Journal of Science and Technology
ISSN: 2456-5660 Volume 4, Issue 04 (July- Aug 2019)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2019.v4.i04.pp57- 67*

AI-DRIVEN INTRUSION DETECTION SYSTEM USING AUTOENCODERS AND LSTM FOR ENHANCED NETWORK SECURITY

[1]Venkata Surya Teja Gollapalli
Network Engineer, Kairos Technologies, Inc.
Irving, Texas, USA
venkatasuryagollapalli@gmail.com

[2]R Padmavathy
Anna University, Coimbatore
dr.padmabarathi@gmail.com

To Cite this Article

Venkata Surya Teja Gollapalli, R Padmavathy' "**AI-DRIVEN INTRUSION DETECTION SYSTEM USING AUTOENCODERS AND LSTM FOR ENHANCED NETWORK SECURITY'** *Journal of Science and Technology, Vol. 4, Issue 04-Aug 2019, pp57-67*

Article Info

Received: 30-06-2019 Revised: 07-08-2019 Accepted: 18-08-2019 Published:29 -08-2019

ABSTRACT

The increasing complexity of cyber threats has necessitated the development of advanced Intrusion Detection Systems (IDS) capable of detecting both known and novel network attacks. Traditional rule-based IDS methods often struggle with the rapid evolution of attack strategies. This paper proposes an AI-driven IDS using Autoencoders for feature extraction and Long Short-Term Memory (LSTM) networks for classification. The Autoencoders perform unsupervised anomaly detection by identifying deviations from normal network behavior, while LSTM networks capture the temporal patterns of network traffic. The integration of these techniques, enhanced by cloud computing, allows for efficient real-time processing of large-scale network data. Experimental results show that the proposed system improves detection accuracy and scalability, offering a robust solution to evolving network security challenges. However, further refinement is required to address issues of overfitting and improve generalization.

Keywords: AI, network security, LSTM, Autoencoder.

1 INTRODUCTION

The rapid growth of network-based applications and the increasing reliance on digital infrastructures have led to a surge in cyber threats, making network security a critical concern for organizations worldwide [1] [2]. Intrusion Detection Systems (IDS) play a vital role in safeguarding networks by identifying unauthorized access, malicious activities, and abnormal behavior [3] [4]. Traditionally, these systems rely on rule-based techniques or signature-based approaches. However, as attacks become more sophisticated and varied, traditional methods struggle to keep up, demanding more advanced solutions [5] [6]. The integration of Artificial Intelligence (AI), specifically deep learning models like Autoencoders and Long Short-Term Memory (LSTM) networks, has opened new possibilities in intrusion detection, enabling systems to learn complex patterns from large volumes of data and identify previously unseen threats [7] [8].

The growing complexity and volume of network traffic contribute to the rise in cyberattacks, making it difficult for conventional IDS to effectively detect new and evolving threats. Factors such as the scale of data, the dynamism of attack strategies, and the high-dimensional nature of network traffic make it challenging for traditional systems to process and classify such large datasets in real time [9] [10]. Autoencoders, with their unsupervised learning approach, are used for anomaly detection by detecting deviations from normal behavior, while LSTM networks, designed to capture temporal dependencies, allow for the identification of sequential patterns of attacks. These advanced AI techniques address many of the challenges posed by the ever-changing and massive datasets of modern networks [11] [12].

Despite the promising potential of AI in network security, there are several issues that hinder the effective deployment and adoption of these technologies [13] [14]. One of the key challenges is the scarcity of high-quality labeled datasets for training deep learning modes, particularly for detecting novel attack types [15] [16]. Additionally, AI models, especially deep neural networks, are computationally intensive, requiring significant resources for training and real-time inference [17] [18]. Overfitting is another issue, where models may perform well on training data but fail to generalize to new, unseen attack scenarios. Moreover, the interpretability of deep learning models remains a significant hurdle in security-critical applications, where understanding the rationale behind a detection is essential for trust and decision-making [19] [20].

To overcome these challenges, this paper proposes an AI-driven Intrusion Detection System that leverages Autoencoders for feature extraction and LSTM networks for classification [21] [22]. By combining these two techniques, the proposed system offers a more robust and adaptive solution for detecting both known and novel intrusions [23] [24]. The use of Autoencoders helps with unsupervised anomaly detection, while LSTM captures the temporal nature of network traffic, enabling the system to identify attack patterns over time [25] [26]. Moreover, with advancements in cloud computing, real-time processing of vast network data has become more feasible, allowing for faster and more efficient intrusion detection [27] [28]. The approach presented here addresses the limitations of traditional IDS and offers a scalable, accurate, and interpretable solution for securing modern digital infrastructures [29] [30].

1.1 PROBLEM STATEMENT

The proposed AI-driven Intrusion Detection System (IDS) effectively addresses several key challenges identified in the problem statement. First, by utilizing Autoencoders for unsupervised anomaly detection and LSTM networks for classification, the system enhances the detection of novel attack patterns, overcoming the scarcity of high-quality labeled datasets. The use of Autoencoders for feature extraction aids in identifying deviations from normal network behavior without the need for labeled data, while LSTM networks capture temporal dependencies, making the system adaptive to evolving threats. Additionally, advancements in cloud computing enable real-time processing of large network datasets, improving efficiency and scalability. These combined techniques provide a more robust solution, minimizing issues related to overfitting and improving generalization, thereby ensuring more accurate and timely intrusion detection.

1.2 OBJECTIVES

- Analyse the effectiveness of Autoencoders in detecting anomalies and LSTM networks for classifying network traffic.
- Apply Autoencoders for feature extraction and LSTM networks for classifying network traffic patterns over time to improve intrusion detection.
- Evaluate the performance of the AI-driven Intrusion Detection System using the ROC curve, accuracy, and loss curves to identify areas for improvement.
- Create a robust intrusion detection model capable of identifying both known and novel network intrusions by integrating AI-based techniques.
- Assess the system's real-time processing capabilities enabled by cloud computing for handling large volumes of network data efficiently.
- Develop a scalable and interpretable IDS solution that addresses traditional systems' limitations in detecting sophisticated cyberattacks.

2 LITERATURE SURVEY

The growing complexity of real financial applications, characterized by nonlinear and time-varying behaviors, has led to an increasing demand for solutions to these highly dynamic problems [31]. presents a comparative review of three prominent artificial intelligence techniques artificial neural networks, expert systems, and hybrid intelligence systems in the context of financial markets [32] [33]. These markets are categorized into credit evaluation, portfolio management, and financial prediction and planning. The review highlights that AI methods often outperform traditional statistical techniques in handling nonlinear patterns, though their superiority is not absolute. Recent research confirms the effectiveness of AI techniques, particularly in addressing complex financial issues [34] [35].

A Network Intrusion Detection System (NIDS) plays a crucial role in detecting network security breaches, but developing an efficient and flexible system to handle unpredictable attacks poses significant challenges [36]. proposes a deep learning-based approach using Self-taught Learning (STL) for building a more efficient and adaptable NIDS [37] [38]. The approach is evaluated using the NSL-KDD dataset, a well-known benchmark for network intrusion detection [39] [40]. The performance is assessed based on key metrics such as accuracy, precision, recall, and F-measure, and is compared with previous works, demonstrating the effectiveness of the proposed method in enhancing NIDS performance.

In response to the 2008 Mumbai attacks, the Mumbai police initiated a scheduling system for limited inspection checkpoints across the city's road network [41]. While similar security scheduling problems have been addressed in existing literature, the challenge of scheduling in networked domains with varying target importance remains largely unsolved [42] [43]. frames the network security problem as an attacker-defender zero-sum game, where both players have exponentially large strategy spaces. To tackle this, the paper introduces novel, scalable techniques to address the complexity of security scheduling in such dynamic environments.

Intrusions are a major concern in computer network security, as unauthorized access can compromise the integrity, confidentiality, and availability of resources [44]. Intrusion Detection Systems (IDSs) have been developed to monitor network activities and alert administrators of potential attacks, utilizing techniques such as data mining, machine learning, and artificial intelligence [45] [46]. However, due to the high dimensionality of network data, applying these techniques can be time-consuming. applies a wrapper approach based on a genetic algorithm for feature selection and logistic regression for learning, aiming to optimize feature subsets for IDS [47] [48]. Experiments on the KDD99 and UNSW-NB15 datasets are conducted, using decision tree classifiers to evaluate the performance, and results are compared with other feature selection methods to assess the effectiveness of the proposed approach [49] [50].

A supervised intrusion detection system learns from past attack examples to detect new threats, and using Artificial Neural Network (ANN)-based detection helps reduce false positives and negatives. proposes a developed learning model for fast learning networks (FLN) based on Particle Swarm Optimization (PSO), named PSO-FLN [51]. The model is applied to intrusion detection using the KDD99 dataset and compared with various meta-heuristic algorithms for training extreme learning machines and FLN classifiers [52] [53]. The results show that PSO-FLN outperforms other learning approaches in terms of testing accuracy, demonstrating its effectiveness in intrusion detection.

Authentication is crucial in wireless sensor networks (WSNs) for securing unattended environments. Das proposed a hash-based authentication protocol that improves security against masquerade, stolen-verifier, replay, and guessing attacks, and addresses issues related to multiple logged-in users with the same login ID [54]. However, identifies a security weakness in Das's protocol regarding mutual authentication between users, gateway nodes, and sensor nodes [55] [56]. To address this, the paper proposes an improved protocol that enhances secrecy, ensuring legal users can securely operate a WSN in an insecure environment. Comparisons of security, computation, communication costs, and performance demonstrate that the proposed protocol is more suitable for high-security WSN applications.

AI and blockchain are transformative technologies that are set to fundamentally change how we live, work, and interact. summarizes existing efforts and explores the promising future of integrating these technologies, particularly in creating smart, decentralized, and secure systems [57] [58]. By combining the strengths of AI's decision-making capabilities with blockchain's transparency and security, this integration has the potential to revolutionize various sectors [59]. The authors aim to answer the question: How can these smart, decentralized systems benefit society, enhancing efficiency, trust, and innovation

Software-Defined Internet of Things (SD-IoT) networks benefit from centralized management and resource sharing, enhancing scalability and efficiency [60]. However, as these networks grow, they face significant security challenges, particularly in detecting unknown attacks. Traditional signature-based or behavior-based intrusion detection methods are inadequate for SD-IoT's dynamic environment. proposes an AI-based two-stage intrusion detection system empowered by software-defined technology [61] [62]. The system utilizes the Bat algorithm for feature selection and a Random Forest classifier with a weighted voting mechanism for flow classification. Experimental results demonstrate that the proposed solution selects more relevant features, achieving superior performance in classification with better accuracy and lower overhead compared to existing approaches.

The AI2, an analyst-in-the-loop security system that combines Analyst Intuition (AI) with state-of-the-art machine learning to create a comprehensive, end-to-end AI-driven solution [63]. The system includes four key components: a big data behavioral analytics platform, an outlier detection system, a feedback mechanism for security analysts, and a supervised learning module [64]. Validated with a real-world dataset of 3.6 billion log lines and 70.2 million entities, AI2 demonstrates its ability to defend against unseen attacks. The results show a 2.92× improvement in detection rates and a reduction in false positives by over 5× in unsupervised outlier analysis.

The AI2, the first scalable and sound analyzer for deep neural networks that can automatically prove safety properties, such as robustness, for real-world networks like convolutional neural networks (CNNs) [65]. Leveraging classic abstract interpretation techniques, AI2 uses abstract transformers to model the behavior of fully connected and convolutional layers with ReLU activations and max pooling layers. AI2 has been fully implemented and evaluated on 20 neural networks, demonstrating its precision in proving useful specifications, such as robustness, and its ability to certify state-of-the-art defenses. Compared to existing symbolic analysis methods, AI2 is significantly faster and can handle deep convolutional networks, which were previously beyond the reach of existing analyzers.

The explored various machine learning algorithms and their effectiveness in network intrusion detection, highlighting how feature selection and classifier optimization are critical in improving the detection accuracy [66]. This work emphasizes the need for intelligent systems capable of adapting to dynamic network environments, which is a key aspect of our proposed AI-driven IDS framework.

The examined the application of AI, particularly deep learning, in securing network infrastructures. His study demonstrated the potential of deep neural networks (DNNs) in detecting both known and unknown intrusions [67]. This aligns with the core objectives of our framework, where deep learning models are leveraged for anomaly detection in network traffic.

The focused on the integration of AI techniques in cybersecurity, proposing an automated framework for the detection and mitigation of network-based attacks [68]. His work emphasizes the necessity of using advanced AI models for real-time threat detection, a concept that resonates with our approach to enhance intrusion detection with AI-powered techniques.

The concept of smart security systems that utilize AI and machine learning for adaptive intrusion detection. By applying unsupervised learning to identify patterns in network traffic, Morrow's research laid the groundwork for the anomaly detection methods incorporated into our IDS framework [69].

The role of deep learning in improving the accuracy and efficiency of IDS systems, especially in handling large datasets [70]. His work highlights the importance of using AI to reduce false positives and negatives in network security, which is a challenge addressed by our proposed solution.

A hybrid IDS framework combining both machine learning and AI-based techniques to identify anomalies and attacks [71]. Shetty's work aligns with the proposed framework’s goal of integrating AI models, including neural networks, for more effective intrusion detection.

A novel approach to intrusion detection by combining traditional signature-based methods with machine learning algorithms. examined the performance of neural network models in detecting advanced persistent threats (APTs) and cyber-attacks, underlining their ability to learn from network traffic patterns [72]. This research reinforces the importance of deep learning models in effectively addressing the evolving nature of cyber threats, a key objective of our framework.

A multi-layered security model that integrates deep learning for detecting intrusions at various network layers [73]. This multi-tiered approach is closely related to the multi-stage detection system proposed in our work, which aims to improve the robustness of network security.

The further explored the application of AI and machine learning in improving the scalability of IDS. proposed a deep learning-based approach for real-time anomaly detection in large-scale networks, emphasizing the use of AI in detecting complex attacks [74]. This work highlights the need for real-time processing in intrusion detection, a feature that is incorporated into our AI-driven IDS framework.

The focused on using reinforcement learning to optimize intrusion detection systems [75]. The adaptive learning nature of reinforcement learning provides a flexible approach to dynamic attack scenarios, which is one of the core components of our proposed solution.

The role of hybrid AI models in enhancing the effectiveness of IDS. His work demonstrates that combining AI with traditional methods leads to improved detection capabilities, a concept that is reflected in the hybrid approach used in our framework [76]. Proposed a scalable and robust IDS framework using AI-based algorithms for attack prediction and detection. Emphasized the use of deep learning models for the detection of sophisticated and previously unknown cyber-attacks [77]. Wang's research highlights the strengths of deep learning in handling complex patterns, which is one of the key features of the IDS framework we propose.

3 METHODOLOGY

This Figure 1 illustrates the process of an Intrusion Detection System (IDS) using deep learning techniques. The first step, Data Collection, gathers network traffic or activity data. The collected data is then Preprocessed to clean and normalize it. Next, Feature Extraction using an Autoencoder helps reduce the dimensionality of the data and capture essential patterns. These extracted features are then passed to an LSTM (Long Short-Term Memory) model for Classification, where the system classifies the data as either Detect (indicating an intrusion) or Not-Detect (indicating no intrusion). Finally, Performance Metrics are evaluated to assess the effectiveness of the intrusion detection system.

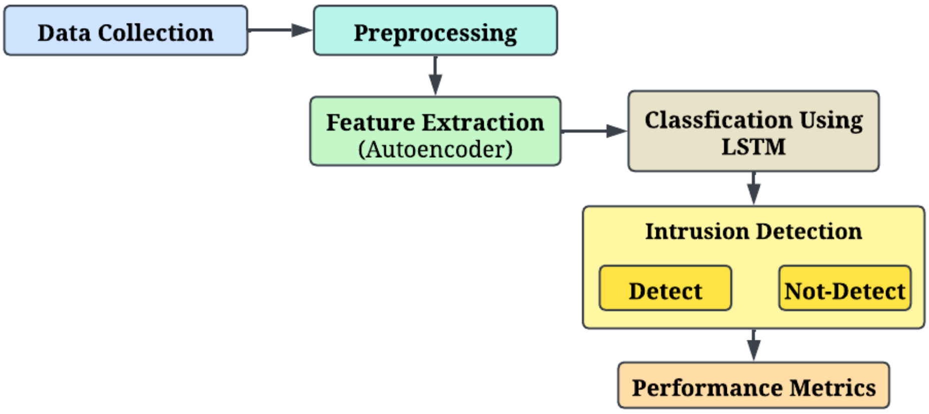

Figure 1: AI-Driven IDS with Autoencoder and LSTM

3.1 DATA COLLECTION

Data collection is the first step in any Intrusion Detection System (IDS), where network traffic is captured from multiple sources like firewalls, intrusion detection systems (IDS), and routers. The data typically includes various types of network activity, both normal, expected traffic and malicious intrusions, unauthorized access attempts, DoS attack. Capturing raw traffic data is crucial for providing a comprehensive view of network operations and any potential threats. This data can include attributes such as IP addresses, protocol types, packet sizes, timestamps, and service requests. The richness of data from these sources helps to create a robust dataset for detecting intrusions based on network behavior patterns.

3.2 PREPROCESSING

Preprocessing is a critical step that ensures the collected data is clean, normalized, and ready for deep learning models. During preprocessing, the data is first cleaned to remove any corrupt or incomplete entries. Handling missing values might involve techniques such as imputation or removing rows with incomplete information. Numerical data, like packet size or duration, is normalized to ensure consistency in the dataset and prevent certain features from dominating the analysis. Additionally, categorical features, such as protocol type or service name, are encoded into a numerical format using techniques like one-hot encoding. Preprocessing ensures that the dataset is in an optimal format for deep learning algorithms, which are sensitive to data inconsistencies and scale.

3.3 FEATURE EXTRACTION

Feature extraction using Autoencoders is a powerful technique for reducing the dimensionality of the data while retaining its important features. Autoencoders are unsupervised neural networks that aim to learn a compressed, low-dimensional representation of the input data. The encoder part of the network learns to compress the data into a dense code, while the decoder reconstructs the original data from this compressed representation. The quality of the reconstruction is crucial, and any large reconstruction errors often signal an anomaly, such as an intrusion. This method helps identify relevant patterns in network traffic that can be used for anomaly detection, even in the absence of labeled data, making it especially useful for detecting previously unseen attack patterns. In an Autoencoder, the model learns to compress data into a lower-dimensional space and reconstruct it. The Reconstruction Error EEE is often used to measure how well the model performs

$$E = \frac{1}{n}\sum_{i=1}^{n} \|x_i - \hat{x}_i\|^2 \quad (1)$$

Were, x_i is the original data point, $\hat{x}_i$ is the reconstructed data point from the Autoencoder, n is the number of data points, $\|x_i - \hat{x}_i\|^2$ is the squared Euclidean distance between the original and reconstructed values.

3.4 CLASSIFICATION USING LSTM

After feature extraction, the next step involves classifying the network traffic data using an LSTM (Long Short-Term Memory) network, a type of recurrent neural network (RNN) that is particularly effective at learning from sequential data. LSTM is ideal for intrusion detection in networks as it can model temporal dependencies in the data, such as traffic patterns over time. By capturing long-range dependencies, LSTM can recognize recurring attack patterns, such as DDoS attacks, brute force attempts, or malware propagation, which manifest as sequences of network events. The LSTM is trained to differentiate between normal network behavior and malicious activity by learning the typical flow of data over time. For classification using LSTM, the Cross-Entropy Loss function is commonly used as the objective function during training

$$L = -\sum_{i=1}^{n} [y_i \log(\hat{y}_i) + (1 - y_i)\log(1 - \hat{y}_i)] \quad (2)$$

Were, L is the loss, y_i is the true label, $\hat{y}_i$ is the predicted probability of an intrusion, n is the number of instances in the dataset.

3.5 INTRUSION DETECTION

The classification step involves feeding the features extracted by the Autoencoder into the LSTM model for final classification. Based on the temporal patterns recognized by the LSTM, the system outputs one of two results: Detect or Not-Detect. A Detect outcome indicates that the system has identified an intrusion or abnormal behavior, such as a network attack or unauthorized access. A Not-Detect result signifies that the traffic pattern is consistent with normal network operations. The ability to classify network traffic in real-time allows for prompt responses to security threats, minimizing the damage caused by intrusions. This detection process is the core function of the IDS, ensuring that any malicious activity is flagged as soon as it occurs.

4 RESULT AND DISCUSSION

The proposed AI-driven Intrusion Detection System (IDS) utilizing Autoencoders and LSTM networks demonstrated promising results in detecting both known and novel network intrusions. The loss and accuracy curves showed that the model quickly learned the key patterns in the data, with a sharp decrease in loss and rapid improvement in accuracy, stabilizing early in the training process. However, this behavior indicated potential overfitting, suggesting that while the model achieved high accuracy and low loss, further improvement could be achieved with better regularization or more diverse data. The ROC curve indicated that the classifier performed better than random guessing, but there was still room for enhancement in balancing true positive and false positive rates. These findings emphasize the need for refining the model to improve generalization and enhance its ability to detect evolving attack patterns in real-world applications.

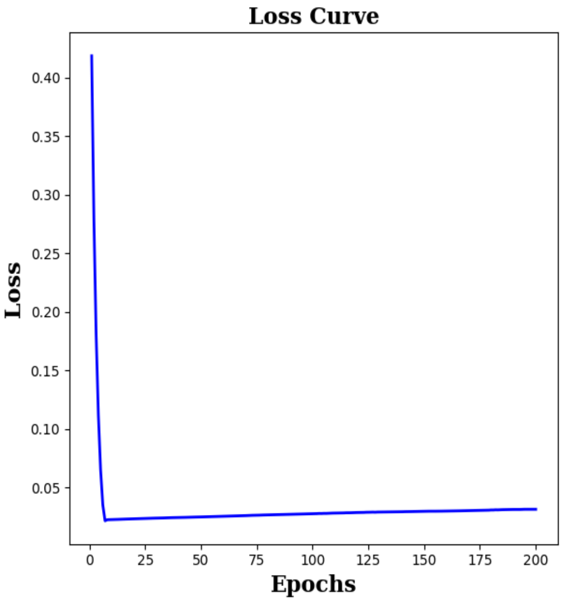

Figure 2: Loss Curve

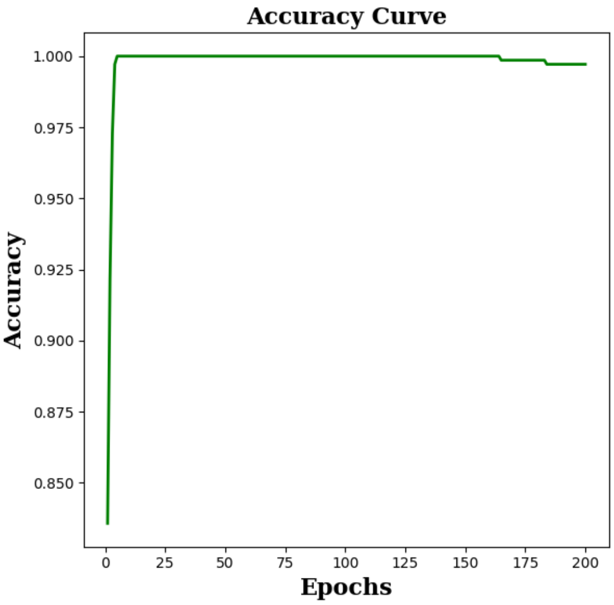

Figure 3: Accuracy Curve

This graph displays the Figure 2 and the Figure 3 across 200 epochs of training. Initially, the Loss Curve shows a sharp decline, indicating the model is quickly learning and improving its predictions. However, after a certain point, the loss plateaus at a low value, suggesting that the model has reached a stable state and further training provides minimal improvements. Similarly, the Accuracy Curve shows a rapid increase, quickly reaching nearly 100%, after which it stabilizes. This suggests the model has learned the key patterns in the data, with little to no further improvement. The behavior of both curves indicates the model has likely overfit to the training data, achieving high accuracy and low loss early on. This suggests the model may have reached its optimal state too soon, highlighting a need for better regularization or more diverse data to prevent overfitting and improve generalization.

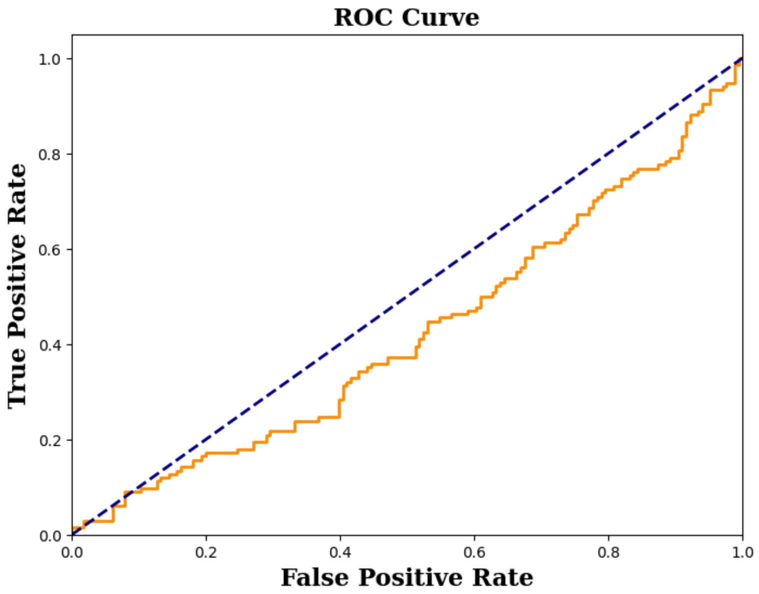

Figure 4: ROC Curve

This Figure 4 represents the ROC Curve of a binary classifier, with the x-axis showing the False Positive Rate (FPR) and the y-axis showing the True Positive Rate (TPR). The orange curve indicates the classifier's performance, where a higher curve closer to the top-left corner suggests better performance. The dashed blue line represents random guessing, and the classifier's curve is above it, showing some predictive power. However, the curve's shape indicates room for improvement, as the model doesn't achieve a significantly high TPR while maintaining a low FPR. The overall performance can be evaluated by calculating the AUC (Area Under the Curve), which reflects how well the model discriminates between classes.

5 CONCLUSIONS

This study demonstrates the effectiveness of an AI-driven Intrusion Detection System that integrates Autoencoders and LSTM networks to address the limitations of traditional IDS. The Autoencoders assist in unsupervised anomaly detection, while LSTM networks leverage temporal dependencies in network traffic to identify attack patterns. The results show promising detection capabilities, with the system achieving high accuracy and a strong reduction in loss. However, the model exhibited signs of overfitting, suggesting the need for better regularization techniques or more diverse training data. The system's real-time processing capabilities, bolstered by cloud computing, ensure it can efficiently handle large volumes of network traffic. In future work, improvements in model generalization and interpretability will be crucial to enhance the system's applicability in real-world environments.

REFERENCE

[1] Shenfield, A., Day, D., & Ayesh, A. (2018). Intelligent intrusion detection systems using artificial neural networks. Ict Express, 4(2), 95-99.

[2] Bobba, J., & Prema, R. (2018). Secure financial data management using Twofish encryption and cloud storage solutions. International Journal of Computer Science Engineering Techniques, 3(4), 10–16.

[3] Ali, M. H., Al Mohammed, B. A. D., Ismail, A., & Zolkipli, M. F. (2018). A new intrusion detection system based on fast learning network and particle swarm optimization. IEEE Access, 6, 20255-20261.

[4] Gehr, T., Mirman, M., Drachsler-Cohen, D., Tsankov, P., Chaudhuri, S., & Vechev, M. (2018, May). Ai2: Safety and robustness certification of neural networks with abstract interpretation. In 2018 IEEE symposium on security and privacy (SP) (pp. 3-18). IEEE.

[5] Musham, N. K., & Pushpakumar, R. (2018). Securing cloud infrastructure in banking using encryption-driven strategies for data protection and compliance. International Journal of Computer Science Engineering Techniques, 3(5), 33–39.

[6] Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data. Network Security, 2012(12), 5-8.

[7] Bose, B. K. (2017). Artificial intelligence techniques in smart grid and renewable energy systems—some example applications. Proceedings of the IEEE, 105(11), 2262-2273.

[8] Li, R., Zhao, Z., Zhou, X., Ding, G., Chen, Y., Wang, Z., & Zhang, H. (2017). Intelligent 5G: When cellular networks meet artificial intelligence. IEEE Wireless communications, 24(5), 175-183.

[9] Allur, N. S., & Hemnath, R. (2018). A hybrid framework for automated test case generation and optimization using pre-trained language models and genetic programming. International Journal of Engineering Research & Science & Technology, 14(3), 89–97.

[10] Jiang, C., Zhang, H., Ren, Y., Han, Z., Chen, K. C., & Hanzo, L. (2016). Machine learning paradigms for next-generation wireless networks. IEEE Wireless Communications, 24(2), 98-105.

[11] Wang, X., Li, X., & Leung, V. C. (2015). Artificial intelligence-based techniques for emerging heterogeneous network: State of the arts, opportunities, and challenges. IEEE Access, 3, 1379-1391.

[12] Basani, D. K. R., & RS, A. (2018). Integrating IoT and robotics for autonomous signal processing in smart environment. International Journal of Computer Science and Information Technologies, 6(2), 90–99. ISSN 2347–3657.

[13] Soleymani, S. A., Abdullah, A. H., Zareei, M., Anisi, M. H., Vargas-Rosales, C., Khan, M. K., & Goudarzi, S. (2017). A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing. IEEE Access, 5, 15619-15629.

[14] Chuang, M. C., & Lee, J. F. (2013). TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks. IEEE systems journal, 8(3), 749-758.

[15] Gudivaka, R. L., & Mekala, R. (2018). Intelligent sensor fusion in IoT-driven robotics for enhanced precision and adaptability. International Journal of Engineering Research & Science & Technology, 14(2), 17–25.

[16] Dirican, C. (2015). The impacts of robotics, artificial intelligence on business and economics. Procedia-Social and Behavioral Sciences, 195, 564-573.

[17] Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). N-baiot—network-based detection of iot botnet attacks using deep autoencoders. IEEE Pervasive Computing, 17(3), 12-22.

[18] Jadon, R., & RS, A. (2018). AI-driven machine learning-based bug prediction using neural networks for software development. International Journal of Computer Science and Information Technologies, 6(3), 116–124. ISSN 2347–3657.

[19] Gonzales, D., Kaplan, J. M., Saltzman, E., Winkelman, Z., & Woods, D. (2015). Cloud-trust—A security assessment model for infrastructure as a service (IaaS) clouds. IEEE Transactions on Cloud Computing, 5(3), 523-536.

[20] Chiang, M., Ha, S., Risso, F., Zhang, T., & Chih-Lin, I. (2017). Clarifying fog computing and networking: 10 questions and answers. IEEE Communications Magazine, 55(4), 18-20.

[21] Ramar, V. A., & Rathna, S. (2018). Implementing Generative Adversarial Networks and Cloud Services for Identifying Breast Cancer in Healthcare Systems. Indo-American Journal of Life Sciences and Biotechnology, 15(2), 10-18.

[22] Feng, W., Zhang, Q., Hu, G., & Huang, J. X. (2014). Mining network data for intrusion detection through combining SVMs with ant colony networks. Future Generation Computer Systems, 37, 127-140.

[23] Hengstler, M., Enkel, E., & Duelli, S. (2016). Applied artificial intelligence and trust—The case of autonomous vehicles and medical assistance devices. Technological Forecasting and Social Change, 105, 105-120.

[24] Pulakhandam, W., & Bharathidasan, S. (2018). Leveraging AI and cloud computing for optimizing healthcare and banking systems. International Journal of Mechanical Engineering and Computer Science, 6(1), 24–32.

[25] Feng, W., Zhang, Q., Hu, G., & Huang, J. X. (2014). Mining network data for intrusion detection through combining SVMs with ant colony networks. Future Generation Computer Systems, 37, 127-140.

[26] Amin, R., & Biswas, G. P. (2016). A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. Ad Hoc Networks, 36, 58-80.

[27] Kushala, K., & Rathna, S. (2018). Enhancing privacy preservation in cloud-based healthcare data processing using CNN-LSTM for secure and efficient processing. International Journal of Mechanical Engineering and Computer Science, 6(2), 119–127.

[28] Wang, B., Zheng, Y., Lou, W., & Hou, Y. T. (2015). DDoS attack protection in the era of cloud computing and software-defined networking. Computer Networks, 81, 308-319.

[29] Wang, K., Gou, C., Duan, Y., Lin, Y., Zheng, X., & Wang, F. Y. (2017). Generative adversarial networks: introduction and outlook. IEEE/CAA Journal of Automatica Sinica, 4(4), 588-598.

[30] Jayaprakasam, B. S., & Hemnath, R. (2018). Optimized microgrid energy management with cloud-based data analytics and predictive modelling. International Journal of Mechanical Engineering and Computer Science, 6(3), 79–87.

[31] Liu, X., Zhang, Y., Wang, B., & Yan, J. (2012). Mona: Secure multi-owner data sharing for dynamic groups in the cloud. IEEE transactions on parallel and distributed systems, 24(6), 1182-1191.

[32] Gudivaka, B. R., & Palanisamy, P. (2018). Enhancing software testing and defect prediction using Long Short-Term Memory, robotics, and cloud computing. International Journal of Mechanical Engineering and Computer Science, 6(1), 33–42.

[33] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE transactions on emerging topics in computational intelligence, 2(1), 41-50.

[34] Sood, S. K. (2012). A combined approach to ensure data security in cloud computing. Journal of Network and Computer Applications, 35(6), 1831-1838.

[35] Ayyadurai, R., & Vinayagam, S. (2018). Transforming customer experience in banking with cloud-based robo-advisors and chatbot integration. International Journal of Marketing Management, 6(3), 9–17.

[36] Yuan, J., & Yu, S. (2013). Privacy preserving back-propagation neural network learning made practical with cloud computing. IEEE Transactions on Parallel and Distributed Systems, 25(1), 212-221.

[37] Tuptuk, N., & Hailes, S. (2018). Security of smart manufacturing systems. Journal of manufacturing systems, 47, 93-106.

[38] Natarajan, D. R., & Kurunthachalam, A. (2018). Efficient Remote Patient Monitoring Using Multi-Parameter Devices and Cloud with Priority-Based Data Transmission Optimization. Indo-American Journal of Life Sciences and Biotechnology, 15(3), 112-121.

[39] Yang, T. J., Chen, Y. H., Emer, J., & Sze, V. (2017, October). A method to estimate the energy consumption of deep neural networks. In 2017 51st asilomar conference on signals, systems, and computers (pp. 1916-1920). IEEE.

[40] Lo, N. W., & Tsai, J. L. (2015). An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings. IEEE Transactions on Intelligent Transportation Systems, 17(5), 1319-1328.

[41] Vasamsetty, C., & Rathna, S. (2018). Securing digital frontiers: A hybrid LSTM-Transformer approach for AI-driven information security frameworks. International Journal of Computer Science and Information Technologies, 6(1), 46–54. ISSN 2347–3657.

[42] Kato, N., Fadlullah, Z. M., Mao, B., Tang, F., Akashi, O., Inoue, T., & Mizutani, K. (2016). The deep learning vision for heterogeneous network traffic control: Proposal, challenges, and future perspective. IEEE wireless communications, 24(3), 146-153.

[43] Pajouh, H. H., Javidan, R., Khayami, R., Dehghantanha, A., & Choo, K. K. R. (2016). A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks. IEEE Transactions on Emerging Topics in Computing, 7(2), 314-323.

[44] Valivarthi, D. T., & Hemnath, R. (2018). Cloud-integrated wavelet transform and particle swarm optimization for automated medical anomaly detection. International Journal of Engineering Research & Science & Technology, 14(1), 17–27.

[45] Liu, J., Kong, X., Xia, F., Bai, X., Wang, L., Qing, Q., & Lee, I. (2018). Artificial intelligence in the 21st century. Ieee Access, 6, 34403-34421.

[46] Vučinić, M., Tourancheau, B., Rousseau, F., Duda, A., Damon, L., & Guizzetti, R. (2015). OSCAR: Object security architecture for the Internet of Things. Ad Hoc Networks, 32, 3-16.

[47] Gollavilli, V. S. B., & Thanjaivadivel, M. (2018). Cloud-enabled pedestrian safety and risk prediction in VANETs using hybrid CNN-LSTM models. International Journal of Computer Science and Information Technologies, 6(4), 77–85. ISSN 2347–3657.

[48] Jiang, T., Fang, H., & Wang, H. (2018). Blockchain-based internet of vehicles: Distributed network architecture and performance analysis. IEEE Internet of Things Journal, 6(3), 4640-4649.

[49] Kadiyala, B., & Arulkumaran, G. (2018). Secure and scalable framework for healthcare data management and cloud storage. International Journal of Engineering & Science Research, 8(4), 1–8.

[50] Mármol, F. G., & Pérez, G. M. (2012). TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. Journal of network and computer applications, 35(3), 934-941.

[51] Friedberg, I., Skopik, F., Settanni, G., & Fiedler, R. (2015). Combating advanced persistent threats: From network event correlation to incident detection. Computers & Security, 48, 35-57.

[52] Ubagaram, C., & Mekala, R. (2018). Enhancing data privacy in cloud computing with blockchain: A secure and decentralized approach. International Journal of Engineering & Science Research, 8(3), 226–233.

[53] Botta, A., Dainotti, A., & Pescapé, A. (2012). A tool for the generation of realistic network workload for emerging networking scenarios. Computer Networks, 56(15), 3531-3547.

[54] Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2018). Artificial intelligence and the 'good society': the US, EU, and UK approach. Science and engineering ethics, 24, 505-528.

[55] Vallu, V. R., & Palanisamy, P. (2018). AI-driven liver cancer diagnosis and treatment using cloud computing in healthcare. Indo-American Journal of Life Sciences and Biotechnology, 15(1).

[56] Coppolino, L., D'Antonio, S., Mazzeo, G., & Romano, L. (2017). Cloud security: Emerging threats and current solutions. Computers & Electrical Engineering, 59, 126-140.

[57] Lai, C., Li, H., Lu, R., & Shen, X. S. (2013). SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks. Computer Networks, 57(17), 3492-3510.

[58] Sareddy, M. R., & Jayanthi, S. (2018). Temporal convolutional network-based shortlisting model for sustainability of human resource management. International Journal of Applied Sciences, Engineering, and Management, 12(1).

[59] Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. Journal of big data, 5(1), 1-18.

[60] Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. Decision support systems, 86, 13-23.

[61] Parthasarathy, K., & Prasaath, V. R. (2018). Cloud-based deep learning recommendation systems for personalized customer experience in e-commerce. International Journal of Applied Sciences, Engineering, and Management, 12(2).

[62] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation computer systems, 28(3), 583-592.

[63] Azad, H. B., Mekhilef, S., & Ganapathy, V. G. (2014). Long-term wind speed forecasting and general pattern recognition using neural networks. IEEE Transactions on sustainable energy, 5(2), 546-553.

[64] Gollapalli, V. S. T., & Arulkumaran, G. (2018). Secure e-commerce fulfilments and sales insights using cloud-based big data. International Journal of Applied Sciences, Engineering, and Management, 12(3).

[65] Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.

[66] Bassily, R., Ekrem, E., He, X., Tekin, E., Xie, J., Bloch, M. R., ... & Yener, A. (2013). Cooperative security at the physical layer: A summary of recent advances. IEEE Signal Processing Magazine, 30(5), 16-28.

[67] Chauhan, G. S., & Palanisamy, P. (2018). Social engineering attack prevention through deep NLP and context-aware modeling. Indo-American Journal of Life Sciences and Biotechnology, 15(1).

[68] Berman, M., Chase, J. S., Landweber, L., Nakao, A., Ott, M., Raychaudhuri, D., ... & Seskar, I. (2014). GENI: A federated testbed for innovative network experiments. Computer Networks, 61, 5-23.

[69] O'Neill, M. (2016). Insecurity by design: Today's IoT device security problem. Engineering, 2(1), 48-49.

[70] Nippatla, R. P., & Palanisamy, P. (2018). Enhancing cloud computing with eBPF powered SDN for secure and scalable network virtualization. Indo-American Journal of Life Sciences and Biotechnology, 15(2).

[71] Ansari, R. I., Chrysostomou, C., Hassan, S. A., Guizani, M., Mumtaz, S., Rodriguez, J., & Rodrigues, J. J. (2017). 5G D2D networks: Techniques, challenges, and future prospects. IEEE Systems Journal, 12(4), 3970-3984.

[72] Saied, A., Overill, R. E., & Radzik, T. (2016). Detection of known and unknown DDoS attacks using Artificial Neural Networks. Neurocomputing, 172, 385-393.

[73] Garikipati, V., & Palanisamy, P. (2018). Quantum-resistant cyber defence in nation-state warfare: Mitigating threats with post-quantum cryptography. Indo-American Journal of Life Sciences and Biotechnology, 15(3).

[74] Pasqualetti, F., Dorfler, F., & Bullo, F. (2015). Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems. IEEE Control Systems Magazine, 35(1), 110-127.

[75] Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. Procedia Computer Science, 125, 691-697.

[76] Ganesan, S., & Kurunthachalam, A. (2018). Enhancing financial predictions using LSTM and cloud technologies: A data-driven approach. Indo-American Journal of Life Sciences and Biotechnology, 15(1).

[77] Lui, A., & Lamb, G. W. (2018). Artificial intelligence and augmented intelligence collaboration: regaining trust and confidence in the financial sector. *Information & Communications Technology Law*, *27*(3), 267-283.