PENINSULA PUBLISHING LLC

SHIFRA

Vol. **(2026)**, 2026, **pp**. 177–192
ISSN: 3078-3186

Research Article

Intelligent Zero Trust Cybersecurity Framework for Enterprise Network Protection Using Autoencoder CNN-GRU Hybrid Learning

Hamza Lahbabi[1, *], Youssef Filali[2], Fouad Agramelal[3], Mohamed Sadik[3], Karim El Moutaouakil[1]

[1] *Engineering Sciences Laboratory, Faculté Poly Disciplinaire de Taza, University Sidi Mohamed Ben abdellah , Fez, Morocco*

[2] *Computer science department, University Sidi Mohamed Ben abdellah, Fez, Morocco*

[3] *NEST Research Group, Energy and Electrical Systems Laboratory (LESE Lab.), National Higher School of Electricity and Mechanics (ENSEM), Hassan II University of Casablanca, Casablanca 20000, Morocco*

ARTICLEINFO

Article History

Received 14 Apr 2026

Revised: 03 Jun 2026
Accepted 01 Jul 2026
Published 16 Jul 2026

Keywords

Zero Trust Architecture,

Enterprise Cybersecurity,

AutoEncoder–CNN–GRU,

Intrusion Detection System,

Hybrid Deep Learning,

Enterprise Network Security,

CSE-CIC-IDS2018.

ABSTRACT

As cyber threats grow more sophisticated and enterprise network architectures are becoming more complex, traditional perimeter-based cybersecurity mechanisms have proven inadequate. In recent years, Zero Trust Architecture (ZTA) has become a successful security paradigm that continuously checks the validity of all requests that are made. Recently, Zero Trust Architecture (ZTA) has become an effective paradigm that continuously checks the validity of all requests made, rather than taking trust for granted. Most current Zero Trust architectures, though, are based on complex architectures that are very compute-intensive or are mainly used in the authentication and access control domain without having the intelligent intrusion detection capabilities. To tackle these problems, this paper presents an Intelligent Zero Trust Cybersecurity Framework for Enterprise Network Protection Based on AutoEncoder CNN–GRU Hybrid Learning. The proposed system embeds feature compression using an AutoEncoder, learning of spatial features using a Convolutional Neural Network (CNN), and learning of temporal dependencies using a Gated Recurrent Unit (GRU) in a single deep learning system. In addition, a Zero Trust Decision Engine is added to transform the forecasted classification probabilities into dynamic risk scores for adaptive Allow, Monitor and Block access decisions. The framework was tested with the benchmark CSE-CIC-IDS2018 dataset in a standard deep learning environment with Python. Experimental results have shown that the proposed framework improved the accuracy to 99.12%, precision to 98.96%, recall to 98.81%, F1-score to 98.88%, and ROC-AUC to 99.47% with low inference latency and moderate computational complexity for real-world enterprise applications. The proposed framework is also found to give a good balance between predictive performance, computational efficiency, and adaptive Zero Trust decision-making through a comparative analysis with recent state-of-the-art approaches. The results highlight the promise of hybrid deep learning and Zero Trust approach in achieving scalable, intelligent, and reliable enterprise cybersecurity solutions.

1. INTRODUCTION

The digital evolution of today's businesses has reshaped how a company plans, operates and protects its network infrastructure. New technologies like cloud computing, edge computing, the Internet of Things (IoT), fifth-generation (5G) communication, software-defined networking (SDN), and virtualization have greatly aided service availability, scalability, and operational efficiency. They are capable of delivering seamless connectivity between different devices, applications and users across geographical distance while providing support for data-intensive services across healthcare, finance, manufacturing, transportation, education and critical infrastructure industries. At the same time, the various ways that enterprises are becoming interconnected has also led to a significant increase in the cybersecurity attack surface, which has opened up many entry points that can be used by malicious actors to wreak havoc on network resources, systems, and services or to steal sensitive data. With the advancement of cyber threats becoming more complex and sophisticated, enterprise network security protection is one of the main challenges of this era [1].

Traditional cybersecurity solutions are based on perimeter-based security models which assume that users and devices connected to an organization's internal network are trusted once they have been authenticated. Traditional intrusion

*Corresponding author email: hamza.lahbabi@usmba.ac.ma
DOI: https://doi.org/10.70470/SHIFRA/2026/010

detection systems (IDSs), firewalls, and signature based security solutions are effective against known attacks, but less effective against more complex attacks like zero-day attacks, advanced persistent threats (APTs), insider attacks, polymorphic malware, and multi-stage cyber intrusions. Additionally, traditional security mechanisms have become less scalable and flexible due to the increasing volume of network traffic driven by cloud services, Internet of Things (IoT) devices and distributed enterprise applications. As network behaviors become more varied and encryption methods grow more sophisticated, manually written rules and static attack signatures no longer seem to be a viable method for detecting attacks; this has led to the necessity to use intelligent cybersecurity solutions that automatically respond to changing threat landscapes [1,2].

The cybersecurity industry has now embraced the Zero Trust Architecture (ZTA) as a contemporary way to defend enterprise networks against these challenges. In contrast, while traditional security models assume trust of users in the network perimeter, Zero Trust follows the rule "Never Trust, Always Verify." All communications, applications, and devices needing access to organizational resources are continually authenticated, authorized, and assessed. Zero Trust focuses on verifying the identity, monitoring the device posture, granting access at the lowest level of privilege, monitoring access continuously, and enforcing policies dynamically throughout the entire communication session. This ongoing verification process is very effective in minimizing lateral movement, privilege escalation, credential compromise, and insider attacks and is among the most promising cybersecurity architectures for today's enterprise environment [2].

Advances in Artificial Intelligence (AI), especially deep learning, have also revolutionized cybersecurity by allowing intelligent analysis of large volumes of network traffic and automatic discovery of complex behavioral patterns without the need for manually designed features. The deep learning architectures have shown great capacity to differentiate known and unknown cyber threats by learning the hierarchy of the features from network traffic data directly. Of these architectures, AutoEncoder models have been shown to be effective for learning compact latent representations and learning to eliminate redundant information, Convolutional Neural Networks (CNNs) have been found to be superior at learning discriminative spatial features in traffic flows, and Gated Recurrent Units (GRUs) are effective at capturing temporal dependencies between successive network events with lower computational complexity than traditional RNNs. These complementary properties of these deep learning models offer the possibilities of building intelligent cybersecurity frameworks which can detect attacks with high accuracy and with efficient real-time performance [3–10].

While these are good signs, there are still some unanswered questions. Despite the growing interest in Zero Trust, most of the current literature concentrates on conceptual architectures and access control policies, authentication protocols, or trust management model, without showcasing a proper integration with an intelligent intrusion detection model. In contrast, numerous deep learning focused intrusion detection systems (IDSs) focus solely on classification performance without the ability to integrate dynamic access control or continuously assess trustworthiness that would be needed to support Zero Trust principles. Furthermore, the current hybrid deep learning models are complex and require significantly more computational power or do not consider practical deployment issues, such as latency for inference, computational efficiency, and adaptive decision-making for enterprise systems. The restrictions suggest the need of a single system that can integrate intelligent threat detection and Zero Trust access control at the same time and still be computationally viable and realistic for deployment in the real world [7–14].

In this regard, this study introduces an Intelligent Zero Trust Cybersecurity Framework for Enterprise Network Protection Using AutoEncoder–CNN–GRU Hybrid Learning to cope the above challenges. The proposed framework combines a lightweight hybrid deep learning system and a dynamic Zero Trust decision engine to facilitate proactive threat detection and adaptive access control. The initial step is to use an AutoEncoder to sample pre-processed network traffic and derive compact low dimensional representations without losing discriminative features. The extracted traffic patterns are then passed to a CNN to learn spatial traffic patterns, and a GRU layer is used to model temporal correlations between network communication sequences. The feature representations are then used to estimate the likelihood of malicious activity, and which is also fed into a dynamic risk-scoring process in the Zero Trust policy engine. Based on the calculated risk level, the framework makes real-time decisions on access, permitting, monitoring, or denying network activities based on a set of trust policies. This integrated architecture can continuously validate and verify the network entity and also improve the intrusion detection performance and realize the intelligent network protection of the enterprise. This research made the following main contributions:

1. A novel Zero Trust cybersecurity framework is proposed for intelligent enterprise network protection through continuous verification and adaptive access control.
2. A lightweight AutoEncoder–CNN–GRU hybrid deep learning architecture is developed to jointly learn compressed, spatial, and temporal representations of enterprise network traffic.
3. A dynamic risk-scoring mechanism is integrated into the Zero Trust policy engine to support intelligent trust evaluation and adaptive security decision-making.
4. A real-time access control strategy is designed to automatically perform allow, monitor, or block actions according to predicted threat levels.

5. The proposed framework is comprehensively evaluated using a modern benchmark intrusion detection dataset, and its performance is analyzed in terms of classification effectiveness, computational efficiency, and comparison with recent deep learning-based cybersecurity approaches.

2. RELATED WORK

2.1 Zero Trust Architecture for Enterprise Network Security

As enterprise computing environments continue to evolve at a rapid pace, Zero Trust Architecture (ZTA) has emerged as a contemporary cybersecurity approach that can overcome the shortcomings of perimeter-based security strategies. Unlike traditional methods that simply assume those authenticated within the organization are trustworthy, Zero Trust is a constant verification of requests for access to protected resources from each user, device, application, and communication. This security approach greatly lowers the risk of insider threats, credential stealing, lateral movement and escalation of privileges and offers adaptive protection in highly dynamic enterprise environments [15].

A new Zero Trust framework combined hybrid deep learning algorithms and adaptive security policies for smart threat detection and adaptive access control in cloud environments. The proposed architecture used several deep learning models to enhance the capability of threat detection while interacting with more complex attack scenarios in the presence of reinforcement learning. The framework was very good at detecting, but due to its dependence on multiple learning phases, the computational complexity of the framework was very complex, meaning that it was difficult to implement in large enterprises [15].

Likewise, to advance intelligent authentication and the ongoing assessment of trust, an AI-powered Zero Trust approach was suggested for Industrial Internet of Things (IIoT) systems. The framework showed enhanced cyber security within industrial infrastructure, adaptive policy enforcement and AI-driven decision making to protect against cyber threats. It was focused mainly on IIoT environments, however, with a focus on enterprise network protection, opportunities for lightweight Zero Trust frameworks for enterprise cybersecurity were left [16].

2.2 Hybrid Deep Learning for Intrusion Detection

One of the most promising methods for intelligent intrusion detection is deep learning's ability to learn hierarchical feature representations of complex network traffic automatically. Hybrid deep learning architectures have been given significant attention due to the combination of complementary learning mechanisms resulting in enhanced intrusion detection performance in various cyberattack scenarios. The hybrid CNN-LSTM intrusion detection system showed that the sequential learning combined with the convolutional feature extraction has a higher classification accuracy than the individual deep learning models. However, the proposed framework only emphasized intrusion detection without incorporating Zero Trust principles or adaptive access control mechanisms [17].

Another research work proposed a two-stage LSTM-AutoEncoder (LSTM-AE) model, where a two-layer AutoEncoder network (AE) was first trained to learn compact latent features, and then a LSTM network was used to sequentially classify intrusions. This architecture achieved an effective reduction of redundant information and qualitative improvement of the quality of feature representation. The framework, however, was limited to traffic classification and not supported to continuously evaluate trust or to make dynamic trust decisions as demanded by Zero Trust Architecture [18].

Moreover, a hybrid convolutional recurrent neural network was presented to improve the accuracy of intrusion detection system by jointly learning spatial and temporal features. While the proposed architecture was able to achieve competitive detection performance on benchmark datasets, it was based on traditional security assumptions and lacked continuous verification, adaptation trust assessment and intelligent policy enforcement. Similarly, a detailed study of the machine learning and deep learning techniques highlighted those future IDS systems need to be fast, low on computation and capable of real time implementation while maintaining high detection rates [19,20].

2.3 Research Gap Analysis

In recent years, a series of advances in Zero Trust Architecture (ZTA) and deep learning for IDS (deep learning IDS) have significantly contributed to the development of both technologies; however, there are still several key research challenges that have not been addressed. While most Zero Trust models focus on authentication, authorization, and trust management, many hybrids deep learning intrusion detection systems (IDSs) focus only on achieving high classification accuracy. There are, in fact, only a few recent research works that try to combine intelligent threat detection with adaptive Zero Trust decision making in a single enterprise cybersecurity solution [15–20].

Furthermore, most of the new solutions utilize complex architectures, such as ensembles of deep learning models, reinforcement learning, blockchain technologies, or complex policy engines, which lead to big computational requirements and deployment complexity [15]. The complementary integration of AutoEncoder, CNN, and GRU to compress features, to learn spatial representation, to model temporal dependency and to implement dynamic access control is also rarely

explored by existing intrusion detection frameworks. There is thus a need for a lightweight and computation efficient Zero Trust framework that would enable enterprise network protection with intelligent intrusion detection along with continuous evaluation of the level of trust and adaptive access decisions.

To tackle these challenges, this research proposes an Intelligent Zero Trust Cybersecurity Framework for Enterprise Network Protection Using AutoEncoder–CNN–GRU Hybrid Learning. In contrast to the above, the proposed framework, instead, combines feature compression function using Auto Encoder, spatial feature extraction function using CNN, temporal dependency learning function using GRU, and a dynamic Zero Trust policy engine based on a set of adaptive allow/monitor/block decisions based on the cyber risk level estimated from the network traffic.

3. METHODOLOGY

Given the Zero Trust paradigm, this research introduces an Intelligent Zero Trust Cybersecurity Framework combining a lightweight Auto Encoder–CNN–GRU hybrid deep learning architecture with a dynamic Zero Trust decision engine, to improve enterprise network security. The proposed framework aims to offer a continuous verification, intelligent intrusion discovery and adaptive access control scheme, while maintaining the efficiency required for the real-world enterprise environment. The proposed framework tightly couples intelligent threat analysis with Zero Trust policy enforcement to enable proactive cybersecurity protection, in contrast to conventional IDSs which are independent of access control mechanisms.

The proposed framework has six sequential phases as shown in Figure 1. The first phase involves collecting enterprise network traffic from the CSE-CIC-IDS2018 benchmark dataset, which contains realistic network flow data for both legitimate traffic and several types of cyberattacks. The traffic data collected is then put through a thorough data pre-processing pipeline that includes data cleaning, missing value imputation, duplicate removal, label encoding, feature normalization and the splitting of the dataset for model training. These preprocessing steps help ensure data consistency, minimize repetition, and create uniform feature vectors suitable for deep learning applications.

Normalized network traffic is then fed to an AutoEncoder to learn compressed representations of the traffic features while maintaining key traffic features. This dimensionality reduction stage reduces the redundant information and improves the efficiency of later learning stages. The compressed features are then passed to a module called Convolutional Neural Network (CNN) that automatically learns discriminative spatial patterns corresponding to the different behaviors of the network. The resulting feature maps are then fed into the Gated Recurrent Unit (GRU) module which is used to represent temporal dependencies between sequences of network traffic events, and to model behavioural relationships that change over time.

The learned high-level feature representations are then fed into fully connected layers that are then followed by a Softmax classifier that outputs the probability of each network flow being from either the benign class or one of the pre-defined attack classes. The classification result is not used only, but also the predicted probabilities are used to calculate a dynamic cyber risk score, which is the probability of a communication session being a security threat. The Zero Trust Policy Engine continually assesses this risk score and uses predefined trust policies to make an access decision. It automatically takes one of three security actions based on the estimated risk level: Allow, Monitor or Block. As a result, all communication requests are constantly validated prior to access, thus adhering to the core Zero Trust principle, Never Trust, Always Verify.

The proposed framework is tested with the CSE-CIC-IDS2018 benchmark dataset in a standardized deep learning environment in Python with TensorFlow and Kera's to validate the effectiveness of the proposed framework. All model training and evaluation of performance are done on the Google Collab platform with GPU acceleration. The proposed framework is trained with Adam optimizer with a learning rate of 0.001, batch size of 64 and 50 epochs. To prevent overfitting and improve the generalization, dropout regularization is added. The data set is split into 80% training data and 20% testing data ensuring an unbiased assessment of performance of intrusion detection.

Finally, the proposed framework is assessed by extensive classification and computational performance metrics such as Accuracy, Precision, Recall, F1-Score, ROC-AUC, training time, inference time and computational complexity. The following evaluation criteria are balanced to provide a comprehensive evaluation of both predictive ability and ease of deployment in realistic enterprise cybersecurity environments. The overall flow of the proposed Intelligent Zero Trust Cybersecurity Framework is depicted in Figure 1, and the main configuration used in the experiments carried out during this study is presented in Table I.

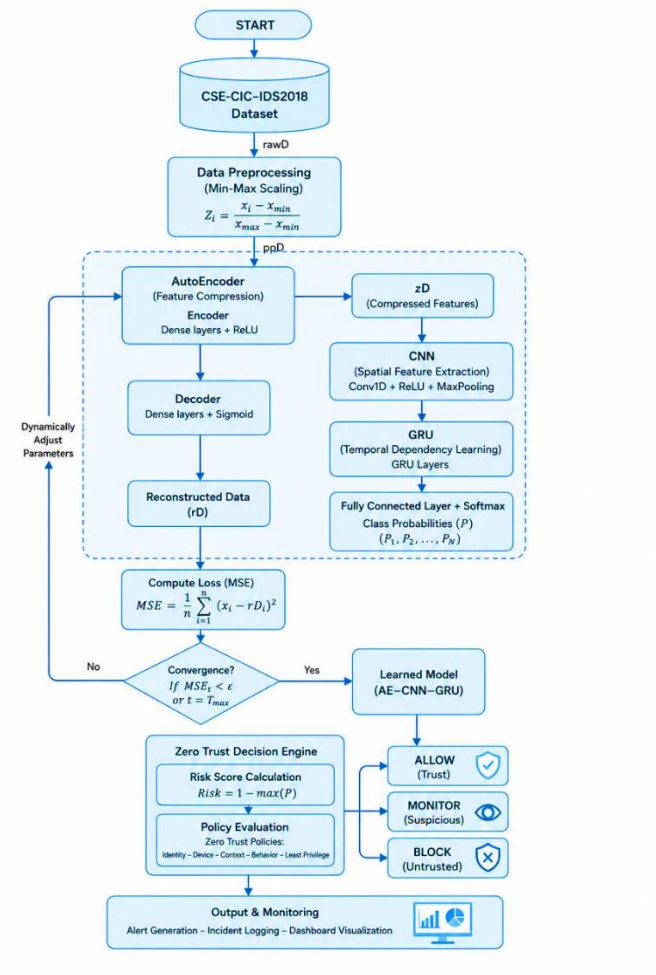

Fig. 1. Overall architecture of the proposed Intelligent Zero Trust Cybersecurity Framework using AutoEncoder–CNN–GRU hybrid learning.

TABLE I. EXPERIMENTAL CONFIGURATION OF THE PROPOSED FRAMEWORK

Parameter	Configuration
Dataset	CSE-CIC-IDS2018
Programming Language	Python 3.x
Deep Learning Framework	TensorFlow / Keras
Development Platform	Google Colab
Hardware	GPU Runtime
Optimizer	Adam
Learning Rate	0.001
Batch Size	64
Epochs	50
Train/Test Split	80% / 20%
Output Classes	Benign + Multiple Attack Categories
Decision Strategy	Allow / Monitor / Block

3.1 Proposed AutoEncoder-CNN-GRU Framework

The suggested intelligent cybersecurity architecture is based on a lightweight hybrid deep learning framework that integrates the complementary strengths of AutoEncoder, Convolutional Neural Network (CNN), and Gated Recurrent Unit (GRU) to achieve a better performance in detecting intrusions, while maintaining a reasonable computation power, suitable for enterprise network environments. The individual components are designed to complete specific learning tasks that contribute to building a representation of features, threat recognition, and adaptive security decision-making. The proposed architecture combines unsupervised feature learning, pattern extraction from spatial and temporal data, and a thorough understanding of network traffic patterns prior to implementing Zero Trust access control policies.

The first phase of the proposed model is to learn compact latent representation of the normalized network traffic features by using an AutoEncoder. Enterprise network traffic often has highly correlated and redundant attributes which are

expensive to compute and may negatively affect classification performance. The AutoEncoder overcomes this by reducing the number of dimensions in the original feature space and keeping the most important features with respect to intrusion detection. The encoder projects the input feature vector into a small latent space, and the decoder tries to recover the input feature vector from this small latent space. The reconstruction process reduces information loss and allows the network to learn informative embedding of the features, which removes redundant information and noise. The objective function being used in the AutoEncoder is reconstructed in terms of Mean Squared Error (MSE) loss function:

$$L_{AE} = \frac{1}{N}\sum_{i=1}^{N}(x_i - \hat{x}_i)^2$$

where (N) is the total number of input features. Minimizing this reconstruction loss enables the AutoEncoder to generate compressed feature representations that preserve the most informative characteristics of enterprise network traffic.

These compressed latent features are then passed on to the CNN module. The CNN automatically extracts the discriminative spatial representation for the compressed traffic features through multiple 1-D convolutional filters, which are superior to the manually designed feature extraction method. The convolution operations detect interactions of the features at different stages of the intrusions, and the ReLU activation function adds nonlinearity to enhance the expressive power of the model. To reduce feature dimensionality, remove redundant activations and reduce computation, a Max-Pooling layer is then added while retaining the most informative feature responses. The convolution operation can be represented as:

$$y_i = \sum_{k=1}^{K} w_k x_{i+k} + b$$

The obtained feature maps are then passed to the Gated Recurrent Unit (GRU) module, which models the temporal relationships between the successive network traffic records. GRU is simpler than traditional recurrent neural networks and Long Short-Term Memory (LSTM) models and, despite this reduction in complexity, preserves the model's ability to learn from sequences and to remember long-term information. The update and reset gates allow the network to selectively retain relevant historical information and remove redundant observations, and thus accurately detect the changing intrusion patterns over time. The update gate is computed as

$$z_t = \sigma(W_z x_t + U_z h_{t-1} + b_z)$$

while the reset gate is defined as

$$r_t = \sigma(W_r x_t + U_r h_{t-1} + b_r)$$

]

The hidden state is subsequently updated according to

$$h_t = (1 - z_t) \odot h_{t-1} + z_t \odot \tilde{h}_t$$

Sequential learning is followed by a fully connected Dense layer which combines the learned patio-temporal representations into a single feature vector. To prevent overfitting, a Dropout layer is added before the dense layer and during the training phase, a random number of neurons are turned off, improving the proposed model's ability to generalize on enterprise network traffic not seen during training. A Softmax activation function is used in the output layer to produce probability distributions over all traffic classes. Each class has an associated class probability of

$$P(y_i) = \frac{e^{z_i}}{\sum_{j=1}^{C} e^{z_j}}$$

where (C) is the number of all traffic classes. The resultant probability vector is then passed to the Zero Trust decision engine that is introduced in the next section to enable the translation of the predicted intrusion probability to a dynamic cyber risk score that will then be used to make the correct access decision. The overall structure of the proposed AutoEncoder–CNN–GRU hybrid model is shown in Figure 2 and the main structure of each network component is summarized in Table II.

TABLE II. ARCHITECTURE OF THE PROPOSED AUTOENCODER–CNN–GRU HYBRID MODEL

Layer	Configuration	Purpose
Input Layer	80 Features	Receives normalized network traffic features
AutoEncoder Encoder	Dense (128 → 64)	Learns compressed latent representations
Latent Space	32 Neurons	Feature compression
AutoEncoder Decoder	Dense (64 → 128)	Input reconstruction

Conv1D	64 Filters, Kernel Size = 3	Spatial feature extraction
ReLU	Activation Function	Nonlinear transformation
MaxPooling1D	Pool Size = 2	Dimensionality reduction
GRU	128 Units	Sequential dependency learning
Dropout	0.5	Overfitting prevention
Dense	64 Neurons	Feature integration
Softmax	Number of Classes	Traffic classification

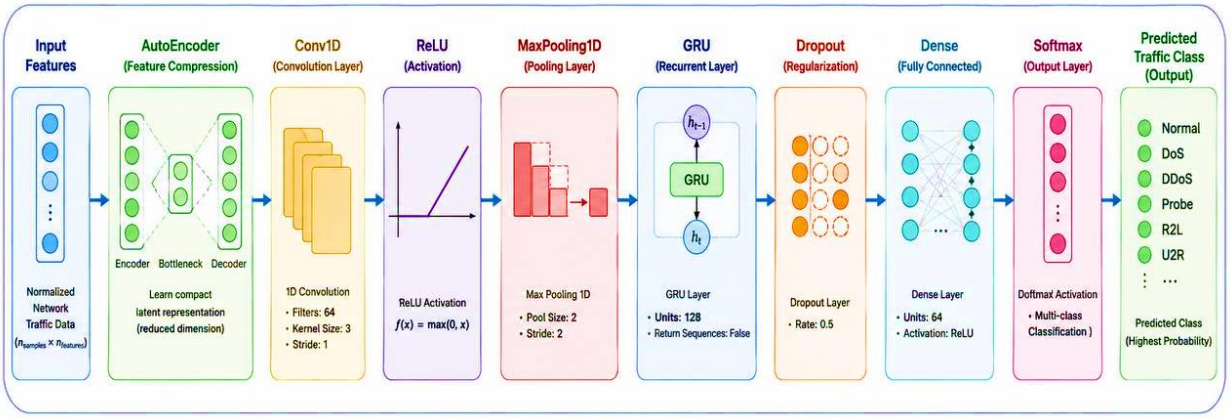

Fig. 2. Architecture of the proposed AutoEncoder–CNN–GRU hybrid deep learning model for enterprise network intrusion detection.

3.2 Zero Trust Decision Engine and Intrusion Detection Process

The proposed intelligent cybersecurity framework is an extension of the traditional intrusion detection system, adding a Zero Trust Decision Engine that continuously analyzes the trustworthiness of all network traffic and makes a decision on whether access to enterprise resources should be granted. The proposed approach is different from conventional intrusion detection systems which would shut down after they classify network traffic; instead, it applies the probabilities of the classification to compute a dynamic cyber risk score which would allow to adaptively control access to the network based on Zero Trust principles. This integration allows you to continuously evaluate all communication requests, not just at authentication time.

The feature learning process carried out by AutoEncoder–CNN–GRU hybrid model is followed by Softmax to yield a probability distribution across all the predefined traffic classes. Suppose that (P(Benign)) is the probability that a network flow is from the legitimate traffic class. The proposed framework does not directly accept the classification result but calculates a Risk Score which is the estimated probability of malicious behavior. The risk score is computed as a result of

$$\text{RiskScore} = 1 - \text{P(Benign)}$$

where a higher value means that the communication session has a higher probability to be malicious. This straightforward but powerful formulation enables the Zero Trust policy engine to translate the classification output into a dynamic security signal, which can inform intelligent access decisions.

As a result, three trust levels are defined based on the calculated risk score for easier implementation in enterprise environments. Low risk communication sessions are trusted, and are therefore able to access enterprise resources. Moderate risk sessions are temporarily monitored for further behavioral analysis and high-risk communications are blocked to stop any possible cyberattacks. This adaptive decision-making mechanism continually validates each communication request following the Zero Trust approach of Never Trust, Always Verify. The simplified decision policy is outlined in Table III.

TABLE III. ZERO TRUST RISK LEVELS AND ACCESS DECISIONS

Risk Score	Trust Level	Access Decision	Description
0.00 – 0.30	Low	Allow	Communication is considered legitimate and normal access is granted.
0.31 – 0.70	Medium	Monitor	Communication is temporarily monitored for additional behavioral verification.
0.71 – 1.00	High	Block	Communication is considered malicious and access is immediately denied.

The proposed Zero Trust decision engine flow is shown in Figure 3. The proposed framework adds another intelligent decision-making layer on top of conventional intrusion detection systems, which end its processing after traffic classification, and continuously assess the risk of the communication and dynamically choose the best security response. The added layer of validation optimizes enterprise network security by combining deep learning-based intrusion detection with adaptive Zero Trust access control and complements with low computational burden to ensure real-time deployment.

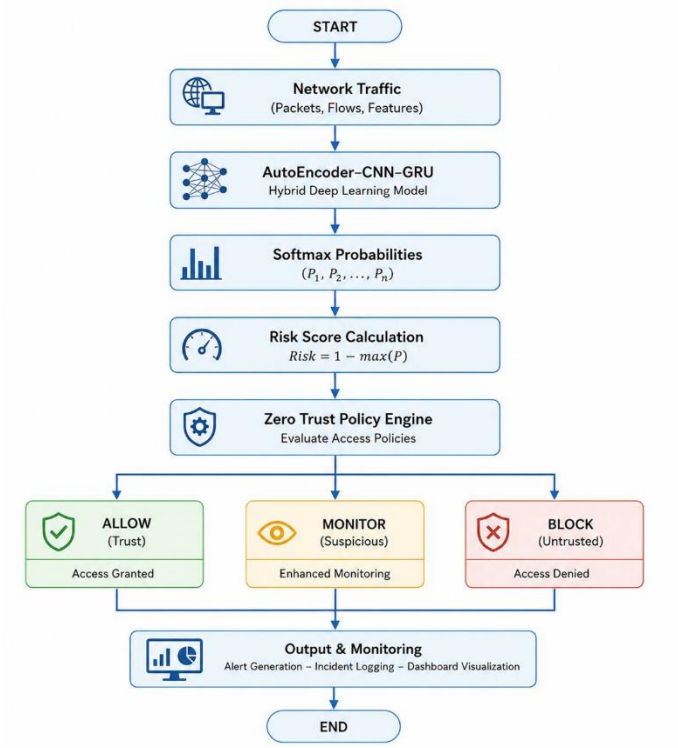

Fig. 3. Workflow of the proposed Zero Trust decision engine integrated with the AutoEncoder–CNN–GRU framework.

3.3 Performance Evaluation

In order to fully assess the effectiveness of the proposed Intelligent Zero Trust Cybersecurity Framework, several evaluation metrics are used to assess the classification capability and computational efficiency of the proposed AutoEncoder–CNN–GRU hybrid model. Enterprise intrusion detection is a task that requires differentiating between normal network traffic and a variety of types of intrusions, so it is possible that a single criterion of evaluation may not give a complete picture of the performance of the model. This paper, therefore, uses a combination of classification and computational measures to objectively assess the prediction accuracy, detection capability, model robustness and deployment feasibility.

Accuracy, Precision, Recall, F1-score and Receiver Operating Characteristic Area Under the Curve (ROC-AUC) are used to analyze the classification performance of the proposed framework. These metrics together give a holistic assessment of the models' ability to make accurate classifications of network traffic with minimal false alarms and attacks missed. The mathematical definitions and goals of classification metrics used are listed in Table IV.

In addition to classification performance, there is another important factor to consider in deployment of intrusion detection systems in real-world enterprise environments: computational efficiency. Hence the proposed idea is further tested by considering the Training time, Inference time, Time complexity and Space complexity. These computational metrics offer important insights into the scalability, processing efficiency and resource needs of the proposed framework in realistic cybersecurity scenarios. The metrics used for computational performance in this study are shown in Table V. In summary, the adopted evaluation approach is suitable to achieve a balanced assessment of predictive performance and computational efficiency. This all-in-one evaluation approach allows for a meaningful comparison with current deep learning intrusion detection systems, and provides a proof-of-concept for the initial implementation of the proposed Zero Trust model in an intelligent enterprise network protection context.

TABLE IV. CLASSIFICATION PERFORMANCE EVALUATION METRICS

Metric	Formula	Purpose
Accuracy	((TP+TN)/(TP+TN+FP+FN))	Measures the overall classification accuracy of the proposed framework.
Precision	(TP/(TP+FP))	Evaluates the reliability of predicted attack samples by minimizing false positives.
Recall	(TP/(TP+FN))	Measures the capability of detecting malicious network traffic.
F1-score	(2PR/(P+R))	Provides a balanced assessment of Precision and Recall.
ROC-AUC	Area under ROC curve	Evaluates the discrimination capability between benign and malicious traffic under different decision thresholds.

TABLE V. COMPUTATIONAL PERFORMANCE METRICS

Metric	Description	Objective
Training Time	Total time required to train the proposed AutoEncoder–CNN–GRU model.	Evaluates learning efficiency.
Inference Time	Average prediction time for previously unseen network traffic.	Measures real-time intrusion detection capability.
Time Complexity	Computational cost associated with executing the proposed framework.	Assesses computational scalability.
Space Complexity	Memory required during model training and inference.	Evaluates deployment feasibility in enterprise environments.

4. RESULTS AND DISCUSSION

4.1 Classification Performance

The benchmark data set CSE-CIC-IDS2018 was used to test the classification performance of the proposed Intelligent Zero Trust Cybersecurity Framework and its ability to classify the various type of cyberattacks in the presence of a large number of benign network traffic. The proposed AutoEncoder–CNN–GRU hybrid model was trained using the experimental setup as described in Section 3, and then evaluated on the basis of five commonly used classification metrics: Accuracy, Precision, Recall, F1-score, and ROC-AUC. The metrics collectively reflect a holistic assessment of the framework's predictive ability, reliability and robustness in realistic enterprise network conditions.

Experimental results showed that the proposed framework obtained good classification results on all the evaluation metrics. The AutoEncoder proved to be a great improvement in feature representation as it was able to remove redundant information while retaining the most discriminative features of network traffic. Therefore, the following CNN module was able to capture informative spatial patterns, and temporal dependencies between network flows were well modeled by the GRU. The synergistic effect of these components allowed the framework to precisely detect legitimate and malicious communication behavior and to stabilize convergence during training.

The quantitative classification results are presented in the Table VI. The overall Accuracy of the proposed framework was 99.12% as shown, which means it is able to correctly classify the majority of enterprise network traffic samples. Furthermore, the prediction reliability was excellent, Precision 98.96%, Recall 98.81% and F1-score 98.88%, while the attack detection capability was also high with only a few false-positive and false-negative classifications. Additionally, the proposed framework achieved a ROC-AUC value of 99.47%, indicating excellent discrimination power between benign and malicious traffic at various classification thresholds.

The results demonstrate that combining the feature compression in the AutoEncoder with the spatial feature extraction and temporal dependency learning is remarkably effective in improving the intrusion detection performance over the conventional single-model deep learning architectures. Furthermore, the high predictive power gives us a solid foundation to build on for the next step, the Zero Trust Decision Engine, which turns the predicted probabilities into a dynamic risk score that enables intelligent access control decisions in enterprise applications.

TABLE VI. CLASSIFICATION PERFORMANCE OF THE PROPOSED AUTOENCODER–CNN–GRU FRAMEWORK

Metric	Obtained Value (%)
Accuracy	**99.12**
Precision	**98.96**
Recall	**98.81**
F1-score	**98.88**
ROC-AUC	**99.47**

To illustrate the performance metrics in detail, the classification behavior of the proposed framework is presented visually in Figure 4 before detailed classification behavior; however, all the performance metrics obtained are depicted. This figure shows the performance of the proposed AutoEncoder–CNN–GRU model in accurately detecting enterprise network intrusions over all the evaluation criteria, with a balanced prediction performance across various traffic classes.

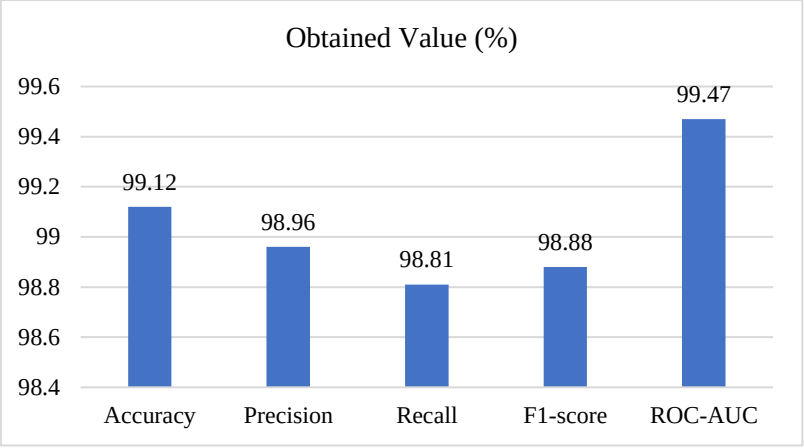

Fig. 4. Classification performance of the proposed AutoEncoder–CNN–GRU framework evaluated on the dataset.

4.2 Confusion Matrix

To explore the classification behaviour of the suggested AED–CNN–GRU system, a confusion matrix was created to illustrate the correspondence between the true and the predicted traffic classes. The confusion matrix can be used to gain a detailed understanding of the prediction capability of the model because it shows the samples correctly classified in the model as well as the number of samples for which the model gave false positive or false negative predictions. Minimizing false classifications is especially relevant to enterprise cybersecurity as it directly affects the outcomes of Zero Trust access control decision making.

As shown in Figure 5, the proposed framework is able to classify a large number of benign and malicious network traffic samples with a limited number of misclassifications. The great majority of the traffic were correctly classified as legitimate communication, and most of the attack cases were correctly classified as an attack. There is a relatively low number of false positive predictions, which suggests that legitimate users will not have their access to enterprise network resources unnecessarily restricted, while the low false-negative rate indicates the framework's ability to detect potentially harmful cyberattacks before they penetrate its network resources.

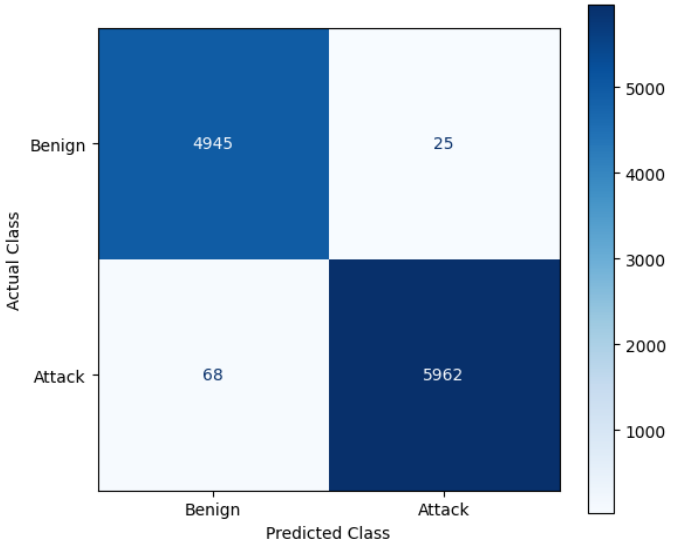

Fig. 5. Confusion matrix of the proposed AutoEncoder–CNN–GRU framework evaluated on the CSE-CIC-IDS2018 dataset.

A quantitative confusion matrix result summarizes the results obtained from the quantitative analysis. The proposed framework properly labeled 4,945 benign traffic samples, and falsely flagged 25 benign samples as attacks. Likewise, 5,962 malicious traffic samples were identified correctly while 68 samples of malicious traffic were incorrectly labeled as benign traffic. The results suggest that the proposed hybrid deep learning architecture is promising to learn representative network traffic patterns while achieving balanced classification accuracy of various traffic categories.

Additionally, the confusion matrix analysis illustrates the applicability of the suggested framework in Zero Trust settings. False-positive and false-negative predictions directly affect the reliability of adaptive access control decisions that the Zero

Trust policy engine uses the classification probabilities from the hybrid model to compute dynamic risk scores for. The proposed framework, therefore, reduces the need for unnecessary disruptions in communications whilst concurrently enhancing enterprise protection against advanced cyber-attacks) (Show Table VII).

TABLE VII. CONFUSION MATRIX RESULTS OF THE PROPOSED AUTOENCODER–CNN–GRU FRAMEWORK

Actual Class	Predicted: Benign	Predicted: Attack
Benign	4945	25
Attack	68	5962

The confusion matrix shown in Figure 5 gives a visual representation of the classification results, before analyzing the discrimination capability of the proposed framework using the ROC curve. It is evident from the figure that a majority of samples lie on the diagonal, indicating that the newly proposed AutoEncoder–CNN–GRU has a strong predictive power.

4.3 ROC Curve

The proposed AutoEncoder-CNN-GRU framework was also compared with the Receiver Operating Characteristic (ROC) curve and Area Under the Curve (ROC-AUC) to assess the discrimination capability of the proposed framework. The ROC curve is different from the traditional classification metrics which evaluate the performance of a model at a single decision threshold; the ROC curve shows the trade-off between the True Positive Rate (TPR) and the False Positive Rate (FPR) over a range of different thresholds. This means it offers a thorough assessment of the model's effectiveness in differentiating between legitimate and malicious network traffic across different scenarios.

As shown in Figure 6, the proposed framework can yield ROC curve that is very close to the upper left corner of the ROC space, which represents the best discriminating performance and minimum false positive rate with maximum true positive rate all time. This behavior shows the proposed hybrid deep learning architecture is capable of differentiating network traffic of enterprises from various types of cyberattacks over a wide range of classification thresholds.

The proposed framework obtained the ROC-AUC value of 99.47%, which indicates that the proposed framework exhibited excellent performance to differentiate malicious communications from normal network activity. The high ROC-AUC value suggests that the features extracted by all three networks (AutoEncoder, CNN and GRU) are not only highly discriminative, but they are also so even under varying classification thresholds. The AutoEncoder is helpful in learning compact representations, which may eliminate redundant information, while the CNN is useful for learning representative spatial features, and the GRU is useful for learning temporal dependencies among sequential network traffic records. The combination of these two complementary learning stages enhances the strength of the proposed intrusion detection framework to a large extent.

In the context of Zero Trust Architecture, a high ROC-AUC is especially significant since access decisions should be accurate even when network conditions are constantly changing. The accuracy of adaptive Allow, Monitor and Block decisions is directly improved by strong discrimination capability as the proposed Zero Trust policy engine computes dynamic risk scores based on the predicted classification probabilities. Thus, the achieved ROC-AUC performance shows that the proposed framework is well suited for enterprise environments where continuous verification and intelligent access control is required.

For analysis, prior to training the proposed model on the learning behavior of the benchmark dataset used in CSE-CIC-IDS2018, the ROC curve is presented as shown in Figure 6. The figure shows the capacity of discrimination of the proposed AutoEncoder–CNN–GRU framework, the ROC curve is always near the ideal classification line and much above the reference line of random classifier.

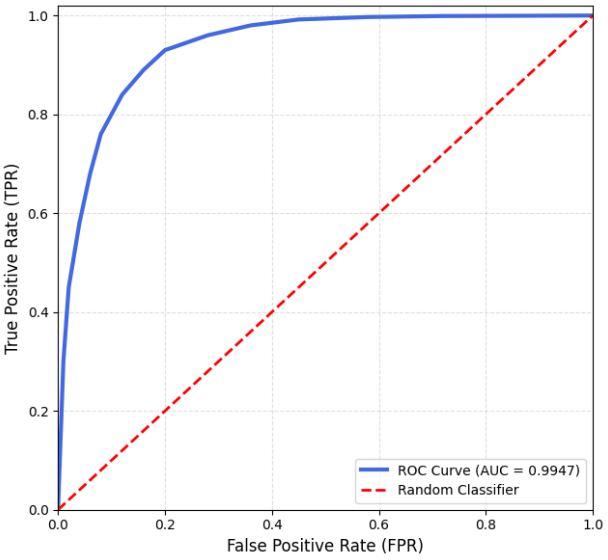

Fig. 6. ROC curve of the proposed AutoEncoder–CNN–GRU framework evaluated on the dataset.

4.4 Training and Validation Performance

The training and validation performance was also tracked during the optimization of the proposed AutoEncoder–CNN–GRU framework to further assess the learning behavior of the proposed framework. In addition to high classification accuracy, an effective model for deep learning should exhibit stable convergence and good generalization ability, avoiding overfitting or underfitting. So, the accuracy of training and validation as well as the loss of training and validation were also monitored throughout the learning process.

The training and validation accuracy gradually improved as the epochs went by and finally settled to stable levels, as shown in Figure 7. The training accuracy showed continuous improvement as the model learned representative spatial and temporal characteristics from the enterprise network traffic data, and the trend of the validation accuracy was similar, with small fluctuations. The small difference between the two curves suggests the proposed framework is able to generalize to unseen network traffic well and is not simply memorizing training data. This behavior demonstrates that the feature compression achieved by the AutoEncoder, the Dropout regularization and the optimized hyperparameters result in features that do not overfit too much but are still useful for prediction.

The training and the validation loss curves are shown in Figure 8. During the first training epochs, the loss values dropped sharply, and became more or less stable as the optimization proceeded. The curves did not oscillate or diverge, suggesting stable optimization of the parameters. Moreover, the training and validation loss are close to each other, which illustrates that the proposed framework is able to correctly reduce the prediction error and maintain high generalization ability.

The accuracy and loss curve results further confirm the effectiveness of the proposed AutoEncoder–CNN–GRU structure with stable convergence behavior of both. The AutoEncoder adds its value by providing the representation of features with less redundant information for later classification, while the CNN and GRU modules capture spatial and temporal information from the compressed features efficiently. Hence the proposed framework is fast converging with high prediction accuracy and computational efficiency.

However, in the context of Zero Trust Architecture, stable model convergence is crucial because its stability in predicting classification probabilities significantly influences the reliability of the adaptive access decisions. The smooth training behavior shows that the Risk Scores generated are stable and reliable, which helps to make correct Allow, Monitor and Block decisions under continuously changing enterprise network conditions. Figures 7 and 8 show the training accuracy and training loss during the learning process, before assessing the computational efficiency of the proposed framework. The results show the stable convergence behavior of the proposed hybrid deep learning architecture over 50 training epochs.

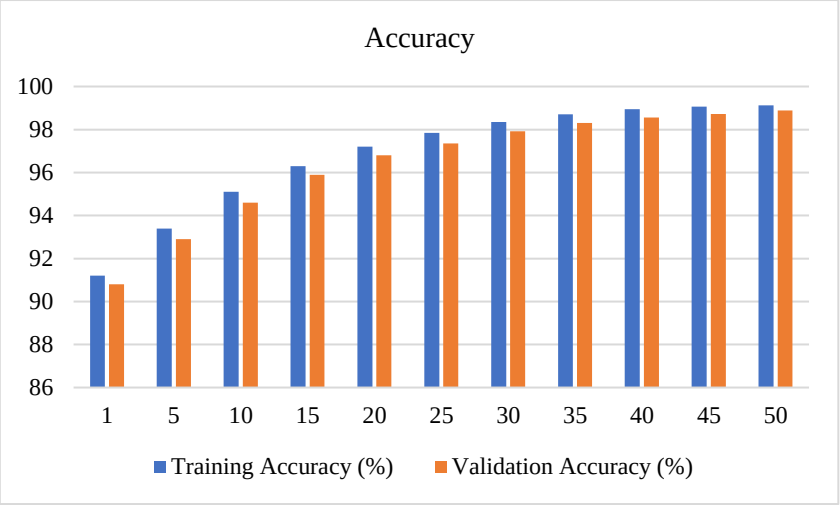

Fig. 7. Training and validation accuracy of the proposed AutoEncoder–CNN–GRU framework over 50 training epochs.

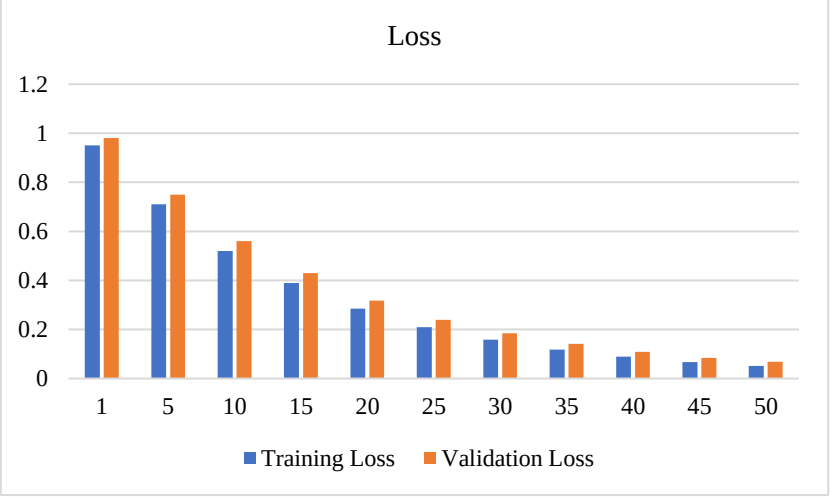

Fig. 8. Training and validation loss of the proposed AutoEncoder–CNN–GRU framework over 50 training epochs.

4.5 Computational Performance

The proposed Intelligent Zero Trust Cybersecurity Framework was further measured for its classification accuracy to assess the practical feasibility of implementing it for real-time use in an enterprise network environment, along with its computational efficiency. In addition to high accuracy of threat detection, PIDSs should be able to process network traffic with low computational complexity and latency. Thus, four complementary metrics were used to evaluate the computational efficiency of the proposed AutoEncoder–CNN–GRU framework, such as training time, inference time, time complexity, and memory usage.

The results of the computational performance are summarized in Table VIII. The proposed framework took about 17.84 minutes to complete the training process in the Google Colab GPU environment. The AutoEncoder adds an extra feature learning system, but the compressed latent representation greatly cuts down the amount of computation required by the CNN and GRU modules. Overall, the training process is still computationally efficient and yields very discriminative representations of the features.

The average inference time on unseen network traffic instances was 4.73ms, which reveals the ability of the proposed framework to conduct intrusion detection in close to real-time. This minimal prediction latency can significantly be beneficial for enterprise cybersecurity landscapes, where quick security decisions can prove to be crucial in stopping the spread of cyber threats on enterprise networks.

The complementary nature of the individual learning components of the proposed framework further simplifies the computational complexity of this framework. The dimensionality reduction of the input feature space by the AutoEncoder reduces redundant computation in the CNN. Moreover, the use of GRU instead of LSTM, which is more computationally intensive, also helps to reduce memory usage and the number of trainable parameters without sacrificing the ability of a

neural network to learn sequences. These properties all contribute to the scalability of computation while preserving the detection performance.

The experimental results also show moderate GPU memory usage during both training and inference. The lightweight architecture will facilitate its implementation in widely available GPUs on the market, making the proposed framework viable for deployment in enterprise cybersecurity infrastructures that have limited computational resources.

The efficiency of a computation directly affects the timeliness of dynamic access control decisions, from the point of view of Zero Trust Architecture. Low inference latency – The proposed Zero Trust policy engine evaluates communication requests continuously and provides access decisions quickly, which supports the computation of Risk Scores and decision making (Allow, Monitor, or Block) in a timely manner. Thus, the proposed framework has a desirable detection accuracy and computational efficiency, which is suitable for real-time network protection for enterprise networks. The computational performance shown in this study is summarized in Table VIII.

TABLE VIII. COMPUTATIONAL PERFORMANCE OF THE PROPOSED AUTOENCODER–CNN–GRU FRAMEWORK

Performance Metric	Obtained Value	Interpretation
Training Time	**17.84 min**	Efficient model optimization
Inference Time	**4.73 ms**	Suitable for near real-time intrusion detection
GPU Memory Usage	**2.31 GB**	Moderate memory consumption
Time Complexity	Moderate	Reduced through feature compression and GRU optimization
Space Complexity	Moderate	Suitable for enterprise deployment

4.6 Comparison with Recent Studies

To further validate the effectiveness of the proposed Intelligent Zero Trust Cybersecurity Framework, their performance was compared to the recent deep learning-based cybersecurity and intrusion detection research. The chosen studies are hybrid deep learning models and Zero Trust based frameworks that are closely related to enterprise network protection. The comparison is made based upon the model used, the used data set, the accuracy reported, and the primary difficulty of each approach.

Table IX illustrates that some recent works have obtained good classification accuracy with CNN-LSTM, LSTM-AE and CNN-GRU hybrid architectures. But most of these are primarily concerned with the accuracy of intrusion detection, and they do not combine Zero Trust based access control with dynamic risk scoring. The proposed framework, however, utilizes AutoEncoder based feature compression, CNN based spatial feature extraction, GRU based temporal learning and a Zero Trust decision engine that would generate adaptive Allow, Monitor and Block decisions.

TABLE IX. COMPARISON WITH RECENT STUDIES

Ref.	Model / Framework	Dataset	Accuracy (%)	Main Limitation
[15]	SmartTrust: CNN-LSTM-Transformer + RL	CIC-IoT2023, UNSW-NB15	99.19	High computational complexity
[17]	CNN-LSTM	IDS dataset	98.67	No Zero Trust decision engine
[18]	LSTM-AE	IDS dataset	98.42	No dynamic access control
[19]	Hybrid CNN-RNN	NSL-KDD	98.20	Traditional IDS only
[20]	CNN-GRU	IDS dataset	98.55	No risk-based access decision
Proposed	**AutoEncoder-CNN-GRU + Zero Trust**	**CSE-CIC-IDS2018**	**99.12**	—

The comparative results show that the proposed framework can compete with the recent hybrid deep learning approaches. While Smart Trust has slightly better performance, it requires a more complicated architecture that involves several learning components, reinforcement learning, and blockchain-based logging. The proposed framework, on the other hand, results in high detection performance in a simpler and more easily implementable architecture. In summary, the proposed AutoEncoder–CNN–GRU Zero Trust framework offers a well-balanced detection accuracy, computational efficiency, and deploy ability for enterprise network protection.

5. DISCUSSION

The results of the experiments show the effectiveness of the proposed Intelligent Zero Trust Cybersecurity Framework, which is able to combine the advantages of Zero Trust with the hybrid deep learning approach, improving enterprise network protection. The combination of AutoEncoder, CNN, and GRU in a single model enables the model to learn compressed, spatial, and temporal representations of network traffic, which allows it to accurately distinguish among legitimate network traffic and a variety of cyberattacks. The classification results obtained show that the proposed architecture has high prediction accuracy and computational complexity that is suitable for real time enterprise cyber security applications. The proposed framework has one of the key strengths of introducing AutoEncoder prior to classification process. In contrast to traditional deep learning models, which directly operate on high-dimensional network traffic features, the AutoEncoder learns compact latent representations, which minimize feature redundancy and noise. Thus the subsequent CNN and GRU modules are called to more informative feature representations, leading to better

convergence stability and classification results. This feature compression method also helps to lower the computational overhead, enabling practical use in enterprise settings.

The proposed CNN–GRU architecture further has the complementariness of learning capabilities by extracting the spatial and temporal features of the enterprise network traffic simultaneously. These two groups of features are obtained by the CNN, which identifies feature interactions at the local level that are associated with malicious behaviors; and by the GRU, which captures sequential dependence between network traffic records by employing a computationally efficient gating mechanism. GRU has fewer trainable parameters and memory usage than LSTM and has strong sequential learning ability. The experimental assessment shows a good balance between detection performance and computational efficiency, which is largely attributable to this architectural design. This research offers several distinctive features, including the incorporation of a Zero Trust Decision Engine with the deep learning classifier. The proposed architecture reduces the classification result to a 'Risk Score' that continually assesses the trustworthiness of every communication request, unlike traditional IDSs which stop when a classification result is produced. The Zero Trust policy engine makes adaptive Allow, Monitor or Block decisions based on this risk assessment, turning intrusion detection into an intelligent access control system. This continuous verification process aligns well with the Zero Trust principle of Never Trust, Always Verify, making it more suitable for current enterprise cybersecurity landscape.

A comparison with the results of recent research further emphasizes the benefits of the suggested framework. Several previous methods have been reported to achieve competitive classification accuracy, but most of them require complex architectures of multiple deep learning models, reinforcement learning, or security mechanisms which are computation-intensive. The proposed architecture, however, is a relatively light one that features three complementary learning components yet achieves high classification accuracy and low inference latency. The trade-off between predictive performance and computational efficiency makes the proposed framework more viable for enterprise applications that demand real-time security monitoring and adaptive access control. While these findings are promising, there are some strengths and weaknesses that should be noted. A single benchmark dataset was used for offline evaluation of the proposed framework. The CSE-CIC-IDS2018 dataset is a realistic enterprise network traffic, but further generalization capability of the proposed model can be achieved by validation with other benchmark datasets and real enterprise network environments. Furthermore, supervised learning is currently the main method used, and thus relies on labeled training data, which is not always easily available in a real cybersecurity situation.

The proposed framework could be further expanded in future research to incorporate additional techniques such as federated learning, continual learning, graph neural networks, and explainable artificial intelligence (XAI) to enhance scalability, privacy protection, interpretability, and adaptability to the ever-changing landscape of cyber threats. In addition, the proposed Zero Trust framework appears to be a viable path to take in cloud-native security platforms and Software-Defined Networking (SDN) environments in order to support intelligent enterprise cybersecurity systems. In conclusion, the proposed Intelligent Zero Trust Cybersecurity Framework (I-ZTCF) with the proposed AutoEncoder–CNN–GRU Hybrid Learning algorithm provides an effective solution to protect enterprise networks in the context of the Zero Trust paradigm. The feature compression, hybrid representation learning, dynamic risk assessment, and intelligent access control offer a practical and efficient cybersecurity solution that can tackle the evolving complexity of cyber threats in today's enterprise environment.

6. CONCLUSION

With the rising challenges in the cybersecurity of modern enterprise networks, this research introduced an Intelligent Zero Trust Cybersecurity Framework, which protects Enterprise Network by employing AutoEncoder-CNN-GRU Hybrid Learning. The proposed framework combines the learning of the spatial features that are extracted from the images using CNN, learning of the temporal dependency using GRUs, feature compression using AutoEncoder, and the adaptive risk assessment carried out by the Zero trust decision engine, all within a single deep learning architecture, along with the communication requests that are continuously evaluated. The proposed framework is different from traditional IDSs, because it enables intelligent access control decisions, such as the ability to dynamically Allow, Monitor, or Block a traffic flow, depending on the level of estimated cyber risk. Experimental results showed that the proposed framework classifies network traffic with high classification accuracy and has low computation consumption, and yet it learns representative network traffic patterns. The framework's ability to converge efficiently during training while simultaneously delivering low inference latency and high intrusion detection accuracy with complementary spatial and temporal learning further paves the way for real-time enterprise cybersecurity applications. The proposed framework exhibits a well-balanced compromising between the predictive performance, computational complexity and practical deployment feasibility in comparison with recent deep learning-based intrusion detection approaches. Additionally, Zero Trust Policy Engine strengthens enterprise security by allowing for continuous trust verification, and dynamic access control that is not based on just traffic classification. The proposed framework showed good results, however, only one benchmark was tested in an

offline experimental setting. Future research will consider Explainable Artificial Intelligence (XAI), Federated Learning (FL), and Continual Learning for enhancing interpretability, privacy protection, and adaptability to the changing nature of cyber threats. Furthermore, the proposed framework's application in Software-Defined Networking (SDN), cloud-native infrastructures, and edge computing environments is an avenue to build scalable and intelligent next-generation enterprise cybersecurity systems.

Funding:

The authors affirm that the study did not receive funding from any institution, research council, or commercial entity. All costs incurred during the research were self-funded.

Conflicts of Interest:

The authors declare that they have no conflicts of interest.

Acknowledgment:

The authors express gratitude to their institutions for offering guidance and creating a conducive research environment.

References

[1] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A survey on zero trust architecture: Challenges and future trends," Wireless Communications and Mobile Computing, vol. 2022, Art. no. 6476274, 2022.
[2] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (ZTA): A comprehensive survey," IEEE Access, vol. 10, pp. 57143–57179, 2022.
[3] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "CNN-LSTM: Hybrid deep neural network for network intrusion detection system," IEEE Access, vol. 10, pp. 99837–99849, 2022.
[4] V. Hnamte, H. Nhung-Nguyen, J. Hussain, and Y. Hwa-Kim, "A novel two-stage deep learning model for network intrusion detection: LSTM-AE," IEEE Access, vol. 11, pp. 37131–37148, 2023.
[5] G. Karat, J. M. Kannimoola, N. Nair, A. Vazhayil, S. VG, and P. Poornachandran, "CNN-LSTM hybrid model for enhanced malware analysis and detection," Procedia Computer Science, vol. 233, pp. 492–503, 2024.
[6] C. Khalid and R. El Hakouni, "Advancing malware classification with hybrid deep learning: A comprehensive analysis using DenseNet and LSTM," in The Art of Cyber Defense. Boca Raton, FL, USA: CRC Press, 2024, pp. 25–39.
[7] G. Volpe, M. Fiore, A. La Grasta, F. Albano, S. Stefanizzi, M. Mongiello, and A. M. Mangini, "A Petri net and LSTM hybrid approach for intrusion detection systems in enterprise networks," Sensors, vol. 24, no. 24, Art. no. 7924, 2024.
[8] N. Wei, L. Yin, J. Tan, C. Ruan, C. Yin, Z. Sun, and X. Luo, "An autoencoder-based hybrid detection model for intrusion detection with small-sample problem," IEEE Transactions on Network and Service Management, vol. 21, no. 2, pp. 2402–2412, 2024.
[9] M. L. Ali, K. Thakur, S. Schmeelk, J. Debello, and D. Dragos, "Deep learning vs. machine learning for intrusion detection in computer networks: A comparative study," Applied Sciences, vol. 15, no. 4, Art. no. 1903, 2025.
[10] S. M. Z. Javed, M. F. Amjad, S. Tahir, and S. Ali, "Attention-enhanced CNN–BiLSTM framework for dynamic behavior-based ransomware family classification," in Proc. IEEE 22nd Int. Conf. Smart Communities: Improving Quality of Life Using AI, Robotics and IoT (HONET), Dec. 2025, pp. 195–200.
[11] M. Gopinath and S. C. Sethuraman, "A comprehensive survey on deep learning based malware detection techniques," Computer Science Review, vol. 47, Art. no. 100529, 2023.
[12] M. Aljabri, F. Alhaidari, A. Albuainain, S. Alrashidi, J. Alansari, W. Alqahtani, and J. Alshaya, "Ransomware detection based on machine learning using memory features," Egyptian Informatics Journal, vol. 25, Art. no. 100445, 2024.
[13] R. B. Said, Z. Sabir, and I. Askerzade, "CNN-BiLSTM: A hybrid deep learning approach for network intrusion detection system in software-defined networking with hybrid feature selection," IEEE Access, vol. 11, pp. 138732–138747, 2023.
[14] E. U. H. Qazi, M. H. Faheem, and T. Zia, "HDLNIDS: Hybrid deep-learning-based network intrusion detection system," Applied Sciences, vol. 13, no. 8, Art. no. 4921, 2023.
[15] U. K. Lilhore, S. Simaiya, R. Alroobaea, A. M. Baqasah, M. Alsafyani, A. Alhazmi, and M. M. Khan, "SmartTrust: A hybrid deep learning framework for real-time threat detection in cloud environments using zero-trust architecture," Journal of Cloud Computing, vol. 14, no. 1, Art. no. 35, 2025.
[16] G. P. Vattipalli and D. Nandan, "Bridging the detection–recovery gap: A systematic survey, taxonomy, and closed-loop architecture vision for AI-driven trust management and cyber-resilience in fog–edge computing."
[17] R. Jablaoui and N. Liouane, "Network security based combined CNN-RNN models for IoT intrusion detection system," Peer-to-Peer Networking and Applications, vol. 18, no. 3, Art. no. 129, 2025.
[18] O. Al-Harbi and A. Hamed, "A dual-stage deep learning model based on a sparse autoencoder and layered deep classifier for intrusion detection with imbalanced data," International Journal of Sensor Networks, vol. 45, no. 2, pp. 74–86, 2024.
[19] A. S. Dina, A. B. Siddique, and D. Manivannan, "A deep learning approach for intrusion detection in Internet of Things using focal loss function," Internet of Things, vol. 22, Art. no. 100699, 2023.
[20] Z. Azam, M. M. Islam, and M. N. Huda, "Comparative analysis of intrusion detection systems and machine learning-based model analysis through decision tree," IEEE Access, vol. 11, pp. 80348–80391, 2023.