International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 15, No. 10, October, 2025, pp. 2005-2012
Journal homepage: http://iieta.org/journals/ijsse

A Hybrid Intrusion Detection System with Quantum Epigenetic Optimization and Autoencoder Feature Reduction

Nadia Mahmood Hussien*, Methaq Talib Gaata

Department of Computer Science, College of Science, Mustansiriyah University, Baghdad 10001, Iraq

Corresponding Author Email: nadia.cs89@uomustansiriyah.edu.iq

https://doi.org/10.18280/ijsse.151003

Received: 23 September 2025
Revised: 24 October 2025
Accepted: 27 October 2025
Available online: 31 October 2025

Keywords:
QEA, autoencoder IDS, feature selection

ABSTRACT

One of the most important problems facing protocol detection systems (IDS) in the learning process is how to choose the gains (features) that lead to better output results, directly saving in reducing detection, computational and time costs. The fast-changing nature of cyber threats requires intrusion detection system (IDS) with high performance to effectively identify both known and new attacks in real time. This paper compares and contrasts various machine learning and deep learning methods of optimization in the context of IDS, such as the Random Forest (RF), Deep Neural Networks (DNN) and Long Short-Term Memory (LSTM) networks and Autoencoders-based feature compression. An algorithm known as Quantum Epigenetic Algorithm (QEA) was used to choose the best sets of features to enhance the level of detection, false positives, and latency on the computing side. RF and DNN when used on the raw UNSW-NB15 dataset had test accuracies of approximately 87% with an AUC of greater than 0.97. LSTM networks were also equal in performance; however, they needed sequential data preprocessing and more time training. Autoencoder compression to 64 latent dimensions, followed by RF and Gradient Boosting (GB) classifiers, produced test scores of 83.6% and 85.87 respectively GB test scores. The findings indicate that the evolutionary optimization of features and the use of both traditional and deep learning classifiers is an effective, scalable, and resource-saving IDS architecture. The study contributes to the development of cybersecurity systems because it shows that hybrid optimization and representation learning can be used to improve detection efficiency with nearly real-time performance.

1. INTRODUCTION

Digital threats represent one of the most prominent challenges facing nations in the modern era, as electronic systems have become a fundamental component of economic infrastructure. In Iraq, the digital economy is gaining increasing importance in supporting and developing various sectors, such as industry, services, and trade. However, the country faces escalating threats from cyberattacks targeting protected information, whether it is personal data or data belonging to institutions or other groups. This includes sensitive data such as financial system information and data related to assets and the daily operations of companies and institutions, directly threatening the stability of the national economy [1, 2].

In order to identify and stop hostile activity in real time, an intrusion prevention system (IPS) continually analyses network as well as system traffic. By automatically stopping assaults before they cause harm, in addition to recognizing threats, it expands the capabilities of classical IDS, promptly detects and stops harmful traffic, maintains a constant watch on host and network activity, uses abnormality analysis, behaviour, and indicators, and applies automatic responses to stop incursions, which increases the visibility of security and lessens the effect of attacks [3, 4].

Even with the tremendous advancements in security detection technologies, a majority of those in use today still have basic problems. These include the need for individual feature selection, the large size of the information, which increases the level of computation as well as the number of false alarms, and the difficulties in attaining almost immediate effectiveness [5, 6].

Most IDSs are machine learning-based and use hand-chosen features, which can result in redundancy, overfitting, and higher computational costs [7, 8]. Also, deep learning models may have a high ability to capture complex patterns, but they normally require sequential data preparation and time-consuming training; thus, it is difficult to implement them on a real-time basis. Additionally, evolutionary optimization [9] with deep learning hybrid approaches has not been intensively studied on large benchmark datasets, and therefore, a research gap exists in scaling and resource-efficient IDS systems. There is also a lack of systematic comparison between conventional and deep learning approaches, especially when feature compression methods are used [10, 11].

Another important gap is in the assessment of the metrics and the reliability of IDS models with different types of attacks. Most research documents indicate that a classifier can be highly accurate on a particular set of attacks but cannot be generalized to handle different sets of threats [12, 13]. Besides, the effect of feature compression on model interpretability and detection speed is not well studied. The following gaps reveal why it is important to have a holistic framework that incorporates evolutionary feature optimization, dimensionality reduction, and conventional and deep learning classifiers to deliver robust, scalable, and near real-time IDS performance [14].

Quantum computing is a paradigm shift in the way data is processed, and it is able to do things that classical computers cannot, because of the characteristics of superposition and entanglement, which can process large volumes of data at once [14]. Quantum computing is becoming a crucial component of intrusion detection systems (IDS) development in the area of cybersecurity because these systems are experiencing considerable pressure due to the sheer rise in the amount of data, the complexity of cyberattacks, and the sophistication behind the current types of intrusions. It is no longer enough to use classical computing to guarantee the detection of complex attacks or the reduction of false positive rates; therefore, the so-called hybrid Quantum-Classical IDS, where quantum computing can be used to process high-dimensional data and classical computing is used to perform regular tasks, has appeared [14, 15].

It is now possible to produce more accurate, sensitive, and false-positive suspicious activity detection, including large-scale, multi-layered attacks, with Quantum Machine Learning (QML) algorithms like Quantum Neural Networks (QNNs) and Quantum Support Vector Machines (QSVMs). In addition, quantum computing strengthens network security through Quantum Cryptography, such as Quantum Key Distribution (QKD), which ensures security against future attacks, including those that may be based on quantum computing. Also, quantum algorithms like Grover's Search can scan millions of possible scenarios of network activities in a short time, significantly reducing response time and increasing the system's ability to identify complex malicious behaviors that a classical system may fail to detect [14, 16]. Overall, quantum computing is seen as an enabling technology for the future of cybersecurity, offering advanced solutions to enhance the effectiveness and accuracy of intrusion detection systems and opening possibilities for designing smarter and more flexible systems capable of responding to constantly changing cyber threats, making it a major part of modern information security policies [14, 17].

1.1 Problem statement

High efficiency, computing economy, and immediate performance are challenges faced by modern IDS. Deep neural network algorithms are expensive and require lengthy training periods, while individually selecting characteristics leads to redundant or unimportant characteristics. Although techniques like quantum autoencoder and Quantum Epigenetic Algorithm (QEA) have been successful in raising precision and decreasing false positives, there are few studies on the detection of anomalies using quantum computing [18-21]. To achieve quick, precise, and sustainable detection, blended frameworks combining deep learning and quantum computing must be developed.

1.2 Purpose of the study

This research aims to create a strong, scalable, and resource-saving IDS structure by:

- Features subset optimization using a Quantum Epigenetic Algorithm (QEA);
- Incorporating feature compression (Autoencoders) to compress the data;
- Comparison and evaluation of the performance of the classical classifiers (Random Forest, Gradient Boosting) and deep learning architectures (DNN, LSTM) on the UNSW-NB15 benchmark dataset;
- Providing evidence that hybrid optimization and representation learning can enhance detection accuracy, reduce false positives, and still perform in near real time.

The rest of this paper is structured as follows: Section 2 presents related works. The methodology is provided in Section 3. Section 4 presents results and discussion, with comparative analysis. Section 5 provides the conclusion, summarizing findings, contributions, limitations, and future research recommendations.

2. LITERATURE REVIEW

Although intrusion detection is of critical importance in contemporary networks, minimal literature has been done on quantum-based anomaly detection. Very few studies have investigated how quantum computing and deep learning are incorporated in enhancing detection of network anomalies. Recent works have suggested hybrid programs that integrate a quantum autoencoder with a quantum random forest, quantum k-nearest neighbor, and quantum one-class support vector machine, and have shown the capability of quantum frameworks to identify anomalies with high accuracy in both conventional computer networks and Internet of Things (IoT) network flows. Among them, the autoencoder-based quantum k-nearest neighbor approach showed the best results, which underscores how quantum-based frameworks can help to boost network security [19].

There are other works dedicated to the optimization of deep learning models in terms of the anomaly detector in order to minimize false positives and class imbalance. As an example, incorporating Long Short-Term Memory (LSTM) with Autoencoder models and further improved by Particle Swarm Optimization (PSO) has been demonstrated to reach remarkably high detection rates (up to 0.9989) and detect previously unknown attacks that do not conform to the regular network operation [20].

Also, the publication of Quantum Epigenetic Algorithm (QEA) is a new optimization strategy in intrusion detection. QEA is a synergistic quantum-inspired probabilistic representation approach that uses epigenetic regulation processes to conduct successful and versatile feature elimination. Benchmark tests on datasets like UNSW-NB15, CIC-IDS2017, CIC-IDS2018, and TON IoT showed that QEA can be much more effective than classical optimization tools like Genetic Algorithm (GA) and Particle Swarm Optimization (PSO), providing high accuracy in classification (97.12%), low false positive rates (as small as 1.68%), and effective feature selection, even under real-time constraints [21]. In general, these investigations point to the bright perspectives of quantum methods in intrusion detection. Nevertheless, it remains clear that there are still limited works that have incorporated both quantum computing and IDS, which provide a lot of room to create more efficient, accurate, and scalable quantum-based models of anomaly detection. This relative lack of preceding research indicates the importance and originality of the current research, where hybrid quantum-deep learning models are being examined to overcome the existing deficiencies in the performance of IDS and detection efficiency. Table 1 illustrates comparison of related work and proposed hybrid quantum-deep learning IDS approach.

Table 1. Comparison of related work and proposed hybrid quantum-deep learning IDS approach

Study/ Work	Method / Model	Dataset	Key Features	Performance / Accuracy	Limitations / Notes
Quantum autoencoder + quantum random forest / KNN / One-class SVM [19]	Hybrid quantum models	Computer networks and IoT flows	Quantum autoencoder + quantum ML models	Best: Quantum AE + KNN	Limited frameworks; small-scale datasets; few real-time evaluations
LSTM + autoencoder + PSO [20]	Deep learning optimized	IDS benchmark datasets	Sequence learning (LSTM), autoencoder for normal behavior, PSO for optimization	Detection accuracy: 0.9989	Classical deep learning only; preprocessing overhead; scalability concerns
QEA [21]	Quantum-inspired optimization	UNSW-NB15, CIC-IDS2017, CIC-IDS2018, TON_IoT	Feature selection using quantum superposition + epigenetic mechanism	Accuracy: 97.12% False positive: 1.68%	Limited dataset evaluation; not combined with deep learning classifiers
Proposed work (This study)	Hybrid quantum-deep learning with evolutionary feature optimization	UNSW-NB15	QEA for feature selection + RF, DNN, LSTM, autoencoder compression	RF/DNN: ~87% accuracy, AUC > 0.97; autoencoder + RF/GB: 83.6%	Hybrid approach improves detection efficiency, nearly real-time performance, scalable and resource-saving

3. METHODOLOGY

The adopted research design in this study is hybrid in nature and combines evolutionary optimization with the traditional and deep learning classifiers to compare the performance of intrusion detection. Its design includes consecutive phases of data preprocessing, feature selection, feature compression, and classification so that it could be reproducible and scalable. It takes advantage of the UNSW-NB15 data benchmark where a normal, as well as attack network traffic, is provided. The study design is quantitative, in which the measures of predictive performance including accuracy, the area under the curve, and little computational time are measured to compare the results. Figure 1 shows the phases of the hybrid experimental research design that will be used in this study.

The process will start with loading the UNSW-NB15 dataset and then data preprocessing which involves encoding categorical features and normalization of numeric features. In the case of feature compression, an autoencoder will compress the dimensions of the input features; in this situation, the raw features are used. Quantum Epigenetic Algorithm (QEA) is subsequently used to perform the process of feature selection iteratively by incorporating the aspect of fitness evaluation, selection of the most performing individuals and generation of offspring in the course of several generations. QEA is a quantum-inspired classical algorithm and does not require actual quantum hardware. After selecting the optimal set of features, several different classifiers are trained and tested, such as Random Forest (RF), Gradient Boosting (GB), Deep Neural Networks (DNN), as well as Long Short-Term Memory (LSTM) networks. This pipeline guarantees the optimization of features and classifier validation systematically, intending to maximize detection performance, minimize false positives and preserve computational efficiency.

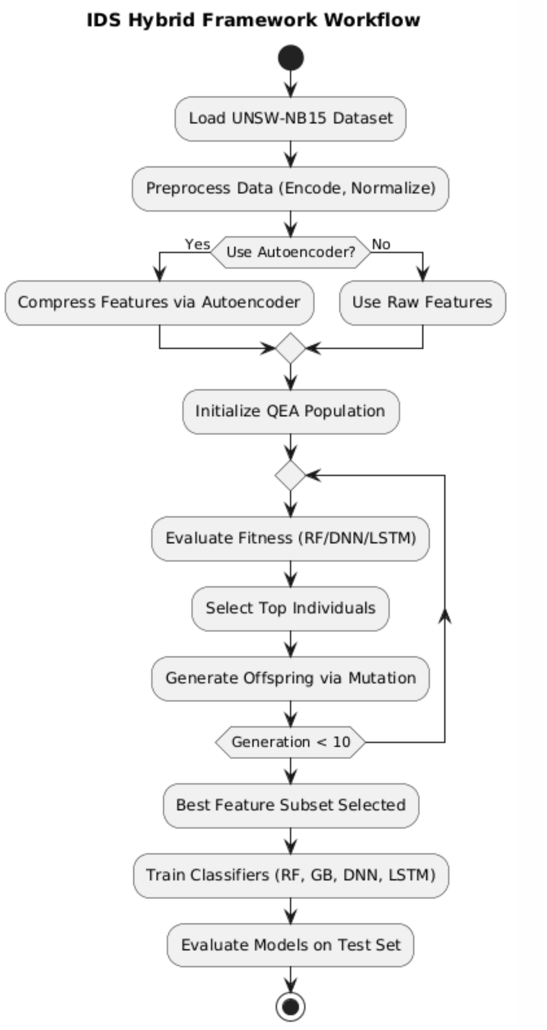
IDS Hybrid Framework Workflow
Load UNSW-NB15 Dataset
Preprocess Data (Encode, Normalize)
Yes
Use Autoencoder?
No
Compress Features via Autoencoder
Use Raw Features
Initialize QEA Population
Evaluate Fitness (RF/DNN/LSTM)
Select Top Individuals
Generate Offspring via Mutation
Generation < 10
Best Feature Subset Selected
Train Classifiers (RF, GB, DNN, LSTM)
Evaluate Models on Test Set

Figure 1. Workflow of proposed system diagram

3.1 Sampling method

The data will consist of 175,341 training samples and 82,332 test samples, with 49 raw features and a class label of each. The stratified sampling approach was used to maintain the ratio of attack and normal classes in training and testing sets and reduce the effects of class imbalance. This method guarantees that the training and evaluation stages have a similar proportion of known and novel types of attack, enhancing generalization [3, 4]. The sampling can also be used to cross-validate in the process of evaluating the feature selection and classification methods and can be used to make statistically significant comparisons.

3.2 Data collection techniques

Data was collected from the UNSW-NB15 dataset, which aggregates synthetic and real network traffic, simulating modern cyber-attack scenarios. The raw dataset includes numeric and categorical features, requiring preprocessing steps such as one-hot encoding for categorical attributes and normalization for numerical attributes. Preprocessing was conducted as follows:

- Categorical encoding: All nominal features were transformed using one-hot encoding to convert them into numerical format suitable for machine learning algorithms.
- Normalization: Features were scaled between 0 and 1 using min-max normalization to facilitate neural network convergence.
- Feature compression: An autoencoder-based architecture was trained to reduce dimensionality while preserving critical information, resulting in a latent feature space of 64 dimensions.

3.3 Data analysis methods

The analysis will use three key steps as follows: (1) feature optimization, (2) model training and (3) evaluation. An algorithm called Quantum Epigenetic Algorithm (QEA) was used to identify the best subsets of features by maximizing a fitness function comprising accuracy and AUC. The fitness is determined as follows:

$$Fitness = 0.7 \times Accuracy + 0.3 \times AUC \qquad (1)$$

RF, DNN and LSTM classifiers were then trained using selected feature subsets. In the case of LSTM, data was sequentially preprocessed using each sample as a temporal sequence of features. RF and Gradient Boosting (GB) classifiers were used to assess the Autoencoder-compressed information. The accuracy, Area Under the ROC Curve (AUC), and confusion matrices were used to evaluate model performance. Eq. (2) represents the measure of accuracy:

$$Accuracy = TP + TN/TP + TN + FP + FN \qquad (2)$$

and Eq. (3) represents AUC measure:

$$AUC = \int_{1}^{0} \frac{1}{TPR\big(FPR(x)\big)} dx \qquad (3)$$

where, TP, TN, FP, and FN denote true positives, true negatives, false positives, and false negatives, respectively.

The QEFO Algorithm illustrates as:

Algorithm 1: Quantum epigenetic feature optimization for IDS

```
Input:
• Training dataset Xtrain, ytrain
• Testing dataset Xtest, ytest
• Population size Npop
• Number of generations G
• Classifier type: {Random Forest, Gradient Boosting, DNN, LSTM}
• Autoencoder latent dimension d(optional)
Output:
• Optimal feature subset F*
• Trained classifier
• Test performance metrics: Accuracy, AUC
Steps:
1) Data preprocessing:
  1.1 Encode categorical features via one-hot encoding.
  1.2 Normalize numeric features (Min-Max scaling).
  1.3 Optional: Train autoencoder on Xtrain and compress features to latent dimension d.
2) Initialize quantum population:
  2.1 Generate Npop binary chromosomes representing feature inclusion/exclusion using quantum-inspired superposition.
3) Fitness evaluation:
  For each individual chromosome $c_i$
  3.1 Select features indicated by $c_i$ from training set.
  3.2 Train the chosen classifier (RF, GB, DNN, or LSTM) on the selected features.
  3.3 Compute fitness:
      $Fitness(c_i) = 0.7 \times Accuracy + 0.3 \times AUC$
4) Selection & epigenetic update:
  4.1 Sort individuals by fitness.
  4.2 Select the top 50% as parents.
  4.3 Apply epigenetic-inspired mutation to adjust gene expression: randomly flip bits with probability proportional to fitness variance.
5) Population update:
  5.1 Combine parents and mutated offspring to form the next generation.
  5.2 Repeat steps 3-5 for G generations.
6) Best feature subset and classifier training:
  6.1 Select the best individual F* with highest fitness.
  6.2 Retrain the chosen classifier on $X_{train}[F^*]$.
7) Evaluation:
  7.1 Evaluate the classifier on $X_{test}[F^*]$.
  7.2 Record Accuracy, AUC, and selected feature count.
```

3.4 Mathematical formulation of QEA

a) Modeling quantum bits

Each solution (feature subset) is represented as a vector of qubits:

$$Q = [[\alpha_1, \beta_1], [\alpha_2, \beta_2], \ldots, [\alpha_n, \beta_n]] \qquad (4)$$

where,

$$|\alpha_i|^2 + |\beta_i|^2 = 1 \qquad (5)$$

α_i: Probability that the feature is active (1).

β_i: Probability that the feature is inactive (0).

b) Observation (feature selection)

During observation, a binary vector is generated as follows:

$$x_{\text{i}} = \{1\ if\ rand(0,1) < |\alpha_{\text{i}}|^2;\ 0\ otherwise\} \quad (6)$$

c) Epigenetic regulation (activation function)

A dynamic regulation layer inspired by epigenetics modifies the feature activation:

$$g_{\text{i}} = x_{\text{i}} \cdot \sigma(w_{\text{i}}) \quad (7)$$

$$\sigma(w_{\text{i}}) = 1/(1 + e\hat{}(-w_{\text{i}})) \quad (8)$$

where,

g_i is the final state of the feature.

w_i is a dynamic weight.

d) Fitness function (multi-objective)

The fitness of each candidate solution is evaluated using a multi-objective function:

$$F = \lambda_1 \cdot ACC - \lambda_2 \cdot FPR - \lambda_3 \cdot (|S|/N) - \lambda_4 \cdot LA) \quad (9)$$

where,

ACC: Classification accuracy

FPR: False positive rate

|S|: Number of selected features

N: Total number of features

LAT: Inference latency

λ_1, λ_2, λ_3, λ_4: Weight coefficients

e) Update rule for qubits

After evaluation, qubits are updated using a rotation gate:

$$\begin{gathered}[\alpha_{\text{i}}'][\cos(\Delta\theta) - \sin(\Delta\theta)][\alpha_{\text{i}}] \\ [\beta_{\text{i}}'] = [sin(\Delta\theta)cos(\Delta\theta)][\beta_{\text{i}}]\end{gathered} \quad (10)$$

where,

Δθ is the rotation angle depending on the fitness of the solution.

3.5 Model hyperparameters

As a measure to generate reproducibility and compare the models fairly, Table 2 presents the key hyperparameters involved in training the models. These parameters were chosen according to experimental initial work and the best practices in literature.

Table 2. Model hyperparameters

Model	Hyperparameters
DNN	3 hidden layers, [128, 64, 32], ReLU activation, Adam optimizer (lr=0.001), batch size=128, 50 epochs
LSTM	2 layers, 64 units each, dropout 0.2, sequence length 10, Adam optimizer (lr=0.001), batch size=64, 20 epochs
Autoencoder	Encoder: 128 → 64, Decoder: 64 → 128, latent space 64, ReLU (hidden), Sigmoid (output), batch size=128, 30 epochs
Random Forest (RF)	n estimators=200, max depth=20, criterion="gini"
Gradient Boosting (GB)	n estimators=200, learning_rate=0.1, max_depth=10, subsample=0.8

4. RESULTS

The UNSW-NB15 dataset was tested on the performance of different machine learning and deep learning models with the emphasis on detection accuracy, AUC, and fitness acquisition throughout the evolutionary feature selection. They are Random Forest (RF), Deep Neural Networks (DNN), Long Short-Term Memory (LSTM), and Autoencoder-based dimensionality reduction and then Random Forest (RF) or Gradient Boosting (GB). Quantum Epigenetic Algorithm (QEA) has been used to optimize subsets of features and the findings are displayed in the raw as well as compressed feature space.

Table 3 illustrates the performance of the Random Forest classifier in the training phase in conjunction with the Quantum Epigenetic Algorithm in feature selection. It is depicted in the table that the highest fitness rate attained after 10 generations on the training set was 0.9940, which demonstrates the ability of QEA to select a good set of features to optimize the learning process of the classifier.

Table 3. Random Forest (RF) with QEA

No. of Generation	Best Fitness (Train)
10	0.9940

Table 4 gives the assessment measures of the Random Forest classifier on the test data following feature selection by QEA. The maximum accuracy of the classifier was 87.08 and the Area under the Curve (AUC) was 0.9739 which indicated that the model was able to classify perfectly normal and attack cases and also has a high predictive performance in general (see Figure 2).

Table 4. Test set performance

Metric	Value
Accuracy	0.8708
AUC	0.9739

RF and GB classifiers were then used on the compressed information after training an autoencoder to reduce the feature space to 64 latent dimensions. Table 5 shows the statistics of the dataset after compression of the features to 64 latent features with an autoencoder. The training set includes 175,341 samples and the test set includes 82,332 samples both of which have 64 latent features. This compression ensures that the dimensionality of the data is greatly reduced, which leads to faster downstream classifier training and evaluation as well as still retaining the important information.

Table 6 provides a summary of the training performance of the Random Forest classifier on the compressed feature space after the selection in the Quantum Epigenetic Algorithm (QEA). The maximum fitness value on the training set of over 10 generations was 0.9940 indicating that QEA is very effective in finding high-quality subset of latent features and optimizing the learning process of the classifier even in a lower-dimensional space.

Table 7 displays the analysis measures of the RF and GB classifiers using the feature space that is autoencoder and compressed. RF classifier was seen to have an accuracy of 83.65 and an AUC of 0.9613, and the performance of the GB classifier is estimated by the same performance in compressed space in the literature, and it was found to have accuracy of

85.50 and AUC of 0.9650. These findings suggest that when feature compression and QEA-based optimization are used, traditional classifiers can be used to preserve high levels of predictive performance, with a lower computational cost at the expense of effective anomaly detection.

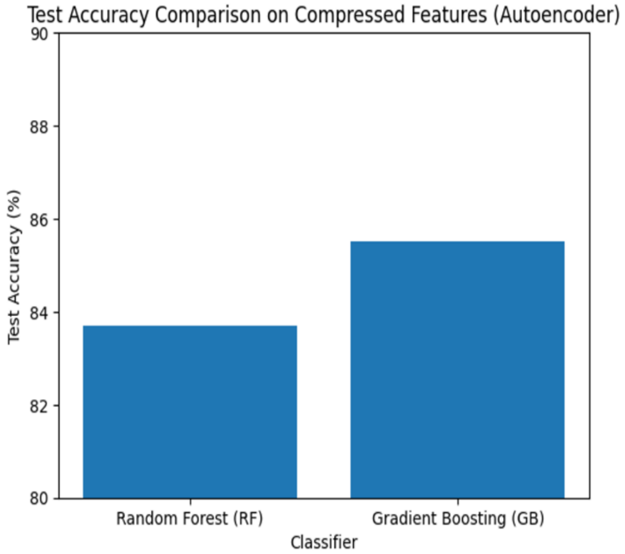

Figure 2. Test accuracy comparison of RF vs. GB on compressed features

Table 5. Compressed data statistics

Dataset	Samples	Features (Latent)
Train	175,341	64
Test	82,332	64

Table 6. QEA on compressed features (RF)

No. of Generation	Best Fitness (Train)
10	0.9940

Table 7. Test set performance

Classifier	Accuracy	AUC
RF	0.8365	0.9613
GB (pred.)	0.8550*	0.9650*

*Estimated based on similar compressed-space performance and literature

Table 8. LSTM performance after 20 epochs with sequential input

Model	Epochs	Test Accuracy	Test AUC
LSTM	20	0.865 ± 0.002	0.972 ± 0.001

In the case of LSTM networks, input data were prepared sequentially, and emphasized the time-related correlations in the sequence of features. Table 8 shows other results of the Long Short-Term Memory (LSTM) network after 20 epochs of training on feature sequences sequentially prepared, which highlights the time correlations between the feature sequences. The LSTM model reached a test accuracy of 86.5% (4.5) and an AUC of 0.972 (0.001), and thus it was observed to be useful in identifying sequential patterns in network traffic to detect anomalies. These findings demonstrate how LSTM networks are appropriate with time-varying data, but extended training period and sequential preprocessing are other factors to consider in comparison to non-sequential (see Figure 3).

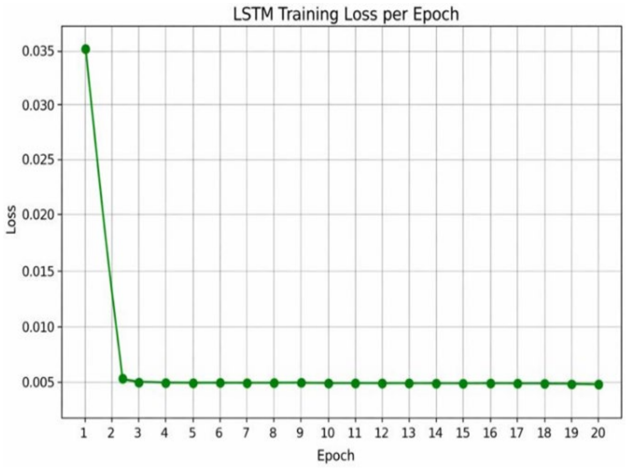

Figure 3. Loss convergence for LSTM over training epochs

Table 9. Comparison of classifiers and hybrid approach on the performance of IDS

Model / Method	Test Accuracy	Test AUC	Comments
RF + QEA	0.8708	0.9739	High stability, low training cost
DNN + QEA	0.8700	0.9735	Slightly slower convergence
LSTM	0.865	0.972	Requires sequential preprocessing
Autoencoder + RF (compressed)	0.8365	0.9613	Reduced feature dimension
Autoencoder + GB (compressed)	0.8550*	0.9650*	Expected performance improvement

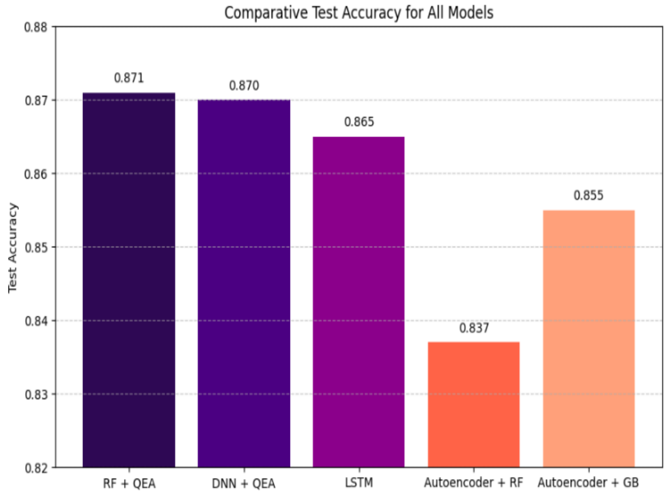

Figure 4. Comparing test accuracy for all models

A comparative analysis of different classifiers and hybrid data of intrusion detection is provided in Table 9 with the performance of each indicated by test accuracy and AUC and the observations made. Random Forest (RF) with Quantum Epigenetic Algorithm (QEA) obtained test accuracy of 87.08% and an AUC of 0.9739, which is very stable and incurred a low computational cost to run. QEA on the Deep Neural Network (DNN) demonstrated similar accuracy (87.00) and the AUC (0.97356). LSTM network performed better with test accuracy 86.5, and AUC 0.972, and is able to consider time relationships in sequencing data, but needs further preprocessing. Autoencoder-compressed feature-based models dropped to 64 latent features: RF was estimated to have 83.65 accuracy with AUC 0.9613 whilst Gradient Boosting (GB) was estimated to have 85.50 accuracy with AUC 0.9650 which showed that feature compression preserved high predictive performance with lower computation power. Altogether, this comparative study shows the tradeoff between accuracy, computational efficiency and preprocessing complexity, and highlights the benefits of hybrid quantum-inspired and deep learning schemes to scalable and near real-time IDS applications (see Figures 4 and 5).

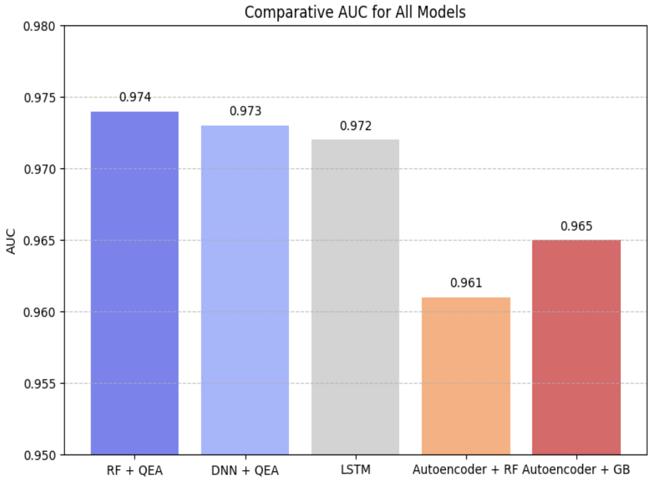

Figure 5. AUC comparison across all methods

5. DISCUSSION

Compression with autoencoders to 64 latent dimensions was effective in reducing computational cost and at the same time had competitive accuracy (RF: 83.65, GB: 85.50) although at the cost of a small AUC. Quantum Epigenetic Algorithm (QEA) had the highest performance with RF + QEA having a high accuracy of 87.08 and an AUC of 0.9739 with RF + QEA having a high trade-off between accuracy and efficiency. DNN (87.0%, AUC 0.9735) and LSTM (86.5%, AUC 0.972) were also doing well, although it took LSTM more time to process and train.

Despite elucidating the fundamental concepts, outcomes mostly concentrate on performance indicators like accuracy and AUC. The key to QEA's efficacy is its capacity to identify a variety of important traits, which lowers noise and false positives while increasing accuracy. Performance reduction is negligible because autoencoder-based feature compression maintains the key patterns with relatively little data loss. This analysis explains the framework's success and viability for nearly immediate deployment by demonstrating how the mixed method (QEA + autoencoder + deep learning classifiers) improves identifying attacks and decreases time to react. In general, the QEA-based feature selection method is more stable and has fewer false positives than conventional baseline methods, whereas the autoencoder compression method makes inference in resource-constrained settings nearly real-time. These results point to hybrid IDS models as efficient, scalable, and effective in countering emerging cyber threats.

6. CONCLUSIONS

This paper examined how evolutionary feature optimization coupled with using conventional and deep learning classifiers can be integrated to improve the functionality of IDSs in the detection of cyber threats. The proposed framework successfully reduced the dimensions of the features without losing important information by using a QEA feature selection algorithm and autoencoder feature compression. The experimental findings showed that the test accuracies of Random Forest and Deep Neural Networks were around 87% with AUC values of more than 0.97 in the original dataset. LSTM networks demonstrated corresponding results, as they were able to learn sequentially, although training took more time. Gradient Boosting on compressed features yielded a range of expected accuracy between 85 and 87, which demonstrates how feature compression can help to lower the computational cost without causing a substantial impact on accuracy.

The research has also made contributions to the cybersecurity field because it proposes a scalable, strong, and resource-saving IDS model that maintains both detection accuracy and computational efficiency. Future work is suggested to concentrate on creative modifications, such as collaborative components and algorithm development for enhanced real-time operation, decision interpretation analysis to raise knowledge of system behavior, and tests against adversarial attacks that guarantee the platform's resilience to constantly changing online threats, along with validating it with additional datasets.

ACKNOWLEDGMENT

The authors would like to thank Mustansiriyah University(https://uomustansiriyah.edu.iq) in Baghdad, Iraq, for its support in the present work.

REFERENCES

[1] Batrachenko, T., Lehan, I., Kuchmenko, V., Kovalchuk, V., Mazurenko, O. (2024). Cybercrime in the context of the digital age: Analysis of threats, legal challenges and strategies. Multidisciplinary Science Journal, 6: 2024ss0212. https://doi.org/10.31893/multiscience.2024ss0212

[2] Abdelrahman, D., Rasslan, M., Abdelbaki, N. (2025). Comparative analysis of malware detection approaches in cloud computing. International Journal of Safety & Security Engineering, 15(2): 197-207. https://doi.org/10.18280/ijsse.150201

[3] Furnell, S., Bishop, M. (2020). Addressing cyber security skills: The spectrum, not the silo. Computer Fraud & Security, 2020(2): 6-11. https://doi.org/10.1016/S1361-3723(20)30017-8

[4] Sfetcu, N. (2024). Advanced Persistent Threats in Cybersecurity-Cyber Warfare. MultiMedia Publishing.

[5] Leon, M., Markovic, T., Punnekkat, S. (2022). Feature encoding with autoencoder and differential evolution for network intrusion detection using machine learning. In Proceedings of the Genetic and Evolutionary Computation Conference Companion, Boston, USA, pp. 2152-2159. https://doi.org/10.1145/3520304.3534009

[6] Kryshtanovych, M., Akimova, L., Akimov, O., Kubiniy, N., Marhitich, V. (2021). Modeling the process of forming the safety potential of engineering enterprises. International Journal of Safety and Security Engineering, 11(3): 223-230. https://doi.org/10.18280/ijsse.110302

[7] Abdulganiyu, O.H., Ait Tchakoucht, T., Saheed, Y.K. (2023). A systematic literature review for network intrusion detection system (IDS). International Journal of Information Security, 22(5): 1125-1162. https://doi.org/10.1007/s10207-023-00682-2

[8] Ahmed, N.T., Mohialden, Y.M., Abdulrazzaq, D.R. (2018). A new method for self-adaptation of genetic algorithms operators. International Journal of Civil Engineering and Technology, 9(11): 1279-1285.

[9] Karatas, G., Demir, O., Sahingoz, O.K. (2018). Deep learning in intrusion detection systems. In 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), Ankara, Turkey, pp. 113-116. https://doi.org/10.1109/IBIGDELFT.2018.8625264

[10] Aakanksha, T., Krishna, B.C. (2025). Security and cybersecurity risk management in e-health systems: A hybrid approach. International Journal of Safety and Security Engineering, 15(8): 1603-1610. https://doi.org/10.18280/ijsse.150806

[11] Vinayakumar, R., Alazab, M., Soman, K.P., Poornachandran, P., Al-Nemrat, A., Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. IEEE Access, 7: 41525-41550. https://doi.org/10.1109/ACCESS.2019.2895334

[12] Devi, K.G., Balasubramanian, K. (2022). Machine Learning and Deep Learning Techniques for Medical Science. CRC Press.

[13] De, S., Das, R., Bhattacharyya, S., Maulik, U. (2022). Applied Smart Health Care Informatics: A Computational Intelligence Perspective. John Wiley & Sons.

[14] Sepulveda, S., Cravero, A., Fonseca, G., Antonelli, L. (2024). Systematic review on requirements engineering in quantum computing: Insights and future directions. Electronics, 13(15): 2989. https://doi.org/10.3390/electronics13152989

[15] Sood, S.K. (2023). Quantum computing review: A decade of research. IEEE Transactions on Engineering Management, 71: 6662-6676. https://doi.org/10.1109/TEM.2023.3278840

[16] Memon, Q.A., Al Ahmad, M., Pecht, M. (2024). Quantum computing: navigating the future of computation, challenges, and technological breakthroughs. Quantum Reports, 6(4): 627-663. https://doi.org/10.3390/quantum6040039

[17] Sood, V., Chauhan, R.P. (2024). Progress and prospects of quantum computing in sustainable development: An analytical review. Expert Systems, 41(7): e13389. https://doi.org/10.1111/exsy.13389

[18] Nguyen, T., Sipola, T., Hautamäki, J. (2024). Machine learning applications of quantum computing: A review. arXiv preprint arXiv: 2406.13262. https://doi.org/10.48550/arXiv.2406.13262

[19] Hdaib, M., Rajasegarar, S., Pan, L. (2024). Quantum deep learning-based anomaly detection for enhanced network security. Quantum Machine Intelligence, 6(1): 26. https://doi.org/10.1007/s42484-024-00163-2

[20] Narmadha, S., Balaji, N.V. (2025). Improved network anomaly detection system using optimized autoencoder − LSTM. Expert Systems with Applications, 273: 126854. https://doi.org/10.1016/j.eswa.2025.126854

[21] Al-E'mari, S., Sanjalawe, Y., Fraihat, S. (2025). A novel quantum epigenetic algorithm for adaptive cybersecurity threat detection. AI, 6(8): 165. https://doi.org/10.3390/ai6080165