RESEARCH ARTICLE OPEN ACCESS

Innovative Architecture for Firewall Anomaly Detection Using Convolutional Recurrent Neural Networks

Asfiya Shireen Shaikh Mukhtar[1],
[1]Shivaji science college Congress Nagar Nagpur,

Prof. R. N. Jugele[2]
[2]Shivaji science college Congress Nagar Nagpur,

ABSTRACT

More sophisticated methods for finding anomalies in network firewalls must be developed due to the increasingly complex nature of assaults. For faster recognition of anomalies in network firewalls, this research presents an innovative approach that utilizes recurrent neural networks (RNN) and convolutional neural network networks (CNN). The suggested approach takes recourse to RNN, particularly LSTM (long-short-term memory) systems, to capture intervals within a data stream and CNN to perform successful spatial extraction of features from unfiltered network activity. The Propose research design a Hybrid Model Using CNN and RNN. The objective to develop a Convolution Recurrent Neural Network (CRNN) architecture for Firewall anomaly detection. The system in question is better capable of recognizing complicated trends and dynamic hazards due to this dual strategy. This design incorporates attentive techniques to decide on key characteristics and reduce the computational burden for the purpose to additionally optimize throughput. The architecture's effectiveness in immediate fashion firewalls detection of anomalies is proven by its ability to scale for high-traffic circumstances or the ability to respond according to recognized and unidentified patterns of attack. The present research proposes an established solution to the rising issues surrounding secure network connectivity through the integration of the benefits of recurrent and convolutional networks.

Introduction

Conventional firewall structures, that depend on stable sets of rules and signature-based authentication operations, are growing progressively less effective in addressing modern safety challenges as attacks tend to develop in sophistication and breadth. Threats include persistent and advanced threats (APT), denial of service (DDoS), and zero-day vulnerabilities offer significant obstacles for conventional networks monitoring skills. Since algorithms that utilize deep learning can adapt to shifting patterns of attack and offer better recognition of irregularities within network information, there exists a growing curiosity in employing them to perform malware detection as a solution to these difficulties.

In activities integrating detection of patterns and sequential evaluation of information, Convolutional Neural Networks (CNN) and Recurrent neural network (RNN), especially LSTM (Long Short-Term Memory) relationships, have proven outstanding accuracy. RNNs are excellent for preserving the changing patterns of network activity as they can simulate temporal relationships in data that is sequential, and CNN algorithms. are exceptionally successful at identifying spatial characteristics from intricate information. While CNNs and RNNs were utilized separately for surveillance of networks, there remains much to discover concerning how to incorporate both of them into one design for firewall detection of anomaly.

With the objective to establish a Convolutional Recurrent Neural Network (CRNN) model particularly for firewalls anomaly identification, this study offers an innovative structure that integrates CNN and RNN. The recommended method enables superior tracking of existing and potential hazards by employing CNN for extraction of features and RNN for analysing historical connections in information about traffic. Furthermore, the construction integrates awareness approaches that boost concentrate on essential stream elements, eliminating false alarms and enhancing the precision of detection.

The primary objective of this investigation is to establish a deep learning-powered security framework that can recognize various kinds of internet breaches in immediate fashion, is precise, and is extensible. The development of Unique architecture offers flexible, adjustable network firewalls capable of defend against the most recent generation of internet assault becomes achievable in a significant way through this research.

LITERATURE REVIEW

The implementation of deep learning algorithms in an assortment of disciplines generated a radical change in the identification of anomalies area. A method known as data mining has been suggested in the discipline of computing in clouds [6], which employed extensive knowledge to identify abnormalities in the complicated network of cloud computing systems. Their strategy probably comprised using regular patterns of behaviour for training a model, and then inspecting for variations that could suggest functional irregularities or security problems. Extending on this concept, Cen and Li [7] proposed an approach for DL-based abnormal activity recognition in internet-based environments, carefully investigating patterns in networks to enhance safety and performance.

In the discipline of health care imaging, a study [8] accomplished achievements in detecting irregularities in MRIs of the brain by integrating global and localized characteristics in neural network-based convolutional structures. The purpose of this confluence was to improve specificity in order that neurological issues might be recognized and addressed promptly. A deviation detection technique built around auto encoder artificial neural networks was introduced as an evolution to control systems for factories [9]. With the goal to detect irregularities indicating of failures or security threats, the researchers probably examined the success rate of automated encoders in preserving the fundamental structure of normal operational information. Aversano et al. [10] focused their sights on the global Web of Everything and addressed the discipline of inexpensive DL-based discovery of anomalies. Their investigation evaluated artificial neural networks' resilience through an assortment of patterns. Integrating sources of data across the Internet of Things (IoT) to detect abnormal trends and enabling proactive questions showed the adaptable nature of extensive knowledge for improving abnormality methods for detection

In along with growing the mathematical foundations of detection of anomalies, scientists have been developing practical use in real-life situations throughout the internet of things, healthcare imaging, industrial automation, and Internet of Things (IoT) environments using artificial neural networks like automatic encoders and convolutional neural networks. This developing interdisciplinary research setting not only enhanced abnormality detection's robustness but additionally highlighted how dynamic deep learning will play a role influencing the creation of secure, reliable, and adaptive platforms across an assortment of areas in the decades to come.

The development of methods for DL triggered a fundamental change in the discipline of distributed anomaly identification. For the purpose of to discover discrepancies, Chalapathy and Chawla [11] performed a thorough examination examining at the DL landscape. The study they conducted comprised an in-depth examination of multiple DL methods, frameworks, and their utilization in identifying anomalous scenarios. Ashiku and Dagli [12] concentrated particularly on using deep learning methods in network breach prevention.

They examined how effectively DL recognized network breaches, as well as definitely investigated at novel artificial neural network structures developed for this kind of safety use application. With the goal to investigate combinations of methods for deep learning methodologies for detecting breaches of networks, Wanjau et al. [13] performed a systematic review of the available literature. This review most likely evaluated and appraised the wealth of work on combining deep learning techniques with different strategies for improving the reliability and robustness of systems for intrusion detection. A novel approach employing t-distributed stochastic parametric simulation has been proposed by Yao et al. [14]. For detection of attacks on networks, Neighbour Embedding is utilized with an echelon-based artificial neural network. The benefits of integrating reduction of dimensionality techniques with deep learning architectures for improving malware detection performance were definitely examined in this dissertation. Elkhadir & associates [15]. produced an addition to the research by recommending a modification for the detection of intrusions into networks, Linear Discriminant Analysis (LDA) uses geometrical mean. To enhance an intrusion detection technique's discrimination ability, the researchers apparently investigated the potential application of geometric mean LDA for an extraction of features method. Through encompassing a variety of subjects, such architectural layout, systematic examinations, novel technique, and mixed methods, these research together offer an in-depth comprehension of the role of DL for network anomaly detection. In the context of shifting security questions, the analysis of different strategies reflected an ongoing effort to further improve the preciseness, effectiveness, and scalability of intrusion detection technologies for systems.

METHODOLOGY

A variety of systematic methods are utilized in the development of an innovative design for Convolutional Recurrent Neural Network (CRNN)-based firewall detection of anomalies with the goal to address the challenges associated with recognizing irregularities in network activity, particularly when it involves integrating CNN and RNN elements. By integrating deep learning algorithms as leveraging simultaneous temporal sequence prediction (by RNNs) as well as spatial extraction of features (by CNNs), the approach allows the recognition of both immediate and long-term structures in network activity.

Convolutional Neural Network (CNN)

Maintaining network security is made more difficult by the increasing complexity and amount of network traffic as well as the changing nature of cyber threats. Network security measures are vulnerable because traditional rule-based firewalls and intrusion detection systems frequently fail to identify complex abnormalities And zero-day assaults.

A potent remedy for firewall anomaly detection is a Convolutional Neural Network (CNN), a deep learning model made to identify spatial and hierarchical patterns. A CNN can monitor network traffic records, identify harmful trends, and categorize abnormalities in real time by utilizing its capacity to automatically extract features from high-dimensional data.

The process of using a Convolutional Neural Network (CNN) model for firewall anomaly detection involves several sequential steps.

1. Data Collection
2. Data Preparation
3. CNN Model Design
4. Model Training
5. Model Evaluation
6. Real-Time Deployment
7. Model Updating and Maintenance
8. Feedback Loop

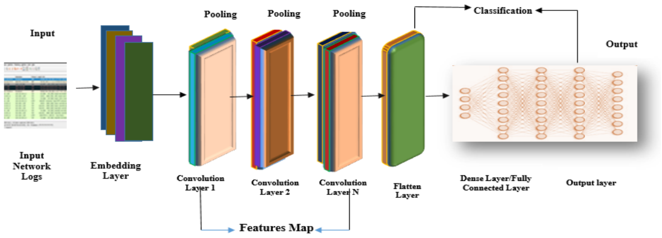


Fig 1: Convolutional Neural Network (CNN) Model

Recurrent Neural Networks (RNNs):

Strong and clever intrusion detection systems are now essential for maintaining network security in the current era of growing cyber threats. As a first line of protection, firewalls are developing beyond static rule-based systems to include cutting-edge methods like deep learning and machine learning. Recurrent neural networks (RNNs) are one of them that have drawn a lot of interest because of its capacity to analyse sequential input and identify intricate patterns over time.

One type of artificial neural network intended for sequential data analysis is called a recurrent neural network. In contrast to conventional neural networks, RNNs are able to recognize relationships in time-series data because they preserve a hidden state that serves as memory. Long Short-Term Memory (LSTM) networks and Gated Recurrent Units (GRUs), two variations of RNNs, are appropriate for managing long-term dependencies since they tackle issues like the vanishing gradient problem.

The process of using a **Recurrent** Neural Network (RNN) model for firewall anomaly detection involves several sequential steps.

1. Data Pre-processing
2. RNN Architecture
3. Training
4. Deployment

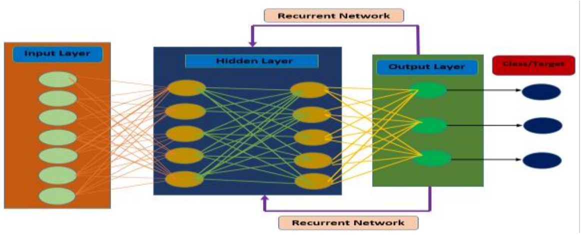


Fig 2: Recurrent Neural Network (RNN) model.

Convolutional Recurrent Neural Network (CRNN) Model:

Traditional firewall systems face increasing difficulties in the ever-changing field of cybersecurity due to complex and changing cyber threats. This research presents a ground-breaking solution—a revolutionary architecture for firewall anomaly detection—in recognition of the shortcomings of rule-based techniques. Along with three deep learning models—Neural Network, CNN_RNN, and Feedforward Neural Network—the architecture incorporates a variety of machine Network, CNN_RNN, and Feedforward Neural Network—the architecture incorporates a variety of machine learning models, such as Logistic Regression, KNeighboursClassifier, Gaussian NB, Linear SVC, and Random Forest Classifier. By adding cognitive processes that can self-adapt to new dangers, this combination seeks to go beyond the limitations of traditional system.

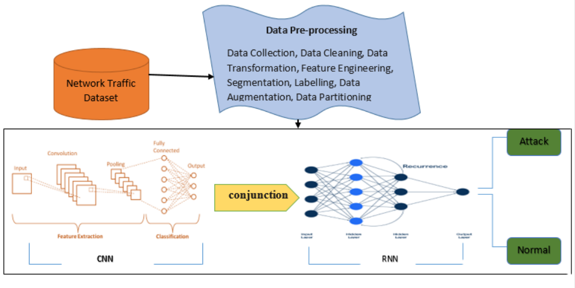


Fig 3: Convolutional Recurrent Neural Network (CRNN) Model:

Blending machine learning models:

A key component of the innovative firewall anomaly detection architecture is the use of machine learning models, which enhances the system's capacity to identify and react to unusual patterns in network traffic. Classifier is one of the machine learning models that have been thoughtfully included into the design. The capacity of the system to adjust and learn from changing cyber threats is facilitated by the distinct qualities that each model. By allowing the system to dynamically examine and react to intricate patterns, this integration represents an evolution from rigid rule-based techniques and improves the overall resilience of anomaly detection. The design seeks to provide a thorough and flexible security mechanism by utilizing a variety of perspectives offered by these machine learning models, resolving the complex issues that accompany current cyber threats.

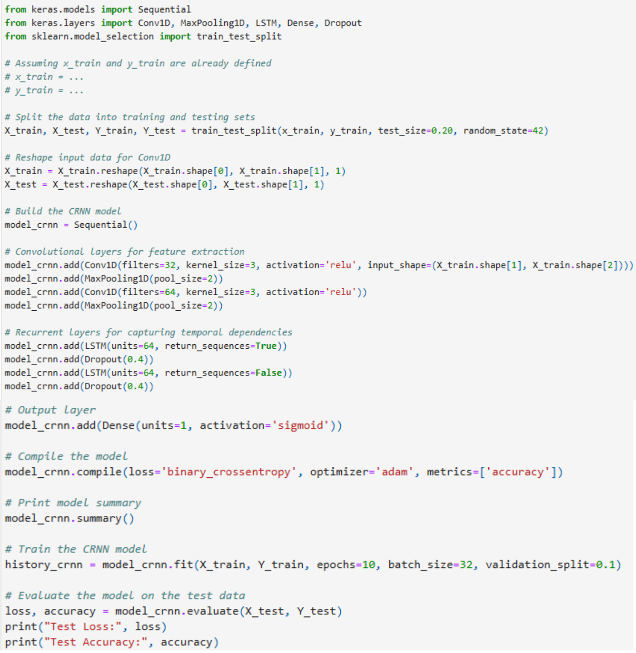
Blending deep learning models:

The incorporation of DL models emerges as a critical element in the endeavour to advance anomaly detection inside the innovative architecture for firewall anomaly detection. This intentional inclusion enables the algorithm to recognize complex relationships and patterns within the network traffic data by utilizing the hierarchical feature extraction capabilities built into deep learning [5]. The design aims to go beyond conventional limits by utilizing the flexibility and complexity management of these deep learning models, providing a more complex and nuanced method of anomaly identification by incorporating deep learning models, the architecture's overall effectiveness in strengthening cybersecurity defences is reinforced. This represents a paradigm change towards intelligent, self-learning systems that can adjust to the dynamic nature of existing cyber threats.

Results:

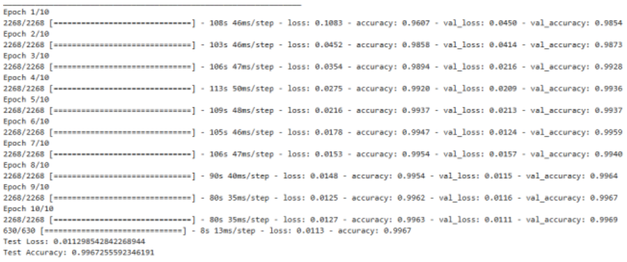
CRNN (Convolutional Recurrent Neural Network) Model:

When evaluating a firewall intrusion detection system (IDS) using a Convolutional Recurrent Network (CRN) (a combination of Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN)), the key performance metrics include training accuracy**,** validation accuracy, training Loss**,** validation Loss, also display the gap between training accuracy**,** validation accuracy as shown below.



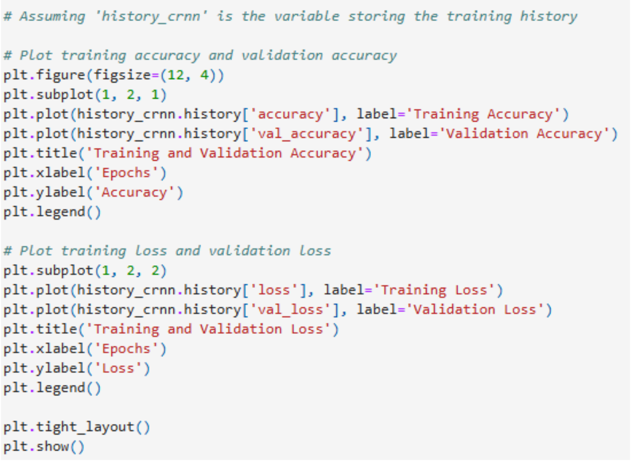
```python
from keras.models import Sequential
from keras.layers import Conv1D, MaxPooling1D, LSTM, Dense, Dropout
from sklearn.model_selection import train_test_split

# Assuming x_train and y_train are already defined
# x_train = ...
# y_train = ...

# Split the data into training and testing sets
X_train, X_test, Y_train, Y_test = train_test_split(x_train, y_train, test_size=0.20, random_state=42)

# Reshape input data for Conv1D
X_train = X_train.reshape(X_train.shape[0], X_train.shape[1], 1)
X_test = X_test.reshape(X_test.shape[0], X_test.shape[1], 1)

# Build the CRNN model
model_crnn = Sequential()

# Convolutional layers for feature extraction
model_crnn.add(Conv1D(filters=32, kernel_size=3, activation='relu', input_shape=(X_train.shape[1], X_train.shape[2])))
model_crnn.add(MaxPooling1D(pool_size=2))
model_crnn.add(Conv1D(filters=64, kernel_size=3, activation='relu'))
model_crnn.add(MaxPooling1D(pool_size=2))

# Recurrent layers for capturing temporal dependencies
model_crnn.add(LSTM(units=64, return_sequences=True))
model_crnn.add(Dropout(0.4))
model_crnn.add(LSTM(units=64, return_sequences=False))
model_crnn.add(Dropout(0.4))
# Output layer
model_crnn.add(Dense(units=1, activation='sigmoid'))

# Compile the model
model_crnn.compile(loss='binary_crossentropy', optimizer='adam', metrics=['accuracy'])

# Print model summary
model_crnn.summary()

# Train the CRNN model
history_crnn = model_crnn.fit(X_train, Y_train, epochs=10, batch_size=32, validation_split=0.1)

# Evaluate the model on the test data
loss, accuracy = model_crnn.evaluate(X_test, Y_test)
print("Test Loss:", loss)
print("Test Accuracy:", accuracy)
```

Fig 4: Develop the Convolutional Recurrent Neural Network (CRNN) Model



```
Epoch 1/10
2268/2268 [==============================] - 108s 46ms/step - loss: 0.1083 - accuracy: 0.9607 - val_loss: 0.0450 - val_accuracy: 0.9854
Epoch 2/10
2268/2268 [==============================] - 103s 46ms/step - loss: 0.0452 - accuracy: 0.9858 - val_loss: 0.0414 - val_accuracy: 0.9873
Epoch 3/10
2268/2268 [==============================] - 106s 47ms/step - loss: 0.0354 - accuracy: 0.9894 - val_loss: 0.0216 - val_accuracy: 0.9928
Epoch 4/10
2268/2268 [==============================] - 113s 50ms/step - loss: 0.0275 - accuracy: 0.9920 - val_loss: 0.0209 - val_accuracy: 0.9936
Epoch 5/10
2268/2268 [==============================] - 109s 48ms/step - loss: 0.0216 - accuracy: 0.9937 - val_loss: 0.0213 - val_accuracy: 0.9937
Epoch 6/10
2268/2268 [==============================] - 105s 46ms/step - loss: 0.0178 - accuracy: 0.9947 - val_loss: 0.0124 - val_accuracy: 0.9959
Epoch 7/10
2268/2268 [==============================] - 106s 47ms/step - loss: 0.0153 - accuracy: 0.9954 - val_loss: 0.0157 - val_accuracy: 0.9940
Epoch 8/10
2268/2268 [==============================] - 90s 40ms/step - loss: 0.0148 - accuracy: 0.9954 - val_loss: 0.0115 - val_accuracy: 0.9964
Epoch 9/10
2268/2268 [==============================] - 80s 35ms/step - loss: 0.0125 - accuracy: 0.9962 - val_loss: 0.0116 - val_accuracy: 0.9967
Epoch 10/10
2268/2268 [==============================] - 80s 35ms/step - loss: 0.0127 - accuracy: 0.9963 - val_loss: 0.0111 - val_accuracy: 0.9969
630/630 [==============================] - 8s 13ms/step - loss: 0.0113 - accuracy: 0.9967
Test Loss: 0.011298542842268944
Test Accuracy: 0.9967255592346191
```

Fig 5: Calculate Total Loss and Accuracy of CRNN Model.



```python
# Assuming 'history_crnn' is the variable storing the training history

# Plot training accuracy and validation accuracy
plt.figure(figsize=(12, 4))
plt.subplot(1, 2, 1)
plt.plot(history_crnn.history['accuracy'], label='Training Accuracy')
plt.plot(history_crnn.history['val_accuracy'], label='Validation Accuracy')
plt.title('Training and Validation Accuracy')
plt.xlabel('Epochs')
plt.ylabel('Accuracy')
plt.legend()

# Plot training loss and validation loss
plt.subplot(1, 2, 2)
plt.plot(history_crnn.history['loss'], label='Training Loss')
plt.plot(history_crnn.history['val_loss'], label='Validation Loss')
plt.title('Training and Validation Loss')
plt.xlabel('Epochs')
plt.ylabel('Loss')
plt.legend()

plt.tight_layout()
plt.show()
```

Fig 6: Training accuracy and validation accuracy of CRNN Model.

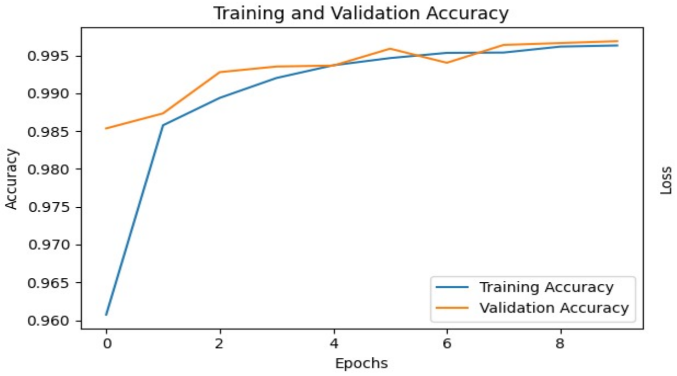


Fig 7: Plot Training and validation Accuracy of CRNN Model.

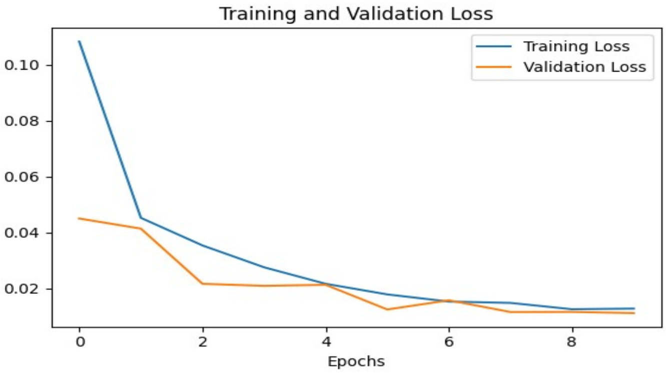


Fig 8: Plot Training and validation Loss of CRNN Model

Conclusion:

The constraints of conventional methods are surpassed through a revolutionary architectural for firewall anomaly detection, becoming an effective solution in contemporary cybersecurity. Through the incorporation of physical and behavioural analysis, the system provides a more durable and adaptive technique for recognizing both existing and emerging hazards. This architecture assures enhanced precision, adaptability, and continuous surveillance as cyber-attacks change, offering networks in unpredictable situations with greater protection. A growing need for versatile, sophisticated defences in networked environments is satisfied with this approach, which serves as an advancement forward in countering the growing variety of attacks. In the propose research work we examine the training accuracy**,** validation accuracy and training Loss**,** validation Loss of CRNN (Convolutional Recurrent Neural Network) Model for Firewall Intrusion Detection.

Reference

[1] A. Zainal, M. A. Maarof, S. M. Shamsuddin and A. Abraham, " Ensemble of One-Class Classifiers for Network Intrusion Detection System," 2008 The Fourth International Conference on Information Assurance and Security, Naples, Italy, 2008, pp. 180-185, doi: 10.1109/IAS.2008.35.

[2] T. Xia, G. Qu, S. Hariri and M. Yousif, "An efficient network intrusion detection method based on information theory and genetic algorithm," PCCC 2005. 24th IEEE International Performance, Computing, and Communications Conference, 2005., Phoenix, AZ, USA, 2005, pp. 11-17, doi: 10.1109/PCCC.2005.1460505.

[3] M. Vartouni, M. Teshnehlab, and S. S. Kashi, “Saosa: Stable adaptive optimization for stacked auto-encoders,” Neural Processing Letters, vol. 52, no. 1, pp. 823–848, 2020.

[4] Gong, Ren Hui & Zulkernine, M. & Abolmaesumi, P. (2005). A software implementation of a genetic algorithm-based approach to network intrusion detection. 246- 253. 10.1109/SNPD-SAWN.2005.9.

[5] Pal, Biprodip & Hasan, Md. Al. (2012). Neural network & genetic algorithm-based approach to network intrusion detection & comparative analysis of performance. Proceeding of the 15th International Conference on Computer and Information Technology, ICCIT 2012. 150-154. 10.1109/ICCITechn.2012.6509809.

[6] Hesham Altwaijry, Saeed Algarny, Bayesian based intrusion detection system, Journal of King Saud University - Computer and Information Sciences, Volume 24, Issue 1, 2012, Pages 1-6, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2011.10.001

[7] Hasan, Md. Al & Nasser, Mohammed & Pal, Biprodip& Ahmad, Shamim. (2013). Intrusion Detection Using Combination of Various Kernels Based Support Vector Machine. International Journal of Scientific and Engineering Research. 4. 1454-1463.

[7] Elkhadir, Zyad & Khalid, Chougdali&Benattou, Mohammed. (2018). Improving Network Intrusion Detection Using Geometric Mean LDA. International Journal of Network Security. 820-826. 10.6633/IJNS.201809.20(5).02).

[8] Yao, H., Li, C., & Sun, P. (2020). Using Parametric t-Distributed Stochastic Neighbor Embedding Combined with Hierarchical Neural Network for Network Intrusion Detection. Int. J. Netw. Secur., 22, 265-274.

[9] Jin Gao, Jiaquan Liu, Sihua Guo, Qi Zhang, Xinyang Wang, "A Data Mining Method Using Deep Learning for Anomaly Detection in Cloud Computing Environment", Mathematical Problems in Engineering, vol. 2020, Article ID 6343705, 11 pages, 2020. https://doi.org/10.1155/2020/6343705

[10] Junjie Cen, Yongbo Li, "Deep Learning-Based Anomaly Traffic Detection Method in Cloud Computing Environment", Wireless Communications and Mobile Computing, vol. 2022, Article ID 6155925, 8 pages, 2022. https://doi.org/10.1155/2022/6155925

[11] Lerina Aversano, Mario Luca Bernardi, Marta Cimitile, Riccardo Pecori, Luca Veltri, "Effective Anomaly Detection Using Deep Learning in IoT Systems", Wireless Communications and Mobile Computing, vol. 2021, Article ID 9054336, 14 pages, 2021. https://doi.org/10.1155/2021/9054336

[12] R. Chalapathy and S. Chawla, “Deep learning for anomaly detection: A survey,” arXiv preprint arXiv:1901.03407, 2019.

[13] Lirim Ashiku, CihanDagli, Network Intrusion Detection System using Deep Learning, Procedia Computer Science, Volume 185, 2021, Pages 239-247, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2021.05.025

[14] JOUR Wanjau, Stephen Wambugu, Geoffrey Oirere, Aaron 2022/06/01 16 Network Intrusion Detection Systems: A Systematic Literature Review of Hybrid Deep Learning Approaches 10 10.35940/ijese.

[15] Q. Niu and X. Li, “A high-performance web attack detection method based on CNN-GRU model,” in Proceedings of the 2020 IEEE 4th Information Technology, Networking, Electronic and Automation