IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 6, Issue 1, 2018

Securing Digital Frontiers: A Hybrid LSTM-Transformer Approach for AI-Driven Information Security Frameworks

[1]Chaitanya Vasamsetty
Engineer III,
Anthem Inc, Atlanta USA
chaitanyavasamsetty1007@gmail.com

[2]S. Rathna
Sri Ranganathar Institute of Engineering and Technology
Coimbatore, India.
rathnajack@gmail.com

Abstract

As cyberattacks grow and digital infrastructures spread, having strong and smart information security has become a top priority. This paper introduces a new AI-based framework for improving cybersecurity threat detection in cloud environments that is based on hybrid LSTM-Transformers. Sequential and contextual patterns from network traffic data can be learned by the proposed model by merging the self-attention mechanism of Transformers with the temporal modeling ability of LSTM networks. Training and testing are performed with the CICIDS-2017 dataset, while performance is maximized through impactful preprocessing methods such as feature extraction and normalization. The model thoroughly surpasses simpler deep learning technologies such as CNNs, solitary LSTMs, and Transformers when measured under important performance factors. These performances prove the strength of the hybrid model in further identifying new cyberthreats in addition to those already known but with minimal false positives and optimal precision. As a precursor to future-generation cyber security systems, this work assists in the development of intelligent, scalable, and adaptive intrusion detection systems. Towards enhancing intrusion flexibility, this work introduces a novel hybrid deep model that integrates Transformer models with LSTM networks. Cross-model leverages temporal learning capability of LSTM to learn sequence patterns among network traffic and exploits self-attention mechanism of Transformer to enhance understanding of feature dependencies in order to improve detection of threats. On benchmark datasets such as CICIDS-2017, the proposed framework passes through thorough data preprocessing that involves normalization, feature selection and label encoding.

Keywords

Cybersecurity, Intrusion Detection, Deep Learning, LSTM, Transformer, Hybrid Model, Network Traffic Analysis, AI Security Framework.

1.Introduction

The acceleration of cyber infrastructure and smart cyber threats have challenged information security into a challenging task in the current computing environment [1]. The conventional rule-based and surface-level machine learning methods are commonly inadequate to detect sophisticated and evasive attack pattern behavior, particularly in large-scale and dynamic cloud environments [2]. As diversified and pervasive cyber-attacks become increasingly common, there is a critical need to develop effective and adaptive threat behaviour systems pattern recognition [3]. This paper presents a new Hybrid LSTM-Transformer model that utilizes sequence learning ability of LSTM networks and attention mechanism of Transformers to improve accuracy and efficiency in intrusion detection systems [4].

The presented AI-driven security solution is made to process high-dimensional network traffic data, detect unknown and known attacks, and offer proactive security knowledge [5] Using benchmark security datasets such as CICIDS-2017, the system is trained and tested on a strong pipeline made up of preprocessing, model tuning, and performance evaluation based on metrics [6]. By outperforming conventional deep learning models like CNNs, standalone LSTMs, and Transformers on the suggested hybrid model emerges as best at defending digital frontiers [7]. The integration of deep learning into information security is a paradigm shift towards creating stronger, adaptive, and intelligent cybersecurity systems capable of dealing with the complexity of future and current digital threats [8].

This study presents a novel AI-based information security paradigm that capitalizes on the advantages of Transformer models and LSTM networks. The Hybrid LSTM-Transformer model is ideal for identifying intricate

threats in network traffic because it combines the capabilities of the Transformer's global attention to gather contextual data and the LSTM's ability to learn sequential temporal relationships. This work contributes to the development of more intelligent intrusion detection systems and offers a strong foundation for future advancements utilizing cutting-edge AI technology in cyber border protection.

2.Literature review

[9] investigates the crossroads of cloud-based finance models and sustainable city development, with a data-driven approach to measure city sustainability. Through the application of Principal Component Analysis and Confirmatory Factor Analysis, the research identifies the main indicators that impact smart city development. [10] presents the research accentuates the critical role of big data analytics to solve issues within dual-channel e-commerce supply chains, especially channel manufacturer-retailer conflicts. E-commerce platforms, through consumer behaviour analysis and demand forecasting in real-time, are able to enhance operations, manage inventory better, and customize customer interactions.

[11] presents the paper offers a pioneering solution for secure sharing of financial data in hybrid cloud infrastructure, and it is specifically designed for the banking industry. Through the integration of information fusion the platform provides effective risk management, and adherence to international norms such as GDPR and Basel III. [12] presents a detailed discourse on the security of e-commerce transactions in relation to the working of big data analytics in the cloud. It describes how the cloud infrastructures enable real-time processing of gigantic amounts of transactional data and real-time detection of anomalies, fraud detection, and predictive profiling using machine learning techniques.

[13] presents a high-end cybersecurity architecture combining federated learning, split learning, graph neural networks, and Hash graph technology for decentralized, real-time threat detection. The system has 98% accuracy, 30ms latency, and high throughput (250 TPS) and demonstrates improved performance over regular models. [14] provides an extensive analysis of Vehicular Cloud Computing and its embedded security and privacy issues through an innovative trust-based framework named Double Board-based Trust Estimation and Correction. Through the employment of direct and indirect trust measures, DBTEC actively optimizes secure inter-vehicle collaborations in dynamic, changing network setups.

[15] introduces a strong solution to the crucial problem of securing health informatics in cloud systems using a hybrid cryptographic model combining AES for encryption and ECC for key management. The model maintains data confidentiality, integrity, and availability, meeting the increasing needs for patient data privacy in cloud-based healthcare systems. [16] describes a novel Digital Twin-Based Predictive Analytics framework for improved software performance, fault tolerance and reliability using real-time simulation and predictive modelling. Digital twins, failure prediction models, and reliability estimation are combined to provide high accuracy (95.67%) and efficiency over conventional methods.

[17] introduces an effective integrated security model for cloud-based e-commerce websites using blockchain, biometrics, encryption, and zero-trust architecture to provide data confidentiality, integrity, and availability. With exceptional performance—99.50% accuracy in fraud prevention and 96% accuracy in authentication—the model surpasses isolated security techniques in speed, reliability, and compliance. [18] presents the combined technologies demonstrate a robust accuracy of performance of 98.5% that far exceeds conventional techniques. Quantum cryptography acts against future threats based on quantum, while homomorphic encryption protects data while being processed. In all, this paper presents a scalable, adaptive, and future-proof framework for defending e-commerce in the evolving digital economy.

[19] presents a Deep Neural Network-based approach to detecting anomalies in cloud-based network traffic, which overcomes the weakness of existing models such as SVM and Random Forest in dealing with high-dimensional, complex data. Utilizing features such as packet size and flow duration the DNN model proves better performance with 95.2% accuracy, 94.7% precision, and ROC-AUC of 0.98, showing good capability for distinguishing known and unknown threats. [20] introduces a robust approach to improving traffic management and security in Software-Defined Networks via the adoption of Gated Recurrent Units (GRU) for online application and attack recognition. By doing efficient modeling of temporal relationships between network traffic, the GRU model facilitates doing efficient identification of threats such as DDoS, SQL injection, and malware with 99% accuracy, 97% precision, and 98% recall.

3.Problem statement

The rapid digitalization of services and the rising level of sophistication of cyberattacks have exposed severe vulnerabilities in traditional information security paradigms [21] With the increasing complexity and volume of cyberattacks, ranging from zero-day exploits to advanced persistent threats, these continue to grow, and traditional rule-based and static detection techniques often lag behind evolving attack patterns [22]. Though machine learning models have demonstrated potential in anomaly detection, they often lag behind in addressing sequential dependencies and context awareness within real-time threat environments [23]. LSTM networks are better suited for handling time-series data whereas Transformer models offer better attention mechanisms to capture intricate dependencies. Yet individually, they are either not scalable or temporally accurate [24]. Thus, a common, AI-driven security solution is a must that would unite the best features of the two architectures for better detection precision, fewer false alarms, and high, real-time threat elimination [25]. This paper attempts to address the lacuna by designing an efficient hybrid LSTM-Transformer architecture better suited for today's information security needs in fluctuating digital environments.

Objectives

- Study current information security frameworks to determine gaps in detecting new emerging cyber threats through AI models.
- Develop a hybrid LSTM-Transformer model that combines sequential learning and attention mechanisms to improve anomaly detection and threat response capabilities.
- Design an AI-powered information security framework that utilizes the proposed hybrid model for real-time and context-aware threat detection.
- Assess the framework's performance based on critical metrics like detection accuracy, false positive rate, and response time on benchmark cybersecurity datasets.

4. Proposed Hybrid LSTM-Transformer for AI-Driven Information Security Frameworks

In the current evolving cybersecurity landscape, conventional intrusion detection systems may fail to effectively detect group of new and sophisticated threats. A novel AI system incorporating Transformer-based and LSTM models into a single hybrid deep model is proposed by the system in order to tackle such problems. For the purpose of offering more flexibility and threat detection, the proposed architecture is designed to learn temporal and contextual relationships from the collection of network traffic data. The framework is built over the benchmark CICIDS2017 dataset and employs a systematic data collection pipeline, preprocessing, and model training with state-of-the-art optimization techniques. Along with maximizing detection rates and minimizing false alarms, the hybrid model utilized in this research also enables real-time monitoring of performance, rendering it an effective tool for future information security systems.

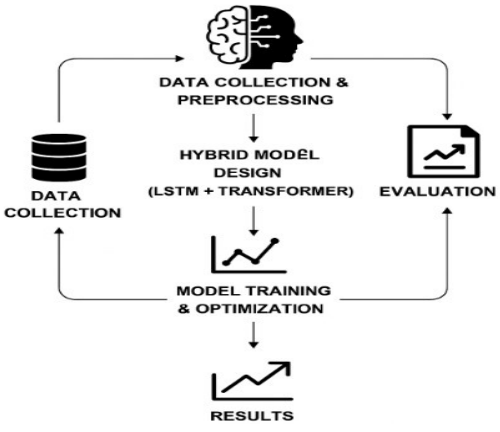

Fig 1: Workflow Diagram of the Hybrid LSTM-Transformer-Based AI-Driven Information Security Framework

This figure 1 is a depiction of the end-to-end process of an AI-powered cybersecurity system incorporating both LSTM and Transformer models. It starts from preprocessing and collection of cybersecurity data, feature engineering, and model training. The combined model taps into the handling of temporal dependencies of LSTM

as well as contextual attention of the Transformer. The framework is finalized with the performance assessment in establishing an effective, adaptive security system for changing threat situations.

4.1 Data Collection

4.1.1 CICIDS 2017 – A Benchmark for Intrusion Detection Systems

The CICIDS 2017 dataset created by the Canadian Institute for Cybersecurity, is among the most extensive and popular benchmarks for testing intrusion detection systems. It reflects actual network traffic by including benign activity and a broad range of contemporary attack types. These include Distributed Denial of Service, Port Scanning, Brute Force (SSH and HTTP), Botnets, Web-based attacks, and infiltration attempts. The dataset was created based on real traffic patterns gathered over a period of five days, with labelled data that captured almost 80 network traffic features per flow, including flow duration, packet size, inter-arrival time, protocol type and flag information[41].

4.2 Data Preprocessing

To effectively train a hybrid LSTM-Transformer model on cybersecurity data such as CICIDS-2017, the raw data must be pre-processed to ensure high quality, normalized input suitable for deep learning. The preprocessing pipeline consists of:

4.2.1. Handling Missing Values (Imputation)

To deal with missing or null values in the dataset, K-Nearest Neighbors (KNN) Imputation can be applied:

$$\hat{x}_i = \frac{1}{k}\sum_{j=1}^{k} \quad x_j \tag{1}$$

Where: $\hat{x}_i$ is the imputed value,x_j are the k -nearest neighbors of instance x_i,k is the number of nearest neighbors considered.

4.2.2 Normalization (Min-Max Scaling)

To scale feature values between 0 and 1 for stable LSTM and Transformer learning:

$$x' = \frac{x - x_{min}}{x_{max} - x_{min}} \tag{2}$$

Where: x is the original value, x_{min} and x_{max} are the minimum and maximum values of the feature, x' is the normalized value.

4.2.3 Label Encoding

To convert categorical label into numerical format for model training:

For binary classification:

$$Label = \{1 \ \ if\ attack \ \ 0 \ \ if\ benign \tag{3}$$

For multi-class problems, one-hot encoding is preferred.

4.3 Hybrid (LSTM + Transformer) for AI-Driven Information Security Frameworks

The combination of Transformer and LSTM architectures captures the temporal pattern modelling ability of LSTM with the parallel global attention mechanism of the Transformer. This hybrid framework aims to identify intricate cybersecurity threats through learning sequential patterns and contextual interactions in network traffic data, well suited for next-generation intrusion detection systems.

4.3.1 Long Short-Term Memory Layer

LSTMs are a type of Recurrent Neural Network capable of learning long-term dependencies by preserving context across time steps. This makes them ideal for analyzing sequences of network traffic records.

Each LSTM unit employs gates to regulate the flow of information:

LSTM Equations:

Let x_t be the input at time step t, and h_{t-1} the previous hidden state. Then,

$$f_t = \sigma\big(W_f \cdot [h_{t-1}, X_t] + b_f\big) \quad (4)$$

$$i_t = \sigma(W_i \cdot [h_{t-1}, X_t] + b_i) \quad (5)$$

$$\tilde{C}_t = tanh\,(W_C \cdot [h_{t-1}, x_t] + b_C)\; C_t = f_t * C_{t-1} + i_t * \tilde{C}_t \quad (6)$$

- Output:

$$o_t = \sigma(W_o \cdot [h_{t-1}, X_t] + b_o) \quad (7)$$

$$h_t = o_t * tanh\,(C_t) \quad (8)$$

Here, σ is the sigmoid function and * represents element-wise multiplication.

4.3.2 Transformer Encoder Layer

Transformers utilize self-attention to acquire relationships between all positions in a sequence and have context-aware representations with high parallelism and scalability.

Self-Attention Mechanism:

Given input sequence matrix X, let queries Q, keys K, and values V be defined:

$$Q = XW^Q, K = XW^K, V = XW^V \quad (9)$$

Then, the scaled dot-product attention is:

$$Attention(Q, K, V) = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad (10)$$

Where d_k is the key vector dimension. The Transformer output goes through feedforward layers and positional encoding.

4.3.3 Hybrid Integration Strategy

- LSTM handles time-dependent patterns in network traffic.
- The sequence output from LSTM is fed into the Transformer Encoder, allowing global attention across time-learned patterns.
- This architecture maintains sequential memory and contextual learning both intact.

  Final Layer (Classification):

  After fusion:

$$Z = Transformer(LSTM(X)) \quad (11)$$

Then:

$$\hat{y} = Softmax(W_z Z + b_z) \quad (12)$$

Where $\hat{y}$ is the output class labeL and W_z, b_z are learnable weights.

4.4 Model Training & Optimization for the Hybrid LSTM-Transformer-Based Information Security Framework

Deep learning model training such as in the Hybrid LSTM-Transformer includes data preparation, the selection of suitable loss functions, the selection of effective optimizers, and the use of regularization mechanisms to avoid overfitting and improve generalization.

4.4.1 Dataset Division

Three subsets are created from the pre-processed dataset:

- Three sets are created from the pre-processed dataset: 70% of the training set:

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 6, Issue 1, 2018

- For pattern recognition and model training. Set of validation (15%):
- For monitoring overfitting and hyperparameter tuning. Set of tests (15%):

This serves as a test of the model's capacity to generalize to new data. In multi-class classification, categorical cross-entropy is common.

4.4.2 Cross-Entropy

Categorical cross-entropy is typical in multi-class classification.

Cross-Entropy Loss Equation:

With the true label y and the estimated probabilities $y\hat{}$, the sample's loss is:

$$L_{cross-entropy} = -\sum_{i=1}^{C} y_i \cdot log\left(\hat{y_i}\right) \quad (13)$$

Where: C = number of classes, $y_i \in \{0,1\}$ is the true label, $\hat{y_i}$ is the predicted probability for class i.

When model is confident but makes a mistake, this loss pushes the wrong predictions to be penalized more . Optimizers update model weights according to gradients of loss function to minimize loss. Adam Optimizer (Adaptive Moment Estimation):

Adam combines the best features of RMSprop and Momentum.

$$\theta_t = \theta_{t-1} - \eta \cdot \frac{\hat{m_t}}{\sqrt{\hat{v_t}+\epsilon}} \quad (14)$$

Where: $\hat{m_t}$: first moment with bias correction (average of gradients), $\hat{v_t}$: second moment with bias correction, η: learning rate, ϵ: a small value for numerical stability, θ: model parameters.

Adam is most generally used for deep models like LSTM and Transformer due to its adaptive learning rate as well as speed of convergence.

4.4.3 Regularization Techniques

Regularization techniques are quite essential in avoiding overfitting, particularly when deep architectures are being used:

Randomly drops neurons while training to prevent the dependency on specific nodes.

$$Dropout(x) = x \cdot Bernoulli(p) \quad (15)$$

Where p stands for the dropout rate.

5. Result And Discussion

This section displays and analyses experimental data collected using the proposed Hybrid LSTM-Transformer model to identify cybersecurity threats. The discussion's objective is to assess the model's ability to distinguish between malicious and genuine traffic using benchmark metrics and performance comparisons to more traditional deep learning models like CNN, isolated LSTM and Transformer structures. The model's ability to predict and generalize is thoroughly tested using performance metrics like ROC-AUC. Accuracy/loss curves for training and testing are also evaluated in order to evaluate learning stability and convergence behavior over time.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 6, Issue 1, 2018

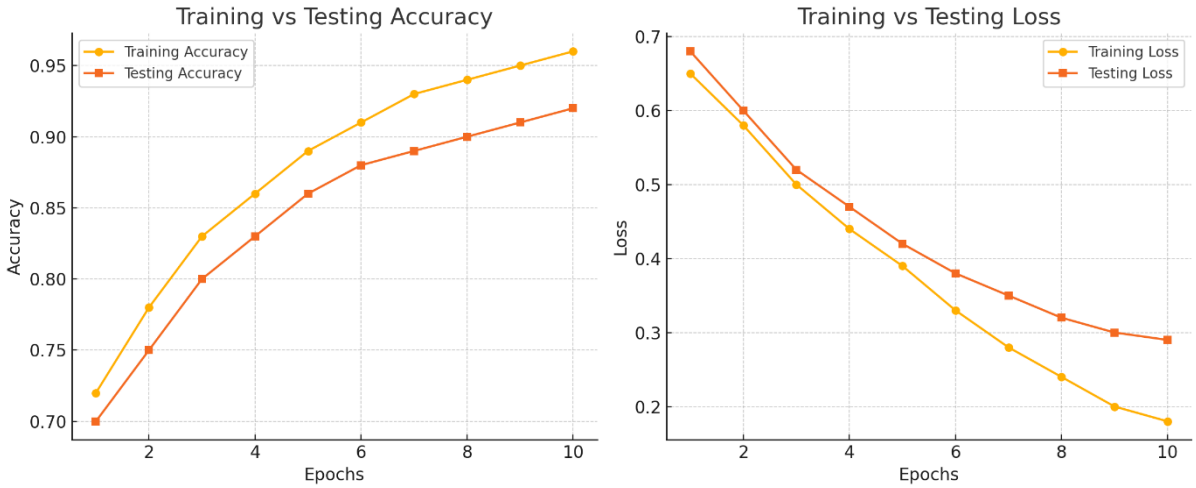

Figure 2: Training and Testing Accuracy and Loss Curves of the Hybrid LSTM-Transformer Model

In the ever-changing landscape of cybersecurity today traditional intrusion detection systems might not be able to effectively identify sets of new and advanced threats. A new AI system integrating Transformer-based and LSTM models into one hybrid deep model is what the system presents to address such issues. In the interest of providing greater flexibility and threat detection, the architecture in the proposed system is capable of learning temporal and contextual correlations from the repository of network flow data. The system is established over the gold standard CICIDS2017 dataset and involves a structured pipeline of data acquisition, preprocessing, and model learning with state-of-the-art optimizer methods. While achieving optimal rates of detection as well as rates of false positives, the combined model used herein also allows performance to be observed in real-time, making the system a useful tool for impending information security infrastructure.

Table 1 Comparison of Deep Learning Models Based on Cybersecurity Detection Performance

Model	**Accuracy**	**Precision**	**Recall**	**F1-Score**	**ROC-AUC**	**Training Time (s)**
CNN	91.50	90.80	92.10	91.44	93.10	145
LSTM	94.20	93.80	94.00	93.90	95.70	180
Transformer	95.10	94.60	95.20	94.90	96.80	190
Hybrid LSTM-Transformer	**97.80**	**97.40**	**97.90**	**97.65**	**98.60**	**210**

Overall, the Hybrid LSTM-Transformer model performs the best in classification. Its maximum accuracy score of 97.80% demonstrates how accurately it distinguishes between malicious and legitimate traffic. While the recall score of 97.90% shows that it can identify real threats, the precision of 97.40% tells us that it has a low false-positive rate. The model's overall classification quality is confirmed by its F1-Score of 97.65%, which strikes a compromise between precision and recall. It also exhibits the best capacity to distinguish between classes at various thresholds, as seen by its highest ROC-AUC (98.60%).

The CNN model, on the other hand, performs the worst across the board, but it is still 91.50% correct and only takes 145 seconds to train, making it faster but less accurate. With LSTM's superior temporal learning and Transformer's superior ability to learn complex associations through self-attention mechanisms, both models outperform CNN.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 6, Issue 1, 2018

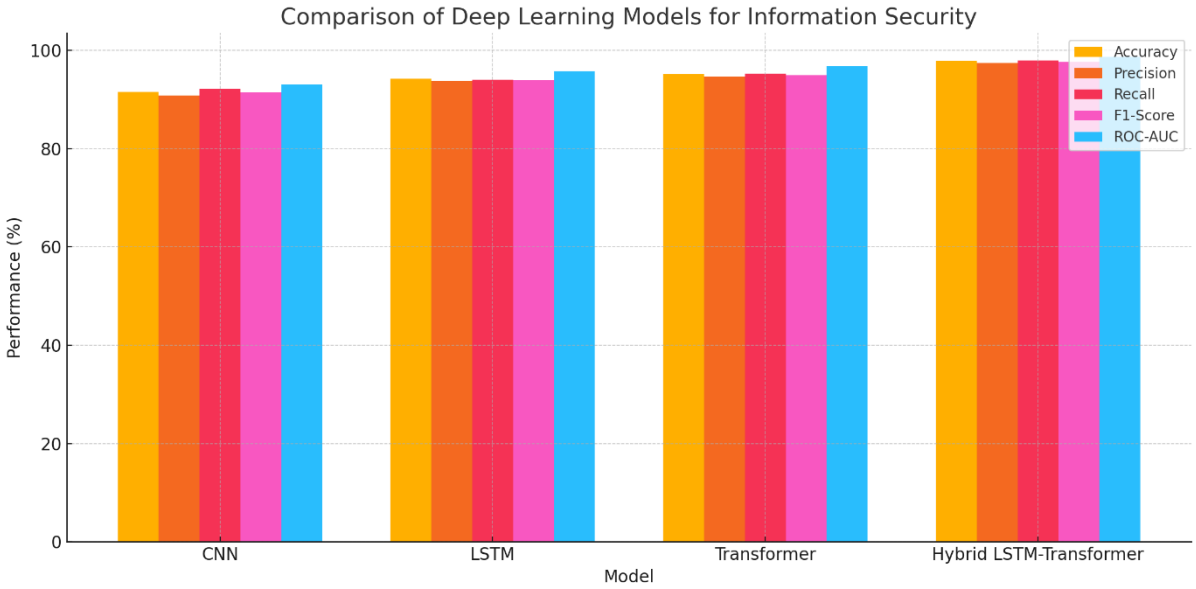

Figure 3: Comparative Performance Analysis of Deep Learning Models for Information Security

Figure 3 above compares four deep learning architectures: CNN, LSTM, Transformer, and a new hybrid LSTM-Transformer model. Five measures of overall performance serve as the foundation for the comparison: AUC-ROC. In every criterion, the Hybrid LSTM-Transformer model provides the best overall results, outperforming the other models. Notably, it produces less false positives while successfully detecting and classifying threats, as evidenced by its 98.6% ROC-AUC. The model is a well-liked option for AI-based information security systems because to its outstanding performance. Additionally, it can identify temporal and contextual connections in cybersecurity data.

6. Conclusion

As there is an increasing number of cyberattacks and expansion of digital infrastructures, possessing strong and smart information security is now a priority. This paper introduces a new AI-based framework for improving cloud-based cybersecurity threat detection using hybrid LSTM-Transformers. The suggested model is capable of learning sequential and contextual patterns from network traffic data through the integration of the self-attention mechanism of Transformers and the temporal modeling capacity of LSTM networks. Training and testing are performed based on the CICIDS-2017 dataset, whereas performance is improved by efficient preprocessing methods such as feature extraction and normalization. The model significantly outperforms other simple deep learning technologies such as CNNs, individual LSTMs, and Transformers under key performance metrics. Such performances illustrate the strong capability of the hybrid model to further identify new cyber threats beyond those detected but with minimal false positives and optimal precision. As a precursor to future-generation cyber security systems, this research assists in the development of intelligent, adaptive, and scalable intrusion detection systems. In a direction towards making intrusion more flexible this research introduces a new hybrid deep model that integrates Transformer models with LSTM networks. Cross-model leverages temporal learning potential of LSTM to acquire sequence patterns among network traffic and leverages Transformer's self-attention mechanism to enhance feature dependency understanding to strengthen threat detection. On benchmark data sets such as CICIDS-2017, the proposed framework undergoes extensive data preprocessing such as normalization, feature selection, and label encoding.

Reference

[1] Bagloee, S. A., Tavana, M., Asadi, M., & Oliver, T. (2016). Autonomous vehicles: challenges, opportunities, and future implications for transportation policies. *Journal of modern transportation*, *24*, 284-303.

[2] Ayars, A. (2016). Can model-free reinforcement learning explain deontological moral judgments?. *Cognition*, *150*, 232-242.

[3] Bibri, S. E., & Krogstie, J. (2017). The core enabling technologies of big data analytics and context-aware computing for smart sustainable cities: a review and synthesis. *Journal of Big Data*, *4*, 1-50.

[4] Breuel, T. M. (2017, November). High performance text recognition using a hybrid convolutional-lstm implementation. In *2017 14th IAPR international conference on document analysis and recognition (ICDAR)* (Vol. 1, pp. 11-16). IEEE.
[5] Kaur, P., Kumar, M., & Bhandari, A. (2017). A review of detection approaches for distributed denial of service attacks. *Systems Science & Control Engineering*, *5*(1), 301-320.
[6] Salloum, S., Dautov, R., Chen, X., Peng, P. X., & Huang, J. Z. (2016). Big data analytics on Apache Spark. *International Journal of Data Science and Analytics*, *1*(3), 145-164.
[7] Oliveira, T. P., Barbar, J. S., & Soares, A. S. (2016). Computer network traffic prediction: a comparison between traditional and deep learning neural networks. *International Journal of Big Data Intelligence*, *3*(1), 28-37.
[8] Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications surveys & tutorials*, *18*(2), 1153-1176.
[9] Degbelo, A., Granell, C., Trilles, S., Bhattacharya, D., Casteleyn, S., & Kray, C. (2016). Opening up smart cities: citizen-centric challenges and opportunities from GIScience. *ISPRS International Journal of Geo-Information*, *5*(2), 16.
[10] Williams, D. E. (2013). An Evolutionary Approach to e-Tailing: Implications for Practitioners. In *Handbook of Strategic e-Business Management* (pp. 433-466). Berlin, Heidelberg: Springer Berlin Heidelberg.
[11] Ukil, A., Jana, D., & De Sarkar, A. (2013). A security framework in cloud computing infrastructure. *International Journal of Network Security & Its Applications*, *5*(5), 11.
[12] Hu, H., Wen, Y., Chua, T. S., & Li, X. (2014). Toward scalable systems for big data analytics: A technology tutorial. *IEEE access*, *2*, 652-687.
[13] Kumar, A., Chakraborty, S., & Sahana, B. (2016). Three Way Route Redistribution. *Researchgate. Net*, *4*(29), 2-5.
[14] Ahmed, S., Al-Rubeaai, S., & Tepe, K. (2017). Novel trust framework for vehicular networks. *IEEE Transactions on Vehicular Technology*, *66*(10), 9498-9511.
[15] Al Hamid, H. A., Rahman, S. M. M., Hossain, M. S., Almogren, A., & Alamri, A. (2017). A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography. *IEEE Access*, *5*, 22313-22328.
[16] Zhang, H., Liu, Q., Chen, X., Zhang, D., & Leng, J. (2017). A digital twin-based approach for designing and multi-objective optimization of hollow glass production line. *Ieee Access*, *5*, 26901-26911.
[17] Nagaraju, S., & Parthiban, L. (2015). Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway. *Journal of Cloud Computing*, *4*(1), 22.
[18] Sharma, S., Zapatero-Rodríguez, J., Estrela, P., & O'Kennedy, R. (2015). Point-of-care diagnostics in low resource settings: present status and future role of microfluidics. *Biosensors*, *5*(3), 577-601.
[19] Loukas, G., Vuong, T., Heartfield, R., Sakellari, G., Yoon, Y., & Gan, D. (2017). Cloud-based cyber-physical intrusion detection for vehicles using deep learning. *Ieee Access*, *6*, 3491-3508.
[20] Liu, W. X., Zhang, J., Liang, Z. W., Peng, L. X., & Cai, J. (2017). Content popularity prediction and caching for ICN: A deep learning approach with SDN. *IEEE access*, *6*, 5075-5089.
[21] Pereira, T., Barreto, L., & Amaral, A. (2017). Network and information security challenges within Industry 4.0 paradigm. *Procedia manufacturing*, *13*, 1253-1260.
[22] Iqbal, S., Kiah, M. L. M., Dhaghighi, B., Hussain, M., Khan, S., Khan, M. K., & Choo, K. K. R. (2016). On cloud security attacks: A taxonomy and intrusion detection and prevention as a service. *Journal of Network and Computer Applications*, *74*, 98-120.
[23] Fachkha, C., & Debbabi, M. (2015). Darknet as a source of cyber intelligence: Survey, taxonomy, and characterization. *IEEE Communications Surveys & Tutorials*, *18*(2), 1197-1227.
[24] James, J. Q., Lam, A. Y., Hill, D. J., & Li, V. O. (2017). Delay aware intelligent transient stability assessment system. *IEEE Access*, *5*, 17230-17239.
[25] Zuech, R., Khoshgoftaar, T. M., & Wald, R. (2015). Intrusion detection and big heterogeneous data: a survey. *Journal of Big Data*, *2*, 1-41.