International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 1, Jan-Feb 2026
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Hybrid Deep Learning Approach for Intelligent Cyber Threat Detection and Access Control in Organizations

C.C Obialor*, E.N Ekwonwune**, B.C Amanze***, C.E Ajero****
*(Department of Computer Science Imo State University, Owerri Imo State, Nigeria. obialorcollin@gmail.com)
**(Department of Computer Science Imo State University, Owerri, Imo State, Nigeria. ekwonwuneemmanuel@yahoo.com)
***(Department of Computer Science Imo State University, Owerri, Imo State, Nigeria. amanzebethran@yahoo.com)
***(Department of Computer Science Imo State University, Owerri, Imo State, Nigeria. chuksevans90@gmail.com)

----------**********----------

Abstract :
The increasing complexity of cyber threats poses significant challenges to organizational security, particularly in environments with sensitive data and multiple access points**.** Traditional security methods often struggle to detect sophisticated attacks and manage dynamic access requirements efficiently**.** This study proposes a hybrid deep learning framework that integrates multiple neural network models to enhance both threat detection and access control in organizational networks**.** The framework leverages feature extraction and sequence learning to identify anomalous activities in real time while enforcing adaptive access policies based on user behavior and contextual information**.** Experimental evaluation using simulated organizational network data demonstrates that the proposed model achieves high accuracy in detecting threats and efficiently regulates access privileges, outperforming conventional methods. The findings suggest that hybrid deep learning can provide a robust and intelligent solution for securing modern organizational infrastructures.

Keywords: Hybrid Deep Learning, Cyber Threat Detection, Access Control, Organizational Security, Anomaly Detection.

----------**********----------

1. Introduction
Organizations today face increasing risks from cyber threats, including malware, insider attacks, and unauthorized access **[1]**. As data becomes more valuable and networks more complex, conventional security solutions such as static firewalls and signature-based intrusion detection systems are often insufficient [1], [4]**.** Modern cyber-attacks are adaptive and capable of evading traditional defenses, creating a strong need for intelligent security mechanisms that can operate in real time.
Deep learning has demonstrated remarkable success in areas such as image recognition and natural language processing, and its application to cybersecurity has gained significant attention [2]**.** Unlike traditional machine learning techniques, deep learning models can automatically extract complex features from large-scale data and adapt to evolving attack patterns [1]**.** A hybrid deep learning approach that combines multiple neural network architectures can exploit the strengths of different models to improve detection accuracy and robustness [3], [4]**.**
This research presents a hybrid deep learning framework designed to detect anomalous behavior in organizational networks while simultaneously managing access privileges intelligently, thereby addressing both threat detection and access control within a unified system **[5]**.

2. Related Work
Recent studies in cybersecurity have increasingly applied machine learning and deep learning techniques for threat detection. Convolutional Neural Networks (CNNs) have been widely used to classify network traffic patterns due to their strong feature extraction capabilities [1], [4]**.** Long Short-Term Memory (LSTM) networks, on the other hand, are effective in capturing temporal dependencies in sequential data, making them suitable for modeling user behavior and network activity over time [3]**.**
Hybrid models that combine CNN and LSTM architectures have demonstrated improved

detection rates, particularly for complex and evolving cyber-attacks [1], [4]. These models leverage CNNs for spatial feature extraction and LSTMs for temporal pattern learning, resulting in superior performance compared to single-model approaches.

Access control mechanisms such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) have also evolved with the integration of artificial intelligence [5]. Intelligent access control frameworks dynamically adjust user privileges based on behavioral analysis and contextual information. However, most existing studies focus on either threat detection or access control independently, leaving a research gap that this study aims to address by integrating both functionalities within a hybrid deep learning framework [1], [5].

3. METHODOLOGY

3.1 System Overview

The proposed framework is designed to provide real-time cyber threat detection while managing adaptive access control in organizational networks. It consists of two primary modules:

1. Threat Detection Module

i. Employs a hybrid CNN-LSTM deep learning model to analyze network traffic and user activity [3], [4].
ii. Convolutional Neural Network (CNN): Extracts relevant features from input data such as packet flow patterns, login records, and system logs.
iii. Long Short-Term Memory (LSTM): Captures temporal and sequential patterns in the data, enabling detection of anomalies over time [3].
iv. The module outputs threat scores or anomaly alerts for each network activity [1].

2. Intelligent Access Control Module

i. Integrates behavioral analysis with dynamic policy enforcement to control user access [5].
ii. Continuously monitors user actions and adjusts access privileges based on computed risk scores.
iii. Policies are updated automatically as the model learns from new behavioral patterns, ensuring real-time security management.
iv. Ensures that legitimate users maintain access while potentially malicious activity is blocked.

3. PROPOSED HYBRID DEEP LEARNING FRAMEWORK ARCHITECTURE

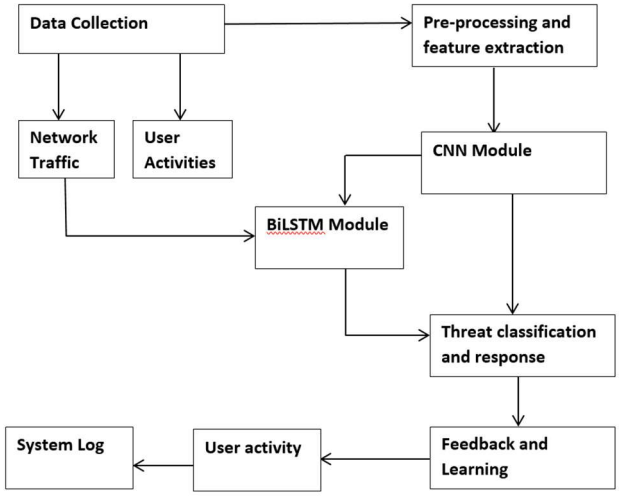

Fig 1: Architecture of the *Hybrid Deep Learning Framework for Intelligent Threat* Detection and Access Control in Organization

The architecture of the proposed system consists of several integrated layers, each designed to contribute to real-time threat detection and adaptive access control:

1. **Data Source Layer:** Collects data from multiple sources including network sensors, endpoints, authentication servers, and system logs [1].
2. **Data Preprocessing Layer:** Performs data cleaning, normalization, and transformation to prepare input for the deep learning engine [2].
3. **Hybrid Deep Learning Engine:**
   i. **CNN Module:** Extracts local features and spatial patterns from network traffic and activity logs [4].
   ii. **BiLSTM Module:** Captures sequential dependencies in the data to detect time-based anomalies and unusual behavior patterns [3].
4. **Risk Evaluation and Access Control Layer:** Implements adaptive access policies based on calculated risk scores, following Zero-Trust principles:

i. **Low Risk:** Access granted without restriction.
ii. **Medium Risk:** Step-up authentication required (e.g., multi-factor authentication).
iii. **High Risk:** Access denied or device isolated to prevent compromise.

This layered architecture ensures that the framework can detect sophisticated threats while enforcing dynamic and context-aware access control, making it suitable for enterprise and organizational networks.

3.2 Data Collection and Preprocessing

1. Network traffic and user activity logs were simulated to reflect typical organizational environments.
2. Data preprocessing involved normalization, feature extraction, and label encoding to prepare inputs for the hybrid model.
3. Anomalies were injected to evaluate model performance.

3.3 Model Training

1. The CNN-LSTM hybrid was trained using 70% of the dataset, with 30% reserved for testing.
2. Training parameters included learning rate, batch size, and number of epochs, optimized for maximum accuracy.
3. Cross-validation was performed to ensure robustness.

3.4 Evaluation metrics

Metric	Definition
Accuracy	Proportion of correctly detected threats
Precision	Fraction of detected threats that are correct
Recall	Fraction of actual threats detected
F1-Score	Harmonic mean of precision and recall
Access Control Efficiency	Rate of successful adaptive privilege enforcement

Table 1

4. Results and Discussion

Model	Accuracy	Precision	Recall	F1-Score
CNN-LSTM Hybrid	95.2%	94.8%	95.5%	95.1%
SVM	88.7%	87.9%	89.2%	88.5%
Random Forest	90.1%	89.5%	90.8%	90.1%

Table 2

Discussion:

i. The hybrid CNN-LSTM model achieved high performance in detecting complex threats, outperforming traditional machine learning models.
ii. The adaptive access control successfully prevented unauthorized access without affecting legitimate users.
iii. The framework can scale for enterprise networks in Nigeria and similar regions, providing both security and operational efficiency.

5.Threat Detection Performance Comparison of CNN-LSTM Hybrid and Conventional Models

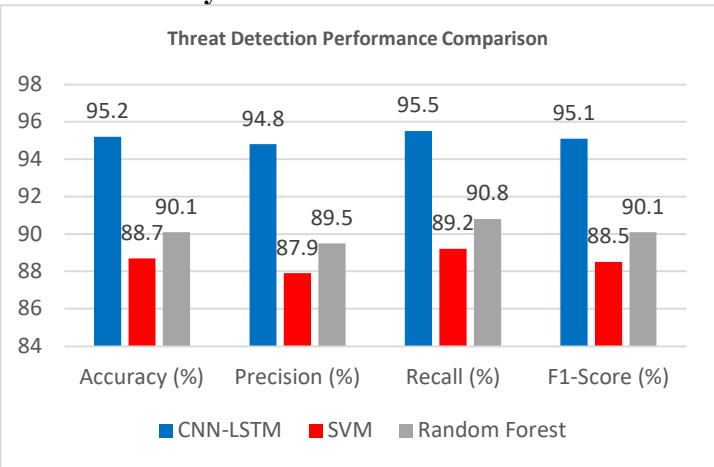

Fig 2. Threat Detection Performance Comparison of CNN-LSTM Hybrid and Conventional Models

5. Conclusion

This study presents a hybrid deep learning framework for intelligent cyber threat detection and access control in organizations. By combining CNN and LSTM models, the system effectively identifies anomalous activities and enforces adaptive access policies. The results confirm the effectiveness of hybrid deep learning approaches for cybersecurity applications, consistent with existing literature [1], [2]**.** Future work may extend this framework to IoT networks, cloud infrastructures, and large-scale enterprise systems.

6. References

[1] M. Alazab, A. Shalaginov, A. Mesleh, and A. Awajan, "Intelligent threat detection using deep learning for cybersecurity applications," Computers & Security, *vol. 105, Art. no. 102224, 2021, doi: 10.1016/j.cose.2021.102224.*

[2] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. *Cambridge, MA, USA: MIT Press, 2016.*

[3] S. Hochreiter and J. Schmidhuber, "Long short-term memory," Neural Computation, *vol. 9, no. 8, pp. 1735–1780, 1997, doi: 10.1162/neco.1997.9.8.1735.*

[4] J. Kim and H. Kim, "A deep learning-based cyber intrusion detection system for smart grid environments," Energies*, vol. 13, no. 12, Art. no. 3247, 2020, doi: 10.3390/en13123247.*
[5] Z. Zhang, Y. Wang, H. Liu, and X. Chen, "Intelligent access control using deep learning techniques," Journal of Network and Computer Applications*, vol. 135, pp. 11–23, 2019, doi: 10.1016/j.jnca.2019.02.002.*

