**Journal of Information Systems Engineering and Management**
2025, 10(10s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

# Tp-DyHEQN: Trust Priority based Dynamic Homomorphic Elliptic Curve Encryption Algorithm Enabled Blockchain based Deep Learning Model for Secure Data Sharing

Jolly R. Nikhade[1], Dr. Shrikant V. Sonekar[2]
*[1]PGTD of Computers, RTMNU Nagpur*
*jollynikhade21@gmail.com*
*[2]Professor, Department of CSE,*
*J D College of Engineering and Management, Nagpur*
*srikantsonekar@gmail.com*

**ARTICLE INFO**

Received: 20 Nov 2024

Revised: 26 Dec 2024

Accepted: 18 Jan 2025

**ABSTRACT**

In recent times, data transmission in Wireless Sensor Network environments has become more prevalent. Nevertheless, these networks encounter numerous challenges during data transmission, including decreased network longevity, lower security, and lower energy efficiency. Furthermore, while authentication techniques ensure data authenticity, current mechanisms have security flaws such as identity spoofing, lack of transparency and scalability issues. Therefore, to overcome these challanges, a blockchain-based trust model known as trust priority-based dynamic homomorphic elliptic curve encryption algorithm enabled quantum convolutional neural network (Tp-DyHEQN), which enables secure data sharing and energy-efficient routing. The proposed trust priority-based energy loss minimization algorithm (Tp-EMA) enables energy-efficient routing, which minimizes the energy consumption of nodes and enhances the lifetime of the network. Additionally, the Tp-DyHEQN model detects the malicious activities of nodes, thus maintaining data privacy and safeguarding the network from unauthorized node activities. Moreover, the dynamic homomorphic elliptic curve encryption approach allows for computations to be performed on encrypted data without needing to decrypt it first enhancing network scalability and data integrity. The validation results prove that, compared to conventional approaches the proposed algorithm exhibits superior attack detection performance with an accuracy of 96.18% and a maximum privacy ratio of 0.92 for 500 nodes.

**Keywords:** Trust-based cluster head selection, Blockchain, secure data sharing, Deep learning, Data encryption

## 1. Introduction

With the emergence of innovative features, including mobility, flexibility, Wireless Sensor Networks (WSN) are becoming an important role of people's daily lives for their usual activities [25]. These networks are more efficient and are employed in many sectors such as home automation, industry, military, commerce, healthcare sectors, environment, and transportation because of their convenience as well as wider aspects of usage [5][9-11][1]. WSN is a package of distributed self-directed devices that gather information and wirelessly communicate with each other and also detect the physical changes in the surroundings [10]. They can sense, process, and commune with each other without any manual intervention and can send the data to the destination using different communication protocols [13-18][8]. The sensor nodes in WSN are smaller in size which can process the data and make transfer through RF frequency channels. These sensors are multifunctional, cost-effective, and also consume very low power which increases their demand from various sectors [17].

In addition, the WSN and communication technologies also serve as the basic part of IOT, in which the entire network is affected in case of failure of any sensor node [4]. Since IOT works with less human interaction, there is no limit for location and environment which leads to concerns in recovery, energy, and security [3]. For mobile ad-hoc networks, there are some classical flat routing algorithms such as Dynamic Source Routing (DSR) Destination

Sequence Distance Vector Routing (DSDV) [20], and Ad hoc On-Demand Distance Vector Routing (AODV) [19], where due to the sleeping mechanisms the communication links could be unavailable which leads to their poor performance in WSN [15]. Besides these routing protocols are important for efficiently delivering data from source to destination across Wireless Sensor IOT networks, they also have some limitations such as short battery life, void holes, Low Packet Acceptance Ratio (PAR), noise, because of the usage of terrestrial medium for communication [2].

To overcome the abovementioned issues, a decentralized storage mechanism are needed which could significantly improve the efficiency and data transparency that could build trust among the users without any interference from third parties [7]. Blockchain technology, which was first proposed in 2008, can address the aforementioned issues by deploying smart contracts, which contain nodes to monitor the distributed ledger's state and all system agreements. These networks, which can resolve trust difficulties between unknown entities through distributed and tamper-proof ledgers, are often classified into three categories: public, private, and consortium [21,22][14]. The transactions between the entities in the network are confirmed by the miners which validate the transaction using various consensus mechanisms [24][18]. Transaction data is recorded in the ledger, which is kept up to date by the distributed ledger, whenever there is an interaction between Block Chain entities. It has a chain-like appearance and is impenetrable since every block carries the hash of the one before it. Each block includes a hash, nonce, timestamp, and merkle root, all of which are linked to one another via a chain [23]. This research proposed a blockchain-based WSN to overcome the existing limitations which allows a secured communication without any tampering between the nodes.

The primary objective is to provide a robust data sharing and authentication scheme for blockchain-enabled WSN networks. The utilization of quantum computing principles in the Tp-DyHEQN model enhances the attack detection ability and safeguards the shard as well as stored information. The DyHEC algorithm and the PoA consensus mechanism verify the identity of sensor nodes, thereby preventing unauthorized access. Further, the Tp-EMA algorithm creates optimal paths based on the maximum trust score and minimum energy loss. The key highlights of the research are mentioned as follows,

- **Trust priority-based dynamic homomorphic elliptic curve encryption algorithm:** The algorithm leverages the benefits of three different encryption techniques thus reducing the complexity of the key management process. Further, the proposed algorithm prevents data tampering issues and also improves the integrity of the data. The node with the maximum trust score is identified as CH, thus minimizing the routing relay and offering scalable network performance.
- **Trust priority-based dynamic homomorphic elliptic curve encryption algorithm enabled quantum convolutional neural network:** The Tp-DyHEQN model processes vast amounts of data at unprecedented speeds, making it particularly suitable for dynamic attack detection in the WSN environment. This enables quicker detection and response to malicious activities, effectively reducing the computational complexity and overhead issues. Additionally, the DyHEC algorithm the scalability and flexibility of WSNs, enables quicker detection and response.

The remaining sections of the article are structured as follows, section 2 discusses the related works. The system model for the authentication and secure data sharing scheme is detailed in section 3 and section 4 demonstrates the working flow of the proposed algorithm. The s comparative analysis and simulation outcomes are discussed in section 5. Section 6 encapsulates the research conclusion and future works.

## 2. Related works

Authentication and secure data sharing is a crucial challenge in WSN networks, this section explores the advantages of the implemented methods with its inherent challenges.

Saba Awan *et al.* [1] presented trust management and routing mechanisms using blockchain technology, which leveraged the Rivest–Shamir–Adleman (RSA) algorithm for data encryption that improved network security and enabled secure routing. The deployment of trust trust-based approach in the presented approach effectively classified the malicious and legitimate nodes, which offered a high packet delivery ratio. However, the real-world applicability of the model is limited. An efficient and secure trust model was designed by Nadeem Javaid *et al.* [2] and the established technique utilized the Dijkstra algorithm for efficient routing. Moreover, the distributed IPFS systems provided cost-effective storage and enhanced the transparency of the model. Privacy leakage was the major challenge of this approach, and the evaluation results showed a lack of comparison with the existing protocols.

Abdul Rehman, *et al.* [3] implemented a clustering approach to enhance the security and energy efficiency of WSN. The integration of blockchain technology in the distribution systems improved layer-by-layer security and privacy from several attacks. However, the data transportation efficiency decreased with the increased data quantity. To improve authentication and secure data sharing in WSN Asad Ullah Khan, *et al.* [4] established a consortium blockchain approach. Further, the secure key management and IPFS storage system involved in this approach enhanced the security of the system. The established method proved superior results in terms of average gas consumption, execution time, and response time. Despite its superior performance, the system increased the transaction latency, which created scalability and trade-off challenges.

Murat Dener, and Abdullah Orman [5] utilized a secure authentication framework, which combined the three different cryptographic algorithms with blockchain smart contracts. The blockchain-enabled authentication protocol offered a high level of security in WSNs when considering energy and memory constraints. However, the established authentication protocol did not obtain accurate results. A cost-effective multi-hop routing mechanism was introduced by Muhammad Faisal and Ghassan Husnain [6]. The incorporation of energy efficient routing protocol selected a suitable cluster head (CH) for secure data sharing and minimized energy consumption. Further, data and credentials were stored in the cloud storage system, which avoid tampering attacks. However, the introduced framework did not safeguard the network lifetime and to improve network performance it necessitated additional consortium mechanisms.

Zahoor Ali Khan, *et al.* [8] designed a quality routing framework in WSN using blockchain and deep learning techniques. The Proof of Authority (PoA) mechanism was incorporated to resolve the computational overhead problems. The validation results proved that the implemented technique was more resilient against potential threats and vulnerabilities, also PoA minimized cost consumption. However, the ensemble deep learning models created complexities and required vast datasets for training. Jing Xiao *et al.* [9] initiated a swarm intelligence method for WSN that addressed the shortcomings of the conventional methods such as resource availability, and tampering effects. To resolve several security risks in the WSN framework, an efficient clustering framework was enabled in this approach, which enhanced the quality of clustering outcomes. The utilization of blockchain techniques ensured data encryption and tamper resistance. However, the swarm intelligence algorithm often struggled with local optimal problems, thus leading to increased complexity.

Volkan Gangal *et al.* [26] designed a low-energy adaptive clustering hierarchy (LEACH-AHP) protocol for energy-efficient routing. The LEACH-AHP algorithm determined the best route based on the energy and distance level to the CH and base station. Despite its superior performance, the LEACH-AHP algorithm necessitated high computational demand, which limits its practical applicability. Ashwinth Janarthanan and VidhushaVidhusha [27] implemented a deep learning-based Ebola optimization search routing algorithm (EOSA). The incorporation of efficient data aggregation schemes and blockchain technology offered superior validation results with minimum transmission delay. The routing performance of the EOSA model heavily relied on weight matrix adjustment, which affected the scalability of the routing procedure.

The game theory-based Generative Adversarial Network (GTGAN) model was initiated by K. H. Vijayendra Prasad and Sasikumar Periyasamy [28] to enable efficient routing in WSN. The ranking-based approach was leveraged to select the best route for a secure data-sharing process. However, the performance of the GTGAN model was lacking in terms of network management due to limited flexibility and scalability. Muneeswari G. *et al.* [29] utilized an energy-aware routing mechanism using the Sand Cat Swarm Optimization Algorithm (SCSOA), which improved the convergence performance of the protocol and facilitated a high packet delivery ratio. Despite its advantages, the established technique was not suitable for large-scale situations.

### 2.1 Challenges

The key challenges addressed from the conventional methods for secure data sharing and energy-efficient routing in WSN are mentioned as follows,

- The research utilized the LEACH protocol and did not consider the factors such as energy and trust factor for CH selection, which limited the performance CH selection process, and the consensus algorithms such as Proof of Stake (PoS) and PoA were not fully explored [6].
- The lack of encryption algorithms in the secure authentication framework limited the data security and increased latency, energy, and memory usage [5].

- The SCSOA-based routing protocol was not deemed suitable for large-scale applications additional encryption algorithms were required to improve model trust effectively [29].
- A notable challenge of the deep learning-based EOSA algorithm was the dependency on the adjustment of the weight matrix to attain the desired outcomes. However, creating an optimal weight matrix often proved difficult in system scalability [27].

### 2.2 Problem Formulation

In WSN, security remains a pivotal challenge, in which the data packets are transmitted from one node to another via wireless channels. In general network security can be affected by two different factors such as internal and external attacks [1]. While external attacks are caused by sensor nodes that are not part of the network, internal attacks are caused by the malevolent actions of interior sensor nodes. The secure routing issue in WSN is resolved by the network's nodes' dependability, which offers a dependable path for packets and the choice of a secure mobility model. When the secure routing protocol and encryption technology are used, the security model's trust value is high.. The overall trust value of the node in the mobility model $(T_{mob})$ is denoted as

$$T_{mob} = T_{in} + T_{\sec} + T_{nm} + T_{rel} \tag{1}$$

where $T_{in}$ indicates the initial trust value of the node, $T_{nm}$ denotes the node's trust value in the mobility model, $T_{\sec}$ represents the trust value of a node in the security model, and $T_{rel}$ represents the trust value of a node in the reliability model. Based on the trust score, the CH should be selected because each node should be given a score and the node that has a higher value of trust score is considered as CH. For the selected cluster network this varies for each time. Further, based on the trust score average residual energy of the CH is also seen as a high value, and the residual energy $A(l)$ should be represented as

$$A(l) = \frac{\sum_{g=1}^{M} \xi_r(\tau_g)}{M} \tag{2}$$

where $\xi_r$ signifies the residual energy of the $g^{th}$ selected CH, $M$ denotes the total CH nodes, $\tau_g$ indicates the sets of CH. The residual energy and area coverage rates directly impact the CH selection process based on the trust score. The area coverage rate $C_{area}$ is defined as the proportion of the total area covered by the node to the total monitoring area, which is mathematically formulated as follows,

$$C_{area} = \frac{n_{area}}{n_{total}} \tag{3}$$

where $n_{area}$ specifies the total area enclosed by the node, and $n_{total}$ denotes the total monitoring area. Based on the coverage rate, the energy consumption by the nodes in data transfer is in an optimal way. The total initial energy $\xi_{tot}$ in the network model is calculated as

$$\xi_{tot} = \xi_{CHg} + \xi_{Ni} \left| \xi_N \in \tau_g \cup G_h, i \in 0,1,\ldots.n \right. \tag{4}$$

where $\xi_{Ni}$ indicates the $i^{th}$ node's initial energy, $\xi_{CHg}$ represents the energy of CH, $G_h$ denotes the forward node set. Thus, the trust-based CH selection makes effective data transfer between base station and sensor nodes with minimization in energy consumption. After the selection of effective CH, improved encryption techniques are deployed to make secure data transmission and detection of malicious sensor nodes using Tp-DyHEQN model.

## 3. System Model for secure data sharing and authentication

The utilization of Blockchain-based WSN has evolved as a significant approach for authentication and secure data sharing. The detailed system model is shown in Figure 1. In the WSN environment, initially, the nodes are deployed, and from that the node with the best parameters such as maximum energy and trust is selected as CH. The node data gathered from the sensor nodes are stored in the blockchain layer through CH. The blockchain is a unique data-sharing scheme, which is in a distributed ledger format. Each block in the structure comprises data, the head and the body is the two components that make up each block. The head section contains the block number, nonce value, and timestamp, hash value of the previous and current blocks. Similarly, the body portion contains the transactions and data. The hash value of the previous block in the head section is not present in the first block. While the block number indicates the block number, the Nonce value, or "Number Only Used Once," indicates a number or value that can only be used once. The nonce is frequently utilized in cryptographic hash algorithms and authentication procedures. In addition, the data encryption scheme utilized in the device layer encrypts the node data and enhances the network's resilience against malicious activities. Further, the deep learning approach is incorporated to detect the malicious activities of the node and make an impact on the trust score of the nodes. The deployment of the inherent properties of blockchain and WSN systems can significantly improve the security of data against diverse malicious activities and offer superior performance in several applications including healthcare, industrial automation, and military.

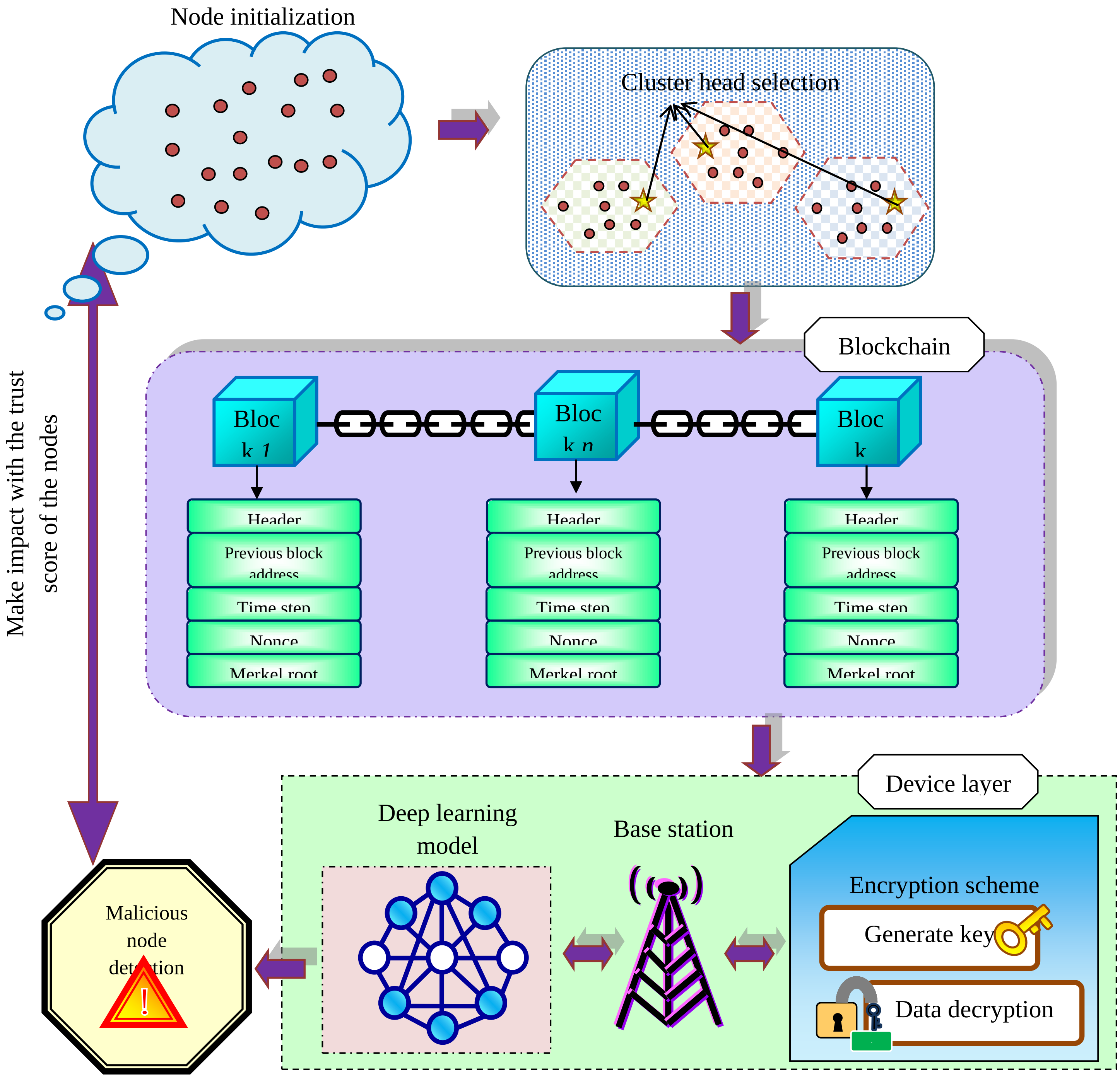


Figure 1: System Model for secure data sharing and authentication

## 4. Proposed Methodology for secure data sharing and authentication using Tp-DyHEQN

The research aims to securely share data in WSN based on Blockchain technology. Firstly, the initialization of nodes in the network takes place. Followed by initialization, the alive nodes in the network are selected to minimize time and complexity. CHs are selected for each network of nodes on a trust-based process and these CHs are responsible for gathering data from the sensor nodes and passing it to the base station. This data is routed, which is a process of selecting the path to avoid traffic in a network and for this secure data routing, a trust priority-based energy minimization algorithm is used that gives high emphasis to the priority of the network flow and reduces energy consumption. The node data is securely transfered to the base station and then Quantum Convolutional Neural Network (QCNN) is used to detect any presence of malicious nodes in the transmitted data. For secured blockchain transactions, the data is encrypted and transmitted to the base station using a DyHEC algorithm. Finally, the encrypted data is securely transmitted to the destination node through base station.

### 4.1 Node Initialization

In WSN, node initialization is the process of setting sensor nodes to communicate with each other, which maintains confidentiality and integrity of the data transferred within the network. Let us consider $n$ sensor nodes with some attributes such as node ID $N_{id}$, the position of the node $N_p$, and node data $Q_t$, which are mathematically considered as follows

$$X = \{x_i | i = 1,....n\} \tag{5}$$

$$x_i \in \{N_{id}, N_p, Q_t\} \tag{6}$$

Further, the sensing region of the node $s_r$ is considered as $R$, and the communication radius $c_r$ is represented as $2R$. The node's sensing area is a circular closed region with node coordinates as the radius $R$ and center denote the $X$ collection of sensor nodes. The position coordinates of the source node $x_i$ are signified as $(u_i, v_i)$ and the coordinates of the destination point $x_j$ are $(u_j, v_j)$.

### 4.2 Alive Node selection

Alive node is referred to as the sensor nodes, which are active in the network without depleting their energy. Alive node selection is the process of choosing operational nodes that can perform routing and data transmission. The longevity and efficiency of WSN relies on alive nodes, and the selection process involves choosing nodes with optimal positioning, and adequate residual energy for performing secure communication. Initially, all nodes are considered as alive nodes, and during transmission the nodes that lose their total energy are considered dead nodes. The energy required for the sensor node to transmit $\delta$ a bit data packet to the node $x_j$ is derived as follows,

$$\xi_{tx}(x_i, x_j) = \begin{cases} a_{tx} + e_{fs} d^2(x_i, x_j)\delta, & d(x_i, x_j) < D_0 \\ a_{tx} + e_{mp} d^4(x_i, x_j)\delta, & d(x_i, x_j) \geq D_0 \end{cases} \tag{7}$$

where $D_0$ specifies the threshold distance, $e_{fs}$ and $e_{mp}$ indicates the coefficient for energy dissipation in free space and multipath respectively. $a_{tx}$ and $a_{rx}$ denotes energy dissipation for transmitting and receiving 1 bit of data. The energy consumption for receiving the bit is given as $\xi_{tx}(x_j)$,

$$\xi_{tx}(x_j) = a_{rx}(\delta) \tag{8}$$

Therefore, the node with maximum energy is considered an alive node, which is suitable for transmitting data packets from source to destination. The alive nodes are then formed into clusters based on its trust value.

### 4.3 Trust-based cluster head selection

The trust-based CH selection and cluster formation is a significant approach, which enhances the network performance and reliability of the network. The trust-based CH selection technique hinges on the formulation of clusters within the network in which nodes are grouped together and among them, a cluster with maximum trust and energy efficiency is selected as CH. The CH is responsible for communication management between nodes. In this research, the clustering and selection of CH is performed using Particle swarm optimization (PSO). The PSO algorithm simulates the social behaviors such as flocking and schooling of birds and fishes respectively. In the context of WSN, the PSO algorithm is widely used for CH selection, which is superior for improving network efficiency and longevity [30]. The algorithm works based on the swarm of particles, which represents potential solutions (nodes) and moves around the search space to find optimal Clustering configuration and CH. By using this algorithm each node in the sensing region adjusts its position based on its own experience and the experience of neighbor nodes, effectively sharing information to find the best node as CH. Further, the nodes that are near the BS with similar properties are formed as clusters. In addition, the objective function of the PSO algorithm is computed based on the maximum trust value. The node with maximum trust is considered the CH. The mathematical formulation of trust-based CH selection is mentioned as follows,

Initially, the nodes in the sensing region are assumed as $X = \{x_i | i = 1,....n\}$ and each node has its own position and velocity vector, in which $x_{v\gamma}(t)$ and $x_{P\gamma}(t)$ represents the node velocity and position in $\gamma^{th}$ dimension during the time $t$. The vector $\Delta_i$ represents the solution (node) inside the issue space and has a dimension equal to some variables. The variables record their individual best optimal placements as well as the best local solution within the specified region. As a result of varying their velocities, or accelerating toward $Gl_{best}$ and $x_{best}$ with various stochastic factors, each placement element gets closer to optimal points. By using basic vector mathematics, it is straightforward to calculate the equations to update location and velocity, which is expressed as follows,

$$x_{v\gamma}(t+1) = wgt.x_{v\gamma}(t) + \wp_1 rand_1 \left(x_{best}(t) - x_{P\gamma}(t)\right) + \wp_2 rand_2 \left(Gl_{best}(t) - x_{P\gamma}(t)\right) \tag{9}$$

$$x_{P\gamma}(t+1) = x_{v\gamma}(t+1) + x_{P\gamma}(t) \tag{10}$$

where $wgt$ indicates the inertial weight, $rand_1, rand_2$ represents the random number, and $\wp_1, \wp_2$ indicates the constant coefficients. The key features of the PSO algorithm including its simplicity, faster performance, and multi-objective convergence in linear problems offer superior advancements in Cluster formation and CH selection process. In this research, based on the PSO algorithms the sensor nodes are divided into five clusters $Cl_N$, which are represented as $Cl_N | N = 1,....,5$. The sets of CHs selected using the PSO algorithm with trust factor is mentioned as $\tau_g$.

#### 4.3.1 Trust Priority-based Energy Loss Minimization Algorithm

The Tp-EMA is a sophisticated approach designed for optimizing the node's energy consumption during data transmission in WSN, which prioritizes the nodes based on their trust score and node availability. The risk of data loss in the network is minimized via the usage of trusted nodes, thus improving the data integrity. In the proposed Tp-EMA, the initial trust score $T_{scr_i}$ and energy of the node $\xi_i$ are considered as 1. The energy loss during transmission $(\xi_{loss})$ can be calculated by the proportion of energy loss per round $\xi_{LR}$ with a trust score per round $T_{SR}$, which is mathematically formulated as

$$\xi_{loss} = \frac{\xi_{LR}}{T_{SR}} \tag{11}$$

In addition, the total energy loss for the distance factor $\xi_{loss}(D_T)$ can be mathematically evaluated as follows.

$$\xi_{loss}\left(D_T\right) = \frac{\xi_{LR}}{T_{SR}} D_T \tag{12}$$

Where $\left(D_T\right)$ denotes the distance factor, which is calculated between the CH and node $i$, for instance, the trust score is inversely proportional to energy loss and distance factor. If the sensor node $i$ is malicious, then the initial trust score of the node gets reduced certain range, which is represented as

$$T_{\Re} = T_{scr_i} - \widehat{Z} \tag{13}$$

where $T_{\Re}$ indicates the node's trust score and round $\Re$, $\widehat{Z}$ represents the constant value, when the trust score of the node is reduced, then the energy loss of the node is increased. Else, the trust score is increased to a certain range.

$$T_{\Re} = T_{scr_i} + \widehat{Z} \tag{14}$$

Furthermore, the remaining energy of the node $\xi_{rem}$ can be evaluated based on the difference between the node's initial energy and the total energy loss $\left(Tot\xi_{loss}\right)$ from the node, which is expressed as

$$\xi_{rem} = \xi_i - tot\xi_{loss} \tag{15}$$

The Pseudocode of the Tp-EMA algorithm is depicted in algorithm 1. Thus, the Tp-EMA effectively optimizes the energy loss of nodes and maximizes the trust score for facilitating efficient routing for data transmission.

Algorithm 1: Pseudocode of Tp-EMA scheme

```
Pseudocode of Tp-EMA
Start
Initialize trust score $T_{scr_i} = 1$ and energy $\xi_i = 1$
Calculate energy loss for each round.
        $\xi_{loss} = \frac{\xi_{LR}}{T_{SR}}$
If the node $i$ is malicious,
        Calculate the trust score as $T_{\Re} = T_{scr_i} - \widehat{Z}$
Else
        Calculate the trust score as $T_{\Re} = T_{scr_i} + \widehat{Z}$
Calculate the remaining energy loss.
        $\xi_{rem} = \xi_i - tot\xi_{loss}$
End
```

## 4.4 Data transfer through blockchain

In WSN, secure data sharing remains a crucial challenge, therefore, this research leverages the blockchain-based data sharing scheme using the PoA consensus mechanism, which ensures data integrity. In addition, to ensure the security of data packets the Modified Dynamic AES with Homomorphic Encryption technique is used in this research, which dynamically encrypts and decrypts data and makes it more resilient to cyber-attacks. The Elliptic Curve Digital Signature Algorithm (ECDSA) incorporates verifying the signature (sign) of the data and suggests additional security for data transmission. Moreover, the Ethereum for data transfer initializes a decentralized platform that improves transparency and security. The flow of data within the network is extremely managed and the data from the CH is securely transmitted through BS and efficiently routed to the respective destination node. The detailed procedure of the secure data transfer phase is explained in the following section,

### 4.4.1 Data encryption and sign generation using DyHEC algorithm

In this data encryption phase, initially, the data from the particular nodes $Q_t$ are encrypted using the DyHEC mechanism [31]. The encryption rounds in this algorithm dynamically vary according to the encryption key size. While maintaining a superior level of security, the DyHEC algorithm uses the same key for encryption and decryption, which simplifies the key management process. In this research, the DyHEC algorithm processes the data with 128 bits in 10 rounds. During the encryption process, each round involves four different transformations including shift rows, mix columns, substitute bytes (SubBytes), and add round key transformation. The SubBytes transformation is the initial step in every round. At this point, the nonlinear S-box is used to replace a byte in the state with one more byte. However, the fixed number of S-boxes in the traditional algorithm is often vulnerable to attacks [32]. Therefore, to overcome this issue, this research generates dynamic S-boxes that enhance data security and adaptability. Following by SubBytes transformation, ShiftRow is deployed to modify the state, which moves the state's bytes cyclically to the left in each row instead of starting at row zero. The bytes from row zero stay in this process, and no permutation is performed. There is only one circular shift to the left in the first row of bytes. MixColumn is another important stage in the state process, which is not involved in the multiplication. In matrix transformation, every byte in a row is multiplied by every value (byte) in the state column. The AddRoundKey step of the proposed DyHEC algorithm is the most prominent in which the input data, also known as the state, and the key are both organized as $4 \times 4$ byte vectors. AddRoundKey can offer significantly higher security while encrypting data. The foundation of this process is formulating a connection between the encrypted text and the key. The encrypted data $En_{Q_t}$ and the symmetric key $S_K$ generated from the DyHEC algorithm, adds an extra layer of security through ensuring data integrity. The schematic illustration of the data encryption process using the proposed scheme is depicted in Figure 2.

Further, the symmetric key $S_K$ is encrypted using the partial homomorphic encryption (PHE) scheme, which preserves the confidentiality of the data by providing high-level security and allows calculations to be performed on encrypted data without decrypting. The proposed DyHEC algorithm addresses several challenges including latency and computational overhead. The primary function of the DyHEC algorithm is classified into key generation, encryption, and decryption [33].

*Key Generation:* In the key generation process, Let $J$ and $L$ are considered as two prime numbers and the integer $z$ is the product of the two prime numbers $(z = JL)$. Then Euler's phi function $\varphi$ is computed as $\varphi = (J-1)(L-1)$. Further, another prime $b$ is chosen, which is in the range of $1 < b < \varphi$. The greatest common divisor (GCD) is calculated for the chosen prime and Euler's phi function, which is represented as $GCD(b, \varphi)$. Moreover, $q$ is evaluated by calculating the multiplicative inverse of $b$, which is expressed as follows

$$bq \equiv 1 \bmod \varphi \tag{16}$$

Finally, the private $k_1$ and public keys $k_2$ are derived as follows,

$$k_1 = (b, z) \tag{17}$$

$$k_2 = (q, z) \tag{18}$$

*Encryption:* In the encryption process, the symmetric key $S_K$ generated from the previous stage is converted into a cipher text $(\Psi)$, which is represented as follows,

$$\Psi = E(S_K) = S_K^b \bmod z \tag{19}$$

The incorporation of PHE in the DyHEC algorithm maintains data integrity and also ensures the privacy of data without hindering the data transmission process.

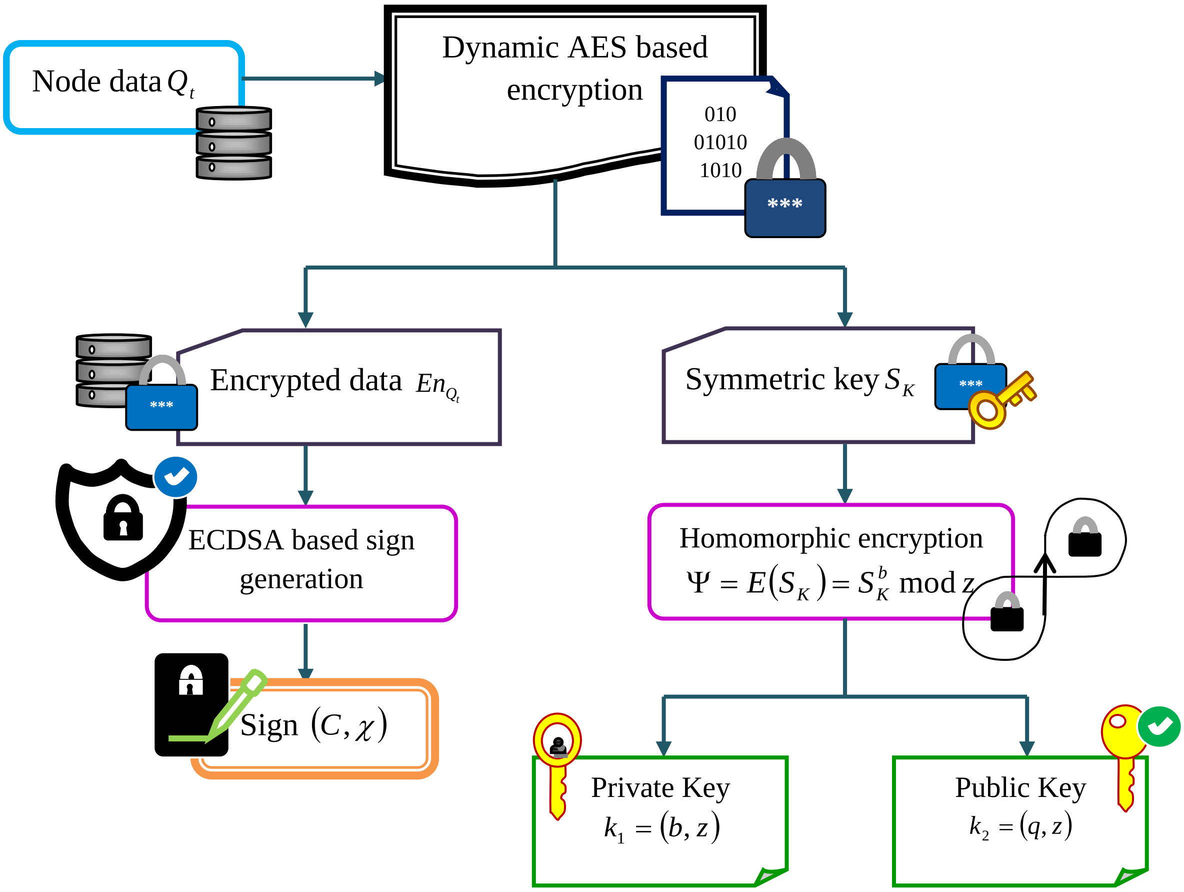


Figure 2: Data encryption using the DyHEC algorithm

Sign generation is the known as the method of creating a unique digital signature for each message to enhance the authenticity of the data. In the sign-generation phase, the integration of ECDSA in the DyHEC algorithm generates a sign for the encrypted data $En_{Q_t}$ . The DyHEC algorithm prevents data tampering issues and also improves the integrity of the data, which mainly focuses on the discrete logarithm problem [34]. Further, the proposed algorithm leverages four-point multiplication operations and comprises three procedures such as sign generation, key generation as well as sign verification. The aforementioned procedures are performed using the domain parameters $\Theta = \{h, m, f, O, Y, F, \Phi\}$, which $h, m$ represent the arbitrary coefficients, $\Phi$ denote the cofactor, $f$ denote the odd prime, $Y$ signify the order point, $O$ signify the base point, and $F$ represent the field representation. The DyHEC algorithm improves the efficiency of the encryption scheme by using smaller keys.

***Key generation:*** The key generation process is formulated as follows, initially, for key generation a random number $\alpha$ within the range of $[1, Y-1]$, and the public key is calculated as $B = P_k O$, where $P_k$ denotes the private key of an entity $w$.

***Sign Generation**:* The entity of CH $\tau_g$ and the domain parameters $\Theta = \{h, m, f, O, Y, F, \Phi\}$, are used to sign the data $En_{Q_t}$, which is estimated based on the subsequent process, initially a pseudorandom integer $\beta$ within the range of $[1, Y-1]$ is selected and the following calculation is performed as $\beta O = (p_1, r_1)$, further the variable $p_1$ is change into an integer $\tilde{p}_1$. Sign of the encrypted data $(C, \chi)$are calculate using the subsequent equations

$$C = p_1 \bmod Y \tag{20}$$

$$\chi = \beta^{-1}\{H(EnQ_t) + P_k C\} \tag{21}$$

where $H$ denotes the secure hash algorithm-1 (SHA-1).

### 4.4.2 Sign verification and data decryption

The signed data, encrypted key$(\Psi)$, original data $Q_t$, and encrypted node data $En_{Q_t}$, are transferred into the base station. Further, the base station verifies the sign to confirm the digital signature's authenticity using the DyHEC algorithm. If the sign verification is successful then the symmetric key $S_K$ decryption is performed that converts the cipher text into its original form. In addition, the decrypted symmetric key is used to decrypt the original data received from the nodes. Moreover, the proposed Tp-DyHEQN model is deployed to detect the presence of an attack in the received data. The detailed description of sign verification and data decryption is provided as follows,

***i) Sign verification:*** Sign verification is the process of validating the authenticity of a digital signature, which improves the security, integrity, and confidentiality of data transmission in WSN. To verify the signature of CH $\tau_g$ on $En_{Q_t}$, the base station obtains an authenticated copy of $\tau_g$ domain parameters $\Theta = \{h, m, f, O, Y, F, \Phi\}$. Sign verification using the DyHEC algorithm is explained as follows, initially the integers $C$ and $\chi$ are check whether they are in the range of $[1, Y-1]$ and the hash of the encrypted data can be calculated as follows

$$H = SHA - 1(EnQ_t) \tag{22}$$

Further, the variables $\vartheta_1 = HU \bmod Y$ and $\vartheta_2 = CU \bmod Y$ are calculated for signature verification, in which $U = \chi^{-1} \bmod Y$. By performing point addition, the set of integers are formed as follows

$$\vartheta_1 O + \vartheta_2 B = (p_0, r_0) \tag{23}$$

The newly generated signature can be formulated as follows

$$\mu = p_0 \bmod Y \tag{24}$$

If the newly generated signature and the original signature of the encrypted data same $\mu = C$ then accept the signature as a valid sign.

***ii) Key decryption:*** The proposed DyHEC algorithm is used to recover the cipher text $\Psi$ of the symmetric key using the private key pair $(q, z)$. The key decryption process ensures authenticity and avoids unauthorized access or data transfer in WSN. The mathematical formulation of the key decryption process is described in equation (13)

$$S_K = Dec(\Psi) = \Psi^q \pmod z \tag{25}$$

The symmetric key is further responsible for node data decryption that guarantees the confidentiality of the sensitive node data.

***iii) Data decryption using*** $S_K$ : Data decryption involves the conversion of encrypted data back into its original form. The conversion procedure is typically done using a symmetric decryption key, which can resolve privacy barriers that inhibit the sharing process in the WSN environment. Here, the original node data $Q_t$ should be derived from $En_{Q_t}$ using $S_K$. The final round of the decryption process comprises Inverse ShiftRows $(I_{SR})$, Inverse SubBytes $(I_{Sb})$, and Inverse AddRoundKey $(I_{ARK})$. The original data can be decrypted as follows,

$$Q_t = \left\{ I_{SR}\left( I_{Sb}\left( I_{ARK} \oplus En_{Q_t} \right)\right) \quad ; w = \iota - 1 \qquad (26)$$

where $w$ represents the round factor which decreased for each round $\iota$.

### 4.5 Malicious node detection using trust priority-based dynamic homomorphic elliptic curve encryption algorithm enabled deep learning model

In WSN, secure data transmission from node to base station remains a quite challenging task, because some nodes execute malicious activities through transmitting wrong information to the target nodes. Besides, the dispersed nature of WSNs makes them prone to several attacks, which can degrade the network quality and increase computational complexity [8]. Therefore, several malicious node detection techniques were developed for WSN. However, the conventional machine learning-based approaches including support vector machines (SVM), Decision Tree (DT), and Artificial Neural Network (ANN), have inherent limitations such as data complexity, and lack of interpretability problems. Moreover, the correlation techniques established for malicious node detection hindered the detection accuracy and also increased the probability of misjudgment issues [35]. Moreover, the deep learning approaches required large amounts of annotated data, were prone to misclassifying legitimate nodes as malicious, and low-level reliability [36]. As a result, the research proposes a Tp-DyHEQN model to tackle the aforementioned shortcomings. The Tp-DyHEQN model leverages the benefits of quantum CNN with the proposed DyHEC algorithm.

The Tp-DyHEQN model consists of an input layer, a single quantum 2dimensional (2D) layer, a convolutional 2D layer, and a fully connected (FC) layer with Rectified Linear Unit (ReLU) activation, which is depicted in Figure 3. Initially, the input data $Q_t$ with a dimension of $(n \times 35)$ undergoes a quantum filter circuit and the first step is to specify the data in quantum Hilbert space that increases exponentially with respect to the number of qubits. The 2D quantum layer in the Tp-DyHEQN model includes data encoding, quantum convolution, and quantum pooling layers. The data encoding layer is responsible for encoding the input data $Q_t$ into a quantum state. In the Tp-DyHEQN model, amplitude encoding is performed to convert the classical data into a quantum state that minimizes the number of parameters required for encoding and also reduces the system complexity [37]. The encoding process expresses the amplitudes of a $y$ qubit quantum state $\left|\phi(Q_t)\right\rangle$ as input data $Q_t = \{Q_{t1}, \ldots\ldots Q_{tN}\}^{\mathrm{T}}$ of dimension $\mathrm{N} = 2^y$.

$$\Upsilon_\phi(Q_t) : Q_t \in \square^{\mathrm{N}} \rightarrow \left|\phi(Q_t)\right\rangle = \frac{1}{\|Q_t\|} \sum_{V=1}^{\mathrm{N}} Q_t^V \left|V\right\rangle \qquad (27)$$

Where $\left|V\right\rangle$ signifies the $V^{th}$ computational basis state, $\Upsilon_\phi(Q_t)$ denotes the unitary transformation. Moreover, instead of being an inner product as in the classical example, the quantum convolutional operation is a unitary transformation of a state vector, which is a linear map that converts one vector to another, while a traditional convolution process is a linear map that creates a scalar from a vector. Half of the qubits are traced out by the pooling in the Tp-DyHEQN model, whereas parameterized two-qubit is typically included in the pooling layer and the control qubits are traced out after the gate procedures for controlled-unitary gates. Ultimately, the circuit's result is determined by evaluating a fixed number of output qubits.

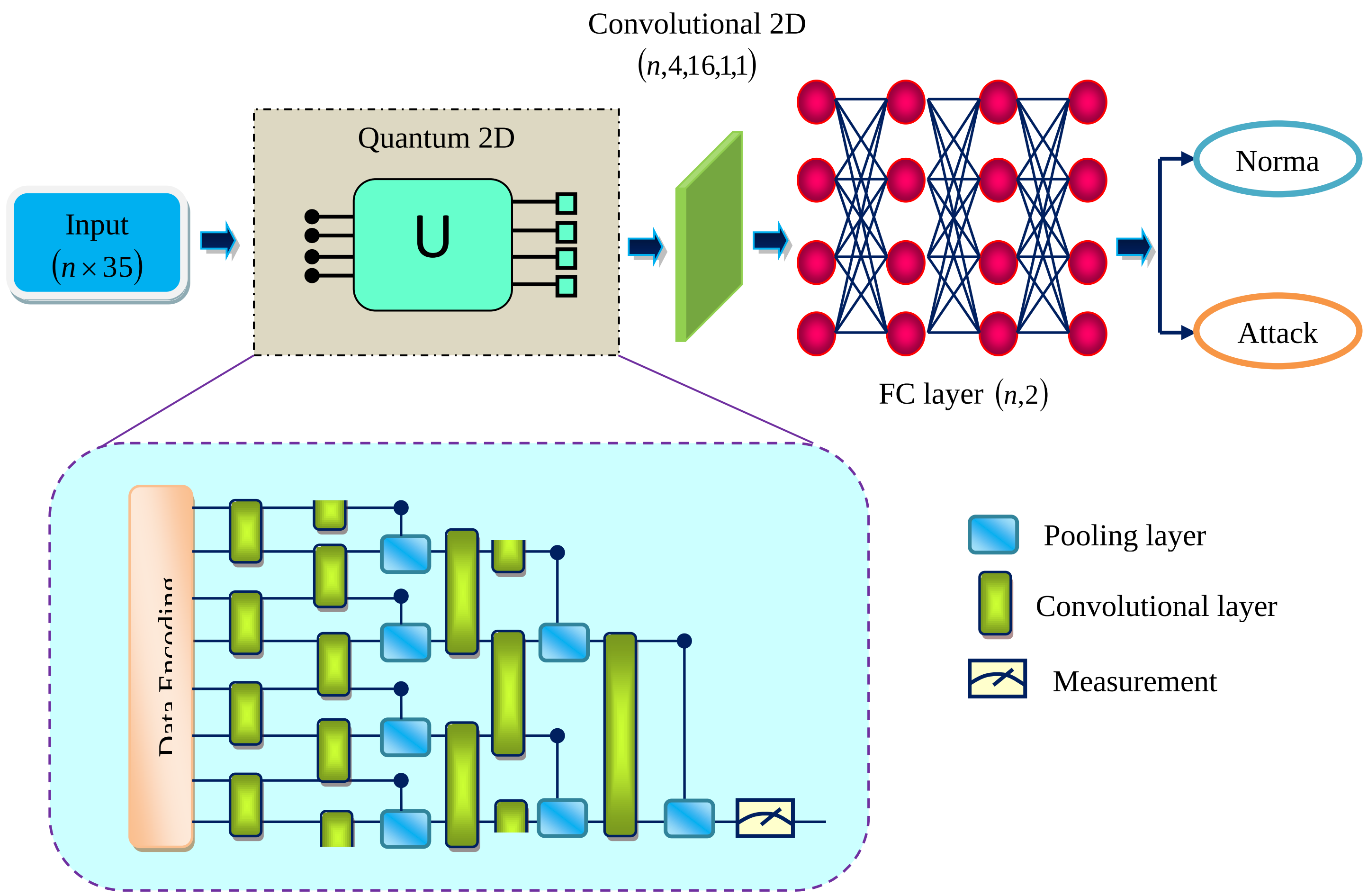


Figure 3: Architecture of Tp-DyHEQN model

Followed by a quantum 2D circuit, the convolutional 2D layer is deployed, which learns meaningful features from the previous layer and the extracted features using this layer are denoted as $K_Q$, which further undergoes the FC layer. The quantum FC layer is defined as a parametrized Hamiltonian up to a second-order correlation, which comprises Pauli operators $\bar{\lambda}_K$ and Hamiltonian identity operators $\Gamma$ that are represented as

$$\aleph = \varepsilon^{y_1}\Gamma + \sum_{y_2} \varepsilon^{y_2} \bar{\lambda}_K^{y_2} + \sum_{y_2, y_3} \varepsilon^{y_2, y_3} \bar{\lambda}_K^{y_2} \bar{\lambda}_K^{y_3} \tag{28}$$

Where $\aleph$ denotes the Hamiltonian matrix, $\varepsilon^{y_1}, \varepsilon^{y_2}, \varepsilon^{y_2, y_3}$ represents the parameters, and $y_1, y_2 y_3$ indicates the qubits [38]. The attack detection output of the Tp-DyHEQN model $\ell(\upsilon)$ is measured as follows,

$$\ell(\upsilon) = \langle \upsilon | \aleph | \upsilon \rangle \tag{29}$$

where $\upsilon$ represents the non-linear activation. If any attack is detected by the Tp-DyHEQN model, it minimizes the trust score of the WSN nodes, which prevents the network from unauthorized access and offers secure data transmission.

## 5. Results and Discussion

The following section describes the simulation setup and comparative results of the Tp-DyHEQN with 100 and 200-node analysis. Furthermore, the attack detection performance of the Tp-DyHEQN model is assessed in terms of recall, accuracy, F1 score, and precision. The routing performance of the Tp-EMA scheme is analyzed via delay (ms), privacy ratio, alive nodes, and energy.

### 5.1 Experimental Setup

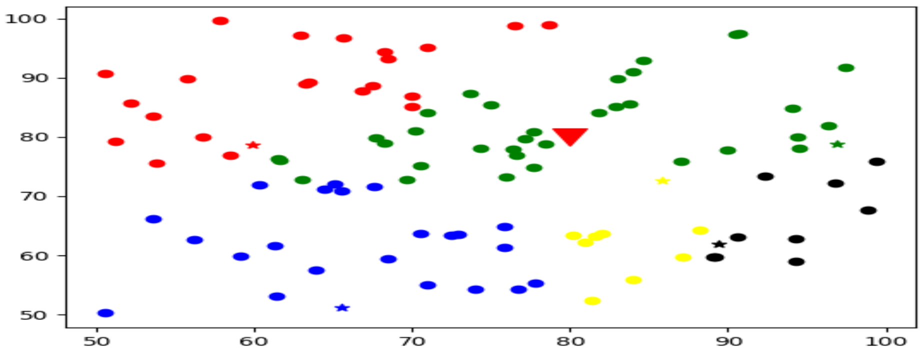
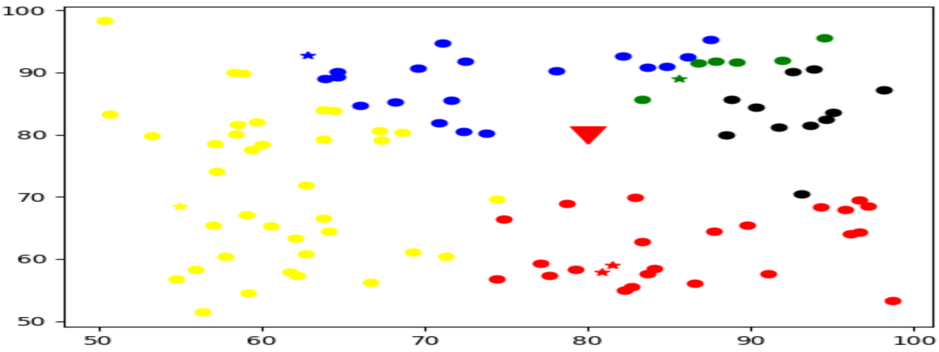
The execution of the proposed research for malicious node detection and energy-efficient secure routing can be performed in a Windows 10 operating system using PyCharm software, which ensures compatibility and sufficient processing power. With the 16 GB of RAM, the system is well-equipped to handle large datasets. Further, the BotIoT dataset [39] is used for simulating IoT botnet attacks, in which the attack information is in comma-separated values (CSV) format. The dataset contains the attack types including Reconnaissance, Service Scan, Exploits, Generic, denial of service (DoS), Fuzzers, Shellcode, Worms, and Distributed DoS (DDoS) attacks.

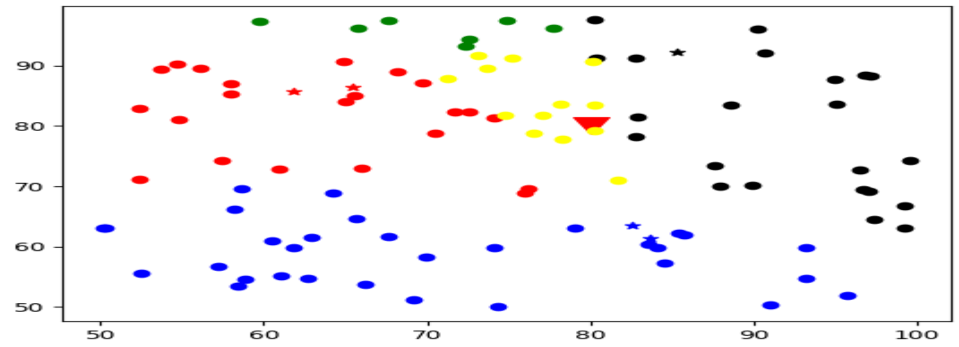
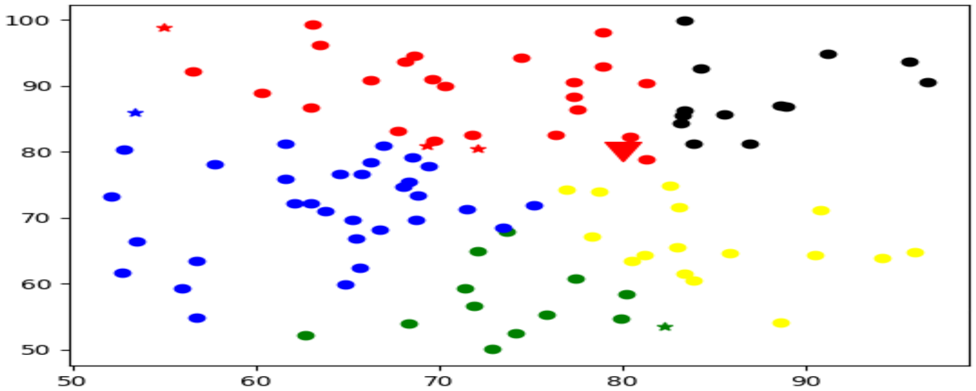
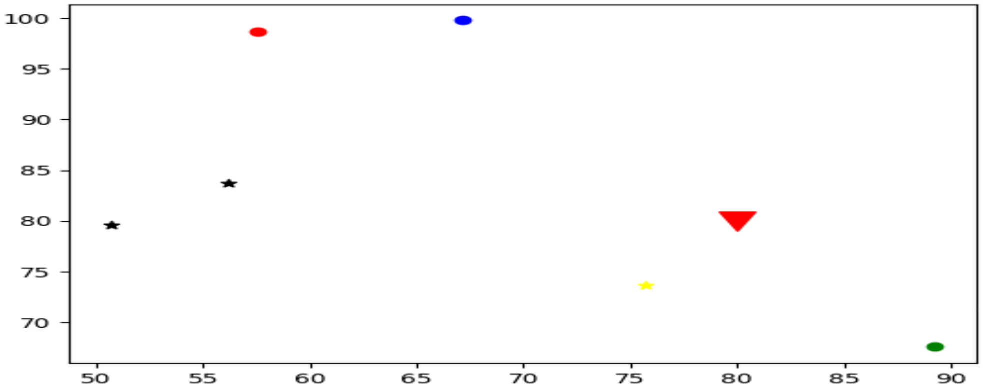
### 5.2 Performance Metrics

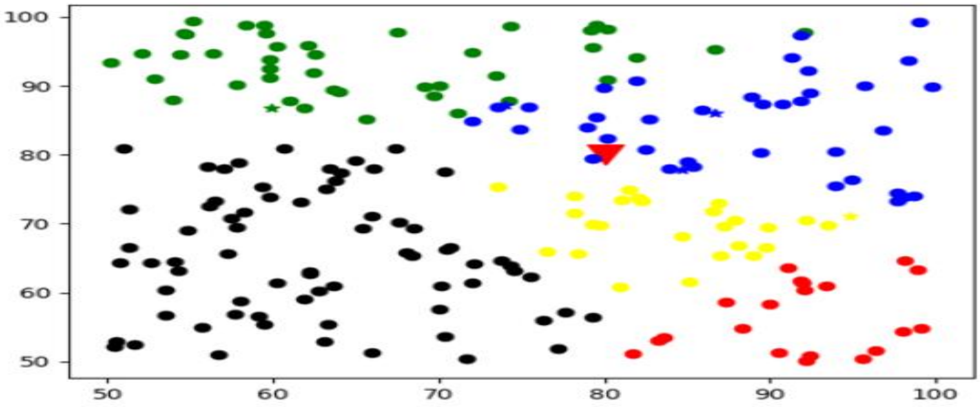
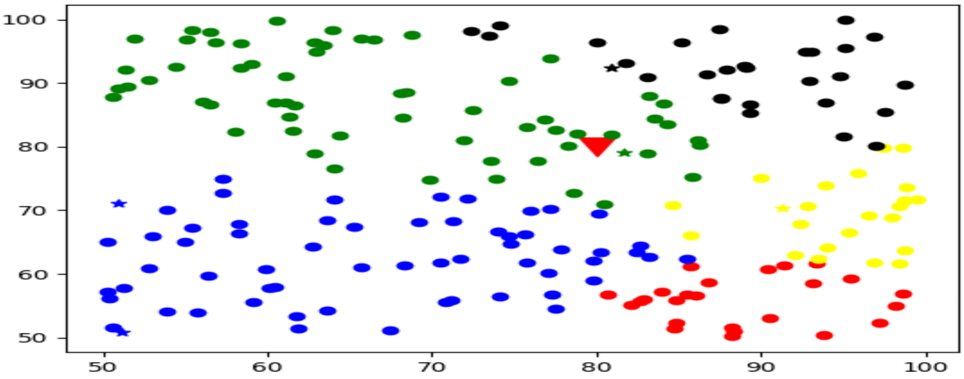
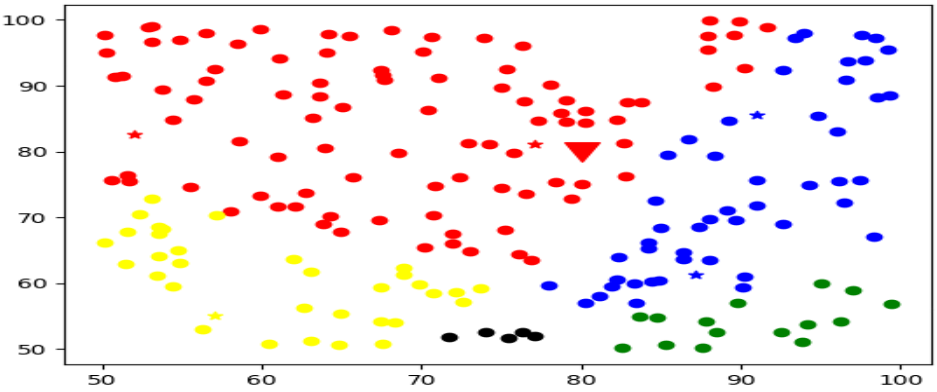
The attack detection performance of the Tp-DyHEQN approach is evaluated using the metrics accuracy, precision, F1 score and recall. In addition, the routing performance of Tp-EMA is measured in terms of delay, alive nodes, energy value, and privacy ratio.

### 5.3 Simulation results

Figure 4 illustrates the simulation results obtained using the Tp-DyHEQN model, in which the analysis is done through 100 and 200 nodes. The deployment of PSO algorithm for cluster formation and CH selection is represented by the red, green, yellow, blue, and black dots, in which each color represents the distinct color. The triangle icon indicates the base station and the star icons signify the CH. In addition, the figure depicts the simulation results of nodes with 1000, 2000, 3000, and 3500 rounds. The 3500th round contains a minimal number of nodes, which exhibits that the Tp-DyHEQN model eliminates the dead nodes. Moreover, the gradual decrease in the number of nodes as the rounds progress underscores the model's approach to energy management. The Tp-DyHEQN model prevent the redundant expenditures of the collective energy through the elimination of nodes with depleted energy reserves, thus enhances the overall system performance.

| **Number of nods/ rounds** | **100 nodes** |
|---|---|
| **Node initialization** |  |
| **1000 rounds** |  |

| | |
|---|---|
| **2000 rounds** |  |
| **3000 rounds** |  |
| **3500 rounds** |  |
| | **200 nodes** |

| | |
|---|---|
| **Node initialization** |  |
| **1000 rounds** |  |
| **2000 rounds** |  |

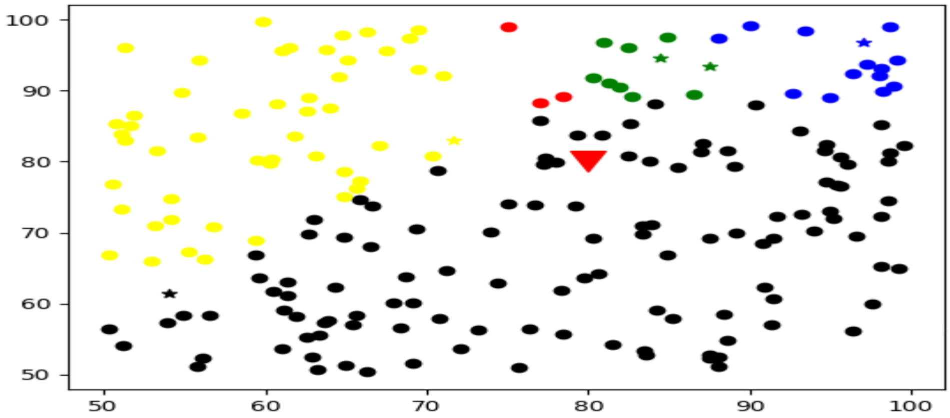
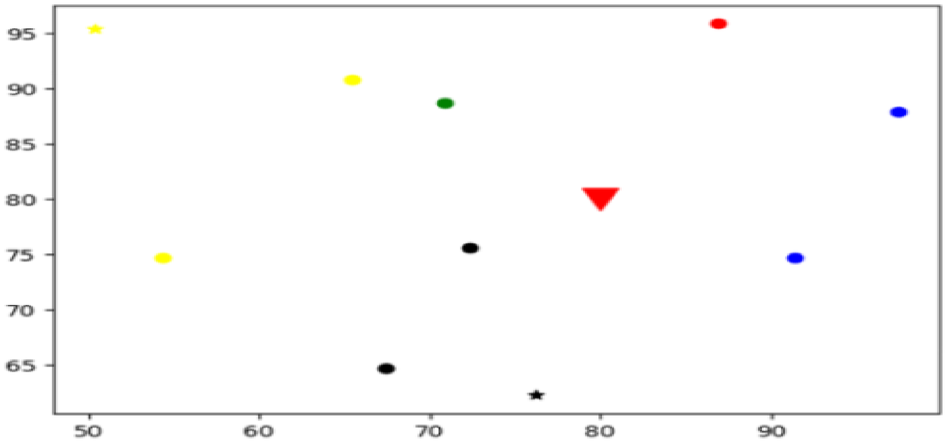
| | |
|---|---|
| **3000 rounds** |  |
| **3500 rounds** |  |

Figure 4: Simulation results

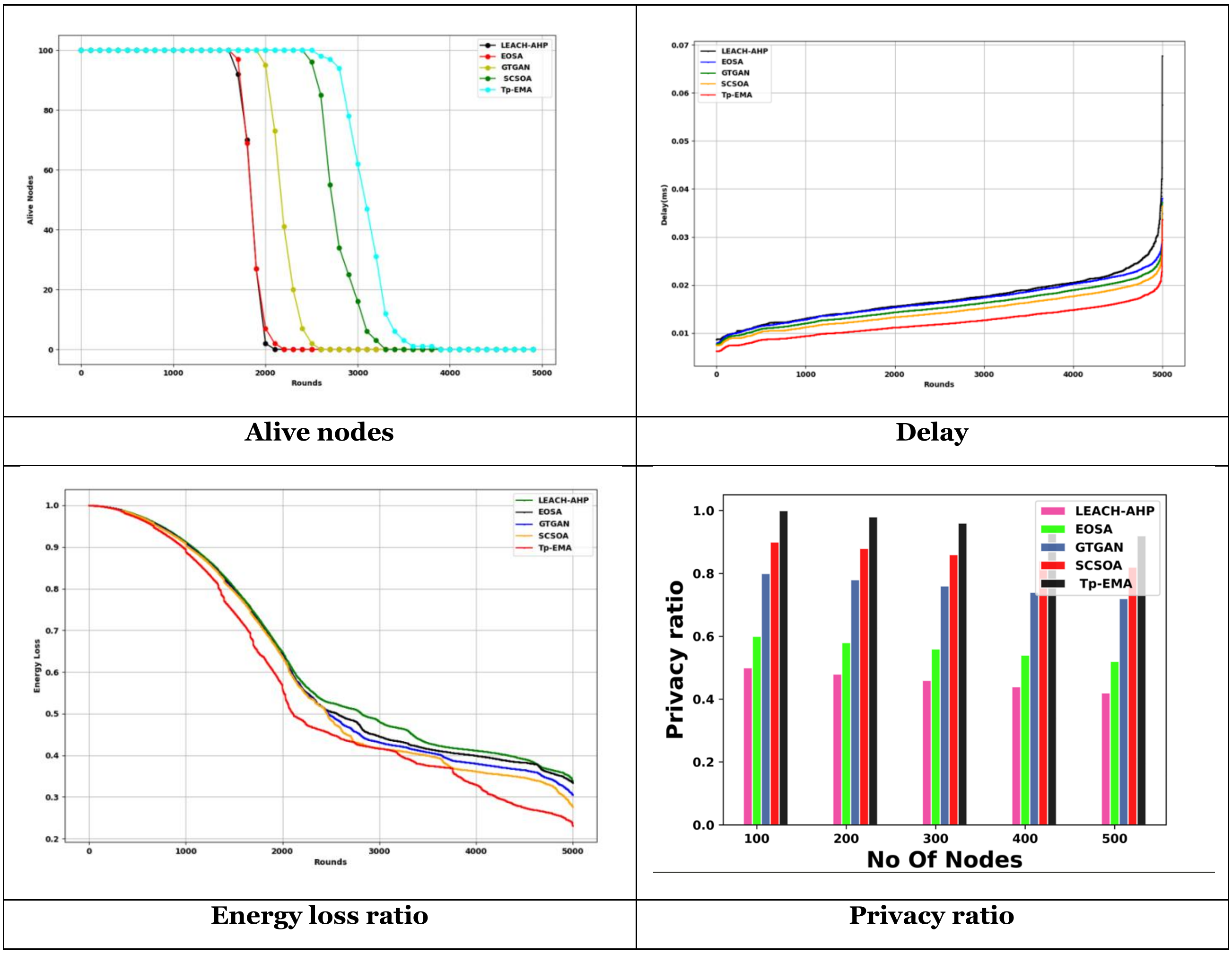
### 5.4 Comparative Methods

The routing performance of the Tp-EMA is compared with conventional routing protocols such as LEACH-AHP [26], EOSA [27], GTGAN [28], and SCSOA [29]. In addition, the attack detection performance of the Tp-DyHEQN model is compared with the existing techniques such as RSA [1], Dijkstra algorithm [2], Heterogeneous gateway-based energy-aware multi-hop routing (HMGEAR) [8], Attribute-based access control (A-BAC) [7], Energy-Efficient Adhoc On-demand Distance Vector (EEAODV) [6], Secure Clustering Routing Method based on Blockchain and Swarm Intelligence (BS-SCRM) [9], and SVM [40].

#### 5.4.1 Comparative Analysis with 100 nodes

The routing performance of Tp-EMA is compared with the traditional routing algorithms such as LEACH-AHP, EOSA, GTGAN, and SCSOA, with several metrics including alive nodes, delay, energy loss, and privacy ratio depicted in Figure 5. At 2500 rounds, the LEACH-AHP algorithm has 2 alive nodes, and the EOSA algorithm has 7 alive nodes, while the proposed Tp-EMA has 98 alive nodes. At 3200 rounds, the existing algorithms lost their node energy, but the proposed Tp-EMA scheme has 31 alive nodes. Thus the results exhibit that the Tp-EMA prolongs the lifetime of the network and improves energy efficiency. The packet transmission delay of the Tp-EMA scheme at 4000 rounds is 0.014 milliseconds (ms), while the other algorithms such as LEACH-AHP and EOSA increase the delay by 0.020 ms, 0.017ms respectively. In terms of the energy loss ratio, initially, all algorithms have an equal energy of 0.99, whereas the number of rounds increase the energy value decreases. The GTGAN algorithm has an energy loss ratio of 0.304 for 5000 rounds, while the proposed Tp-EMA scheme has a minimum energy loss ratio of 0.23. Therefore, the Tp-EMA scheme facilitates energy-efficient routing and secure data sharing in WSN.

Moreover, the Tp-EMA scheme has a 0.92 privacy ratio for 500 nodes, while the existing algorithms including LEACH-AHP, EOSA, GTGAN, and SCSOA have less privacy ratio of 0.42, 0.52, 0.72, and 0.82 respectively. The higher privacy ratio of the Tp-EMA scheme exhibits a more robust approach to protecting confidentiality and data integrity within the network.



**Alive nodes**

**Delay**

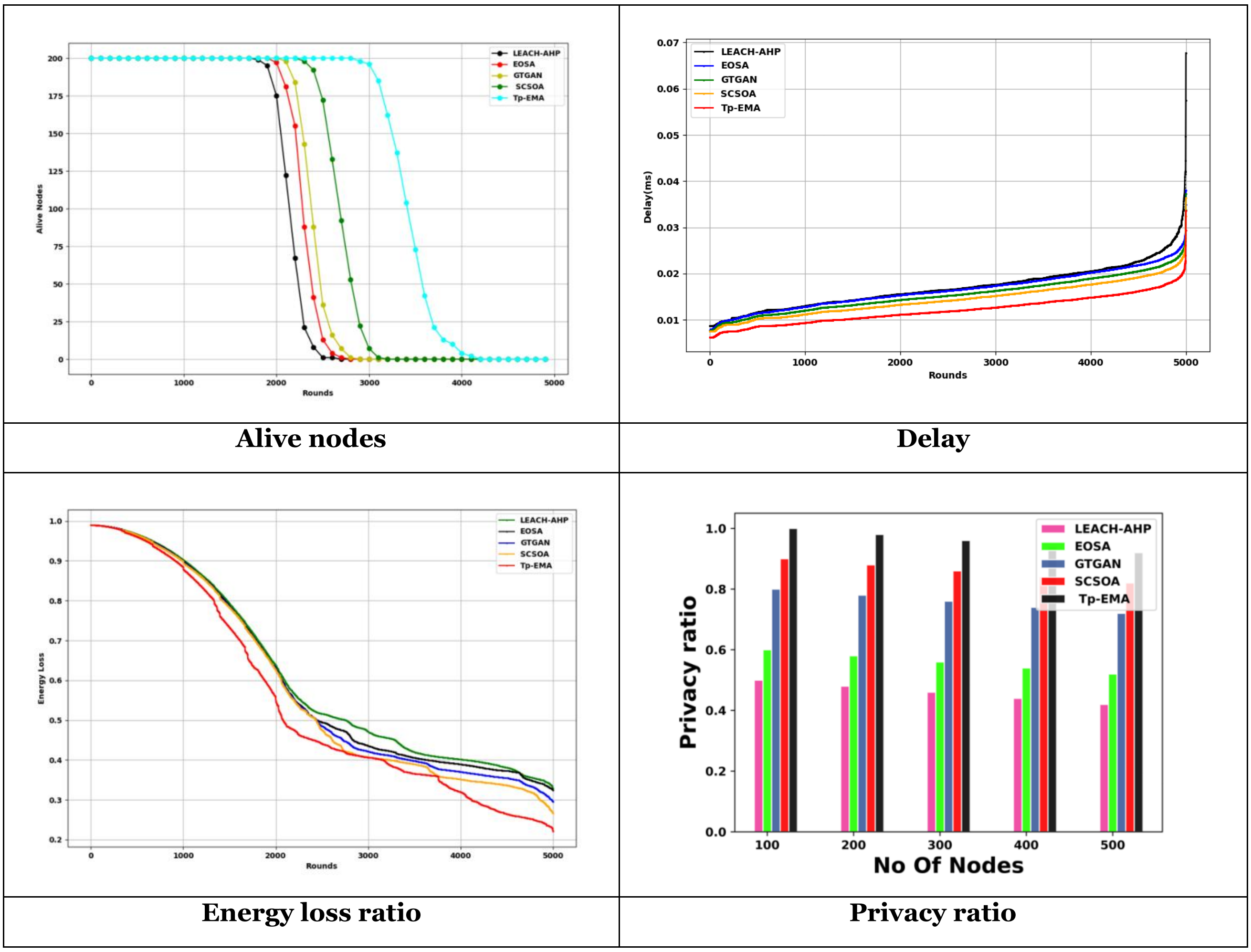
**Energy loss ratio**

**Privacy ratio**

Figure 5: Comparative Analysis with 100 nodes

### 5.4.2 Comparative Analysis with 200 nodes

Figure 6 compares the routing performance of the Tp-EMA with the conventional routing algorithms LEACH-AHP, EOSA, GTGAN, and SCSOA in terms of the aforementioned performance metrics. The Tp-EMA scheme has 198 alive nodes at 2600 rounds, compared to 8 live nodes for the LEACH-AHP algorithm and 41 live nodes for the EOSA algorithm. The current algorithms lost node energy around 3500 rounds, but the 73 nodes in the suggested Tp-EMA scheme are still alive. As a result, the data shows that Tp-EMA increases energy efficiency and extends network lifetime. The Tp-EMA scheme's packet transmission delay at the 4000 round is 0.015 ms, but other methods, such as GTGAN and SCSOA, cause a delay of 0.019 ms and 0.018 ms respectively. During data transmission, the Tp-EMA scheme has a lower energy loss ratio of 0.40 at 3000 rounds, on the other hand, the existing algorithms SCSOA and EOSA have energy loss ratios of 0.42 and 0.47. Thus, the results demonstrate that the Tp-EMA scheme enables an efficient route for secure data transmission with minimum energy loss. Moreover, the Tp-EMA scheme has a 0.92 privacy ratio for 500 nodes, while the existing algorithms including LEACH-AHP, EOSA, GTGAN, and SCSOA have less privacy ratio of 0.42, 0.52, 0.72, and 0.82 respectively.



Alive nodes

Delay

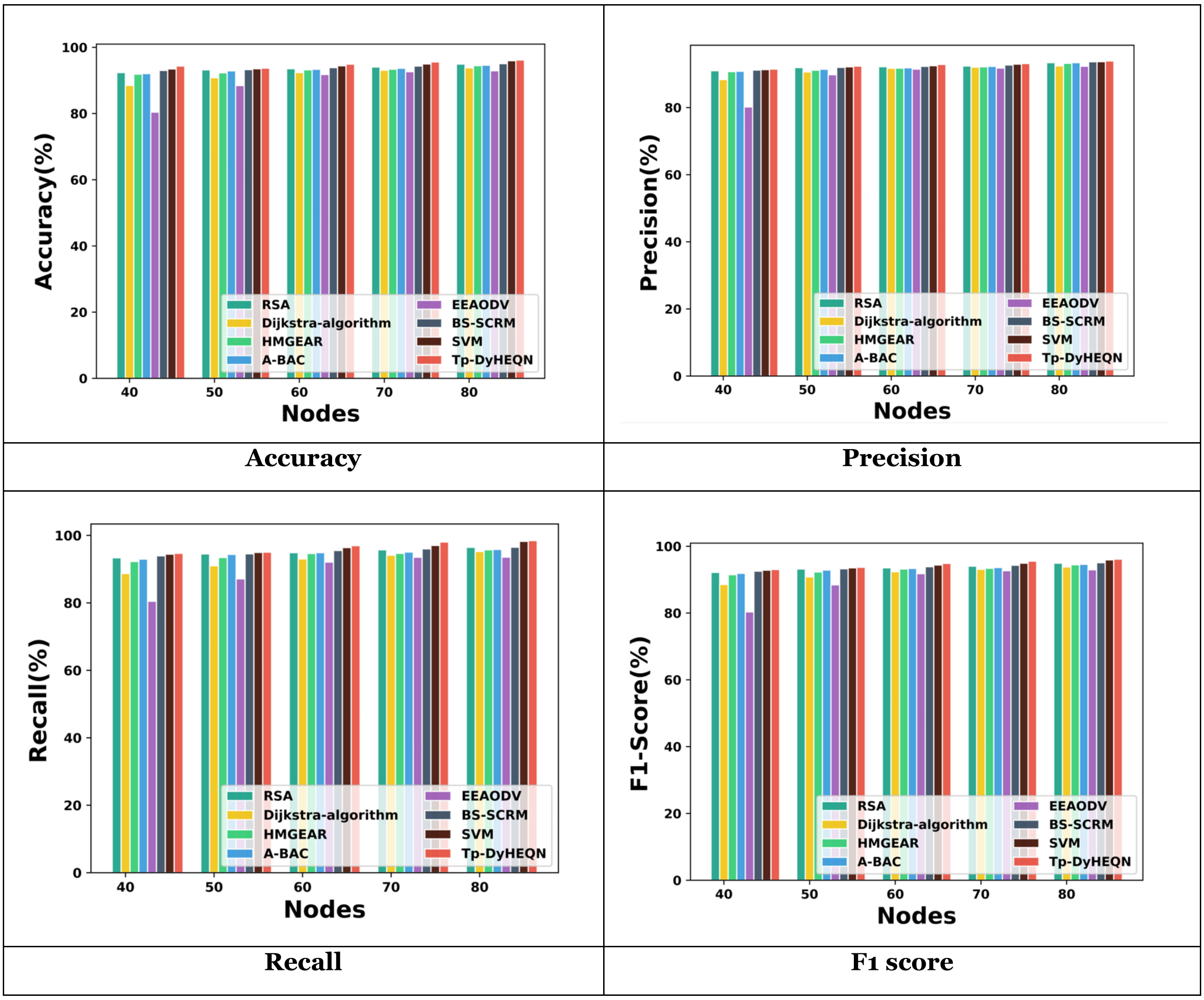
Energy loss ratio

Privacy ratio

Figure 6: Comparative Analysis with 200 nodes

### 5.4.3 Comparative Analysis of Tp-DyHEQN model with training percentage analysis

The attack detection performance of the Tp-DyHEQN model is compared with the conventioanl techniques such as RSA, Dijiksra algorithm, HMGEAR, A-BAC, EEAODV, BS-SCRM, and SVM, which is graphically represented in Figure 7. For 90% of training, the Tp-DyHEQN model gets an accuracy of 96.18% and it shows performance enhancement over techniques such as A-BAC, SVM, and RSA by 1.65%, 0.23%, and 1.30% respectively. With the recall measure of 98.46%, the Tp-DyHEQN model outperforms the conventional Dijiksra algorithm by 3.29%, and EEAODV by 5.00%. The high recall value represents that the majority of malicious nodes are correctly identified, which reduces the risk of undetected attacks in the network. Moreover, the Tp-DyHEQN model obtains a precision of 93.90%, which surpasses the existing techniques including HMGEAR, EEAODV, and RSA by 0.75%, 1.685, and 0.54% correspondingly. In terms of F1 score, the Tp-DyHEQN model attains 96.13%, which shows an improved performance of 3.335 over EEAODV, 1.12% over BS-SCRM, and 2.42% over the Dijiksra algorithm. The higher F1 score exhibits the trade-off between precision and recall that improves the model's robustness against malicious activities.



Accuracy

Precision

Recall

F1 score

Figure 7: Comparative Analysis of Tp-DyHEQN model with training percentage analysis

### 5.5 Comparative Discussion

The comparative discussion of the Tp-DyHEQN model for malicious node detection tasks is explained in Table 1. While conventional algorithms such as RSA, the Dijkstra algorithm provides robust security, which is computationally intensive and has limited processing capabilities. In addition, the HMGEAR approach faces challenges in balancing energy consumption across the network, which is crucial for prolonging the network's lifespan. Moreover, the SVM technique necessitates a significant amount of data for training, which might not be feasible in WSNs with, limited bandwidth and storage. The aforementioned shortcomings are resolved in this Tp-DyHEQN model using its unique quantum computing principles, trust-based CH selection, and dynamic homomorphic encryption standards The Tp-DyHEQN model offers superior detection performance with a maximum accuracy of 96.18, thus improving data integrity and scalability.

Furthermore, in terms of efficient routing, the LEACH-AHP protocol commonly used for finding the shortest path in routing may not scale efficiently in dynamic WSN environments, potentially leading to suboptimal routing decisions. The GTGAN model lacks its performance in network management due to limited flexibility and scalability. Furthermore, the SCSOA introduces complexity and overhead. In contrast with other routing algorithms, the proposed Tp-EMA scheme prioritizes the routes based on the trust score and minimum energy loss, which enhances the life span of the network and offers data integrity with a minimal energy loss ratio of 0.44. The detailed comparison of the existing routing algorithms with the Tp-EMA model is delineated in Table 2.

Table 1: Comparative Discussion with 90% of training

| Metrics/ methods | Accuracy (%) | Precision (%) | Recall (%) | F1 score (%) |
|---|---|---|---|---|
| **RSA** | 94.93 | 93.39 | 96.47 | 94.91 |
| **Dijkstra-algorithm** | 93.82 | 92.42 | 95.22 | 93.81 |
| **HMGEAR** | 94.46 | 93.20 | 95.72 | 94.45 |
| **A-BAC** | 94.60 | 93.38 | 95.82 | 94.59 |
| **EEAODV** | 92.94 | 92.33 | 93.54 | 92.94 |
| **BS-SCRM** | 95.07 | 93.65 | 96.49 | 95.06 |
| **SVM** | 95.96 | 93.67 | 98.25 | 95.92 |
| **Tp-DyHEQN** | **96.18** | **93.90** | **98.46** | **96.14** |

Table 2: Comparative Discussion with 2900 rounds

| | **100 nodes with 2900 rounds** | | | | **200 nodes with 2900 rounds** | | | |
|---|---|---|---|---|---|---|---|---|
| **Metrics/ methods** | **Alive nodes** | **Delay (ms)** | **Energy loss ratio** | **Privacy ratio** | **Alive nodes** | **Delay (ms)** | **Energy loss ratio** | **Privacy ratio** |
| LEACH-AHP | 0 | 0.017 | 0.48 | 0.42 | 0 | 0.017 | 0.51 | 0.52 |
| EOSA | 0 | 0.015 | 0.44 | 0.52 | 0 | 0.015 | 0.49 | 0.72 |
| GTGAN | 0 | 0.016 | 0.53 | 0.72 | 0 | 0.016 | 0.48 | 0.72 |
| SCSOA | 25 | 0.017 | 0.42 | 0.82 | 22 | 0.17 | 0.47 | 0.82 |
| **Tp-EMA** | **78** | **0.012** | **0.41** | **0.92** | **198** | **0.012** | **0.44** | **0.92** |

## 6. Conclusion

In conclusion, this research presents a Tp-DyHEQN model for facilitating data integrity and confidentiality in a WSN environment. The combination of quantum computing principles in the Tp-DyHEQN model adds a layer of security through quantum-resistant algorithms, making the system resilient against malicious activities of nodes. Moreover, the Tp-EMA scheme works based on the trustworthiness of nodes, which optimizes the energy loss that occurs during transmission. Furthermore, the Tp-DyHEQN model not only secures data transmission but also ensures efficient and scale data sharing using optimal routing mechanisms. The utilization of the DyHEC algorithm simplifies the key management process and facilitates two-level security for the data obtained from nodes. The inherent security properties of blockchain including cryptographic security, non-repudiation, and auditability improve the network security and facilitate secure data sharing among nodes. The experimental results obtained for the Tp-EMA scheme demonstrate superior performance with a minimum packet transmission delay of 0.015 ms, which is superior to the existing routing algorithms. Additionally, the attack detection performance of the Tp-DyHEQN model with 90% of training data shows a superior detection accuracy of 96.18%. In the future, additional hybrid optimization algorithms will be required to optimize the cluster formation and CH selection process.

## References

[1] Awan, S., Javaid, N., Ullah, S., Khan, A.U., Qamar, A.M. and Choi, J.G., 2022. Blockchain-based secure routing and trust management in wireless sensor networks. Sensors, 22(2), p.411.

[2] Javaid, N., 2022. A secure and efficient trust model for wireless sensor IoTs using blockchain. IEEE Access, 10, pp.4568-4579.

[3] Rehman, A., Abdullah, S., Fatima, M., Iqbal, M.W., Almarhabi, K.A., Ashraf, M.U. and Ali, S., 2022. Ensuring security and energy efficiency of wireless sensor network by using blockchain. Applied Sciences, 12(21), p.10794.

[4] Khan, A.U., Javaid, N., Khan, M.A. and Ullah, I., 2023. A blockchain scheme for authentication, data sharing and nonrepudiation to secure internet of wireless sensor things. Cluster Computing, 26(2), pp.945-960.

[5] Dener, M. and Orman, A., 2023. Bbap-wsn: a new blockchain-based authentication protocol for wireless sensor networks. Applied Sciences, 13(3), p.1526.

[6] Chandan, R.R., Balobaid, A., Cherukupalli, N.L.S., HL, G., Flammini, F. and Natarajan, R., 2023. Secure modern wireless communication network based on blockchain technology. Electronics, 12(5), p.1095.

[7] Ullah, Z., Raza, B., Shah, H., Khan, S. and Waheed, A., 2022. Towards blockchain-based secure storage and trusted data sharing scheme for IoT environment. IEEE access, 10, pp.36978-36994.

[8] Khan, Z.A., Amjad, S., Ahmed, F., Almasoud, A.M., Imran, M. and Javaid, N., 2023. A blockchain-based deep-learning-driven architecture for quality routing in wireless sensor networks. IEEE Access, 11, pp.31036-31051.

[9] Kandris, D., Nakas, C., Vomvas, D. and Koulouras, G., 2020. Applications of wireless sensor networks: an up-to-date survey. Applied system innovation, 3(1), p.14

[10] Yetgin, H., Cheung, K.T.K., El-Hajjar, M. and Hanzo, L.H., 2017. A survey of network lifetime maximization techniques in wireless sensor networks. IEEE Communications Surveys & Tutorials, 19(2), pp.828-854.

[11] Noel, A.B., Abdaoui, A., Elfouly, T., Ahmed, M.H., Badawy, A. and Shehata, M.S., 2017. Structural health monitoring using wireless sensor networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 19(3), pp.1403-1423.

[12] Sharif, A., Potdar, V. and Chang, E., 2009, June. Wireless multimedia sensor network technology: A survey. In 2009 7th IEEE International Conference on Industrial Informatics (pp. 606-613). IEEE.

[13] Sert, S.A., Onur, E. and Yazici, A., 2015, October. Security attacks and countermeasures in surveillance wireless sensor networks. In 2015 9th International Conference on Application of Information and Communication Technologies (AICT) (pp. 201-205). IEEE.

[14] Awan, S., Javaid, N., Ullah, S., Khan, A.U., Qamar, A.M. and Choi, J.G., 2022. Blockchain based secure routing and trust management in wireless sensor networks. Sensors, 22(2), p.411.

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

[16] Fu, M.H., 2020. Integrated technologies of blockchain and biometrics based on wireless sensor network for library management. Information Technology and Libraries, 39(3).

[17] Kumari, S. and Om, H., 2016. Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines. Computer Networks, 104, pp.137-154.

[18] Amjad, S., Abbas, S., Abubaker, Z., Alsharif, M.H., Jahid, A. and Javaid, N., 2022. Blockchain based authentication and cluster head selection using DDR-LEACH in internet of sensor things. Sensors, 22(5), p.1972.

[19] Pereira, N.C.V.N. and de Moraes, R.M., 2010. Comparative analysis of AODV route recovery mechanisms in wireless ad hoc networks. IEEE Latin America Transactions, 8(4), pp.385-393.

[20] Usop, N.S.M., Abdullah, A. and Abidin, A.F.A., 2009. Performance evaluation of AODV, DSDV & DSR routing protocol in grid environment. IJCSNS International Journal of Computer Science and Network Security, 9(7), pp.261-268.

[21] Guerrero-Sanchez, A.E., Rivas-Araiza, E.A., Gonzalez-Cordoba, J.L., Toledano-Ayala, M. and Takacs, A., 2020. Blockchain mechanism and symmetric encryption in a wireless sensor network. Sensors, 20(10), p.2798.

[22] Khalid, R., Malik, M.W., Alghamdi, T.A. and Javaid, N., 2021. A consortium blockchain based energy trading scheme for Electric Vehicles in smart cities. Journal of Information Security and Applications, 63, p.102998.

[23] Abubaker, Z., Khan, A.U., Almogren, A., Abbas, S., Javaid, A., Radwan, A. and Javaid, N., 2022. Trustful data trading through monetizing IoT data using BlockChain based review system. Concurrency and Computation: Practice and Experience, 34(5), p.e6739.

[24] Moinet, A., Darties, B. and Baril, J.L., 2017. Blockchain based trust & authentication for decentralized sensor networks. arXiv preprint arXiv:1706.01730.

[25] Rathod, T., Jadav, N.K., Alshehri, M.D., Tanwar, S., Sharma, R., Felseghi, R.A. and Raboaca, M.S., 2022. Blockchain for future wireless networks: A decade survey. Sensors, 22(11), p.4182.

[26] Gangal V, Cinemre I, Hacioglu G. A distributed leach-ahp routing for wireless sensor networks. IEEE Access. 2024 Jan 30.

[27] Janarthanan A, Vidhusha V. Cycle-Consistent Generative Adversarial Network and Crypto Hash Signature Token-based Block chain Technology for Data Aggregation with Secured Routing in Wireless Sensor Networks. International Journal of Communication Systems. 2024 Mar 10;37(4):e5675.

[28] Prasad KV, Periyasamy S. Secure-Energy Efficient Bio-Inspired Clustering and Deep Learning based Routing using Blockchain for Edge Assisted WSN Environment. IEEE Access. 2023 Dec 19.

[29] Muneeswari G, Ahilan A, Rajeshwari R, Kannan K, John Clement Singh C. Trust And Energy-Aware Routing Protocol for Wireless Sensor Networks Based on Secure Routing. International journal of electrical and computer engineering systems. 2023 Nov 14;14(9):1015-22.

[30] Vimalarani C, Subramanian R, Sivanandam SN. An enhanced PSO-based clustering energy optimization algorithm for wireless sensor network. The Scientific World Journal. 2016;2016(1):8658760.

[31] Arab A, Rostami MJ, Ghavami B. An image encryption method based on chaos system and AES algorithm. The Journal of Supercomputing. 2019 Oct;75:6663-82.

[32] Shakor MY, Khaleel MI, Safran M, Alfarhood S, Zhu M. Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security. IEEE Access. 2024 Jan 8.

[33] Munjal K, Bhatia R. Analysing RSA and PAILLIER homomorphic Property for security in Cloud. Procedia Computer Science. 2022 Jan 1;215:240-6.

[34] Johnson D, Menezes A, Vanstone S. The elliptic curve digital signature algorithm (ECDSA). International journal of information security. 2001 Aug;1:36-63.

[35] Lai Y, Tong L, Liu J, Wang Y, Tang T, Zhao Z, Qin H. Identifying malicious nodes in wireless sensor networks based on correlation detection. Computers & Security. 2022 Feb 1;113:102540.

[36] JOHN AJ, Roslin E, Wilfred F. Deep Learning model-based malicious node detection system in wireless multimedia sensor Network.

[37] Hur T, Kim L, Park DK. Quantum convolutional neural network for classical data classification. Quantum Machine Intelligence. 2022 Jun;4(1):3.

[38] Oh S, Choi J, Kim J. A tutorial on quantum convolutional neural networks (QCNN). In2020 International Conference on Information and Communication Technology Convergence (ICTC) 2020 Oct 21 (pp. 236-239). IEEE.

[39] BotIoT dataset: https://research.unsw.edu.au/projects/bot-iot-dataset accessed on September 2024.

[40] Borkar GM, Patil LH, Dalgade D, Hutke A. A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: A data mining concept. Sustainable Computing: Informatics and Systems. 2019 Sep 1;23:120-35.