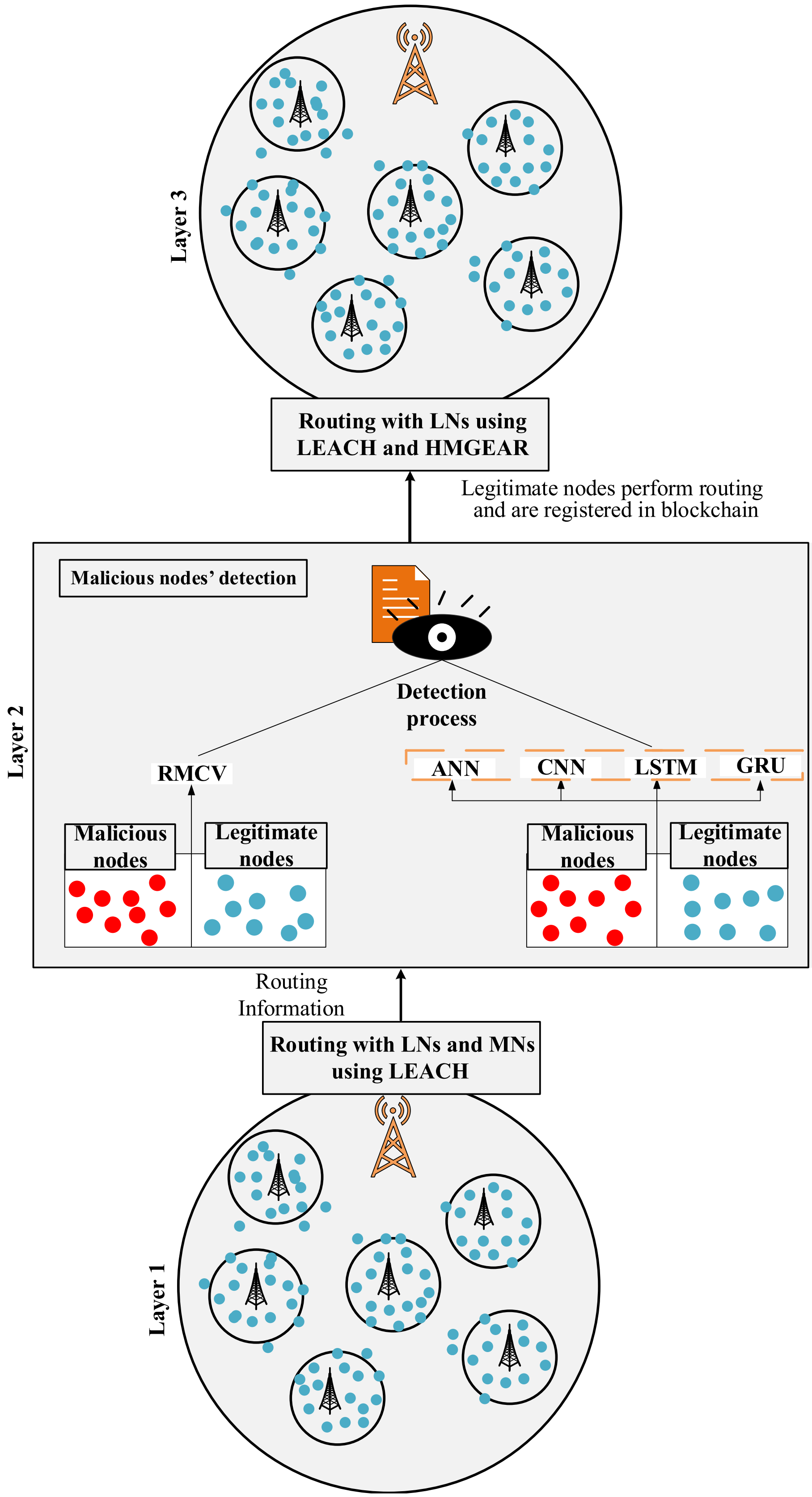


FIGURE 1. Newly proposed 3-layered system model.

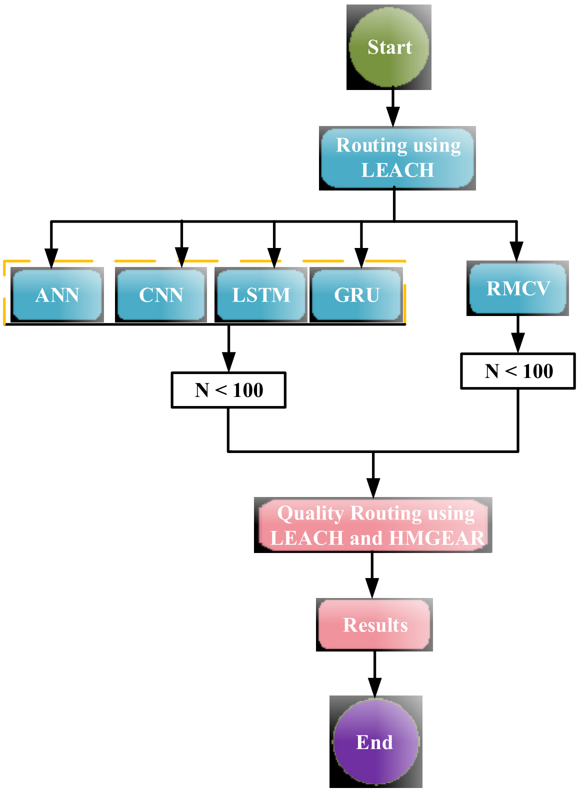


FIGURE 2. Working steps of the system model.

While the ANN contains only three layers: input, hidden, and output. The hidden layer processes the given input and forwards it to the fully connected neurons where the output is generated [40]. Therefore, CNN gives more accuracy than ANN. In the proposed work, LSTM is employed for classification purpose. The issue of gradient vanishing using explicit memory unit is also solved by LSTM. Moreover, anything can be memorized in LSTM using any weights. In this way, LSTM memorizes and performs better than the previous models. Also, in LSTM, the gated mechanism is used to store and pass the information to the next layer. Moreover, LSTM has another feature for smooth and uninterrupted flow of gradients during propagation, which is called constant error carousel. GRU works like LSTM as it uses gates for the information control. GRU is basically an updated version of LSTM having some improvements [41].

Pseudocode: Malicious nodes' detection

1. Routing = LEACH protocol
2. Routing data = load (Data.csv)
3. Data = Data.drop(['lable'])
4. label = label-encode (label)
5. Data = MinMaxScalar.fit_transform(Data) // Normalize
6. Data, label = SMOTE.fit_resample (Data, label) // Balance data
7. Data_Train, Data_Test, Label_Train, Label_Test = train_test_split (Data, label, test size = 0.30, random state=42) // Split data
8. Data_Train = reshape ()
9. Data_Test = reshape ()
10. ANN, CNN, LSTM, GRU // Apply models for classification
11. Results
12. MND = RMCV // Find the trust of nodes
13. LNs = Obtained by DL and RMCV
14. Quality Routing = LEACH-DL, LEACH-RMCV, HMGEAR-DL, HMGEAR-RMCV
15. Results

The information is transferred towards output using two vectors. These vectors decide which information should be passed to the output. To keep the information for a long time, these vectors are trained. However, GRU does not remove irrelevant information. As compared to LSTM, GRU has only one hidden cell state. Therefore, it is more quick to train as compared to LSTM [42]. GRU solves gradient vanishing problem using update and reset gate. If the gradient shrinks, then it back propagates over time and affects the learning, which makes the model untrainable.

GRU gives the advantage over LSTM as it uses less memory and works better than LSTM. GRU also works faster than LSTM. On the other side, the LSTM works better on the datasets having long sequences.

5) *Legitimate nodes*: After MNs are detected using RMCV and DL models, it is observed that the DL outperforms RMCV. DL models find the maximum MNs in the network and removes them. Moreover, the legitimate nodes (LNs) identified by DL models are registered in the blockchain network using a smart contract.

D. TRANSMISSION TIME AND ENERGY CALCULATION

In the proposed model, the time for transmission, in the t-th communication round, to the BS from the n-th client is given using Equation 1 [43].

$$\tau_n^{up}(t) = \frac{\gamma_n i_n(t)}{Blog_2(1 + \frac{P_n(t) h_n(t)}{BN_0})}, \tag{1}$$

where the system bandwidth, transmission power of the n-th node, noise power spectral density and the number of bits are given by n-th node are given by $B, P_n(t), N_0$ and γ_n. In addition, Equation 2 gives the energy consumed by the n-th node in the t-th communication round [43].

$$E_n^{up}(t) = \frac{P_n(t) \gamma_n i_n(t)}{Blog_2(1 + \frac{P_n(t) h_n(t)}{BN_0})}, \tag{2}$$

TABLE 2. The identified problems mapped with the probable solutions and the performed validations.

Identified problems	Proposed solutions	Validations
L1: No mechanism for MND [19]	S1: ANN, CNN, LSTM, GRU	V1: Loss
L2: Grayhole attack [30]	S2: RMCV	V2: Accuracy
		V3: TPR and FPR
		V4: Propagation delay
		V5: Throughput
		V6: Energy consumption
L3: Increased computational cost [20]	S3: PoA	V7: Average transaction cost

E. DATASET DESCRIPTION

The selection of suitable dataset, known as WSN-DS 2016, for sensor networks has been evaluated in [44] for MND. Many datasets are available for MND like KDD99, UNSW-NB15, CICIDS2017 [26], etc. However, these datasets lack the features relevant to our network. The dataset used in the proposed work is chosen because it has the best network flow features. This dataset is generated using the LEACH protocol in a WSN. It contains 19 features and 374662 instances. These instances and features are generated by 100 nodes. It is also a multiclass dataset, which includes one LNs' class and four attackers' classes. Generally, there are different DoS attacks that can be performed on a WSN. These attacks are grayhole, black hole, TDMA, and flooding.

V. SIMULATION RESULTS

The simulation results and their discussion is the subject matter of this section. The selection of a suitable dataset is made for the evaluation of first two limitations L1 and L2 as shown in Table 2. The network area is 100 x 100m^2, which consists of 100 nodes. The dataset is generated by 100 nodes that perform routing using LEACH protocol [39]. The DL models are trained on the given dataset to classify the maliciousness of the routing nodes.

Initially, the preprocessing of dataset is performed in which feature scaling or Min-Max normalization is performed to convert the values into binary (0,1) form and handle the missing values. Then synthetic minority over-sampling technique is used to balance the dataset. Afterwords, ANN, CNN, LSTM, and GRU are trained on the preprocessed dataset. Different performance parameters like accuracy, loss, true positive rate (TPR), FPR, and receiver operator characteristic (ROC), are used for the classification purpose. It is because these parameters are mostly used for the classification purpose as given in [46]. Moreover, RMCV is used to find the trust of routing nodes. Whenever RMCV is employed, the MNs are identified on the basis of their trust scores. The MNs are removed from the network and the simulations are performed using the LNs only. It is to be noted that the number of malicious and non malicious nodes vary from network to network. After finding LNs using RMCV and DL models, routing is performed using LEACH and HMGEAR protocols. In our proposed model, the number of LNs given by RMCV is 67 while the number of MNs is 33. Similarly, the number of LNs given by DL is 90 while the number of MNs is 10.

TABLE 3. Parameters' setting in CNN.

Parameters	Values
No. of convolutional layers	3
No. of maxpooling layers	2
No. of neurons	32, 64, 128
Types of activation functions	Sigmoid, linear, softmax
Loss function	Categorical crossentropy
Optimizer	Stochastic gradient descent
No. of epochs	30
Batch size	128

TABLE 4. Parameters' setting in ANN.

Parameters	Values
No. of dense layers	4
No. of neurons	64, 128, 64, 5
Types of activation functions	Sigmoid, linear, tanh, softmax
Loss function	Categorical crossentropy
Optimizer	Stochastic gradient descent
No. of epochs	30
Batch size	128

TABLE 5. Parameters' setting in GRU.

Parameters	Values
No. of dense layers	5
No. of neurons	100
Types of activation functions	Softmax
Loss function	Categorical crossentropy
Optimizer	Adam
No. of epochs	20
Batch size	256

Tables 3, 4, 5 and 6 show the learning parameters. These parameters control the learning process. From Table 3, it is observed that CNN has 3 convolutional layers and 2 max pooling layers. The number of neurons used in the first convolutional layers is 32, in the second layer is 64, and in the third layer is 128. Moreover, three types of activation functions are used.

The first convolutional layer uses sigmoid activation function, second layer uses linear function and third layer uses softmax function. Furthermore, categorical crossentropy loss function is used for error calculation while stochastic gradient descent optimizer is used for weight updation. The number of epochs is set to be 30 while batch size is taken to be 128 in the CNN.

TABLE 6. Parameters' setting in LSTM.

Parameters	Values
No. of dense layers	5
No. of neurons	100
Types of activation functions	Softmax
Loss function	Categorical crossentropy
Optimizer	Adam
No. of epochs	20
Batch size	256

TABLE 7. Simulation parameters.

Parameters	Values
Sensing Area	100m- 100m
Network interface	Wireless
No. of nodes	100
No. of CHs	Probability based selection
No. of BS	1
Initial Energy for nodes	0.5 J
Initial Energy for BSs	No Energy Constraint
Network Topology	Random Distribution

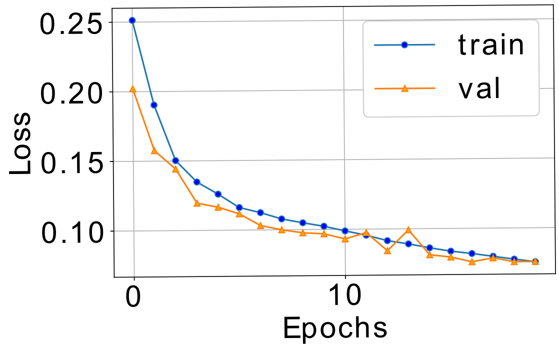


FIGURE 3. Loss during training and validation of GRU.

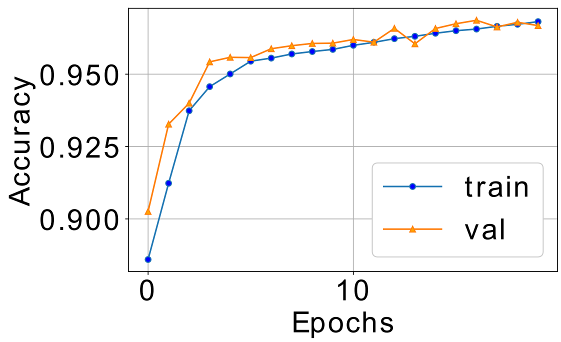


FIGURE 4. Accuracy during testing and validation of GRU.

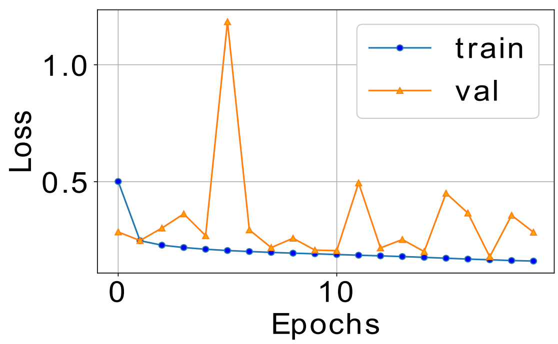


FIGURE 5. Loss during training and validation of CNN.

Table 4 shows the learning parameters used in the ANN. 4 dense layers are used in the ANN. The number of neurons used in the dense layers is 64 in the first layer, 128 in the second layer, 64 in the third layer and 5 in the forth layer. Moreover, four types of activation functions are used. The first dense layer used sigmoid function, second layer used linear function, third layer used tanh function and forth layer used softmax function. Furthermore, categorical crossentropy loss function and stochastic gradient descent optimizer are used. The number of epochs is set to be 30 while the batch size is taken to be 128 in the ANN. Moreover, from Tables 5 and 6, it is observed that GRU and LSTM have 5 dense layers and 100 neurons. The softmax activation function and categorical crossentropy loss function are used in these models. Furthermore, the simulation parameters are given in Table 7.

In the comparison of ANN and CNN, CNN performs well and gives 98% accuracy because it automatically detects the important features from features' list for classification. It is best suited for large datasets and gives the best accuracy. In ANN, each neuron is fully connected in every layer and has to learn extra weight that consumes high computational power. Whereas, the partially connected neurons in CNN consume less computational resources. Therefore, accuracy of ANN is 90%, which is less than that of CNN, similar to the study in [47].

Figs. 5 and 7 show the loss during training and testing of CNN and ANN models. The loss gradually decreases because CNN performs well. The optimizer takes big steps at the beginning and then starts to take the wavy steps. The model minimizes the loss when it gets the best solution for convergence. Figs. 6 and 8 show the model's stability in terms of how well the model performs and gives precise as well as correct MND results. Accuracy of a model shows how accurately it performs classification. In the proposed work, the accuracy of ANN is 90% while the accuracy of CNN is 92%.

Figs. 3 and 4 depict the loss and accuracy of GRU model, respectively. The differences between training and validation loss as well as training and validation accuracy are perfectly minimized in GRU due to the addition of a dropout layer in GRU. Addition of dropout in GRU makes it to perfectly avoid overfitting and achieve better results, i.e., the accuracy and loss obtained by GRU are 0.9668 and 0.0758, respectively.

Figs. 9 and 10 represent the loss and accuracy of the LSTM model, respectively. The curves with blue color show the loss and accuracy of LSTM in training stage while the orange

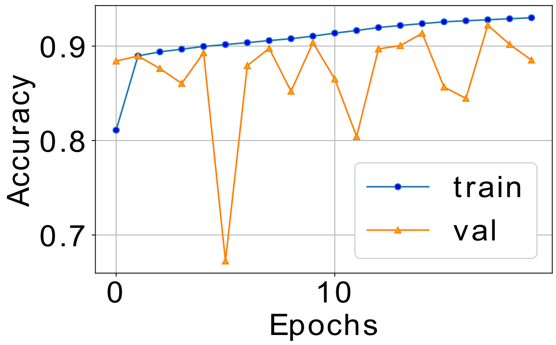


FIGURE 6. Accuracy during testing and validation of CNN.

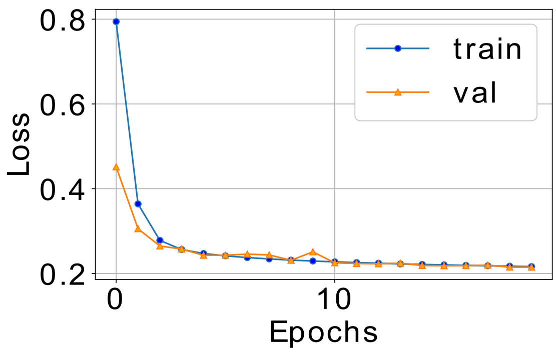


FIGURE 7. Loss during training and validation of ANN.

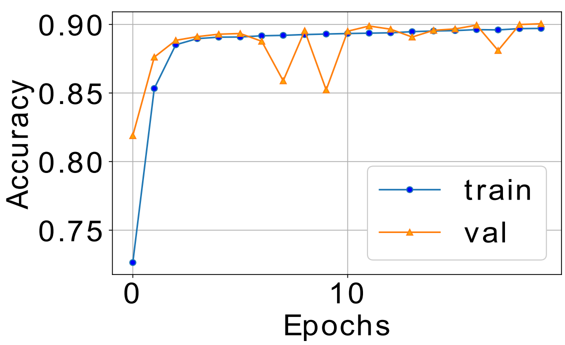


FIGURE 8. Accuracy during testing and validation of ANN.

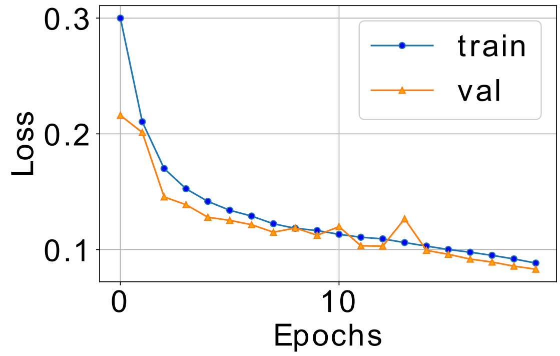


FIGURE 9. Loss during training and validation of GRU.

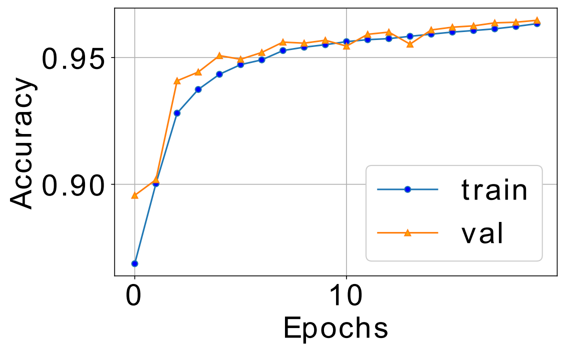


FIGURE 10. Accuracy during testing and validation of GRU.

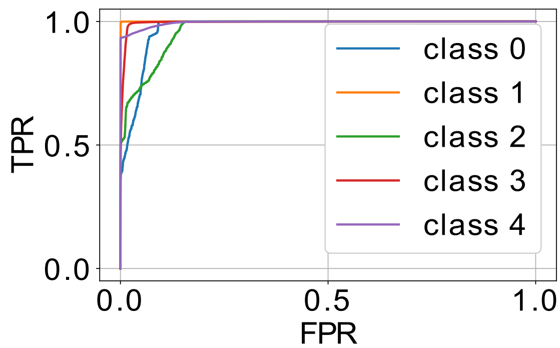


FIGURE 11. TPR and FPR of CNN.

color curves show the accuracy and loss during validation phase. In these plots, the difference between training and validation loss and accuracy are minimized due to the addition of a dropout layer into the LSTM model. Since dropout is used to avoid models from overfitting issue, it is added to avoid LSTM from overfitting. Thus, it is clearly shown in Figs. 9 and 10 that overfitting is successfully avoided. However, at the 14th epoch of the loss plot, the testing curve slightly fluctuates and overfitting occurs, which shows that the model is trained using batches with zero values. In this work, the accuracy and loss of LSTM is 0.9647 and 0.0831, respectively.

Moreover, Figs. 11 and 12 show how well the model differentiates the positive class from the negative class. In the figures, 0 represents the LNs' class while others represent the attackers' classes. These figures also graphically represent TPR and FPR. Both TPR and FPR are given in the form of probability and correspond to the ROC. The ANN model shows high sensitivity, particularity and area-under ROC-curve (ROC-AUC). It also shows that how well the model differentiates between the positive class and the negative class.

Figs. 13 and 14 depict the ROC-AUC of the LSTM and GRU, respectively. High ROC-AUC shows that the model perfectly separates and classifies the classes. In this case, both LSTM and GRU efficiently distinguish the five classes given in the dataset due to their ability to avoid overfitting using dropout regularization. In this way, they obtain generalized results in MND and perfectly differentiates all the classes, as shown in Figs. 13 and 14.

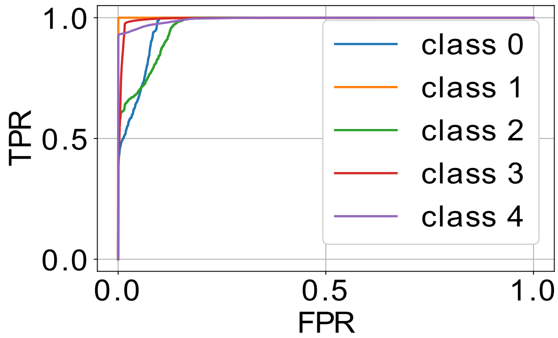


FIGURE 12. TPR and FPR of ANN.

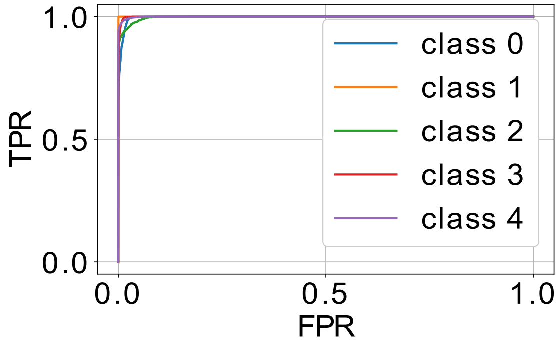


FIGURE 13. TPR and FPR of GRU.

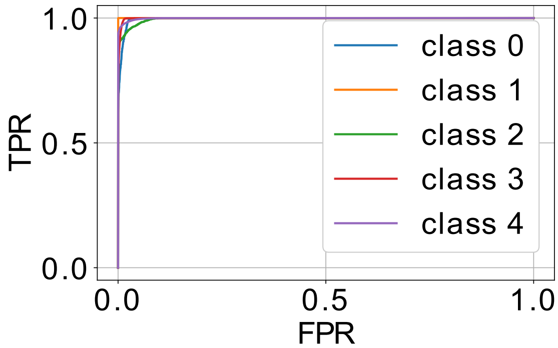


FIGURE 14. TPR and FPR of LSTM.

Figs. 15, and 16 show the network behavior during routing before and after MND. In networking, these parameters are used to show the nodes' performance as given in [5]. The behavior of LEACH, LEACH-RMCV, and LEACH-DL is similar because these all work in the same LEACH environment developed in Matlab [39]. It is worth mentioning that both original LEACH ad HMGEAR are run for 100 nodes. It is also very important to bring into the readers' notice that HMGEAR's only that those concepts are implemeted which are similar to LEACH. Moreover, as LEACH is implemented in MATLAB, HMGEAR is also implemented in MATLAB in the same way as LEACH. After detection and exclusion of the MNs, the LNs left are less than 100. That is why throughput and delay of both LEACH and HMGEAR with $N = 100$ are more than LEACH-RMCV, LEACH-DL, HMGEAR-RMCV,

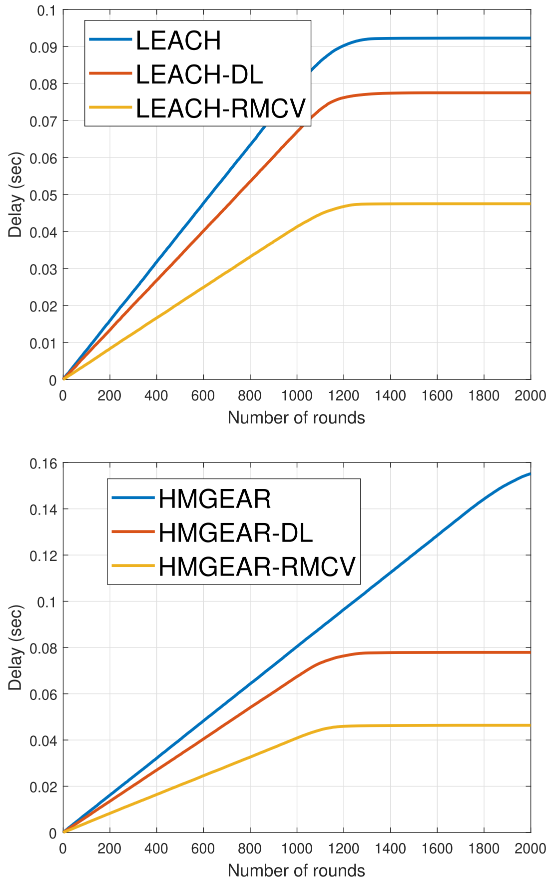
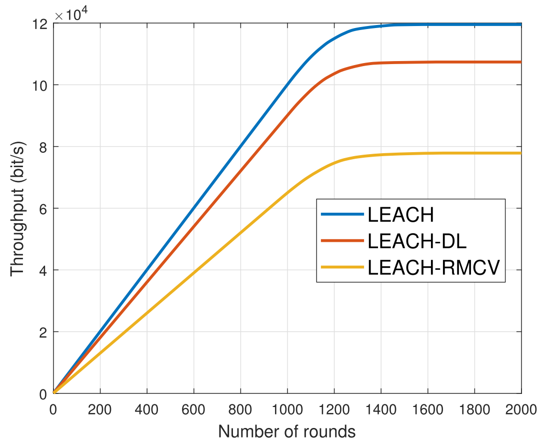


FIGURE 15. (a) Delay using LEACH (b) Delay using HMGEAR.

and HMGEAR-DL with $N < 100$. The original LEACH and HMGEAR calculates throughput and delay of both MNs and LNs. Whereas, LEACH-RMCV, LEACH-DL, HMGEAR-RMCV, and HMGEAR-DL compute these parameters for LNs only. Similar is the case with HMGEAR, HMGEAR-DL and HMGEAR-RMCV.

Figs. 15(a) and 15(b) show the delay that occurs due to the presence of MNs in the network. It is because when routing is performed using LEACH and HMGEAR, no MND is performed. Therefore, the data transmission takes maximum time due to MNs in the network. After the detection and removal of MNs using RMCV and DL models, routing is performed in the presence of LNs only. Therefore, delay is minimized. From the figures, it is observed that LEACH with RMCV and HMGEAR with RMCV detect MNs more accurately than other solutions.

Figs. 16(a) and 16(b) show the total throughput obtained from the network in terms of rounds using LEACH, LEACH-DL and LEACH-RMCV, and HMGEAR, HMGEAR-DL and HMGEAR-RMCV, respectively. The MNs in the network receive the data packets to send them towards destination. Therefore, without MND, both LEACH and HMGEAR show maximum throughput. As compared to LEACH, both LEACH-DL and LEACH-RMCV, due to the MNs' removal, exhibit less throughput. Similar is the case with HMGEAR,



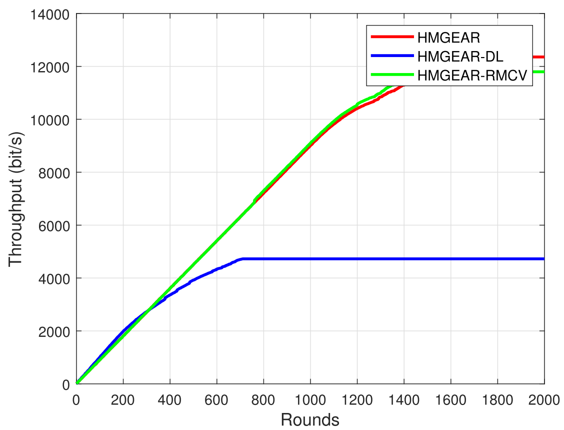
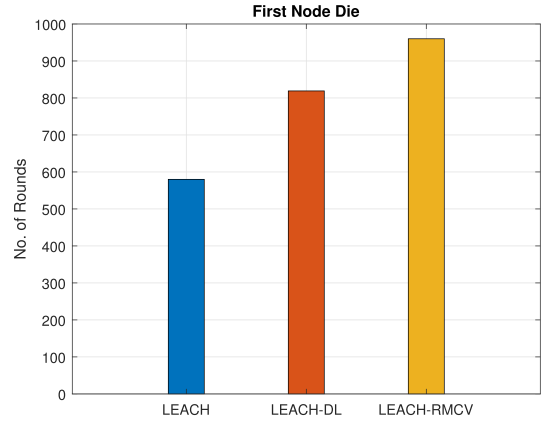


FIGURE 16. **(a) Throughput using LEACH (b) Throughput using HMGEAR.**



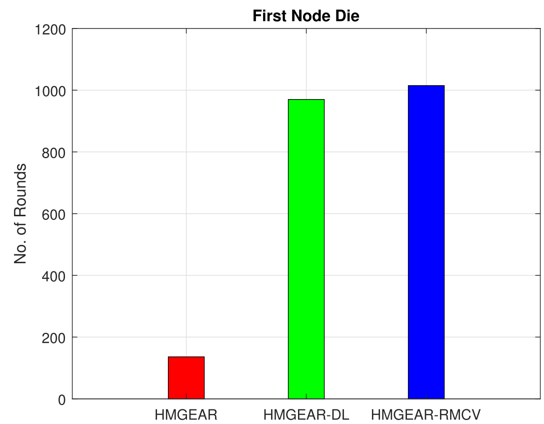


FIGURE 17. **(a) First node die using LEACH (b) First node die using HMGEAR.**

TABLE 8. **Time complexity for training ANN, CNN, LSTM and GRU.**

Method	Time complexity
CNN	$O(n)$
ANN	$O(nt*(ij+jk+kl))$
LSTM	$O(\mathrm{Td_h}^2+\mathrm{Td_hd_i})$
GRU	$O(\mathrm{Td_h}^2+\mathrm{Td_hd_i})$

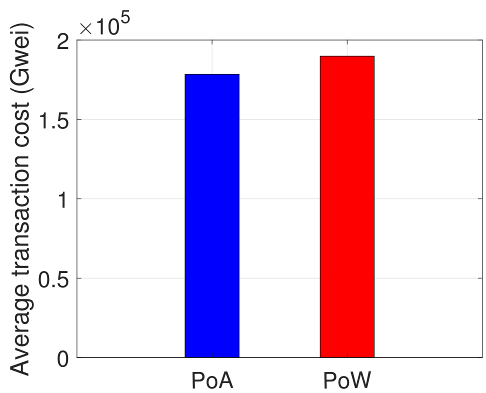


FIGURE 18. **Average transaction cost during nodes' registration.**

HMGEAR-DL and HMGEAR-RMCV. The routing is performed only via LNs in LEACH-DL, LEACH-RMCV, HMGEAR-DL and HMGEAR-RMCV. Consequently, LNs send less number of data packets to the destination.

The rounds at which the first node dies in LEACH and HMGEAR are depicted in Figs. 17(a) and 17(b). The lifetime of the first node is the smallest for both LEACH and HMGEAR, and the largest for LEACH-RMCV and HMGEAR-RMCV. The reason is that the proposed clustering method effectively uses the network's total energy and ultimately helps in extending the network lifetime. In a CNN, the number of features in each feature map is at most a constant times the number of input pixels n (typically the constant is less than 1). Convolving a fixed size filter across an image with n pixels takes $O(n)$ time. It is because each output is just the sum product between k pixels in the image, and k weights in the filter. Where k does not vary with n. Similarly, any max or avg pooling operation does not take more time than linear function in the input size. Thus, the overall runtime is still linear [48].

Suppose that a NN contains n hidden layers, m training examples, x features, and ni nodes in each layer. We tried to find the time complexity for training a NN that has 4 layers having i, j, k and l nodes, with t training examples and n epochs. The overall result was $O(nt*(ij+jk+kl))O(nt*(ij+jk+kl))$ [49], [50].

FIGURE 19. Formal vulnerabilities analysis of smart contract.

Table 8 shows the time complexity of ANN, CNN, LSTM and GRU during training.

The average transaction cost incurred while registering LNs in the blockchain network using PoA consensus mechanism is displayed in Fig. 18. PoA requires low transaction cost than PoW because in this consensus mechanism, the nodes do not have to solve the puzzle to become the miner node as in PoW. The node having the highest authority in terms of wealth becomes the miner in PoA. Whereas, in PoW, that node is regarded as the miner node which succeeds in solving the given puzzle. That is why nodes consume less energy and have less computational cost as given in [5] and [51]. Ropsten environment is used for PoW while Rinkeby is used for PoA [52].

Registration of the LNs is done in the blockchain to indicate that these nodes are legal and a part of the blockchain network.

When LNs are registered in the blockchain network, routing is performed by these LNs using LEACH protocol.

VI. SECURITY ANALYSIS

Blockchain is an emerging technology that is used in industries and other domains. This technology is useful in the area of energy, education, health, etc., [5], [51]. However, it is still vulnerable to various attacks. The main purpose of the proposed model is to detect the MNs in the network and remove them. To tackle the attacks and vulnerabilities, a security analysis is performed. This security analysis evaluates our proposed system's robustness against various attacks, discussed below.

A. VULNERABILITIES IN THE BLOCKCHAIN

The smart contract is a piece of code, which acts as a building block of blockchain technology. The smart contract deals with the SPOF issues. Moreover, the blockchain provides security, transparency, immutability and authenticity of the network. However, various attacks and vulnerabilities can affect the blockchain. These possible attacks are re-entrancy attack, callstack attack, double spending attack, etc. To prevent the network from these attacks, the smart contract is analyzed from security perspective using Oyente tool [51]. The proposed smart contract's security analysis is given in Fig. 19. The smart contract is written for the registration of LNs in our network. The smart contract's vulnerabilities are as follows

1) RE-ENTRANCY ATTACK

It is the attack in which attacker executes the transaction multiple times and no interruption error occurs during the transactions. The attacker calls the function repeatedly while other functions are not allowed to be executed. In our proposed work, the LNs are registered in the network. Moreover, the authorized nodes store their data in the blockchain network while unauthorized nodes are restricted from taking partin the network. For this reason, this attack can not occur on the smart contract.

2) TIMESTAMP DEPENDENCY

In the mining process, the miner generates the blocks, which are added in the blockchain. This attack can occur due to the presence of malicious miners who change the time required for mining process. This attack is unable to happen on our smart contract because the time dependent function is not used in the smart contract. In the proposed work, PoA consensus mechanism is used, in which each miner has the copy of a ledger. When any miner makes any change in the ledger, other miners will also be informed.

3) CALLSTACK DEPTH ATTACK

When any function is called from any other function in the smart contract, its depth is 1023 frames. However, the MN increases the frame size to 1024 and makes it unable to call any other function. Therefore, when an LN calls the function, it will fail because frame size is increased by one and the smart contract will stop working. This attack is not possible on our smart contract. It is because no dependent functions are used.

4) PARITY MULTISIG BUG

In this attack, the attacker attacks the account of a miner node and performs multiple transactions, which make the authorized nodes unable to perform their transactions. However, Fig. 19 shows that there are no chances of this attack on the smart contract. It is because no multiple transactions are performed at a single time.

VII. CONCLUSION AND FUTURE WORK

This paper presents a three-layered architecture. The first layer comprises a WSN with both MNs and LNs. At this layer, LEACH performs routing and a data set is generated [44]. The second layer contains blockchain enabled RMCV and DL models, which detect the MNs. At the third layer, quality routing is performed both with LEACH and HMGEAR only by the LNs found in the second layer. ANN, CNN, LSTM, and GRU models are trained on WSN-DS 2016 dataset generated at the first layer. Simultaneously, the trained DL models also detect the MNs in the network. Additionally, when MNs are removed from the network, the LNs are registered in the blockchain using PoA consensus mechanism. In the simulation results, it is shown that GRU gives 97%, LSTM gives 96%, CNN gives 92%, and ANN gives 90% accurate results. In addition, the transaction cost is calculated and it is observed that less cost is consumed by PoA as compared to the cost consumed by PoW. Moreover, security analysis is performed, which shows that our blockchain network is resilient against different vulnerabilities.

In the future, other DL models will be explored for nodes' classification on even bigger data sets.

REFERENCES

[1] J. Yick, B. Mukherjee, D. Ghosal, "Wireless sensor network survey," *Comput. Netw.*, vol. 52, no. 12, pp. 2292–2330, 2008.

[2] 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.

[3] 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.

[4] S. A. Sert, E. Onur, and A. Yazici, "Security attacks and countermeasures in surveillance wireless sensor networks," in *Proc. 9th Int. Conf. Appl. Inf. Commun. Technol. (AICT)*, Oct. 2015, pp. 201–205.

[5] S. Awan, N. Javaid, S. Ullah, A. U. Khan, A. M. Qamar, and J.-G. Choi, "Blockchain based secure routing and trust management in wireless sensor networks," *Sensors*, vol. 22, no. 2, p. 411, Jan. 2022.

[6] R. Huang, L. Ma, G. Zhai, J. He, X. Chu, and H. Yan, "Resilient routing mechanism for wireless sensor networks with deep learning link reliability prediction," *IEEE Access*, vol. 8, pp. 64857–64872, 2020.

[7] M.-H. Fu, "Integrated technologies of blockchain and biometrics based on wireless sensor network for library management," *Inf. Technol. Libraries*, vol. 39, no. 3, pp. 1–13, Sep. 2020.

[8] S. Kumari and H. Om, "Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines," *Comput. Netw.*, vol. 104, pp. 137–154, Jul. 2016.

[9] S. Amjad, S. Abbas, Z. Abubaker, M. H. Alsharif, A. Jahid, and N. Javaid, "Blockchain based authentication and cluster head selection using DDR-LEACH in Internet of Sensor Things," *Sensors*, vol. 22, no. 5, p. 1972, Mar. 2022, doi: 10.3390/s22051972.

[10] A. U. Khan, M. B. E. Sajid, A. Rauf, M. N. Saqib, F. Zaman, and N. Javaid, "Exploiting blockchain and RMCV-based malicious node detection in ETD-LEACH for wireless sensor networks," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–15, Aug. 2022.

[11] Q. Jiang, S. Zeadally, J. Ma, and D. He, "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks," *IEEE Access*, vol. 5, pp. 3376–3392, 2017.

[12] L. Mishra and S. Varma, "Middleware technologies for smart wireless sensor networks towards Internet of Things: A comparative review," *Wireless Pers. Commun.*, vol. 116, no. 3, pp. 1539–1574, Feb. 2021.

[13] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "HealthBlock: A secure blockchain-based healthcare data management system," *Comput. Netw.*, vol. 200, Dec. 2021, Art. no. 108500.

[14] U. Padmavathi and N. Rajagopalan, "Concept of blockchain technology and its emergence," in *Blockchain Applications in IoT Security*. Hershey, PA, USA: IGI Global, 2021, pp. 1–20.

[15] K. R. Jothi, S. O. Manoj, "A comprehensive survey on blockchain and cryptocurrency technologies: Approaches, challenges, and opportunities," in *Blockchain, Artificial Intelligence, and the Internet of Things* (EAI/Springer Innovations in Communication and Computing), P. Raj, A. K. Dubey, A. Kumar, and P. S. Rathore, Eds. Cham, Switzerland: Springer, 2022, doi: 10.1007/978-3-030-77637-4_1.

[16] 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.

[17] M. Revanesh and V. Sridhar, "Hierarchical block chain-based authentication management scheme for IoT devices," in *Emerging Research in Computing, Information, Communication and Applications*. Singapore: Springer, 2022, pp. 531–541.

[18] S. A. Sert, C. Fung, R. George, and A. Yazici, "An efficient fuzzy path selection approach to mitigate selective forwarding attacks in wireless sensor networks," in *Proc. IEEE Int. Conf. Fuzzy Syst. (FUZZ-IEEE)*, Jul. 2017, pp. 1–6.

[19] K. Haseeb, N. Islam, A. Almogren, and I. U. Din, "Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things," *IEEE Access*, vol. 7, pp. 185496–185505, 2019.

[20] P. K. Sharma and J. H. Park, "Blockchain based hybrid network architecture for the smart city," *Future Gener. Comput. Syst.* vol. 86, pp. 650–655, Sep. 2018.

[21] P. Sharma, S. Jain, S. Gupta, and V. Chamola, "Role of machine learning and deep learning in securing 5G-driven industrial IoT applications," *Ad Hoc Netw.*, vol. 123, Dec. 2021, Art. no. 102685.

[22] T. Hewa, A. Braeken, M. Liyanage, and M. Ylianttila, "Fog computing and blockchain-based security service architecture for 5G industrial IoT-enabled cloud manufacturing," *IEEE Trans. Ind. Informat.*, vol. 18, no. 10, pp. 7174–7185, Oct. 2022.

[23] B. D. Deebak and F. Al-Turjman, "A robust and distributed architecture for 5G-enabled networks in the smart blockchain era," *Comput. Commun.*, vol. 181, pp. 293–308, Jan. 2022.

[24] S. Gurung, D. Lin, A. Squicciarini, and E. Bertino, "Information-oriented trustworthiness evaluation in vehicular ad-hoc networks," in *Proc. Int. Conf. Netw. Syst. Secur.* Berlin, Germany: Springer, 2013, pp. 94–108.

[25] S. Deshpande, J. Gujarathi, P. Chandre, and P. Nerkar, "A comparative analysis of machine deep learning algorithms for intrusion detection in WSN," in *Security Issues and Privacy Threats in Smart Ubiquitous Computing*. Singapore: Springer, 2001, pp. 173–193.

[26] D. Javeed, T. Gao, and M. T. Khan, "SDN-enabled hybrid DL-driven framework for the detection of emerging cyber threats in IoT," *Electronics*, vol. 10, no. 8, p. 918, Apr. 2021.

[27] M. J. Islam, A. Rahman, S. Kabir, M. R. Karim, U. K. Acharjee, M. K. Nasir, and S. Wu, "Blockchain-SDN-based energy-aware and distributed secure architecture for IoT in smart cities," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3850–3864, Mar. 2022.

[28] S. Rathore, J. H. Park, and H. Chang, "Deep learning and blockchain-empowered security framework for intelligent 5G-enabled IoT," *IEEE Access*, vol. 9, pp. 90075–90083, 2021.
[29] A. Rahman, M. J. Islam, A. Montieri, M. K. Nasir, M. M. Reza, S. S. Band, A. Pescape, M. Hasan, M. Sookhak, and A. Mosavi, "SmartBlock-SDN: An optimized blockchain-SDN framework for resource management in IoT," *IEEE Access*, vol. 9, pp. 28361–28376, 2021.
[30] Z. Cui, X. U. E. Fei, S. Zhang, X. Cai, Y. Cao, W. Zhang, and J. Chen, "A hybrid blockchain-based identity authentication scheme for multi-WSN," *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 241–251, Apr. 2020.
[31] 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.
[32] A. Moinet, B. Darties, and J.-L. Baril, "Blockchain based trust & authentication for decentralized sensor networks," 2017, *arXiv:1706.01730*.
[33] Y. Tian, Z. Wang, J. Xiong, and J. Ma, "A blockchain-based secure key management scheme with trustworthiness in DWSNs," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 6193–6202, Sep. 2020.
[34] J. Yang, S. He, Y. Xu, L. Chen, and J. Ren, "A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks," *Sensors*, vol. 19, no. 4, p. 970, Feb. 2019.
[35] S. Mori, "Secure caching scheme by using blockchain for information-centric network-based wireless sensor networks," *J. Signal Process.*, vol. 22, no. 3, pp. 97–108, May 2018.
[36] G. Ramezan and C. Leung, "A blockchain-based contractual routing protocol for the Internet of Things using smart contracts," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–14, Nov. 2018.
[37] Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, and Y. Zhang, "A blockchain-based nonrepudiation network computing service scheme for industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3632–3641, Jun. 2019.
[38] F. Jibreel, E. Tuyishimire, and M. I. Daabo, "An enhanced heterogeneous gateway-based energy-aware multi-hop routing protocol for wireless sensor networks," *Information*, vol. 13, no. 4, p. 166, Mar. 2022.
[39] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proc. 33rd Annu. Hawaii Int. Conf. Syst. Sci.*, 2000, p. 10.
[40] Y. E. Karabacak and N. Gürsel Özmen, "Common spatial pattern-based feature extraction and worm gear fault detection through vibration and acoustic measurements," *Measurement*, vol. 187, Jan. 2022, Art. no. 110366.
[41] *Understanding GRU Networks. In This Article, I Will Try to Give A... | by Simeon Kostadinov | Towards Data Science*. Accessed: Aug. 16, 2022. [Online]. Available: https://towardsdatascience.com/understanding-gru-networks-2ef37df6c9be
[42] *Gated Recurrent Unit | Introduction to Gated Recurrent Unit (GRU)*. Accessed: Aug. 16, 2022. [Online]. Available: https://www.analyticsvidhya.com/blog/2021/03/introduction-to-gated-recurrent-unit-gru/
[43] X. Deng, J. Li, C. Ma, K. Wei, L. Shi, M. Ding, W. Chen, and H. Vincent Poor, "Blockchain assisted federated learning over wireless channels: Dynamic resource allocation and client scheduling," *IEEE Trans. Wireless Commun.*, early access, Nov. 10, 2022, doi: 10.1109/TWC.2022.3219501.
[44] I. Almomani, B. Al-Kasasbeh, and M. Al-Akhras, "WSN-DS: A dataset for intrusion detection systems in wireless sensor networks," *J. Sensors*, vol. 2016, Sep. 2016, Art. no. 4731953.
[45] 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.
[46] D. Jia, J. Xin, Z. Wang, and G. Wang, "Optimized data storage method for sharding-based blockchain," *IEEE Access*, vol. 9, pp. 67890–67900, 2021.
[47] I. Almomani and M. Alenezi, "Efficient denial of service attacks detection in wireless sensor networks," *J. Inf. Sci. Eng.*, vol. 34, no. 4, pp. 977–1000, 2018.
[48] M. Rotman and L. Wolf, "Shuffling recurrent neural networks," in *Proc. AAAI Conf. Artif. Intell.*, May 2021, vol. 35, no. 11, pp. 9428–9435.
[49] *What is Big-O Complexity of Classifying an Image Using CNN?* Accessed: Aug. 16, 2022. [Online]. Available: https://stats.stackexchange.com/questions/527142/what-is-big-o-complexity-of-classifying-an-image-using-cnn
[50] *What is the Time Complexity for Training a Neural Network Using Back-Propagation?* Accessed: Aug. 16, 2022. [Online]. Available: https://ai.stackexchange.com/questions/5728/what-is-the-time-complexity-for-training-a-neural-network-using-back-propagation
[51] M. B. E. Sajid, S. Ullah, N. Javaid, I. Ullah, A. M. Qamar, and F. Zaman, "Exploiting machine learning to detect malicious nodes in intelligent sensor-based systems using blockchain," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–16, Jan. 2022.
[52] C. Regueiro, I. Seco, S. de Diego, O. Lage, and L. Etxebarria, "Privacy-enhancing distributed protocol for data aggregation based on blockchain and homomorphic encryption," *Inf. Process. Manage.*, vol. 58, no. 6, Nov. 2021, Art. no. 102745.

ZAHOOR ALI KHAN (Senior Member, IEEE) is currently the Division Chair of Computer Information Science (CIS) and the Applied Media Division, Higher Colleges of Technology, United Arab Emirates. Previously, he holds different academic positions with Dalhousie University, Canada, and Saint Mary's University, Canada. He has more than 19 years of research and development, academia, and project management experience in the IT and engineering fields. He has multidisciplinary research skills on emerging wireless technologies. His research interests include, but are not limited to, the areas of e-health pervasive wireless applications, theoretical and practical applications of wireless sensor networks, smart grids, and the Internet of Things. His research outcomes include several journal articles, book chapters, and numerous conference proceedings, all peer-reviewed. The journal articles have appeared in prestigious and leading journals. Most of his conference articles have been published by the IEEE Xplore, Springer, or Elsevier, and indexed by the Scopus and Thomson Reuters' conference proceeding citation index. He is a Senior Member of the IAENG. His several conference papers have won best paper awards (BWCCA 2012, the IEEE ITT 2017, and EIDWT-2019). He is an editorial board member of several prestigious journals. He also serves as a regular reviewer/organizer for numerous reputed ISI-indexed journals, IEEE conferences, and workshops.

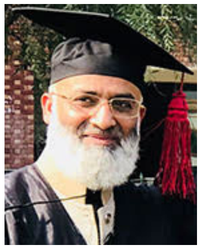
SANA AMJAD received the bachelor's degree in software engineering from COMSATS University Islamabad, Wah Campus, in 2019, and the master's degree in software engineering, with a specialization in blockchain and WSN and classification using AI from the Communications Over Sensors (ComSens) Laboratory, Department of Computer Science, COMSATS University Islamabad, Islamabad Campus, in 2022, under the supervision of Dr. Nadeem Javaid. She is currently a Research Assistant with the ComSens Laboratory. She has authored research publications in international journals and conferences. Her research interests include blockchain in wireless sensor networks and the Internet of Sensors Things, machine learning, and deep learning.

FARWA AHMED received the M.S. degree in electrical engineering from the Department of Electrical and Computer Engineering, COMSATS University Islamabad, Islamabad, in 2017, under the supervision of Dr. Nadeem Javaid. She is currently pursuing the Ph.D. degree with the Department of Aerospace, Mechanical and Electronics Engineering, South East Technical University, Ireland.

ABDULLAH M. ALMASOUD received the B.Sc. degree in computer engineering from King Saud University, Riyadh, Saudi Arabia, and the M.Sc. degree in computer engineering and the Ph.D. degree in computer engineering and electrical engineering from Iowa State University, Ames, IA, USA. Currently, he is an Assistant Professor with the Department of Electrical Engineering, Prince Sattam bin Abdulaziz University, Al-Kharj, Saudi Arabia. His research interests include wireless networks, cognitive radio networks, the Internet of Things, UAV-assisted networking, and RF energy harvesting. He was a recipient of the Best Paper Award at the IEEE Global Communications Conference 2018 on Ad-Hoc and Sensors Networks Symposium.

MUHAMMAD IMRAN (Senior Member, IEEE) was with King Saud University (KSU), Saudi Arabia, as an Associate Professor, where he was the Founding Leader of the WIreless Networks and Security (WINS) Research Group, from 2013 to 2021. He is currently a Senior Lecturer with the School of Science, Engineering and Information Technology, Federation University, Australia. He has published more than 300 research articles in peer-reviewed, highly reputable international conferences (90), journals (198), editorials (15), a book chapter (1), and two edited books. Many of his research articles are among the most highly cited and most downloaded. His research has been cited by more than 11,500 with an H-index of 55 and an i-10 index of 175 (Google Scholar). His research interests include mobile and wireless networks, the Internet of Things, big data analytics, cloud/edge computing, and information security. His research is financially supported by several national and international grants. He has completed several international collaborative research projects with reputable universities. He has received many awards and fellowships.

He served as the Editor-in-Chief for *European Alliance for Innovation (EAI) Transactions on Pervasive Health and Technology* and an Associate Editor for *IEEE Communications Magazine*. He is serving as an Associate Editor for top-ranked international journals, such as *IEEE Network*, *Future Generation Computer Systems*, and IEEE Access. He served/serving as a Guest Editor for about two dozen special issues in journals, such as *IEEE Communications Magazine*, *IEEE Wireless Communications Magazine*, *Future Generation Computer Systems*, IEEE Access, and *Computer Networks*. He has been involved in about 100 peer-reviewed international conferences and workshops in various capacities, such as the chair, the co-chair, and a technical program committee member. He has been consecutively awarded an Outstanding Associate Editor of IEEE Access, in 2018 and 2019.



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 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 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 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 Editor of *Sustainable Cities and Society* journal.