Quantum Readout and Gradient Deep Learning Model for secure and sustainable data access in IWSN

Omar A. Alzubi[1]

[1]**Prince Abdullah Bin Ghazi Faculty of Information and Communication Technology**
Al-Balqa Applied University, Al-Salt, Jordan

Corresponding author:
Omar A. Alzubi[1]

Email address: o.zubi@bau.edu.jo

ABSTRACT

The Industrial Wireless Sensor Network (IWSN) is a surface-type of Wireless Sensor Network (WSN) that suffers from high levels of security breaches and energy consumption. In modern complex industrial plants, it is essential to maintain the security, energy efficiency, and green sustainability of the network. In an IWSN, sensors are connected to the Internet in a non-monitored environment. Hence, non-authorized sensors can retrieve information from the IWSN. Therefore, to ensure that data access between sensors remains sustainable and secure, energy-efficient authentication and authorization are required. In this paper, a novel Quantum Readout Gradient Secured Deep Learning (QR-GSDL) model is proposed to ensure that only trustworthy sensors can access IWSN data. The major objective of this QR-GSDL model is to create secure, energy-efficient IWSN to attain green sustainability and reduce the industrial impact on the environment. First, using the quantum readout and hash function, a registration method is designed to efficiently perform the registration process. Next, a gradient secured deep learning method is adopted to implement the authentication and authorization process in order to ensure energy-saving and secure data access. Simulations are conducted to evaluate the QR-GSDL model and compare its performance with that of three well-known models: online threshold anomaly detection, machine learning-based anomaly detection, and dynamic CNN. The simulation outcomes show that the proposed model is secure and energy-efficient for use in the IWSN. Moreover, the experimental results prove that the QR-SGDL model outperforms the existing models in terms of energy consumption, authentication rate, authentication time, and false acceptance rate.

Subjects: Artificial Intelligence, Data Mining and Machine Learning, Security and Privacy, Computer Networks and Communications
Keywords: Security, Machine Learning, Deep Learning, Data Privacy, Industrial Wireless Sensor Network, Quantum Readout, Authentication, Authorization, Energy Consumption
Terminologies: Industrial Wireless Sensor Network ($IWSN$), authentication rate (AR), authentication (AT), false acceptance rate (FAR)

INTRODUCTION

The underlying rationale for the recent conceptualization of the Industrial Internet of Things (IIoT) has been to leverage the Internet of Things (IoT) and apply its advantages to the industrial wireless sensor networks (IWSNs) in order to create interconnected industrial environments. IWSNs play an essential part in the management and operation of industrial machinery across a wide range of sectors. The main task of an IWSNs is to monitor the performance of different devices through the collection, storage, and retrieval of data in real-time in an industrial environment. The application of the IWSNs framework in such systems is intended to increase optimization and improve industrial automation processes. Regardless of its advantages, the IWSN suffers from many security and privacy issues like data leaking, node compromise, authentication and authorization problems, data loss, and many more. The authentication problem is the most widespread concern among all the issues because all the sensing devices are located

46 and accessed remotely. A false authentication may hamper the complete security of the system. The first
47 security step must be strong so that no unauthorized user can access the system. Several authenticated key
48 agreement schemes are proposed, but they are limited to only one device at a time. In some scenarios, the
49 IIoT networks are closed so no unauthorized user can access the internal networks of the system. But,
50 still, the authentication problem for insider users is present. An insider attack can be possible and creates
51 an issue if the authentication mechanism is not much strong. Thus, these issues motivated us to design
52 a dynamic deep learning-based solution named the Quantum Readout Gradient secured Deep Learning
53 (QR-GSDL) for the authenticity of the sensor-based IIoT networks. The proposed model will work on a
54 different layer for insider user authentication and authorization purpose. The proposed authentication
55 steps included an improvement in the authentication rate with minimum time consumption and delay.

56 One of the most well-known models that has been utilized in the Industrial Internet of Things (IIoT)
57 domain is the online threshold anomaly detection model. It employs a learning method based on statistical
58 formulations to distinguish the characteristics of devices and flag any differences in those characteristics
59 as anomalies Li et al. (2019). The model is independent in terms of device operations because statistical
60 data about the system is acquired by using the IoT application program interface. For this model, multiple
61 machine learning techniques have been introduced in the training process, and the performance on normal
62 systems was designed in a similar manner. The model is able to detect anomalous activities in an efficient
63 manner by summing cumulative operations and using localized outliers, thereby improving accuracy and
64 simultaneously reducing false alarms. However, despite improvements in the accuracy and false alarm
65 rates, this model does not address the issue of the security of data communication in the context of the
66 industrial sector.

67 The other well-recognized model that has been employed in the IIoT is the machine learning-based
68 anomaly detection model Zolanvari et al. (2019). This model was developed to address the most prevalent
69 susceptibility in the IIoT, namely, the injection attack. There are three main forms of injection attacks
70 that can be mitigated by applying machine learning techniques: command injection, structured query
71 language, and backdoor attacks. Through the adoption of a machine learning-based approach, not only
72 was it demonstrated that the attack detection rate was improved, but there was also a steep reduction
73 in the value of the mean absolute error. However, despite the improvement in the attack detection rate
74 and the minimization of the mean absolute error, the false-negative rate was not minimized by machine
75 learning-based anomaly detection. In other words, anomaly intruders were still incorrectly detected, thus
76 leading to a lack of overall efficacy.

77 In Yuan et al. (2020), a dynamic CNN (DCNN) technique is planned to learn the hierarchical local
78 nonlinear dynamic features of soft sensor modeling. Every 1D process sample in DCNN is dynamically
79 increased into a 2D data sample with lagged unlabeled process variables, comprising both spatial cross-
80 relationships and temporal auto-correlations. Then, to derive the local nonlinear spatial-temporal function
81 from the 2D sample data matrix, the convolutional and pooling layers are alternately used. In addition, the
82 concept of how the local nonlinear spatial-temporal function can be taught from the network is studied for
83 DCNN. In an industrial hydrocracking process, the efficacy of the proposed DCNN is tested. However,
84 the authors did not provide any proof of the energy efficiency of their approach Alzubi et al. (2020b)
85 Alzubi et al. (2020a).

86 In this paper, a deep learning-based solution is presented to overcome the security issues that currently
87 exist in the authentication and authorization protocol for the industrial wireless sensor network (IWSN).
88 The proposed solution employs a novel model named the Quantum Readout Gradient secured Deep
89 Learning (QR-GSDL) model. This model first verifies the authenticity of a given sensor seeking access
90 to data in the IWSN by using a quantum readout and hash (QRH) function. This registration process
91 facilitates effective validation and therefore reduces the false acceptance rate. Next, the security issues
92 inherent in the authentication and authorization procedure are addressed by using a gradient sparse auto
93 deep learning algorithm. This type of algorithm was adopted because it was envisaged that its usage
94 would lead to an improvement in the authentication rate (AR) with minimum time consumption and delay.
95 Accordingly, the designed model substantially minimizes the false acceptance rate (FAR), leading to an
96 improvement in both the authentication rate and authentication time (AT).

97 We believe that the best-suited real-world environment to implement our proposed QR-GSDL model
98 is in industrial applications such as machine health, automated metering, remote monitoring, and staff
99 management. The only requirement is that the pre-defined setting of IWSN be stationary.

RELATED WORK

With the advancement of technologies, because of their benefits over conventional wired networks, wireless sensor networks (WSNs) have fantastic deployment opportunities for industrial scenarios. However, fully integrated mechanized processes and wireless networking conditions allow the high security and low energy consumption requirements of industrial wireless sensor networks (IWSNs) more stringent. We will discuss the relevant work in this section from the point of view of security and energy consumption. Many researchers presume industrial wireless sensor networks and present different authentication and authorization schemes. However, these schemes were not ideal for IWSN. This is due to the fact that in terms of energy efficiency and computing overhead, node authentication by cluster head on a regular basis results in considerable overhead.

Several studies have been conducted in the area of deep learning to make the IoT-enabled WSN more efficient, robust, and secure Alzubi et al. (2019b). The works that are most relevant to this paper include the deep learning model that was proposed in Liang et al. (2020). This model is based on edge computing and aimed at minimizing the traffic (data transmissions) in the network to reduce network congestion while maintaining classification accuracy. However, the method in Liang et al. (2020) did not provide each user with data privacy. Therefore, to address this privacy issue, two privacy-preserving deep learning models named DeepPAR and DeepDPA were presented in Zhang et al. (2020). The DeepPAR model offered a mechanism that prevented a user's information from being leaked to others while keeping the secrecy level dynamically updated. To address this issue, the DeepDPA model applied a set of key management techniques to guarantee the backward secrecy of group participants. However, DeepDPA and DeepPAR were not able to minimize the false acceptance rate. Therefore, the design of the proposed QR-GSDL model is aimed at addressing the data privacy problem while at the same time minimizing the false acceptance rate.

Another deep learning model was proposed in Liao et al. (2019) in order to improve the authentication performance of the IWSN. The model employed three methods to authenticate sensor nodes. Each of these methods was based on a machine learning algorithm. The first one applied an improved algorithm based on a convolution preprocessing neural network (CPNN), the second utilized a deep neural network, and the third one used a convolutional neural network. Although the model required minimal computing resources to reduce the latency in performing multi-node authentication, it failed to reduce the authentication time, even when using a so-called improved CPNN-based algorithm. Hence, it is anticipated that the proposed QR-GSDL model will overcome the time consumption-related shortcoming encountered in Liao et al. (2019) through the use of a quantum readout and hash (QRH) function to verify and validate the authentication of the sensor in a minimal amount of time. It is also envisaged that the use of a QRH function in the proposed QR-GSDL model will also be able to minimize the volume of network traffic and consequently reduce communication costs. Thus, overcoming the communication cost limitation of the deployment-based optimization model that was introduced in Li et al. (2017) to ensure network security and simultaneously improve network lifetime.

Despite the above achievements in the area of deep learning, a survey of the application of deep learning tools in the smart industry presented in Ma et al. (2019) concluded that while deep learning provides an opportunity to solve many classical issues, authentication and authorization problems are not tackled. Therefore, as a first step in addressing these problems, the QR-GSDL model is designed in such a way as to ensure that the gateway node in the IWSN checks the authenticity of the sensor node that is seeking access to information in the IWSN, thereby guaranteeing correct and appropriate authorization.

Other works have also explored methods to improve authentication. For instance, in Chen et al. (2020), a secure authentication scheme was introduced that depended on credential and dynamic IDs for WSNs in IoT environments. For the scheme, an authentication key agreement protocol based on three parties was designed using the Burrows–Abhadi–Needham logic method. It was reported that the scheme was able to ensure low computational and communication costs, but it was admitted that the false acceptance rate was not improved. Consequently, the gradient secured deep learning method is integrated into the proposed QR-GSDL model in order to achieve a reduction in the false acceptance rate.

Jiang et al. propose a re-authentication scheme for the Voronoi graph-based network model. The scheme maintains anonymity while using fewer resources than the previous schemes. The system, however, suggests neighbor wandering, which might not be ideal for a realistic situation. Also, they did prove the efficiency of their model in terms of energy consumption Alrabea et al. (2020) Alzubi et al. (2019a).

In an alternative attempt to improve the security aspect of the WSN, a convolutional technique (CT) was developed in Alghamdi (2019), which involved generating security bits using convolutional codes. The aim of the CT was to protect the WSN from attacks caused by malicious nodes. The designed technique improved network security and minimized computational complexity because no key distribution was needed. However, authentication time was not minimized by CT. Thus, a gradient secured deep learning method is included in the proposed QR-GSDL model in order to attempt to reduce the time consumed in the authentication procedure.

Industrial wireless sensor networks, which are an evolved category of WSN in which sensors are combined to monitor the status of equipment and to control systems in real-time, also have limitations related to security, privacy, and energy. To address these drawbacks in the IWSN context, a lightweight decision-making framework based on trust value identification was designed in Ramesh and Yaashuwanth (2019). The lightweight trust framework was used for quality of service clustering in order to perform the secure routing process. A quantifiable trust value was determined through the cluster head within the cluster. It was claimed that flawed, untrusted, counteract, and malicious nodes could be predicted using this framework. However, the communication cost was not minimized. Therefore, in the QR-GSDL model, quantum sparse auto-encoding and decoding are employed to reduce the communication cost in the IWSN system.

A different protocol named secure directed diffusion was suggested in Sengupta et al. (2018). This protocol depended on binding the node's geographic location and ID in order to induce a cryptographic key based on the location. The produced key then formed the foundation of a neighborhood authentication process for the IWSN. However, only theoretical statements were provided regarding the effectiveness of this authentication process and the computational overhead.

On the other hand, in Qureshi et al. (2020), a centroid position analysis was performed in an attempt to decrease data transmission failure and delay. In addition, a gateway clustering routing protocol was used for cluster head selection from the centroid position. Then the gateway node minimized the load from the cluster head nodes and transmitted the data to the base station. However, security issues were not taken into consideration. Therefore, in our proposed approach, an authentication process is carried out to establish secure communication.

Cooperation between the sensors that are communicating with a central base station is one of the factors that contribute to security. In light of this, cryptographic algorithms based on secret keys were designed in Tahir et al. (2018) in which the ICMetric method employed the device features to generate secret keys for use in cryptographic services. However, the proposed method failed to offer an effective authentication process that at the same time did not increase resource overheads. Hence, in the proposed QR-GSDL model, a gradient secured deep learning algorithm performs the authentication to allow secure data communication.

An energy-efficient data transmission mechanism is proposed to improve emergency data transmission by increasing accuracy and decreasing packet delay Sheikh et al. (2012)Singanamalla et al. (2019) Nazir et al. (2020). It was claimed that the scheme was reliable, but a mechanism for ensuring the security of data transmission was not presented. In contrast, an authentication process is carried out in the QR-GSDL model to enable secure data transmission.

A cooperative mechanism was presented in Iqbal et al. (2017) to reduce both the false alarm rate and energy consumption. The designed mechanism improved the probability of accurate decisions being made at a specified signal level. Also, the suggested mechanism in Iqbal et al. (2017) was reported to be able to achieve a reduction in the false alarm rate, but only for indoor IWSNs. However, it was not particularly efficient in terms of energy consumption in relation to the time needed to perform its computations. Therefore, quantum sparse encoding and decoding are used in our proposed QR-GSDL model in order to reduce computation time Sheikh et al. (2016) Alrabea et al. (2019) Alzubi et al. (2014).

The three issues of security, network lifetime, and coverage were handled in Cao et al. (2020) by converting the disjoint routing paths to address the flow issues. However, despite an improvement being observed in security and coverage, optimization and operation time were not focused on. Therefore, again the quantum sparse encoding and decoding approach is used in the proposed model in order to minimize time consumption.

To address the issue of security, in Cao et al. (2019), multi-objective evolutionary algorithms were designed for a heterogeneous WSN. Moreover, a 3D signal propagation model used the line-of-sight idea to determine the signal path loss. However, the security level was not improved by the designed

210 model. Hence, the gradient secured deep learning model is employed in the current study to perform
211 authentication for secure data communication.

212   Another password-based authentication scheme was proposed in Lee et al. (2018) to verify security
213 with minimal communication and computation cost. However, the communication and computation
214 overheads were not minimized by the developed password-based authentication scheme. Therefore, in the
215 proposed model, quantum sparse encoding and decoding are used with the expectation that this approach
216 can reduce the computation overhead.

217   Lastly, a mutual authentication system integrating temporal credentials and multiple passwords was
218 proposed in Liu et al. (2017) in order to minimize the overheads. However, while the authentication time
219 was reduced, the false alarm rate was not minimized. Therefore, in the proposed QR-SGDL model, the
220 QRH is used to offload the false alarm rate.

221   Motivated by the above issues encountered in related studies, in this work, a novel model for IWSN,
222 named the Quantum Readout Gradient Secured Deep Learning (QR-GSDL) model, is developed in order
223 to improve not only the authentication rate but also the authentication time and false acceptance rate. In
224 the following, an elaboration of the QR-GSDL model is presented.

QUANTUM READOUT GRADIENT SECURED DEEP LEARNING IN IWSN

226 In this section, we present our proposed model, QR-SGDL, which consists of three phases: i) secure and
227 energy-efficient localization, ii) sensor node registration, and iii) authentication. The system model and
228 the three phases of QR-SGDL are elaborated on in the following subsections.

System model

230 Figure 1 provides the system model of IWSN where the QR-SGDL model will be implemented. The
231 IWSN system model comprises four entities: a number of sensor nodes, a number of base stations, a
232 gateway node and a supervisory control unit connected to a network Zolanvari et al. (2019).
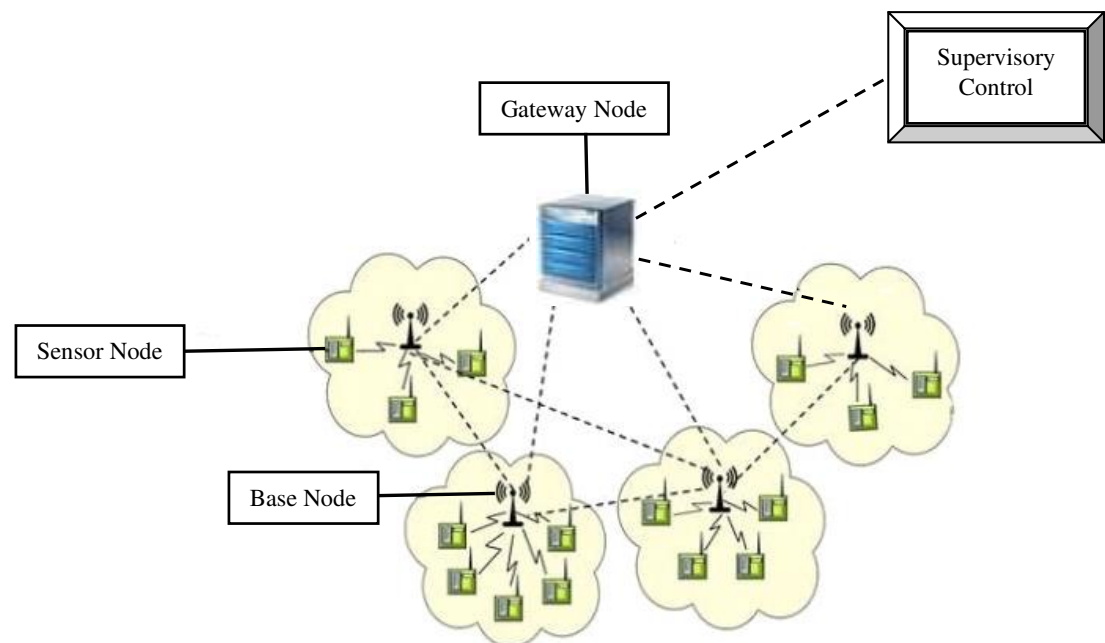
Figure 1. System model for an industrial wireless sensor network.

233   Generally, several different sensors are deployed in an industrial plant for monitoring purposes. Here,
234 the sensors which consume lesser energy for sensing the industrial plants are chosen. These sensors gather
235 the data packets from their adjacent environment and communicate them to the gateway node via one or
236 more base stations. Next, the gateway node transmits the acquired data packets to the supervisory control
237 unit through a secure channel.

238 The gateway node gathered two types of packets- data packets and control packets- from the sensor
239 nodes. Before collecting the data packets, the gateway node ensures that these packets are originated from
240 authenticated sensor nodes and verifies whether the sensor node has been tampered with or not. This will
241 be accomplished by applying the Quantum Readout Hash registration which is explained thoroughly in
242 algorithm 1. After attaining the data, the QR-GSDL method analyzes the data about industrial plants in
243 order to maintain green sustainability.

System architecture of the QR-SGDP model

245 The proposed QR-SGDL model uses deep learning concepts to perform multiple processes in several
246 layers. The deep learning network uses one input layer, two hidden layers, and one output layer for
247 improving security during data access and to improve the green sustainability of the network. The
248 feed-forward fashion deep learning network collects the nodes in the input layer, learns in the hidden
249 layers, and transforms the results into an output layer.

250   The system architecture of the QR-SGDL model is designed to address energy and green sustainability
251 issues by analyzing the industrial plant's data. It also aims to handle security issues such as authentication
252 and authorization in the IWSN by achieving a minimum false acceptance rate.

253   In the IWSN, the upper layer of the architecture is a transmission layer comprising base stations,
254 sensor nodes, gateway node, and supervisory control unit. All of these elements can be found in any
255 industry-enabled architecture, and this configuration realizes the separation of the deep learning model
256 and the IWSN model. The energy-efficient sensor node represents the input part while the supervisory
257 control node represents the calculation part. With the deep learning model enabled in the IWSN, we
258 construct a quantum sparse auto encoder (QSAE). In the proposed model, the QSAE handles energy,
259 green sustainability, and security issues (i.e. authentication and authorization) in the IWSN.

260   During the training stage, the supervisory control unit sends a data access request made by a given
261 sensor to the input layers. The QSAE checks for energy availability, authenticity, and authorization of
262 the sensor by employing the quantum readout function to ensure smooth communication between the
263 sensor and the supervisory control unit with a minimum false acceptance rate. The verification of energy
264 availability, authenticity, and authorization by QSAE will be discussed in the coming sections. The
265 supervisory control unit thus ensures energy consumption, authenticity, and authorization via the gateway
266 node based on this security mechanism. When the sensor has been authenticated and authorized, it is
267 allowed to implement its process.

Sensor node registration phase

269 The registration process for the minimal energy consumed sensor is carried out by the gateway node by
270 means of a QRH model. This QRH model is used because it can accurately verify the authenticity of an
271 object. The registration procedure employed by the QRH model is illustrated by means of an activity
272 diagram in Figure 2.

273   Let us assume that a sensor $S = (S_1, S_2, ..., S_n)$ wants to access the data (or data packets) $DP =$
274 $(DP_1, DP_2, ..., DP_n)$ in IWSN. The sensor registers the sensor's details in the gateway node GN. To mini-
275 mize the false acceptance rate, an integrated QRH function is used. The pseudocode representation of
276 Quantum Readout Hash registration is detailed in Algorithm 1.

Algorithm 1 Quantum readout hash registration

Input: Sensor $S = S_1, S_2, ..., S_n$, Gateway Node GN, Base Station $BS = BS_1, BS_2, ..., BS_n$
Output: Authentic sensor registration
Begin:
    for each Sensor S with Gateway Node GN and Base Station BS **do**
        Obtain identity and request registration using equation 1
        Obtain arbitrary challenge using equation 2
        Obtain single quantum using equation 3
        Obtain interim identity and quasi congruence using equation 4
        Evaluate hash function using using equation 5
        Return: authentic sensor registration
    end for
End
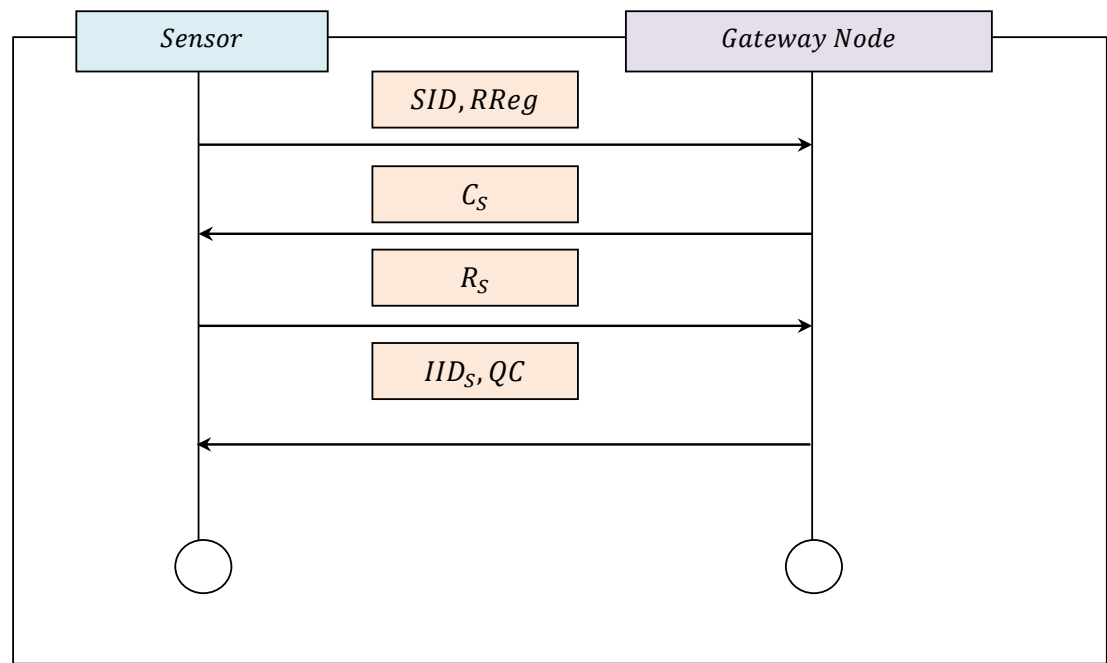
Figure 2. Registration activity diagram.

The sensor registration process explained in Algorithm 1, starts when sensor S chooses an identity SID and relays $(SID, RReg)$ to the gateway node via a secure channel. Here, $RReg$ represents the request made by the sensor for registration.

$$S : (SID, RReg) \rightarrow GN \qquad (1)$$

Upon reception of the request made by the sensor for registration, the gateway node produces an arbitrary challenge C_S for the sensor and sends C_S to the sensor S via a secure channel as given by:

$$GN : (C_S) \rightarrow S \qquad (2)$$

After receiving C_S, the sensor extracts the quantum readout QR outputs $R_S = Q_D(C_S)$ and sends R_S to the gateway node GN. Here, QR outputs R_S to verify the authenticity of quantum data packet Q_D that claims to be from a given source or sensor. A single quantum Q is produced in a random manner for each sensor, therefore minimizing the false accept rate, the energy consumption, and improving the authenticity rate.

$$S : (R_S) \rightarrow GN \qquad (3)$$

Subsequently, the gateway node produces an interim identity IID_S and a set of Quasi Congruence $QC = (qc_1, qc_2, ..., qc_n)$ and then transmits (IID_S, QC) to the sensor S in order to facilitate communication with S.

$$GN : (IID_S, QC) \rightarrow S \qquad (4)$$

Finally, the sensor S input a one-time password OTP for the particular session s and stores them in its base station. Next, S extracts the hash intermediate output $\alpha_s = Q_D(OTP_s)$. The sensor selects the session password $spwd_s$ and inputs $spwd_s$ into the base station which evaluates the hash function β for validation, as presented in Equation 5.

$$\beta = HASH(\alpha_s || spwd_s) \tag{5}$$

By applying the above-integrated functions, it is considered to be possible to achieve authentic sensor registration with a minimum false acceptance rate.

GRADIENT SECURED DEEP LEARNING MODEL

Let us assume that a sensor S wants to acquire industrial plant data from a specific sensor in the IWSN. Then, mutual authentication between the two sensors S_i and S_j has to be established, where the identity of the sensor has to be checked prior to providing access. With authenticated nodes, the gateway node checks sensor node access for guaranteeing energy-efficient authorization. First, authentication is performed by means of gradient secure localization method, and then energy-efficient authorization is done by means of a quantum sparse encoding and decoding approach. The activity diagram for the energy-efficient authentication and authorization procedure is shown in Figure 3.More details are given for the proposed authentication process as a flow diagram, which is shown in Figure 4. The pseudo code representation of Gradient Sparse Auto Deep Learning for energy-efficient and secure communication is detailed in Algorithm 2.
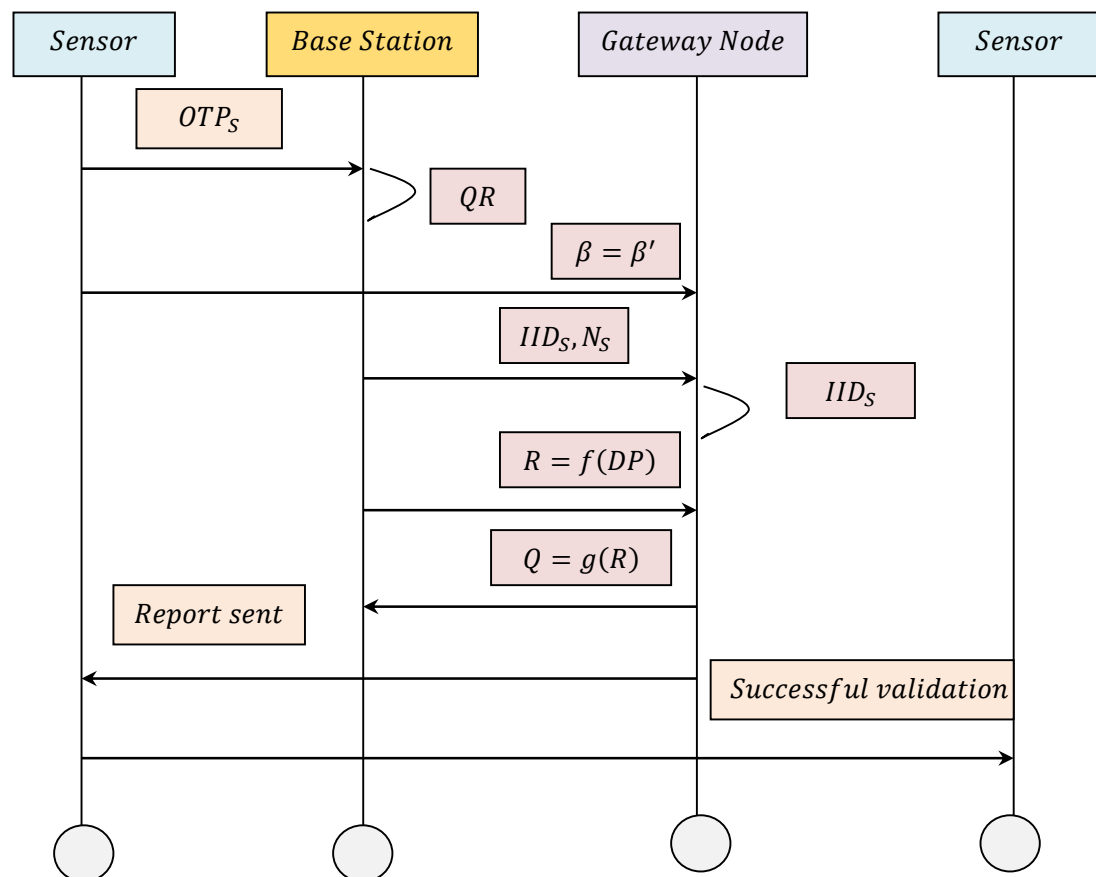
Figure 3. energy-efficient authentication and authorization activity diagram.

As presented in Algorithm 2, the mutual authentication process performed by the gateway node GN and the designated sensor is as follows. First, the sensor S initially inputs a one-time password OTP_S Next, the base station extracts the quantum readout QR output R_S. Then, the gateway node GN calculates $\beta' = HASH(\alpha_s || spwd_s)$ and compares the computed β' with the stored β. In this work, the comparison is done based on the localization concept, whereby industrial data in the IIoT are gathered by

313 sensors in distinct locations and sent to the servers to facilitate analysis. Most of the current localization
314 systems measure local deviation with respect to neighbor based on reachability distance Li et al. (2019)
315 or according to local deviation factor. However, in the real world, those that are present within the
316 IIoT environment may attempt to interrupt this localization process. When successful, such attacks may
317 compromise certain sensors and thus critically falsify the entire environment. To address this issue, first,
318 in this work, an energy-efficient and secure localization method based on gradient associating sensors is
319 presented.
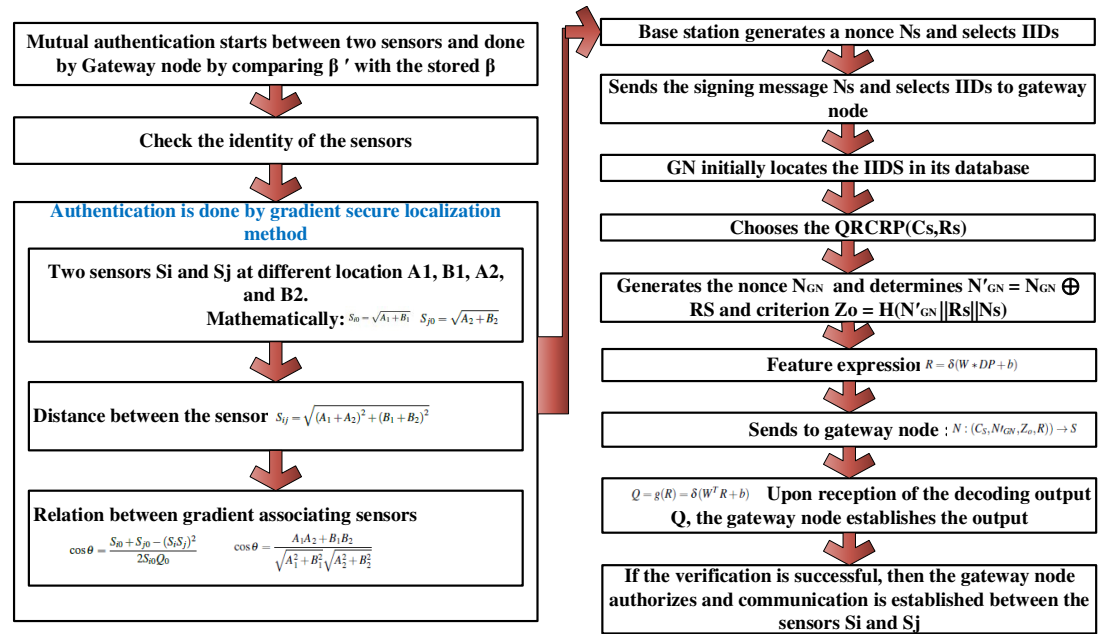
Figure 4. Flow diagram of proposed authentication process

320 Let us consider sensors S_i and S_j at different locations A_1, B_1, A_2 and B_2, mathematically formulated
321 as given below.

$$S_{i0} = \sqrt{A_1 + B_1} \tag{6}$$

$$S_{j0} = \sqrt{A_2 + B_2} \tag{7}$$

322 Based on equations 6 and 7, the distance between the sensors is mathematically calculated by applying
323 equation 8.

$$S_{ij} = \sqrt{(A_1 + A_2)^2 + (B_1 + B_2)^2} \tag{8}$$

324 However, in order to analyze the relation between gradient associating sensors, it is computed by
325 equations 9 and 10.

$$\cos\theta = \frac{S_{i0} + S_{j0} - (S_iS_j)^2}{2S_{i0}Q_0} \tag{9}$$

$$\cos\theta = \frac{A_1A_2 + B_1B_2}{\sqrt{A_1^2 + B_1^2}\sqrt{A_2^2 + B_2^2}} \tag{10}$$

Algorithm 2 Gradient sparse auto deep learning

Input: Sensor $S = S_1, S_2, ..., S_n$, Gateway Node GN, Base Station $BS = BS_1, BS_2, ..., BS_n$

Output: energy-efficient and secure communication

Begin:

  for each Sensor S with Gateway Node GN and Base Station BS **do**

    Obtain energy-efficient secure localization based on gradients associating sensors using equations 9 and 10

    Authentication:

    if disclosed locations equal **then**

      Authentication successful

      Go to **Authorization**

    else

      Authentication is not successful

      Session is terminated

    end if

    Authorization:

    Perform Quantum Sparse Auto-Encoding using equation 11

    Perform Quantum Sparse Auto Decoding using equation 13

    if R=Q **then**

      energy-efficient authorization is successful

      energy-efficient secure communication

    else

      energy-efficient authorization not successful

      Session is terminated

    end if

  end for

End

By introducing the Gradient Secure Localization (GSL) method, security, energy efficiency, and green sustainability can be ensured even in the presence of attacks. In this manner, with the location verification by the GSL method, the precision or exactness of the disclosed locations of the sensors is made in an effective fashion, therefore ensuring authentication. Note that the comparison here is made based on the disclosed locations. If they are not equal, the session is terminated. Upon successful comparison, the base station perceives S as a normal sensor.

Next, the base station generates a nonce N_S and selects IID_S as the interim identity of the sensor, and sends the signing message IID_S, N_S via a secure channel. After obtaining the signing on message, the gateway node GN initially locates the IID_S in its database. The gateway node then chooses the $QRCRP(C_S, R_S)$, generates the nonce N_{GN} and determines $N\prime_{GN} = N_{GN} \oplus R_S$ and criterion $Z_o = H(N\prime_{GN} || R_S || N_S)$. With the obtained criterion, in order to ensure that only authorized sensors communicate with each other, encryption and decryption are conducted using the $QSAE$. Moreover, the presence of three different layers in the system architecture (i.e., input layer, hidden layer, and output layer) reduces the false acceptance rate and ensures more accurate energy-efficient authorization. Here, R represents the feature expression of the output layer and encoding is performed as shown in equation 11.

$$R = \delta(W * DP + b) \tag{11}$$

From equation 11, the data packets required by the sensor are represented as vector $DP = [DP^1, DP^2, ..., DP^n]$, where n denotes the total number of the input sensors. In addition, vector $R = [R^1, R^2, ..., R^m]$, represents the feature expression of the hidden layer, where m represents the sensors of the hidden layers. Finally, b represents the bias vectors and W the weight matrix from input to hidden layer, respectively, while δ denotes the activation function. Finally, the gateway node formulates a message and sends it to the respective sensor as presented in equation 12.

$$N : (C_S, N\prime_{GN}, Z_o, R)) \rightarrow S \tag{12}$$

347   Upon reception of the message as given 12, the base station BS of the corresponding sensor S extracts
348 $R_S = Q_D(C_S)$ and verifies the criterion Z_o. Upon successful verification, the base station asks S to input
349 its identity $S_i ID$ and the sensor identity $S_j ID$ that it needs to access. The decoding process obtains the
350 reconstructed vector R of the output layer from the hidden layer value R, and this is mathematically
351 formulated as in equation 13.

$$Q = g(R) = \delta(W^T R + b) \tag{13}$$

352   In equation 13, $Q = [Q^{(1)}, Q^{(2)}, ..., Q^{(n)}]$ and W^T represents the weight. Upon reception of the decoding
353 output Q, the gateway node establishes the output. If the verification is successful, then the gateway node
354 authorizes the sensor, and successful energy-efficient communication is thus established between the
355 sensors S_i and S_j; otherwise, the process is terminated.

SIMULATION SETUP

357 In order to examine the performance of the proposed QR-GSDL model in an IIoT system operation, a
358 simulation environment is set up using Network Simulator 2 (NS2) with plants data collected by IoT
359 devices downloaded from the Kaggle Website[1]. The dataset is composed of 7 attributes and 16382
360 instances. The attributes are demand_response, area, season, energy, cost, pair no, and distance. The
361 dataset comprises the common information to facilitate the development of a demand response (DR)
362 energy management system for industrial customers. IoT platform improves the inter connectivity of
363 entities in industrial energy management systems and minimizes the energy costs of industrial facilities.
364 In our simulations, networks with a designated number of sensors are distributed in a random pattern
365 within an area of $1500m \ times \ 1500m$. The number of sensors is varied from 50 to 500. The positioning
366 of nodes is made in a random fashion. Finally, the chosen simulation runs were 10 due to the fact that
367 after the 10th run, there was a very small gain in the criteria values. We believe this is an advantage of our
368 proposed model where it converges after a low number of simulation runs compared with the existing
369 models in the literature Li et al. (2019); Zolanvari et al. (2019); Yuan et al. (2020) where they converge
370 after 45 simulation runs. Table 1 provides the simulation parameters used in our work.

Table 1. Simulation parameters

Parameters	Description
Simulation time	$50s$
Area size	$1500m \times 1500m$
Number of sensors	50, 100,150, 200, 250, 300, 350, 400, 450, 500
Sensor placement	Random distribution
Transmission range	$400m$
Simulation runs	10

RESULTS AND DISCUSSION

372 The performance of the proposed QR-GSDL is compared with three well-known models: online threshold
373 anomaly detection Li et al. (2019), machine learning-based anomaly detection Zolanvari et al. (2019),
374 and dynamic CNN Yuan et al. (2020). The performance analysis is based on three measures: energy
375 consumption, false acceptance rate, authentication rate, and authentication time. The experimental results
376 are presented in the form of tables and graphs.

Performance analysis of energy consumption

378 Energy consumption is defined as the product of a number of samples and energy consumed by one sensor
379 node for performing authorization to achieve secured communication green sustainability. It is computed
380 as:

---

[1]kaggle. INDUSTRIAL INTERNET OF THINGS DATA [Online].Website: `https://www.kaggle.com/pitasr/industrialiot` [accessed 27-12-2020].

381   Energy consumption is defined as the product of a number of samples and energy consumed by one
382   sensor node for performing authorization to achieve secured communication green sustainability. It is
383   computed as:

$$EC = \sum_{i=1}^{n} Samples_i \times Energy\,consumed\,by\,one\,sensor\,node \tag{14}$$

384   In Equation 14, the energy consumption EC is computed based on the samples considered for
385   experimentation ($Samples_i$) and energy consumed for authorization to achieve secured communication
386   and green sustainability. It is measured in terms of joules (J). The energy consumed for four different
387   methods is given in Table 2.

Table 2. Energy consumption for different models and sensors

Number of sensors	False acceptance rate			
	QR-GSDL	Online threshold anomaly detection	Machine learning-based anomaly detection	Dynamic CNN
50	13	18	23	25
100	21	28	35	39
150	34	40	46	50
200	49	59	64	67
250	63	70	73	76
300	76	85	89	90
350	94	101	105	108
400	107	115	118	120
450	118	126	129	132
500	134	142	145	149

388   Table 2 and Figure 5 describe the energy consumption of the proposed method compared with the
389   three existing methods for a different number of sensors. The attained results illustrate that When the
390   number of sensors increases, the energy consumption by the sensor during the authorization also gets
391   increased linearly. However the the energy consumption of QR-GSDL model is lesser when compared to
392   Li et al. (2019), Zolanvari et al. (2019), and Yuan et al. (2020). The sample simulations carried out with
393   50 sensors show that the amount of energy consumed by one sensor for authorization using QR-GSDL is
394   0.26J while energy consumed by one sensor using Li et al. (2019) is 0.36J, using Zolanvari et al. (2019)
395   is 0.46J, and using Yuan et al. (2020) is 0.50J. The energy consumption saving is due to the application
396   of the Gradient Sparse Auto Deep Learning algorithm where the gateway node checks data access by the
397   sensors for ensuring energy-efficient and green sustainability. It is clear from the obtained results that
398   QR-GSDL reduces the energy consumption by 13%, 20%, and 28% when compared with Li et al. (2019),
399   Zolanvari et al. (2019), and Yuan et al. (2020), respectively.
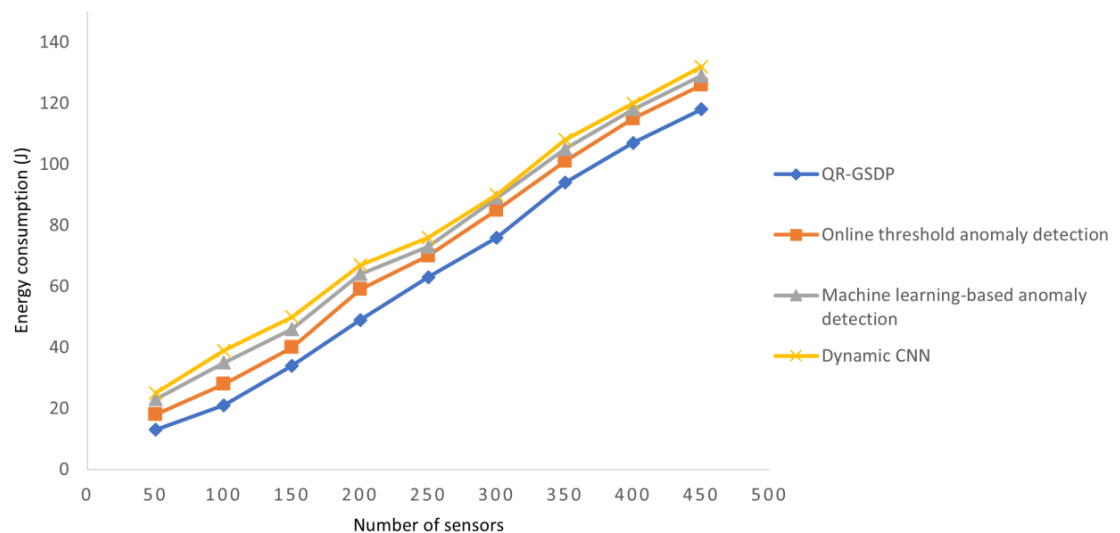
Figure 5. Comparisons of energy consumption.

Performance analysis of false acceptance rate

The false acceptance rate (*FAR*) is a measure of the likelihood that the IWSN will incorrectly accept an access attempt made by an unauthorized sensor. The false acceptance rate is formulated as the percentage ratio of the number of false acceptances (*FA*) to the number of sensors (*Samples*) as input, as in equation 15:

$$FAR = \frac{FA}{Samples} 100 \tag{15}$$

In equation 15, *FA* denotes the false acceptance made and a number of samples (sensors) *Samples* provided as input. It is computed in terms of percentage (%). The results of the false acceptance rate in modeling green sustainability issues in IWSN are summarized in Table 3.

The false acceptance rates generated by the IWSN when using the proposed method and the two compared methods are presented in Table 3 and graphically illustrated in Figure 6.

It can be seen from Table 3 and Figure 6 that when the number of sensors increases, the number of sensors that are checked for authenticity by the supervisory control unit via the gateway node also increased. Correspondingly, in all four models, the false acceptance rate increases. The false rate cannot be optimized by the QR-GSDL model.

However, the proposed model is able to reduce the rate when compared to the three models. As an example, when there are 150 sensors in the simulation, the number of sensors whose information is incorrectly accepted for transmission is 15 using QR-GSDL compared to 28, 45, and 48 using the online threshold anomaly detection Li et al. (2019), machine learning-based anomaly detection Zolanvari et al. (2019), and dynamic CNN Yuan et al. (2020), respectively. Therefore, it can be inferred that the false acceptance rate is improved by QR-GSDL. It is considered that this is due to the application of an integration function, namely, QRH, which verifies and validates the authentication of the corresponding sensor in an effective manner. Also, the application of interim identity and quasi congruence results in the generation of distinct and unique identities that are not stored in the gateway node but held by the supervisory control unit. Hence the level of complexity and the false acceptance rate is reduced using QR-GSDL by 39%, 56%, 58% compared to Li et al. (2019), Zolanvari et al. (2019), and Yuan et al. (2020), respectively.

Table 3. False acceptance rate for different models and sensors

Number of sensors	False acceptance rate			
	QR-GSDL	Online threshold anomaly detection	Machine learning-based anomaly detection	Dynamic CNN
50	8	10	12	13
100	12	15	25	23
150	15	28	45	48
200	25	45	60	50
250	30	50	75	65
300	30	58	80	68
350	25	40	85	79
400	40	65	70	73
450	45	80	95	87
500	40	75	100	82
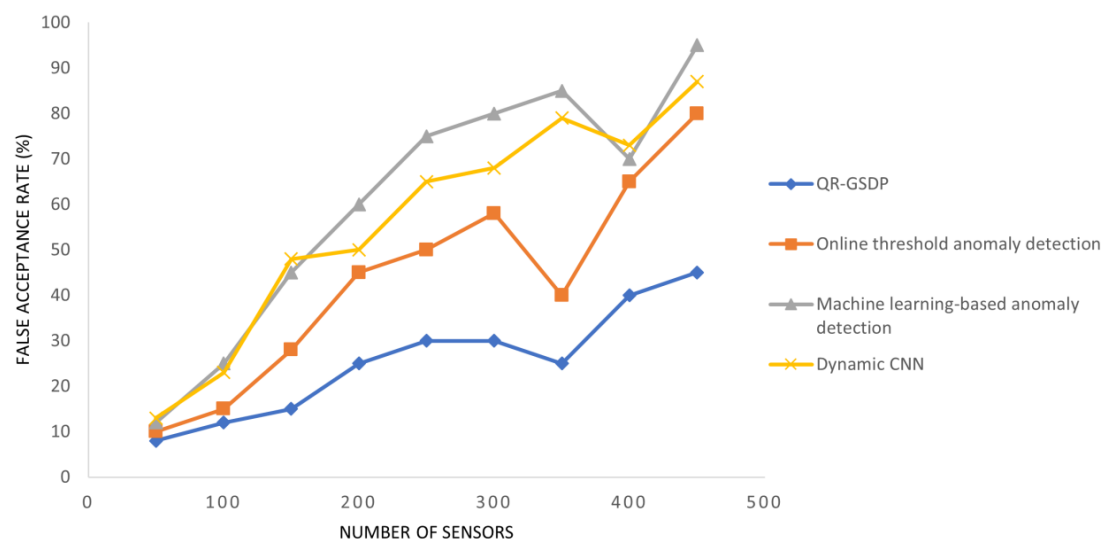
Figure 6. Comparisons of false acceptance rate.

Performance analysis of authentication rate

Authentication rate (*AR*) is calculated as the percentage ratio of successful authentications (*SA*) made by the gateway node to the number of sensors (*Samples*), as in equation 16:

$$AR = \frac{SA}{Samples} 100 \qquad (16)$$

The authentication rates produced by the IWSN for different numbers of sensors (ranging from 50 to 500) when using the three tested methods are presented in Table 4 and Figure 7.

Table 4. Authentication rate for different models and sensors

Number of sensors	False acceptance rate			
	QR-GSDL	Online threshold anomaly detection	Machine learning-based anomaly detection	Dynamic CNN
50	92	88	82	80
100	90	86	80	78
150	85	81	78	74
200	88	83	75	70
250	86	82	74	68
300	88	84	75	70
350	90	85	78	74
400	85	81	75	71
450	87	82	77	73
500	89	85	79	75
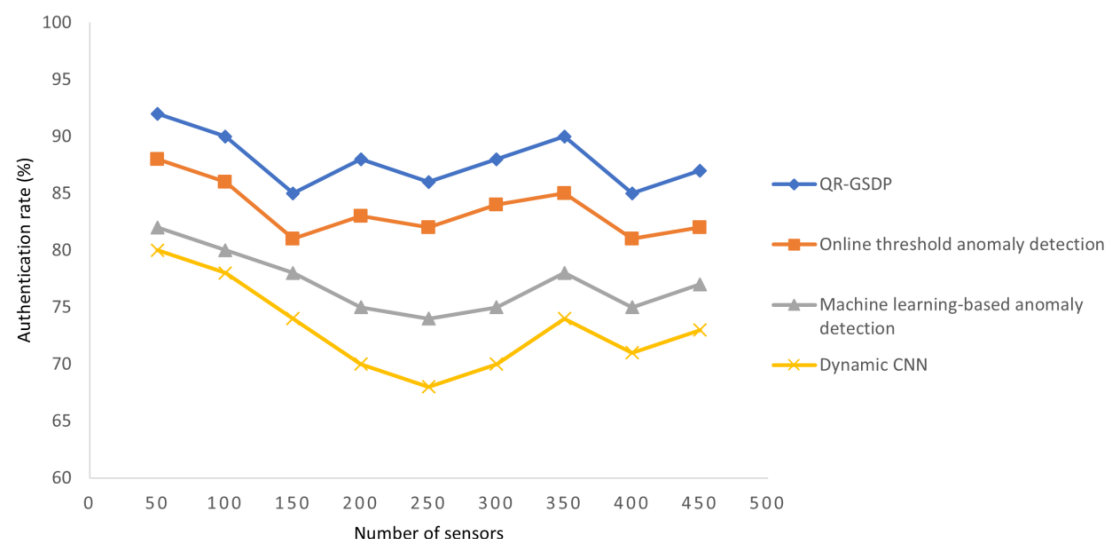
Figure 7. Comparisons of authentication rate.

As the number of sensors increased, the authentication rate for all four models also increased. This is because as the number of sensors increases, the frequency of sensors in the gateway node via the base station increases, so there is a higher probability of a longer amount of time being consumed for encryption and decryption to deal with the request made by each sensor.

However, significant improvement and gain increasing are trends that can be observed with the QR-GSDL approach. For instance, in the case of the simulation using 50 sensors, a total of 46 sensors are correctly authenticated as authentic sensors by the gateway node when applying QR-GSDL, whereas only 44, 41, and 40 sensors are correctly identified by applying Li et al. (2019), Zolanvari et al. (2019), and Yuan et al. (2020), respectively. Thus the authentication rate is higher with QR-GSDL compared to Li et al. (2019), Zolanvari et al. (2019), and Yuan et al. (2020). It is considered that this improvement is due to the application of a gradient sparse auto deep learning algorithm. By applying this algorithm, localization is first achieved using gradients for each sensor in a secure manner, rather than just by identifying the

443 distance between the sensors based on their neighbors Li et al. (2019). Hence the proposed method leads
444 to a higher rate of correct authentications being made by the supervisory control via the gateway node of
445 5%, 8%, and 9% compared to Li et al. (2019), Zolanvari et al. (2019), and Yuan et al. (2020), respectively.

446 **Performance analysis of authentication time**

447 Authentication time refers to the time consumed in authenticating the sensors as either normal or abnormal
448 (malicious). The mathematical formula used to compute authentication time is shown in equation 17:

$$AT = \sum_{i=1}^{n} Samples_i \times Time[R + Q] \tag{17}$$

449 Where AT is authentication time that is measured based on the samples considered for experimentation
450 ($Samples_i$) and the time consumed in encryption (R) and decryption (Q). The value is given in milliseconds
451 (ms). Table 5 and Figure 8 present authentication times of the different models for different numbers of
452 sensors.

Table 5. Authentication time for different models and sensors

Number of sensors	False acceptance rate			
	QR-GSDL	Online threshold anomaly detection	Machine learning-based anomaly detection	Dynamic CNN
50	28.50	35.50	43	47
100	42.40	55.25	65.35	69.75
150	65.25	70.35	80.25	85.35
200	83.50	100.25	125.55	130
250	105.25	125.35	135.35	138.45
300	125.35	140.55	145.55	150.25
350	145.55	175.35	180.25	186.75
400	170	190	200.35	220.15
450	182.35	195.25	225.55	238.15
500	190	200.35	245.55	250.55
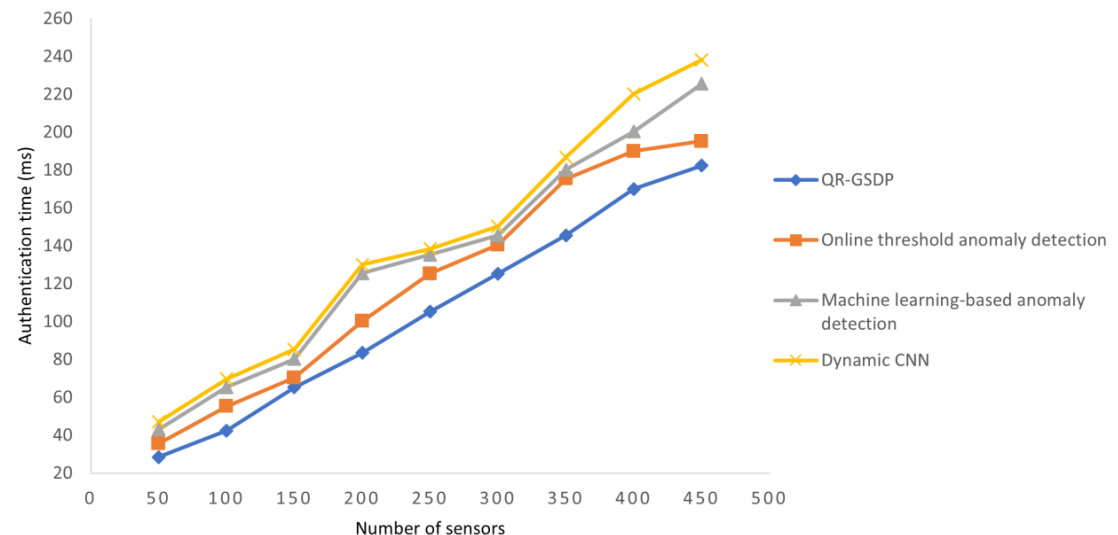
Figure 8. Comparisons of authentication time.

Table 5 and Figure 8 show that a significant improvement in authentication time is achieved by QR-GSDL as compared to Li et al. (2019), Zolanvari et al. (2019), and Yuan et al. (2020). As an example, in the case of the simulation conducted on 50 sensors, a total authentication time of 28.5*ms* was required by QR-GSDL, compared to 35.5*ms*, 43*ms*, and 47*ms* in the case of Li et al. (2019), Zolanvari et al. (2019), and Yuan et al. (2020), respectively. It is considered that this gain is due to the application of the gradient sparse auto deep learning algorithm. Furthermore, the authentication time consumption of the QR-GSDL is 13%, 23%, and 27% lower than that of the online threshold anomaly detection Li et al. (2019), machine learning-based anomaly detection Zolanvari et al. (2019), and dynamic CNN Yuan et al. (2020), respectively.

It can be summarized that the proposed QR-GSDL outperforms the existing methods for the following three reasons: i) Authenticity of the sensors is performed by the supervisory control via the gateway node by using gradients. ii) Authorization of the authenticated sensors to access the data transmitted between them is carried out by using quantum sparse auto- encoding. iii) Intermediate calculations are made at the supervisory control level and not at the gateway node.

CONCLUSION

This paper formalized the authentication and authorization problems in IWSN. The proposed security protocol concentrated on the authenticity and authorization of the massive amount of data interchanged between the sensors. We proposed a Quantum Readout Gradient Secured Deep Learning method to improve authentication rate and time with a minimum false acceptance rate based on our problem formalization. The proposed authentication protocol performs several operations on different layers. The deep learning model uses one input layer, two hidden layers, and one output layer to improve the security model. This protocol first verifies the authenticity of the sensors that want to access the IWSN network data. This was performed by integrating Quantum Readout and Hash functions. To deploy the proposed QR-GSDL method, the location information of the sensors is extracted to reduce the false acceptance rate of the method. The proposed model also includes a minimal energy-based registration process that correctly verifies the login process of the sensors. The Quantum Sparse Auto-Encoding and Decoding model ensures mutual authentication and authorization between the sensor nodes. A comprehensive simulation environment was designed using Network Simulator 2 with different sensors that were run ten times in the simulation with an area size of 1500m × 1500m for the implementation of the QR-GSDL authentication process. The performance of the proposed model is evaluated on the plants' data and compared with the other three similar types of work. The performance comparison is based on the energy consumption, false acceptance rate, authentication rate, and authentication time. The achieved experimental results indicate that our proposed deep learning-based Sparse Auto-Encoding and Decoding model not only ensures better authentication but also better authorization compared to the state-of-the-art

487 methods.

FUTURE WORK

489 Application of the proposed model in the field of the Internet of Things (IoT) is left as future work. It
490 will be interesting to apply some adaptions to the QR-GSDL model and perform experiments to evaluate
491 its performance in the IoT. In addition, it could be interesting to deeply analyze the performance of the
492 QR-GSDL model on different datasets.

REFERENCES

494 Alghamdi, T. (2019). Convolutional technique for enhancing security in wireless sensor networks against
495   malicious nodes. *Human-centric Computing and Information Sciences*, 9(1):38–48.
496 Alrabea, A., Alzubi, O. A., and Alzubi, J. A. (2019). A task-based model for minimizing energy
497   consumption in wsns. *Energy Systems*, 9(1):1–18.
498 Alrabea, A., Alzubi, O. A., and Alzubi, J. A. (2020). An enhanced mac protocol design to prolong sensor
499   network lifetime. *International Journal on Communications Antenna and Propagation*, 10(1):37–43.
500 Alzubi, J. A., Manikandan, R., Alzubi, O. A., , Qiqieh, I., Rahim, R., Gupta, D., and Khanna, A. (2020a).
501   Hashed needham schroeder industrial iot based cost optimized deep secured data transmission in cloud.
502   *Measurement*, 150(3):107077.
503 Alzubi, J. A., Manikandan, R., Alzubi, O. A., Gayathri, N., and Patan, R. (2019a). A survey of specific
504   iot applications. *International Journal on Emerging Technologies*, 10(1):47–53.
505 Alzubi, J. A., Selvakumar, J. ., Alzubi, O. A., and Manikandan, R. (2019b). Decentralized internet of
506   things. *Indian Journal of Public Health Research & Development*, 10(2):251–254.
507 Alzubi, O. A., Alamri, S., Abukharis, S., and Alzubi, J. A. (2014). Packet error rate performance
508   of ieee802.11g under bluetooth interface. *Research Journal of Applied Sciences, Engineering and
509   Technology*, 8(12):1419–1423.
510 Alzubi, O. A., Alzubi, J. A., Dorgham, O., and Alsayyed, M. (2020b). Cryptosystem design based on
511   hermitian curves for iot security. *The Journal of Supercomputing*, 19(3):1–24.
512 Cao, B., Zhao, J., Gu, Y., Fan, S., and Yang, P. (2020). Security-aware industrial wireless sensor network
513   deployment optimization. *IEEE Transactions on Industrial Informatics*, 16(8):5309–5316.
514 Cao, B., Zhao, J., Yang, P., Yang, P., Liu, X., and Zhang, Y. (2019). 3-d deployment optimization for
515   heterogeneous wireless directional sensor networks on smart city. *IEEE Transactions on Industrial
516   Informatics*, 15(3):1798–1808.
517 Chen, C.-T., Lee, C.-C., and Lin, I.-C. (2020). Efficient and secure three-party mutual authentication key
518   agreement protocol for wsns in iot environments. *PLOS ONE*, 15(4):1–28.
519 Iqbal, Z., Kim, K., and Lee, H. (2017). A cooperative wireless sensor network for indoor industrial
520   monitoring. *IEEE Transactions on Industrial Informatics*, 13(2):482–491.
521 Lee, H., Lee, D., Moon, J., Jung, J., Kang, D., Kim, H., and Won, D. (2018). An improved anonymous
522   authentication scheme for roaming in ubiquitous networks. *PLOS ONE*, 13(3):1–33.
523 Li, F., Shinde, A., Shi, Y., Ye, J., Li, X., and Song, W. (2019). System statistics learning-based iot security:
524   feasibility and suitability. *IEEE Internet of Things Journal*, 6(4):6396–6403.
525 Li, R., Ma, W., Huang, N., and Kang, R. (2017). Deployment-based lifetime optimization for linear
526   wireless sensor networks considering both retransmission and discrete power control. *PLOS ONE*,
527   12(11):1–19.
528 Liang, F., Yu, W., Liu, X., Griffith, D., and Golmie, N. (2020). Toward edge-based deep learning in
529   industrial internet of things. *IEEE Internet of Things Journal*, 7(5):4329–4341.
530 Liao, R.-F., Wen, H., Wu, J., Pan, F., Xu, A., Jiang, Y., Xie, F., and Cao, M. (2019). Deep-learning-based
531   physical layer authentication for industrial wireless sensor networks. *Sensors*, 19(11):2440–2457.
532 Liu, X., Zhang, R., and Liu, Q. (2017). A temporal credential-based mutual authentication with multiple-
533   password scheme for wireless sensor networks. *PLOS ONE*, 12(1):1–26.
534 Ma, X., Yao, T., Hu, M., Dong, Y., Liu, W., Wang, F., and Liu, J. (2019). A survey on deep learning
535   empowered iot applications. *IEEE Access*, 7(12):181721–181732.
536 Nazir, S., Alzubi, O. A., Kaleem, M., and Hamdoun, H. (2020). Image subset communication for resource-
537   constrained applications in wireless sensor networks. *Turkish Journal of Electrical Engineering and
538   Computer Sciences*, 13(10):1–15.

Qureshi, K., Bashir, M., Lloret, J., and Leon, A. (2020). Optimized cluster-based dynamic energy-aware routing protocol for wireless sensor networks in agriculture precision. *Journal of Sensors*, 2020(10):1–19.

Ramesh, S. and Yaashuwanth, C. (2019). Enhanced approach using trust based decision making for secured wireless streaming video sensor networks. *Multimedia Tools and Applications*, 79(15):10157–10176.

Sengupta, J., Ruj, S., and Das Bit, S. (2018). An efficient and secure directed diffusion in industrial wireless sensor networks. In *Proceedings of the 1st International Workshop on Future Industrial Communication Networks*, Proceedings of the First International Workshop on Future Industrial Communication Networks (FICN '18), page 41–46, New Delhi, India. Association for Computing Machinery.

Sheikh, H., Tan, H., Ahmad, I., Ranka, S., and Bv, P. (2012). Energy- and performance-aware scheduling of tasks on parallel and distributed systems. *Journal on Emerging Technologies in Computing Systems*, 8(4):1–37.

Sheikh, H. F., Ahmad, I., and Fan, D. (2016). An evolutionary technique for performance-energy-temperature optimized scheduling of parallel tasks on multi-core processors. *IEEE Transactions on Parallel and Distributed Systems*, 27(3):668–681.

Singanamalla, V., Patan, R., Khan, M. S., and Kallam, S. (2019). Reliable and energy-efficient emergency transmission in wireless sensor networks. *Internet Technology Letters*, 2(2):91–96.

Tahir, H., Tahir, R., and McDonald-Maier, K. (2018). On the security of consumer wearable devices in the internet of things. *PLOS ONE*, 13(4):1–21.

Yuan, X., Qi, S., Wang, Y., and Xia, H. (2020). A dynamic cnn for nonlinear dynamic feature learning in soft sensor modeling of industrial process data. *Control Engineering Practice*, 104:104614.

Zhang, X., Chen, X., Liu, J. K., and Xiang, Y. (2020). Deeppar and deepdpa: privacy preserving and asynchronous deep learning for industrial iot. *IEEE Transactions on Industrial Informatics*, 16(3):2081–2090.

Zolanvari, M., Teixeira, M. A., Gupta, L., Khan, K. M., and Jain, R. (2019). Machine learning-based network vulnerability analysis of industrial internet of things. *IEEE Internet of Things Journal*, 6(4):6822–6834.