Securing Genetic Algorithm enabled SDN Routing for Blockchain based Internet of Things

SHAHID ABBAS1, NADEEM JAVAID1,*, (Senior Member, IEEE), AHMAD ALMOGREN2,*, (Senior Member, IEEE), SARDAR MUHAMMAD GULFAM3, ABRAR AHMED3, AYMAN RADWAN4

1Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan
2Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11633, Saudi Arabia
3Department of Electrical and Computer Engineering, COMSATS University Islamabad, Islamabad 44000, Pakistan
4Instituto de Telecomunicacoes and Universidade de Aveiro, Aveiro, Portugal

*Correspondence: Nadeem Javaid (nadeemjavaid@comsats.edu.pk); Ahmad Almogren (ahalmogren@ksu.edu.sa)

ABSTRACT Internet of Things (IoT) is an emerging domain in which different devices communicate with each other through minimum human intervention. IoT devices are usually operated in hostile and unattended environments. Moreover, routing in current IoT architecture becomes inefficient due to malicious and unauthenticated nodes’ existence, minimum network lifetime, insecure routing, etc. This paper proposes a lightweight blockchain based authentication mechanism where ordinary sensors’ credentials are stored. As IoT nodes have a short lifespan due to energy depletion, few credentials are stored in the blockchain to achieve lightweight authentication. Moreover, the route calculation is performed by a genetic algorithm enabled software defined network controller, which is also used for on-demand routing to optimize the energy consumption of the nodes in the IoT network. Furthermore, a route correctness mechanism is proposed to check the existence of malicious nodes in the calculated route. Moreover, a detection mechanism is proposed to restrict the malicious nodes’ activities, while a malicious node’s list is maintained in the blockchain, which is used in the route correctness mechanism. The proposed model is evaluated by performing intensive simulations. The effectiveness of the proposed model is depicted in terms of gas consumption, which shows the optimized utilization of resources. The residual energy of the network shows optimized route calculation, while the malicious node detection method shows the number of packets dropped.

INDEX TERMS Authentication, Blockchain, Heuristic Techniques, Internet of Things, Malicious Node Detection, Route Correctness, Software Defined Network.

I. INTRODUCTION

Geographical exploration has gained much popularity over the past few decades, which is performed using sensors enabled Internet of Things (IoT) devices. It is also forecasted that by 2025, there will be 30 billion IoT connections [1]. Moreover, IoT has a wide range of applications in different domains like industrial IoT [2], smart cities [3], agriculture food chain [4], etc. The IoT networks usually operate in open-access environments, such as smart cities, food production and energy supply. Therefore, the IoT network faces many issues, which capture the interest of researchers to improve its efficiency. The last few decades have been quite active in IoT research, which resulted in a huge amount of proposals for various routing protocols [5], [6], security models [7], [8] and clustering techniques [9] that provide secure and trustful communication in the IoT networks. However, IoT networks are always threatened to be compromised by the external nodes, which mislead the networks by sending false data for their benefit. Therefore, if authentication of the Relay Nodes (RNs) is performed correctly, the traffic could be routed accurately. In addition, routing protocols are required to forward data, which are threatened by malicious RNs.

In [10], authentication of nodes is ensured using a centralized authority that has a single point of failure and trustworthiness issues, which demotivate the nodes from taking
TABLE 1: List of Abbreviations and Acronyms

| Abbreviation | Description |
|--------------|-------------|
| BS           | Base Station|
| CH           | Cluster Head|
| GA           | Genetic Algorithm|
| HBA          | Hybrid Blockchain based identity Authentication|
| IoT          | Internet of Things|
| LRA          | Lightweight Registration and Authentication|
| MND          | Malicious Node Detection|
| PoA          | Proof of Authority|
| PoS          | Proof of Stake|
| PoW          | Proof of Work|
| RNs          | Relay Nodes|
| RCM          | Route Correctness Mechanism|
| SDN          | Software Defined Network|
| WSNs         | Wireless Sensor Networks|
| $Crom(k,i)$  | Next Hop in Route|
| $C_i$        | Gene in the Selected Route k at ith hop|
| $E_{RN}$     | Energy of RN|
| $Fitness(k)$ | Fitness of kth route|
| $ID_{RN}$    | ID of RN|
| $V_{th}$     | The Number of Route|
| $LR_{RN}$    | Location of RN|
| MNL          | Malicious Node’s List|

part in the network’s tasks, such as data forwarding and data storage. Therefore, a blockchain based distributed and tamper-proof data storage mechanism is proposed to authenticate the nodes [11]. However, internal malicious nodes could not be easily identified, which decreases the overall network performance [12]. In literature, many centralized mechanisms are proposed to detect internal malicious nodes. However, these mechanisms are prone to the single point of failure issue that is harmful to the network [13]. In [14], authors propose an authentication scheme using group signature method, which creates opportunities for the nodes to act maliciously. The reason is these nodes can hide behind the group ID. Moreover, the authors in [15] propose a Hybrid Blockchain based identity Authentication (HBA) scheme. However, they do not consider the internal RNs’ malicious behaviour that affects secure data forwarding. Furthermore, in [16], the route is found using a learning model, which decreases the network lifetime.

The blockchain is a distributed and secure data storage platform [17], [18], where every node has a copy of an immutable ledger that contains transactions [19]. The blocks are chained together using the hash addresses. Each block stores the hash of its previous block. The hash of a block is generated using the information stored in it and changing the data of a block also changes its hash. So, it is not possible for an attacker to tamper a block without being noticed [20]. On the other hand, a centralized technology, known as Software Defined Networking (SDN), is used for data routing. In SDN, the data plane and the control plane are separated from each other. The routers of the data plane are dumb devices, which can only forward the packets, whereas, at the control plane, an SDN controller is responsible for making the routing policies.

This paper focuses on authentication of RNs, optimized routing and malicious or dead nodes’ detection from a set of RNs. The public blockchain based Lightweight Registration and Authentication (LRA) mechanism is proposed to restrict the malicious nodes at the initial stage. Moreover, the consensus mechanism, which is the agreement of the participant nodes on the transaction request, is used. The well-known Proof of Work (PoW) consensus mechanism is utilized in the proposed work to develop consensus between distributed entities. It requires high computational capability to solve the predefined puzzle. The puzzle is a mathematical problem, which is tough to solve and easy to verify. The requirement of computational power depends upon the difficulty level of the predefined nonce. The blockchain nodes participate to solve the nonce for getting the reward. The winning node’s result is verified by the other competing nodes in the network. If 51% of the nodes agree on the winning node’s result, the winning node adds the transaction into the block and gets the reward. In this way, a blockchain is created and maintained. It is challenging for the attackers to hack the PoW based blockchain because attackers have to compromise 51% of the network nodes, which is both tedious and expensive. Furthermore, Genetic Algorithm (GA) [21] is used in the SDN controller [22], [23] to find the optimized routes for data forwarding. The SDN controller is integrated with blockchain to secure and check the correctness of the routes. In order to secure the route, the SDN controller broadcasts the routes to the blockchain, where the correctness of the route is also checked using the Route Correctness Mechanism (RCM). Although SDN is a centralized technology used for routing [24]–[26], the proposed scenario involves the blockchain technology to make the network decentralized. The major contributions of our work are as follows:

- the LRA mechanism is proposed to achieve trust in a network,
- GA enabled SDN based routing mechanism is used for finding the optimal route,
- different case studies are performed to check the scalability of the proposed routing mechanism,
- RCM is proposed to validate the calculated route using the smart contract and
- malicious nodes are detected using the Malicious Node Detection (MND) mechanism, which works based on the acknowledgment packets.

The rest of the paper is organized as follows: Section II presents the literature review. Section III discusses the proposed system model. Section IV presents the performance evaluation of the proposed system model. Section V gives the details of security analysis and the paper is concluded in Section VI. The list of abbreviations and acronyms is given in Table 1.

II. RELATED WORK
This section consists of a brief review of existing IoT and Wireless Sensor Networks (WSNs) related research efforts. The efforts are categorized based on the limitations addressed.
A. TRUSTED ROUTING TO AVOID MALICIOUS NODES

1) Problems

In WSNs, the location of most of the new nodes is unknown. So, their generated data is useless until the location is known. Many mechanisms are proposed to address the localization issue. However, the dynamic behavior of nodes makes localization challenging. Moreover, the range-free localization is attractive due to its low cost and adaptive nature. However, malicious nodes’ entrance affects the performance of the localization process [27]. Moreover, the reputation mechanism is necessary for the beacon nodes to enhance the accuracy of localization [28]. Furthermore, the dynamic nature of the WSNs causes packet drop and compromises the integrity of the data. The use of mobile Cluster Heads (CHs) makes data forwarding inefficient in terms of energy consumption. Besides, the number of IoT devices is increasing day by day and it makes the IoT more prone to security issues like lack of privacy [29]. Moreover, different types of internal and external attacks may affect the network. Also, there are two types of detection methods against internal attacks: protocol based methods and trust based methods. However, WSNs require more trusted methods for the detection of malicious nodes because in a centralized environment, there is a single point of failure issue [30]. The existing routing schemes cannot identify the malicious nodes because some malicious nodes can pretend to be legitimate; hence, managing to broadcast incorrect routing information. Therefore, centralized trust value calculation mechanisms are proposed by many authors for the neighboring nodes. However, these mechanisms are difficult to be applied in multi-hop communication. Also, in the case of a third party, it is hard for fairness and transparency to achieve the required remarkable levels [16]. The IoT networks face many issues like lack of storage, high computation costs latency in cloud computing, etc. [31]. In addition, two types of approaches are proposed to preserve privacy: centralized and decentralized. The centralized system fails due to a single point of failure, whereas, the decentralized system is not suitable for IoT because vast amounts of data are generated [32]. The feedback based routing protocols are proposed by existing schemes, which increase the overall routing overheads due to feedback packets. Moreover, re-transmissions due to packet drop result in high energy consumption of nodes [33]. The attackers can easily compromise the IoT and the WSNs due to deployment in a harsh environment, which affects the routing process. The authors propose the public key infrastructure system using the central authority. However, different vendors do not trust the central authority due to data breaches [34].

2) Methods

The blockchain based trust evaluation mechanism is proposed in [27], which avoids the problematic issue of a single point of failure. Moreover, the trust values of the nodes is computed through residual energy, neighbor list and mobility. The list of neighbors is also kept up to date for calculating the degree of the node. The composite trust value is computed based on the weighting sum decision model. For consensus, Proof of Stake (PoS) is used to get rid of the high computational cost of the PoW. Authors in [28] propose three types of trust evaluation mechanisms for WSNs: behavioral based trust, feedback based trust and data based trust. The nodes’ behavioral based trust is calculated using different parameters, including closeness in terms of distance, honesty, interaction time and interaction frequency. In feedback based method, the trust of nodes is computed through trustworthiness, positive feedback rate and credibility. Finally, data based trust of nodes is computed using a direct trust, indirect trust and time of previous interaction. A lightweight routing is presented for secure communication between nodes, to enhance the network lifetime and efficiency [29]. The CH selection is made through the uncertainty principle. In contrast to existing solutions, this model integrates blockchain technology with the routing protocol. Moreover, the CHs generate the private keys to secure their communication with the Base Station (BS). The XOR operation is used to compute the unique hash, which is computationally inefficient. The blockchain is mainly used to store sensors’ locations, IDs, etc. Authors in [30] propose a blockchain based trust model, which calculates some performance parameters of packet delivery for malicious node detection. The threshold is set for the performance parameters of the packets. If performance parameters’ values are more than the threshold, the system revokes the node in the network. In [16], the authors propose a decentralized mechanism that keeps records of the multi-hop routing. Meanwhile, the authors exploit the reinforcement learning for the WSNs. At every stage of the next hop selection, reinforcement learning agent learns and stores the routing information at the blockchain to achieve route security. Moreover, an agent is rewarded for every successful action. Authors in [32] propose the blockchain based decentralized SDN enabled malicious node detection mechanism. In the system model, artificial intelligence techniques are used to make the detection models. The detection models are then shared at the fog layer through the blockchain. Moreover, the SDN controller learns the data forwarding policies from the detection model and directs the data plane accordingly. Meanwhile, the detection models of all the IoT networks are fused over the cloud layer to make a single model. Afterwards, the policies are made by synchronizing the cloud’s models with SDN controllers in fog layer. Kumar et al. [33] propose a trust aware localized routing mechanism using blockchain enabled dynamic class based encryption scheme. The selection of routes is made based on the trust value. The values of nodes are measured using the number of successful transmissions and re-transmissions. The authors in [34] propose the distributed blockchain based contractual routing protocol for the IoT network. Smart contracts are used for route discovery and establishment.

B. AUTHENTICATION OF NETWORK NODES
1) Problems
In previous studies, authentication mechanisms are prone to a single point of failure issue due to the use of a trusted third party. This issue is addressed using the blockchain with cloud and fog nodes. However, the blockchain environment requires enormous resources due to an increase in the number of concurrent transactions [15]. The key management system can also be attacked easily due to the deployment of WSNs in a critical and openly accessed environment [35]. Also, IoT devices are manufactured by different vendors, which hinders interoperability because nodes do not trust each other. Authors tackle interoperability issues through an authentication mechanism [36]. Moreover, there is a need for secure and uninterrupted communication among the devices in the IoT environment. The devices are prone to different attacks, which could cause a huge disaster. The centralized solutions are proposed to secure communication, however, these are vulnerable to a single point of failure [37].

2) Methods
Authors in [15] use a hybrid blockchain, in which they categorize the nodes according to their domains. The BSs are connected to the public blockchain and are used to register and authenticate the CHs. In contrast, a private blockchain is deployed over CHs, which performs the registration and authentication of ordinary sensors. The mutual authentication is performed before communication between two nodes. Moreover, in [35], public key infrastructure is used in OpenPGP to achieve confidentiality. On the other hand, authentication is performed via digital signature. The knowledge based trust evaluation is used where each node gives feedback about other nodes. So, falsifying its identity or submitting incorrect data is difficult. In addition, the authors in [36] propose peer-to-peer authentication protocols, in which blockchain is used to authenticate nodes at different levels. The blockchain uses Merkle tree algorithm to store the nodes’ credentials and take action in case of a dispute. The blockchain is integrated with IoT and SHA-1 is used to hash the credentials. The multilevel authentication is also considered to divide the nodes based on their deployment, while a jamming attack is performed to check the network’s credibility.

C. PRIVACY PRESERVATION FOR CRITICAL NODES
1) Problems
In crowd-sensing, mobile devices are used for data collection. However, they carry critical data about the owner and may result in leakage of private information. Thus, such issues demotivate the users from taking part in crowd-sensing [38], [39]. Moreover, encryption keys are used to achieve secure communication between different layers of nodes in WSNs. However, the symmetric key needs additional storage and a secure channel for data sharing. In contrast, asymmetric encryption has key management issues because normal nodes can forge the keys during key generation process. In addition, distributed privacy schemes cause more storage overhead [40]. Moreover, smart cities require high bandwidth, which is essential for the increasing population. Also, low latency, high mobility, structural scalability and a single point of failure due to centralized architecture are also common issues in smart cities. Meanwhile, privacy and security of nodes could be compromised due to massive data collection [41].

2) Methods
A blockchain based incentive mechanism is proposed to protect private information of nodes [38]. A confusion mechanism is added to the system to protect the group’s information. Double SHA-256 is used to hash the users’ information, which is transparently stored in the blockchain. Every hashed information is stored in the Merkel tree, which can be traced in case of disputes. In addition, when the nodes submit tasks, convertible virtual currency is transferred to the nodes’ account by the blockchain. The authors in [40] propose a blockchain based secure key management scheme. Different levels of sensors are used to reduce the computational load of the BSs. Moreover, symmetric encryption is used to replace asymmetric encryption due to lack of resources. In IoT and smart cities [41], a huge amount of data is generated and collected at the centralized point. Therefore, the raw data is uploaded to the edge layer for pre-processing. At the edge layer, data is aggregated and verified by the edge miners through Itsuk PoW. Meanwhile, SDN and blockchain work concurrently to achieve a distributed and secure environment in smart cities. SDN is mainly used to achieve the network’s architectural scalability by routing the data from a single point.

D. LIGHTWEIGHT MECHANISMS FOR IMPROVING COMPATIBILITY
1) Problems
The blockchain requires highly equipped devices to perform computationally intensive tasks like mining, encryption and hashing to provide security. Additionally, nodes have to synchronize the ledger, which requires high bandwidth and storage [42]. Due to the mobile and diverse behavior of the internet of underwater things [43], the static routing protocol is unsuitable due to the need for extra resources. The authors propose the reactive routing protocol, which is also inefficient in terms of energy utilization in a large-scale network [44]. Moreover, the blockchain requires a permanent connection with blockchain that is impossible in a mobile environment [45], [46]. Also, lightweight clients require high downlink data rate, since they have to synchronize with the ledger [47].

2) Methods
Authors propose the synergistic multiple proves to increase the interoperability between different vendors’ devices [42]. A tolerable level of difficulty depends on the capacity of each node to provide equal ease for taking part in the consensus mechanism. The storage offloading mechanism is proposed to tackle unrelated transactions. A lightchain is developed that helps to avoid overlapping of information. The authors in [44] propose a lightweight routing protocol to address the
limitation of inefficient routing. Here, hello and controlled messages are reduced. Bloom filter is used for privacy in which pseudonyms are provided to the nodes for taking part in the network anonymously. The blockchain is used to store the data securely. The authors in [45] propose an idea for efficient data storage. A limited number of blocks are generated according to the ability of each node. Also, N-1 blocks are removed and only the last one is kept in the rolling blockchain to solve the storage issue. The mobile edge computing based on blockchain framework is proposed for the mining and content caching of the nodes’ data in [46]. To get rid of offloading data storage, nearby access points and users are considered for data sharing. The authors in [47] propose the data aggregation scheme to increase network lifetime and storage efficiency of the blockchain, while lightweight IoT devices carry the header of the information and locate actual value through the Merkel Patricia tree, which is maintained via proof of inclusion.

E. STORAGE MECHANISMS FOR THE WSN NODES

1) Problems
The lack of sensor nodes’ storage and trust between buyer and seller during trading are two main issues in WSNs [48]. Moreover, slow update rate for synchronizing the ledger affects the scalability. The Tangle is proposed to address the issue mentioned above. However, it still has the issue of a high information generation rate. Moreover, IoT nodes require more batteries and bandwidth for transaction validation and communication, respectively [49]. The data is sent to BSs for data processing like aggregation, which is stored on a central database that could be vulnerable to a single point of failure [50].

2) Methods
The authors in [48] propose an incentive based model for storing the data on IPFS. The incentive is provided to IPFS to store a large amount of data. An asymmetric encryption scheme is used. A smart contract is written for the sender and buyer to eliminate the third party. Blockchain and IOTA are decentralized and distributed technologies that are being explored in different fields. Both technologies have an issue of information generation rate, which affects the network performance. The authors in [49] propose the concept of age of information, which controls the traffic in the network.

III. SYSTEM MODEL

This section proposes the LRA mechanism that supports the GA enabled SDN routing. We have considered different scenarios with the variable number of IoT networks (clusters) for checking our system’s scalability, as depicted in Fig. 1. Moreover, after the route calculation, malicious or dead nodes are detected in the packet transmission phase. In addition, the blockchain is used to store the IDs of the malicious nodes. The identified limitations (discussed in Section I), proposed solutions and their validations are mapped in Table 2.

A. ASSUMPTIONS AND NETWORK MODEL

The authentication and on-demand routing mechanisms are proposed based on some basic assumptions necessary to fulfill the network’s requirements. The assumptions for the network are as follows:

- all BSs are secure and have enough resources to deploy blockchain,
- SDN controller is a trusted entity in the network,
- the RNs are considered as static and their distance from each other remains constant,
- the ordinary nodes are assumed to send valid data to the RNs and
- malicious and dead nodes are used interchangeably and only malicious nodes could only perform black hole attack.

B. SYSTEM DESCRIPTION

This subsection presents the workflow of the system model, which is depicted in Fig. 2.

Step 1: The RNs generate registration requests to register themselves on the blockchain.

Step 2: RNs are authenticated by the blockchain to become part of the network.

Step 3: The source node, which has data to forward, sends the request to the blockchain for route discovery.

Step 4: Blockchain forwards the request to the GA enabled SDN controller.

Step 5: The route calculated by the SDN controller is sent back to the blockchain. The RCM validates the route using the Malicious Node’s List MNL, which is already maintained in the blockchain by MND mechanism, as mentioned in Subsection III-G.

Step 6: If the route is correct, it is sent to the requesting (source) node in the network.

Step 7: The requesting node receives the route and checks it by detecting the malicious nodes using an acknowledgment mechanism. If any RN does not send the acknowledgment packet back, the source node resends the packet five times. If no acknowledgment is received, the source node declares the RN as malicious.

Step 8: The detected malicious node’s ID is added to the MNL, which is used by RCM. Then, step 4 is initiated again.

C. WORKING OF BLOCKCHAIN

The blockchain is implemented on the BSs to securely store the credentials of nodes. The blockchain is also used for the authentication of nodes in LRA and for route validation in RCM. Initially, the nodes are registered through a smart contract in the blockchain. Then a transaction is performed and sent to the BSs for validation. The BSs validate the transaction and add it into the block after performing consensus between the miner nodes using the PoW consensus algorithm. In the last, the ledger is shared with all the BSs in the blockchain network. There are many consensus algorithms,
FIGURE 1: Different Scenarios for Proposed Model

which are used to develop consensus between distributed unknown entities, i.e., PoW, PoS, Proof of Authority (PoA), etc. In our model, the PoW consensus mechanism is used to ensure trustworthiness in the network. In PoW, different miner nodes compete with each other in solving the puzzle. The miner node, which solves the puzzle first, becomes responsible for validating the transactions and adding the blocks into the blockchain. However, PoW requires high computational resources to solve the puzzle and add the transaction into the blockchain. The BSs have no constraints, therefore, PoW is used for the mining process. In addition, blockchain is used to get rid of the single point of failure issue. Also, it avoids the bandwidth bottleneck problem of the centralized mechanisms. The blockchain is tamper resistant and saves the network from different attacks like sybil attack, impersonation attack, etc. The working of blockchain can be seen in Fig. 3.
TABLE 2: Mapping of Limitations, Proposed Solutions and their Validations

| Identified Limitations                                      | Proposed Solutions                                      | Validations                      |
|------------------------------------------------------------|----------------------------------------------------------|----------------------------------|
| L1: Authentication of nodes using group signature could be harmful [14] | S1: Lightweight authentication of RNs using blockchain   | V1: Execution and transaction costs over blockchain (6a, 6b) |
| L2: Inefficient energy consumption [16]                    | S2: GA enabled SDN controller to find the optimized route | V2: Energy consumption (7a)      |
| L3: No mechanism for the detection of malicious RNs [15]   | S3: Acknowledgment mechanism                             | V3: Number of malicious nodes and packets dropped (7b) |

D. AUTHENTICATION OF RELAY NODES

The registration and authentication processes are discussed in Algorithm 1. The authentication of the forwarding nodes is essential, as discussed in Section I. In this paper, we propose the LRA mechanism for storing the nodes’ credentials on the blockchain. The authentication of nodes is performed before starting the communication, which protects the network from unauthenticated nodes at an early stage. Equation 1 combines the parameters involved in the registration request of a node.

\[
Reg_{req} = (ID_{RN}, L_{RN}, En_{RN}).
\]
Where $ID_{RN}$, $L_{RN}$ and $En_{RN}$ represent ID, location and energy of the RN, respectively.

If the credentials already exist, RN’s remaining energy is updated. Otherwise, the blockchain stores the $ID_{RN}$, $L_{RN}$ and $En_{RN}$. Before registration, if the node’s energy is less than the specific threshold, it is rejected, otherwise, it is registered in the network. Afterward, authentication of the nodes is performed by comparing their IDs with the already stored IDs on the blockchain. Moreover, nodes’ locations are compared with already stored locations, which must be the same because the nodes are static, according to Algorithm 1.

Algorithm 1: LRA for Forwarding Nodes

1. **Inputs:** $ID_{RN}$, $L_{RN}$, $En_{RN}$;
2. **Outputs:** Message;
3. **Send to BS:** $ID_{RN}$, $L_{RN}$, $En_{RN}$;
4. **if** $ID_{RN}$, $L_{RN}$ Not Stored in Blockchain **then**
   5. **if** $En_{RN}$ $\geq$ threshold **then**
      6. Store $ID_{RN}$, $L_{RN}$, $En_{RN}$;
      7. return Accepted;
   8. **else**
      9. return Rejected;
   10. **end**
11. **else**
12. Update $En_{RN}$;
13. return Updated;
14. **end**

### E. GA ENABLED SDN ROUTING

SDN is a centralized technology that is used for route discovery. It is also used for implementing different policies, which control other parts of the network. SDN consists of two planes: a data plane and a control plane. The data plane only forwards the data to the next hop, according to the policy or route defined by the SDN controller. In contrast, the control plane makes the policies or routes for data forwarding. The defined routes or policies are deployed over the data plane to ensure efficient communication between the nodes. In our scenario, SDN is used for energy-efficient route calculation in an IoT network, using a centralized entity. Therefore, RNs’ energy is saved because the RN itself does not calculate the route. Moreover, the shortest and the most energy-efficient path is calculated through the GA enabled SDN controller to increase network lifetime.

GA is used to find the optimized solutions for the problems [51]. It works on an initially given set of solutions called population. Every solution’s fitness is calculated through a fitness function. Afterward, two parent solutions are selected for crossover and mutation. In the crossover, the tails of the selected parents are exchanged at a selected point to make two new off-springs that have the characteristics of both parents. The point is selected from the gene, where both parents have the same value. This occurs because in wireless communications, nodes must be in the communication range, while after crossover, there are chances of nodes’ presence beyond the communication range. Moreover, the off-springs are modified using the mutation process, which inverts one gene. Furthermore, fitness of the new off-springs is calculated. If the fitness is better than the parents’ fitness, the off-springs replace the parents, otherwise, they are discarded. All the steps are depicted in Fig. 4.

The terminologies of GA and IoT network are mapped in Table 3 and are used interchangeably in the paper.

| GA’s Terminologies | IoT Network’s Terminologies |
|--------------------|-----------------------------|
| Population         | Set of Possible Routes      |
| Chromosomes        | Routes                      |
| Gene               | Hop                         |
| Off-spring         | Newly Generated Route       |
| Parents            | Selected Routes for Crossover |

1) **Initial Population**

In the proposed model, RNs are selected based on their distance from the previously selected node (source or intermediate node) and are added to the forwarder list. This list is utilized to obtain an optimized route from the source node to the destination node. Similarly, every possible route is found through the calculated distance, e.g., for nine nodes, a sub-network is shown in Fig 5a and possible routes from source to destination nodes are shown in Fig 5b. Usually, in GA, the initial population is generated randomly, however, there is a possibility that a node in the route does not exist in the neighbor list of the previous node. This random addition in the route misleads the network and consumes extra resources. Therefore, we calculate the distance of every node from other nodes and maintain the neighbor list according to the communication range.

2) **Fitness Function and Selection of Parents**

The fitness function is used to calculate the fitness value of every route according to the objective. All routes are sorted according to the fitness values. The objective is to minimize the total distance between the source and the destination. If the total distance of the route is small, the fitness value will be large. The fitness value is calculated according to [52].

$$Fitness(k) = \frac{1}{\sum_{i=0}^{N-1} Dist(C_i, Crom(k, i + 1))}.$$  \hspace{1cm} (2)

where $Fitness(k)$ shows the fitness of the $k_{th}$ route, while $Crom(k, i + 1)$ denotes the next hop of the $i_{th}$ hop in the $k_{th}$ route. Moreover, $Dist$ represents the distance between nodes and $C_i$ stands for the current hop in the selected chromosome.

3) **Crossover and Mutation**

To make the routes according to the objective, one-point crossover is performed. The crossover adds more diversity.
in the off-springs by selecting the single common point in both routes or at least one common neighbor. In other words, edges are swapped to form the new route to make the population more diverse. If the fitness of off-spring routes is better than the existing routes, then the prior ones are replaced, otherwise, off-springs are discarded. Moreover, in GA, mutation is performed randomly at the selected gene. Whereas, in our case, mutation is performed when any low-energy node or distant node exists. The selected hop is replaced with some other nodes from the neighbor list. The fitness is calculated again and if the resultant value is greater than prior, new routes replace the previous ones.

F. ROUTE CORRECTNESS MECHANISM

The RCM is necessary for heuristic based routing since the population is updated at every iteration in heuristic techniques like GA. So, the final optimal route may contain the malicious or dead nodes, which increase the energy consumption during packets transmission. In the blockchain, the MNL is maintained by the IoT network. The malicious or dead node detection mechanism is described in Section III-G. The RCM mechanism looks into the resultant route and compares every node’s ID with the MNL already maintained in the blockchain. If a node’s ID is found in the MNL, the blockchain requests route re-calculation from the SDN controller according to Algorithm 2.

G. MALICIOUS NODE DETECTION MECHANISM

The number of IoT devices is increasing day by day. Therefore, there are chances of nodes’ unauthorized entry, which affects the overall network performance. In order to address the aforementioned issue, we propose the LRA mechanism to authenticate the nodes. However, the malicious nodes may exist in the network, even after authentication, because a node can be compromised by an attacker. Additionally, nodes could be dead because of their rapid energy depletion. These both types of nodes cause extra energy consumption over packet drops due to re-transmission. To detect the malicious node, the source node sends the hello packet to the next hop in the calculated route before starting the communication. If the next hop is alive and legitimate, it adds its credentials in an acknowledgment packet and sends it back to the source node according to Algorithm 3. Parallelly, the receiver node forwards the hello packet to check the aliveness of its next hop and so on. If any of the nodes does not send the acknowledgment back, the hello packet is repeatedly sent five more times with same conditions. If the acknowledgment is received, the source node starts the communication, otherwise, the node is declared as malicious or dead. The declared

---

**Algorithm 2: Route Correctness Mechanism**

1. **Inputs:** Route, MNL;
2. **Outputs:** Message;
3. for $i \leftarrow 1$ to Number of Hops in Route do
   1. if Hop not exists in MNL then
      1. Send Route to Network;
      2. return Correct;
   2. else
      1. Re-calculation Request;
      2. return Incorrect;
   end
4. end

**Algorithm 3: Malicious Node Detection Mechanism**

1. **Inputs:** Route, MNL;
2. **Outputs:** Message;
3. for $i \leftarrow 1$ to Number of Hops in Route do
   1. if Hop not exists in MNL then
      1. Send Route to Network;
      2. return Correct;
   2. else
      1. Re-calculation Request;
      2. return Incorrect;
   end
4. end
Algorithm 3: Malicious Nodes’ Detection

1 Inputs: Route;
2 Outputs: Message;
3 Send hello Packet;
4 for $i \leftarrow 1$ to 5 do
5     if Acknowledgement Packet Received then
6         Send Packet to route’s Next Hop;
7         return Route is Correct;
8         break;
9     else
10        Send hello Packet Again;
11        if $i == 5$ then
12            return ID of Malicious Node;
13        end
14     end
15 end

malicious or dead node’s ID is sent to the blockchain. The blockchain deletes the credentials of the malicious node and adds its ID in $MNL$, as discussed in Section III-F. Moreover, this method detects malicious or dead nodes in a very simple way; therefore, it increases the nodes’ lifetime due to less energy consumption. The hello packet is very lightweight and causes less energy consumption. Moreover, maintained $MNL$ also saves energy because it helps in the detection of malicious nodes in the calculated route at an early stage.

IV. PERFORMANCE EVALUATION

In this section, the performance evaluation of the proposed model and methods of experiments are discussed.

A. SIMULATION ENVIRONMENT

We set up the blockchain environment through MetaMask, Ganache and Remix IDE on Windows 10 Pro, 64-bit processor Intel Core m3 of 1.61 GHz processor and 8 GB RAM. The smart contract is written in Solidity language. All simulation parameters with diverse scenarios are listed in Table 4.

| Parameters                  | Values               |
|-----------------------------|----------------------|
| Sensing Area                | 1000$m^2$ - 12000$m^2$ |
| No. of RNs                  | 1000 - 12000        |
| No. of BSs                  | 12                  |
| Wireless Range of RNs       | 250 m               |
| Initial Energy for RNs      | 0.5 J               |
| Initial Energy for BSs      | No. Energy Constraint |
| Network Topology            | Random Distribution  |

B. CONDITIONS FOR THE PROPOSED MODEL

- If any RN does not send the acknowledgment packet back, the source node resends the packet five more times. If no acknowledgment is received, the source node declares the RN as malicious.
- Only BSs are responsible to authenticate the ordinary nodes because blockchain is deployed on the BSs.
- All nodes have to response the hello packet to the source node.
- Only the correct route is sent to the source node to save the resources of the network.
- The declared malicious nodes would not be allowed to participate again in the network.

C. VALIDATIONS

In this section, we have performed the simulations of the proposed model while considering gas consumption, remaining energy of the network and the number of packets dropped. The experimental steps of our model are given as follows.

- Step 1: Authentication
• Step 2: Route Calculation
• Step 3: Malicious Node Detection

Step 1: Authentication

In this section, the performance and effectiveness of our model are evaluated using the gas consumption of the LRA mechanism and it is compared with the existing HBA scheme [15]. The gas consumption in the blockchain environment is a basic unit for calculating the transaction and execution cost. The deployment cost includes transaction and computational costs, which are to be paid by the smart contract caller. The transaction cost is paid for adding a transaction in the blockchain, while the execution cost is paid for executing different operations included in the smart contract. The computational cost of our proposed LRA mechanism is depicted in Fig. 6a and Table 5. The existing technique has a larger message size, therefore, it causes higher gas consumption than the proposed LRA mechanism. The message size is larger in the existing technique because many parameters are taking part in the authentication mechanism. On the other hand, LRA contains fewer parameters, which need to be stored. In addition, the first set of bars depicts deployment cost, which shows the proposed model’s efficiency in terms of gas consumption. Similarly, the second and third sets of bars depict the efficiency of registration and authentication, respectively. The registration cost is higher than the authentication cost because the credentials need to be stored on the blockchain during registration, which requires more cost. In authentication, the credentials have to be compared with already stored credentials only. Therefore, the authentication process requires less gas as compared to the registration process. Similarly, the same reasons are applied to the transaction cost, which is plotted in Fig. 6a and Table 5.

| Cost Name     | Scheme | C1       | C2       | C3       |
|---------------|--------|----------|----------|----------|
| Transaction Cost | HBA    | 405984   | 188497   | 58671    |
|               | LRA    | 302988   | 128111   | 48373    |
| Execution Cost | HBA    | 265312   | 166073   | 72074    |
|               | LRA    | 201385   | 106455   | 62013    |

Note: C1 denotes Deployment, C2 denotes Registration and C3 denotes Authentication.

Step 2: Route Calculation

The GA enabled SDN based routing method is evaluated by calculating the remaining energy of the network after the detection of the new malicious node. There is a minor decrease in the total energy after detection of new malicious node, as seen in Fig. 7a. In our scenario, initially, we simulate the four cases, which are mentioned in Subsection IV-D. Then the blockchain is integrated to keep a record of the nodes’ credentials and ensure route correctness. After this, the cases are implemented by increasing the number of nodes, clusters and logical SDN controllers. These cases include 1, 4, 8 and 12 logical SDN controllers for 1, 4, 8 and 12 clusters, respectively. They are implemented to check the scalability of the proposed model. Each set of bars in Fig. 7a depicts the said four cases. We can see that in each case, the consumed energy is logically increased, as the number of nodes and clusters are increased. Therefore, there is no extra overhead of energy consumption. The collective energy consumption of the network is minimum because the new route is calculated after the detection of the malicious nodes. The new route decreases the packet drop rate, which affects the energy consumption of the nodes. Also, the number of successfully transmitted packets is increased, which is required by an efficient network. Therefore, resource utilization over the transmitted packets is not considered. The minimum energy consumption on every new detection shows the achievement of our work’s objective. Additionally, these tests are performed for the four previously described cases to evaluate the scalability of the proposed model. Moreover, energy consumption is increased logically with the increase in the network size, as shown in Fig. 7a. However, energy consumption does not increase from an expected value. The reason is that the number of hops is minimum in the calculated route due to GA based shortest route selection and the route calculation through
Step 3: Malicious Node Detection

Another issue is the existence of a malicious node in intermediate nodes, which affects the network’s communication. In addition, the MND mechanism is evaluated by the number of packets dropped. If any node becomes malicious or dead and this information is not broadcasted to the network, other nodes’ energy could be depleted due to packet retransmissions. We have calculated the number of packets dropped when any malicious node is detected. In Fig. 7b, the x-axis shows the number of malicious nodes and the y-axis shows the total number of packets dropped. Ultimately, the number of packets dropped increases due to an increase in the number of malicious nodes. However, the number of packets dropped does not increase exponentially because malicious nodes are detected through the lightweight hello message’s acknowledgment. These hello messages are initiated after a specific interval of time to ensure the reliability of the path throughout the network’s lifetime. Figure 7b shows uncertain behaviour because different number of packets are dropped at every iteration. The number of dropped packets is not increasing additively because malicious nodes are detected at different time intervals. Sometimes, malicious nodes are detected right after the last detection. It means the detection mechanism detects the malicious nodes efficiently. Moreover, when any node becomes dead in the path, a new path is calculated by the SDN controller, therefore, packet drop is decreased, which decreases the energy dissipation while increasing the overall network lifetime.

D. CASE STUDIES OF THE PROPOSED MODEL TO VALIDATE SCALABILITY

In order to simulate the proposed model, we consider different number of clusters and logical controllers as follows.

- No. of clusters 1, No. of logical controllers 1
- No. of clusters 4, No. of logical controllers 4
- No. of clusters 8, No. of logical controllers 8
- No. of clusters 12, No. of logical controllers 12

In our scenario, the SDN controller is used for calculating the route for the IoT devices and there could be more than one logical controller. However, the above mentioned simulations are conducted to check the proposed model’s scalability for route calculation time. The average time is approximately the same for different scenarios, as mentioned in Table 6. In the table, columns 2, 3, 4 and 5 have one, four, eight and twelve logical controllers, respectively. Since logical controllers in the SDN control plane work parallelly, there is not much difference between times, taken by logical controllers. Hence, it is verified that our system is scalable for the increased number of IoT devices.

E. CRITICAL ANALYSIS

The proposed work is intended to enhance the IoT network’s performance. The IoT network faces numerous issues like lack of security, minimum network lifetime, insecure routing, etc. Blockchain technology and GA enabled SDN controller are used in combination to secure network communication and increase the network lifetime. The blockchain is used for the LRA and the RCM. The LRA mechanism consumes few resources because the message size is less. However, few credentials may cause impersonation, spoofing and sybil attacks. These attacks can be performed by the brute-force method. In the MND mechanism, we tackle the black hole attack and ensure high packet delivery. However, in this model, more threats like denial of service attack, replay attack, grey hole attack, etc., can occur. Additionally, the GA enabled routing requires much time to calculate the route, which is sometimes unacceptable for the network due to its real-time communication requirements. Moreover, in blockchain, the transactions take considerable time for validation.

V. FORMAL SECURITY ANALYSIS

The formal analysis of the proposed scheme is carried out through implementation. The scheme is specifically designed for the detection of malicious nodes. It consists of two main
TABLE 6: Time Taken by Different Cases

| Cluster No. | No. of Clusters = 1 | No. of Clusters = 4 | No. of Clusters = 8 | No. of Clusters = 12 |
|-------------|---------------------|---------------------|---------------------|----------------------|
|             | No. of Control      | No. of Control      | No. of Control      | No. of Control       |
|             | Planes = 1          | Planes = 4          | Planes = 8          | Planes = 12          |
| 1           | 0.780678            | 0.698778            | 0.707219            | 0.703964             |
| 2           | 0.768295            | 0.744087            | 0.736068            | 0.719232             |
| 3           | 0.702707            | 0.714343            | 0.727246            | 0.742095             |
| 4           | 0.807292            | 0.741775            | 0.720395            |                      |
| 5           | 0.741775            | 0.855588            | 0.782724            |                      |
| 6           | 0.728242            | 0.762140            | 0.717828            | 0.746192             |
| 7           | 0.762140            | 0.717828            |                      | 0.821233             |
| 8           | 0.762140            | 0.717828            |                      | 0.735601             |
| 9           | 0.762140            | 0.717828            |                      | 0.724500             |
| 10          |                     |                     |                     |                      |
| 11          |                     |                     |                     |                      |
| 12          |                     |                     |                     |                      |
| Average     | 0.780678            | 0.744268            | 0.782842            | 0.679002             |

FIGURE 8: Formal Analysis using Oyente Tool

A. BLACK HOLE ATTACK

In this section, we provide the details of our strategy to deal with a black hole attack, as shown in Figure 9. A black hole or packet drop attack occurs in a network when a node receives the packet and does not acknowledge it [56]. Generally, when a node sends the hello packet to its neighbour, it receives an acknowledgment packet in return. To check the robustness of our proposed scheme, we induce the black hole attack by considering one of the nodes in the selected route as malicious. When the malicious node receives the hello packet, it does not send the acknowledgment packet back to the source node. If a node does not send the acknowledgment packet back to the source node after receiving five hello packets, it is considered malicious and its ID is stored on the blockchain. The reason for maintaining the list on the blockchain is to prevent data tampering.

B. SMART CONTRACT ANALYSIS

To maintain the MNL on the blockchain, a smart contract is used, which is written in solidity programming language. Smart contracts enable secure transactions between different nodes without the interference of a third party. However, due to bad programming practices, the smart contracts may become vulnerable to different attacks like DAO attack [53], reentrancy attack [54], transaction ordering attack [55], etc. We analysed our smart contract using the Oyente analysis tool. Oyente is an open-source tool that symbolically executes the smart contract to identify critical vulnerabilities. Fig. 8 shows the Oyente analysis of our proposed smart contract. It is evident that our smart contract is secure against all the commonly known smart contract vulnerabilities. Some of the smart contract vulnerabilities that are closely related to our scheme are discussed as follows.

1) Reentrancy Attack

In a reentrancy attack, a malicious user may interrupt the normal execution of a smart contract function and run the same function multiple times using different parameters without
any errors. The smart contract in our proposed scheme stores the IDs of the malicious nodes in the **MNL**. However, this function can only be executed by the authorized nodes. This restriction prevents malicious users from adding false information to the **MNL**.

### 2) Timestamp Dependency

In this attack, the attacker manipulates the timestamp of the blocks to add false information to the ledger. Since there is no time-dependent function in our smart contract, hence, our scheme is secure against this attack.

### 3) Call Stack Attack

In this attack, the attacker repeatedly calls the external smart contract functions to exceed the 1024 calls. After that, the benign function calls will fail since the limit is already reached. In our scheme, this attack is not possible because our proposed smart contract does not have any external functions.

### 4) Parity Multisig Bug

This attack allows the malicious users to take ownership of the victim’s account. Hence, the attacker can steal funds from that account and perform the functions reserved for the authorized users only. However, the Oyente results show that our proposed smart contract is secure against this attack.

### 5) Transaction Ordering Dependence

In this attack, a malicious miner may attempt to maliciously order the transaction to disrupt the standard functionality of the contract. This attack occurs when the smart contract has functions that are dependent upon the order of the transactions. This attack is not possible in our proposed smart contract because none of the smart contract function has transaction ordering dependence. Moreover, the miners in the proposed scheme are trusted entities; hence, this attack will not occur even if this vulnerability exists.

### VI. CONCLUSION

In this paper, the blockchain is deployed to store the nodes’ credentials for achieving tamper resistance and anonymity to ensure trust and privacy in the distributed network. An LRA mechanism is proposed in which credentials are stored on the blockchain for their further usage in the routing process. GA enabled SDN controller is used for calculating the routes between source and destination node, which results in optimized energy consumption of RNs. The SDN controller uses already stored nodes’ credentials for route calculation. After route calculation, the route is submitted to the blockchain for validation through smart contract based RCM. The RCM compares the route with the **MNL** (generated after the detection of new malicious nodes). If any of the route’s hop exists in the **MNL**, the blockchain resends the route request to the SDN controller, otherwise, it sends the route to the source node. Moreover, an acknowledgment based MND mechanism is proposed, which detects the maliciousness or deadness of RNs. This method allows the source node to detect malicious or dead nodes through a lightweight **hello** message, which results in less energy consumption. The source node sends **hello** message to the neighbor node. If the acknowledgment is not received, **hello** message is sent five more times; otherwise, the communication is started. In the case when no acknowledgment is received, source node declares the respective node as malicious and adds its ID in the **MNL**. The simulation results show the effectiveness of our proposed model in terms of gas consumption, the number of packets dropped and the remaining energy of nodes. The proposed model requires less execution and transaction costs for both registration and authentication of RNs. In the future, we plan to conduct the routing mechanism through different meta-heuristic techniques. Moreover, we will enhance the MND and route calculation mechanism using machine learning techniques. Furthermore, we will conduct an attacker...
model considering syllable attack, impersonation attack, denial of service attack, etc.

ACKNOWLEDGMENT
This work is supported by King Saud University, Riyadh, Saudi Arabia, through Researchers Supporting Project number RSP-2021/184. The work of author Ayman Radwan is supported by FCT / MEC through Programa Operacional Regional do Centro and by the European Union through the European Social Fund (ESF) under Investigador FCT Grant (SG-AHEAD IF/FCT - IF/01393/2015/CP1310/CT0002).

REFERENCES
[1] "https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time?" Last Accessed 15 September, 2021.
[2] Ming, Zhongxing and Mengwei Xu. “NBA: A name based approach to device mobility in industrial IoT networks.” Computer Networks (2021): 107973.
[3] Qureshi, Talha Naem, Nadeem Javaid, Ahmad Almogren, Zain Abubaker, Hisham Almajed and Irfan Mohiuddin. “Attack resistance based topology robustness of scale free internet of things for smart cities”, International Journal of Web and Grid Services, ISSN: 1741-1114.
[4] Shahid, Aatif; Ahmad Almogren, Nadeem Javaid, Fahad Ahmad Al-Zahraei, Mansour Ziaur, and Masoom Alam. “Blockchain based agri-food supply chain: A complete solution.” IEEE Access 8 (2020): 69230-69243.
[5] Javaid, Nadeem, Arshad Sher, Wadood Abdul, Ifthak Arif Niaz, Ahmad Almogren, and Afif Alamri. “Cooperative opportunistic pressure based routing for underwater wireless sensor networks.” Sensors 17, no. 3 (2017): 629.
[6] Javaid, Nadeem. “NADEEM: Neighbor node approaching distinct energy-efficient mates for reliable data delivery in underwater WSNs.” Transactions on Emerging Telecommunications Technologies, (2019): e3805, doi:10.1002/ett.3805.
[7] de Assis, Marcos VO, Luiz F. Carvalho, Joel JPC Rodrigues, Jaime Lloret, and Marco L. Proenca Jr. “Near real-time security system applied to SDN environments in IoT networks using convolutional neural network.” Computers & Electrical Engineering 86 (2020): 106738, doi:10.1016/j.compeleceng.2020.106738.
[8] Javaid, Nadeem, Madassir Ejaz, Wadood Abdul, Afif Alamri, Ahmad Almogren, Ifthak Arif Niaz, and Nadia Guizani. “Cooperative position aware mobility pattern of UAVs for avoiding void zones in underwater WSNs.” Sensors 17, no. 3 (2017): 580.
[9] Yousef, Shamim, Farnaz Derakhshan, Hadi S. Aghdasi, and Hadis Karimpour. “An energy efficient artificial bee colony based clustering in the internet of things.” Computers & Electrical Engineering 86 (2020): 106733.
[10] Waizd, Mohammad, Ashok Kumar Das, Vivekananda Bhat, and Athanasios V. Vasilakos. “LAM-CIoT: Lightweight authentication mechanism in cloud based IoT environment.” Journal of Network and Computer Applications 150 (2020): 102496.
[11] Vishwakarma, Lokendra, and Debasis Das. “SCAB-IoTA: Secure communication and authentication for IoT applications using blockchain.” Journal of Parallel and Distributed Computing (2021).
[12] Yang, Guang, Lie Dai, and Zhiquiang Wei. “Challenges, threats, security issues and new trends of underwater wireless sensor networks.” Sensors 18, no. 11 (2018): 3907.
[13] S. A. Rahman, H. Tout, C. Talhi and A. Mourad, “Internet of Things Intrusion Detection: Centralized, on-Device, or federated learning” in IEEE Network, vol. 34, no. 6, (2020): 310-317.
[14] Kolumban-Antal, Gyorgy, Vladko Lasak, Razvan Bogdan, and Bogdan Groza. “A secure and portable multi-sensor module for distributed air pollution monitoring.” Sensors 20, no. 2 (2020): 403.
[15] Cui, Zhihua, X. U. E. Fei, Shiqiang Zhang, Xingjian Cai, Yang Cao, Wensheng Zhang, and Jinjun Chen. “A hybrid blockChain based identity authentication scheme for multi-WSN." IEEE Transactions on Services Computing 13, no. 2 (2020): 241-251.
[16] Yang, Jidan, Shichen He, Yang Xu, Linweiya Chen, and Ju Ren. “A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks.” Sensors 19, no. 4 (2019): 970.
[17] Li, Jiangfeng, Shili Hu, Yang Shi, and Chenxi Zhang. “A blockchain based trustable framework for IoT data storage and access.” In International Conference on Blockchain and Trustworthy Systems, pp. 336-349. Springer, Singapore, 2019.
[18] Feng, Xiaojian, Jianfeng Ma, Yimin Miao, Qian Meng, Ximeng Liu, Qi Jiang, and Hui Li. “Prunable sharding based blockchain protocol.” Peer-to-Peer Networking and Applications 12, no. 4 (2019): 934-950.
[19] Lazrag, Hilmi, Abdullah Chehri, Rachid Saadane and Moulay Driss Rachamani. “A blockchain based approach for optimal and secure routing in wireless sensor networks and IoT." In 2019 15th International Conference on Signal-Image Technology & Internet Based Systems (SITIS), pp. 411-415. IEEE, 2019.
[20] Nakamoto, S., 2008. Bitcoin: a peer-to-peer electronic cash system (2008).
[21] Mohankumar, B. and K. Karuppasamy. “Network lifetime improved optimal routing in wireless sensor network environment.” Wireless Personal Communications (2021): 1-20.
[22] Medhane, Darshan Vishwasrao, Arun Kumar Sangaiha, M. Shamnim Hosssain, Gisulam Muhammad and Jin Wang. “Blockchain-enabled distributed security framework for next-generation IoT: An edge cloud and software defined network integrated approach.” IEEE Internet of Things Journal 7, no. 7 (2020): 6143-6149.
[23] Gao, Honghao, Xi Qin, Ramón J. Durán Barroso, Walyatt Hussain, Yueshen Xu and Yuyu Yin. “Collaborative learning based industrial IoT API recommendation for software defined device.” The important knowledge discovery perspective,” in IEEE Transactions on Emerging Topics in Computational Intelligence, doi: 10.1109/TETCI.2020.3023155.
[24] Shi, Xiaojun, Yangyang Li, Haiyong Xie, Tengfei Yang, Linchao Zhang, Panyu Liu, Heng Zhang, and Zhiyao Liang. “An Openflow-based load balancing strategy in SDN." C. Mater. Conti. 62 (2020): 38520-398.
[25] Guo, Chao, Juan Guo, Chunjuan Yu, Zhaobin Li, Cheng Gong, and Abdul Wajeeh. “A Safe and Reliable Routing Mechanism of LEO Satellite Based on SDN." CMC-COMPUTERS MATERIALS & CONTINUUM 64, no. 1 (2020): 439-454.
[26] Cheng, Jieren, Jun Li, Naixue Xiong, Meizhu Chen, Hao Guo, and Xinzhi Yao. “Lightweight mobile clients privacy protection using trusted execution environments for blockchain.” CMC-COMPUTERS MATERIALS & CONTINUUM 65, no. 3 (2020): 2247-2252.
[27] Goyat, Rekha, Gulshan Kumar, Mritunjay Kumar Rai, Rahul Saha, Reji Thomas and Tai Hoon Kim. “Blockchain powered secure range-free localization in wireless sensor networks.” Arabian Journal for Science and Engineering 45, no. 8 (2020): 6139-6155.
[28] Kim, Tai-Hoon, Rekha Goyat, Mritunjay Kumar Rai, Gulshan Kumar, William J. Buchanan, Rahul Saha and Reji Thomas. “A novel trust evaluation process for secure location using a decentralized blockchain in wireless sensor networks.” IEEE Access 7 (2019): 184433-184444.
[29] Haseeb, Khalid, Naveed Islam, Ahmad Almogren and Ikram Ud Din. “Intrusion prevention framework for secure routing in WSN based mobile Internet of Things.” IEEE Access 7 (2019): 185496-185505.
[30] She, Wei, Qi Liu, Zhao Tian, Jian-Sen Chen, Bo Wang and Wei Liu. “Blockchain trust model for malicious node detection in wireless sensor networks.” IEEE Access 19 (2021): 38904-38912.
[31] Huang, Yuzhe, Huahu Xu, Honghao Gao, Xiaoqin Ma and Walayat Hussain. “SSUR: An approach to optimizing virtual machine allocation strategy Bsed on user requirements for cloud data center.” IEEE Transactions on Green Communications and Networking 5, no. 2 (2021): 670-681.
[32] Rathore, Shailendra, Byung Wook Kwon and Jong Hyuk Park. “BlockSeoTNet: Blockchain based decentralized security architecture for IoT network.” Journal of Network and Computer Applications 143 (2019): 167-177.
[33] Kumar, M. Hema, V. Mohanraj, S. Suresh, J. Senthilkumar and G. Nagalali. “Trust aware localized routing and class based dynamic block chain encryption scheme for improved security in WSN.” Journal of Ambient Intelligence and Humanized Computing (2020): 1-9.
[34] Sumner, Gholamreza and Cyril Leung. “A blockchain based contractual routing protocol for the internet of things using smart contracts.” Wireless Communications and Mobile Computing 2018 (2018).
[35] Moinet, Axel, Benoît Daries and Jean-Luc Baril. “Blockchain based trust & authentication for decentralized sensor networks.” arXiv preprint arXiv:1706.01730 (2017).
[36] Hong, Sunghyuck. “P2P networking based internet of things (IoT) sensor node authentication by blind.” Peer-to-Peer Networking and Applications 13, no. 2 (2020): 579-589.
[37] Rathee, Geetanjali, M. Balasaraswathi, K. Prabhuj Chandran, Sharmi Dev Gupta and C. S. Boopathi. “A secure IoT sensors communication in-indus-
try 4.0 using blockchain technology." Journal of Ambient Intelligence and Humanized Computing (2020): 1-13.

[38] Jia, Bing, Tao Zhou, Wuyangener Li, Zhenchang Liu and Jiantao Zhang. "A blockchain based location privacy protection incentive mechanism in crowd sensing networks." Sensors 18, no. 11 (2018): 3894.

[39] Guo, Yu, Hongcheng Xie, Yinbin Miao, Cong Wang, and Xiaohua Jia. "FedChain: A federated and privacy preserving crowdsourcing platform on blockchain," in IEEE Transactions on Services Computing, doi: 10.1109/TSC.2020.3031061.

[40] Tian, Youliang, Zuan Wang, Jinbo Xiong, and Jianfeng Ma. "A blockchain based secure key management scheme with trustworthiness in DWSNs," IEEE Transactions on Industrial Informatics 16, no. 9 (2020): 6193-6202.

[41] Sharma, Pradip Kumar, and Jong Hyuk Park. "Blockchain based hybrid network architecture for the smart city," Future Generation Computer Systems 86 (2018): 650-655.

[42] Liu, Yinqiu, Kun Wang, Yun Lin, and Wenyao Xu. “LightChain: A lightweight blockchain system for industrial internet of things,” IEEE Transactions on Industrial Informatics 15, no. 6 (2019): 3571-3581.

[43] Azam, Irfan, Nadeem Javaid, Ashfaq Ahmad, Wadood Abdul, Ahmad Almogren, and Atif Alami. "Balanced load distribution with energy hole avoidance in underwater WSNs," IEEE Access 5 (2017): 15206-15221.

[44] Uddin, Md Ashraf, Andrew Stranieri, Iqbal Gondal, and Venki Balasubramanian. "A lightweight blockchain based framework for underwater IoT," Electronics 8, no. 12 (2019): 1552.

[45] Sergii, Kushch, and F. Prieto-Castrillo. “A rolling blockchain for a dynamic WSNs in a smart city,” arXiv preprint arXiv:1806.11399 (2018).

[46] Liu, Mengting, F. Richard Yu, Yinglei Teng, Victor CM Leung, and Mei Song. "Computation offloading and content caching in wireless blockchain networks with mobile edge computing," IEEE Transactions on Vehicular Technology 67, no. 11 (2018): 11008-11021.

[47] Danzi, Pietro, Anders E. Kalh, Péter Stefánovics and Jan Popovski. "Delay and communication tradeoffs for blockchain systems with lightweight IoT clients." IEEE Internet of Things Journal 6, no. 2 (2019): 2354-2365.

[48] Ren, Yongjun, Yeqing Liu, Sai Ji, Arun Kumar Sangaijash and Jin Wang. "Incentive mechanism of data storage based on blockchain for wireless sensor networks," Mobile Information Systems 2018 (2018).

[49] Rouira-Sugranes, Arnau and Abolfazl Razi. “Optimizing the age of information for blockchain technology with applications to IoT sensors,” IEEE Communications Letters 24, no. 1 (2020): 183-187.

[50] Feng, Huanhuan, Wensheng Wang, Bingqi Chen and Xiaoshuan Zhang, "Evaluation on frozen shellfish quality by blockchain based multi-sensors monitoring and SVM algorithm during cold storage," IEEE Access 8 (2020): 54361-54370.

[51] Harik, Georges R., Fernando G. Lobo and David E. Goldberg. "The compact genetic algorithm," IEEE transactions on evolutionary computation 3, no. 4 (1999): 287-297.

[52] Gupta, Sunet K., Pratyay Kuila and Prasanta K. Jana. "GAR: an energy efficient GA based routing for wireless sensor networks," in International conference on distributed computing and internet technology, pp. 267-277. Springer, Berlin, Heidelberg, 2013.

[53] Ghuleb, Baraq, Ahmed Al-Dubai, Elias Ekonomou, Mamoun Qasem, Imed Romdhani, and Lewis Mackenzie. "Addressing the DAO insider attack in RPL’s Internet of Things networks," IEEE Communications Letters 23, no. 1 (2018): 68-71.

[54] Alkhahifah, Ayman, Alex Ng, Paul A. Watters, and A. S. M. Kayes. "A Mechanism to Detect and Prevent Ethereum Blockchain Smart Contract Reentrancy Attacks." Frontiers in Computer Science 3 (2021): 1.

[55] Liu, Chao, Han Liu, Zhao Cao, Zhong Chen, Bangdao Chen, and Bill Roscoe. "Reguard: finding reentrancy bugs in smart contracts." In 2018 IEEE/ACM 40th International Conference on Software Engineering: Companion (ICSE-Companion), pp. 65-68. IEEE, 2018.

[56] Mishra, Binod Kumar, Mohan C. Niyam, and Prashant Lakkadwala. "Security against black hole attack in wireless sensor network-a review," In 2014 Fourth International Conference on Communication Systems and Network Technologies, pp. 615-620. IEEE, 2014.
ABRAR AHMED received the B.S. degree in computer engineering from COMSATS University Islamabad, (Formerly, COMSATS Institute of Information Technology) Pakistan, in 2006, the M.S. degree from Lancaster University, U.K., in 2008 and the Ph.D. degree in electrical engineering from COMSATS University Islamabad, in 2017. Since 2006, he has been associated with COMSATS University Islamabad, where he currently holds the position of an Assistant Professor. His research interests include wireless channel modelling and characterizing, smart antenna systems, nonorthogonal multiple access techniques and adaptive signal processing.

AYMAN RADWAN received his Ph.D. degree from Queen’s University, Kingston, ON, Canada, in 2009. He is a Senior Research Engineer and an Assistant Professor (Investigador Auxiliar) with the Instituto de Telecomunicações and University of Aveiro, Aveiro, Portugal. He is mainly specialized in coordination and management of EU funded projects. He participated in the coordination of multiple EU projects. He is currently the Project Coordinator of the CELTIC+ Project “SAFE-HOME”, as well as participating in multiple other EU projects. He has also been the Technical Manager of the FP7-C2POWER Project and the Coordinator of the CELTIC projects “GreenT” and “MUSCLES”. His current research interests include the Internet of Things, 5G, 6G and radio resource management.

***