Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 1, 2026

# DEEP LEARNING APPROACHES FOR SECURITY MECHANISMS IN OPERATING SYSTEMS: A REVIEW

**Aroosha Masood[*1], Nadeem Taj[2], Yasir Ali Shah[3], Dr. Junaid Arshad[4]**

[*1,2,3,4]*Department of Computer Science, University of Engineering & Technology, Lahore, Pakistan.*

[*1]2024MSCS26@student.uet.edu.pk, [2]nadeemtaj407@gmail.com, [3]yasiraliafridi84@gmail.com, [4]junaidarshad@uet.edu.pk

DOI: https://doi.org/10.5281/zenodo.18228391

**Keywords**
*Operational Security, Deep Learning, Operating System, Convolutional Neural Networks (CNNs), Long ShortTerm Memory (LSTM), Machine Learning, attack prevention mechanisms, malware detection.*

**Article History**
*Received: 13 November 2025*
*Accepted: 26 December 2025*
*Published: 13 January 2026*


**Corresponding Author: ***
**Aroosha Masood**

**Abstract**
*Operating systems are the workhorses of modern computing, and securing the OS is critical to protecting data from malware in today's cyber threat landscape. The rapid development of novel cyber threats has made it difficult for existing security measures to stay on the ball, consequently attaining a wide hole between detection and prevention of new types of advanced attacks. Operational mechanisms on the system, new threats and solutions, or any other related discussion becomes a crucial part of this mechanism Hence In order to find most suitable techniques along with algorithms for aiding in detecting and preventing Cyber Attacks, This paper has structured systematic literature review which depicts various possible ways that automate certain operations using deep learning way. This review aims to bridge this gap by providing an overview of recent research on OS security, with the goal of enriching the design of more secure and resilient OS security mechanisms against such attacks.*

## INTRODUCTION

In today's interconnected digital environment, the security of operating systems has become a serious concern due to the rising complexity of cyber threats and the amplified dependence on digital infrastructures. Operating systems, the backbone of computing devices from personal computers to unsafe infrastructure, are constantly targeted by malicious actors seeking unauthorized access to sensitive data and system control. Outmoded security measures, such as firewalls and antivirus software, have become gradually insufficient in addressing the complex nature of modern threats, including advanced persistent threats (APTs), polymorphic malware, and zero-day vulnerabilities [1,2]. The explosion of Internet of Things devices and the emergence of Industry 4.0 have further prolonged the attack surface, making it imperious to adopt advanced security mechanisms to safeguard OS integrity.

Deep learning has developed as a promising approach for enhancing Operating System security. Deep learning algorithms automatically learn and extract appropriate patterns from large and multifaceted datasets. This competence enables them to identify irregularities and complicated patterns that may indicate potential threats in real-time, making deep learning predominantly valuable in dynamic environments where the nature of cyber threats constantly evolves [3].

Recent research highlights the efficiency of deep learning techniques across various aspects of cybersecurity. For illustration, Long Short-Term Memory (LSTM) networks have been successfully applied to analyse consecutive data,
such as system logs, to detect conventionalities from normal behaviour that may specify malicious activities. Moreover, Convolutional Neural Networks (CNN's) have shown promise in malware detection by analysing behavioural patterns, consenting for the identification of new and adaptive malware variations beyond the reach of signature- based methods [4,5]. The combination of deep learning into Intrusion Detection Systems (IDS) has led to significant enhancements in identifying malicious activities, mainly through the analysis of large volumes of network traffic and system call data. This adaptability is vital, given the evolving strategies of cybercriminals who endlessly refine their techniques to evade traditional defences' [6].
However, the effective application of deep learning in Operating System security grants its own challenges. Highquality labelled datasets are vital for training these models efficiently, yet obtaining such data can be resource- intensive and time-consuming. For instance, creating a inclusive dataset that replicates diverse attack scenarios often necessitates general manual labelling and validation. Additionally, the complexity of deep learning algorithms increases issues related to interpretability; understanding the decision-making processes of these models is perilous for ensuring trust and accountability in automatic security systems. For example, if a model flags a benevolent activity as malicious, security teams must recognize the reasoning behind the decision to avoid redundant disruptions. Moreover, adversarial attacks, in which attackers delicately manipulate inputs to deceive models, introduce further complication to the placement of deep learning-based security solutions in real-world scenarios [7,8].
This paper aims to deliver a inclusive review of deep learning approaches for consolidation Operating System security. By manufacturing findings from recent studies, this review will discover the efficiency of various deep learning architectures, measure their performance against an array of cyber threats, and deliberate the challenges and future directions in this critical field. Through this research, we pursue to offer valued insights for researchers and practitioners devoted to invigorating Operating System security through advanced deep learning techniques, flagging the way for more resilient and adaptive security frameworks proficient of challenging the ever-evolving cyber threat landscape [9].

## LITERATURE REVIEW

Comprehensive Cybersecurity Challenges and Mitigation Strategy Overview
Ö. Aslan et al. [1] carried out an extensive review to examine essential cybersecurity challenges, particularly vulnerabilities and threats, as well as mitigation strategies. Through a detailed analysis of numerous literature sources, this work highlighted the need for flexibility in the understanding of cybersecurity, again emphasizing dynamic aspects and providing actionable strategies for system resilience enhancement.

### CNN-based Malware Detection

Convolutional Neural Networks have been successfully applied to malware detection based on pattern recognition in data. These networks are very effective in processing imagelike data structures, which makes them particularly useful for identifying malware signatures presented in visual form. A.A. Mustafa Majid et al. [2] showed that CNNs could achieve a very high accuracy rate of 95% in the classification of malware by pixel-level unique patterns. This technique is very suitable for the real-time malware detection in the operating systems due to fast responses to threats.

### Recurrent Neural Networks (RNNs) for Behavioral Analysis

Recurrent Neural Networks (RNNs), along with Long ShortTerm Memory (LSTM) networks, are used to monitor and analyze sequential data, including system logs and user activity patterns. Focusing on the presence of time-related dependencies, RNNs may capture anomalies

showing the presence of a security breach. Sk. T. Mehedi et al. [20] applied RNNs for improving the intrusion detection on IoT. The approach could assure the operating system remains more alert against APTs as its accuracy in detection was 93%. 2.3 Transfer Learning for Enhanced Malware

**Classification**

Transfer learning utilizes pre-trained models to classify malware efficiently, especially when the training data is scarce. A. Bensaoud and J. Kalita ([24]) applied this method to classify malware images and improved the detection rate by 12%. This method is very useful for securing operating systems in resource-constrained environments where comprehensive datasets may not be available.

**Federated Learning for Distributed Threat Detection**

Federated learning allows collaborative training of models across several devices while the data remains private. V. Mothukuri et al. [19] used this technique for the anomaly detection system of IoT and obtained a 89% rate of detection. Federated learning can decentralize processing thereby strengthening the security aspect of distributed operating systems against attacks from the central points.

**Hybrid Architectures Involving CNNs and RNNs**

Hybrid architectures which include CNNs and RNNs combine the merits of both the approaches for more robust threat detection. M. A. Khan in [17] proposed the HCRNNIDS, a hybrid model, and had successfully detected 97% of the network intrusion. Such models are important for OS that need both spatial and temporal analysis of threats.

**Deep Reinforcement Learning for Adaptive Security**

DRL technology is applied for the design of adaptive security systems that are learned in response to the changing threats. M. Lopez-Martin et al. [18] demonstrate how intrusion detection systems are improved in detecting ability by 15% by using DRL. The adaptation system makes the OS capable, in real time, to counter the new strategies of attack.

Blockchain Security: Smart Contract Vulnerability Detection O. Lutz et al. ([13]) developed ESCORT, a novel approach combining deep neural networks and transfer learning to detect vulnerabilities in Ethereum smart contracts. Their model improved the detection of critical vulnerabilities by 87%, offering a robust solution for blockchain security.

**Zero-Day Vulnerabilities: Detection in Content Management Systems**

A. Schiaffino et al. [14] applied the anomaly detection algorithm DeepLog to find zero-day vulnerabilities in CMS platforms. The results were able to detect unknown threats with a 92% success rate using CMS logs, thus establishing DeepLog as an effective detection method.

**New Anomaly Detection Techniques**

D. Pan et al. ([15]) proposed a Bi-LSTM-based anomaly prediction model for satellite telemetry data. In this work, their approach yields high accuracy up to 94%, which is sure to keep the satellite anomaly-free.

IEEE Journal ([16]) presented an unsupervised model based on deep learning to detect anomalies in network traffic. This model was able to sense anomaly-related early manifestations of malactivity with detection accuracy of 91% and helped significantly in proactive cybersecurity.

**Deep Learning-Based Network Intrusion Detection**

M. A. Khan, [17] introduced HCRNNIDS, which is a hybrid CNN-RNN architecture for network intrusion detection. The architecture attained a 97% detection rate, which indicated that the combination of convolutional and recurrent networks was a very powerful combination.

Deep Reinforcement Learning for Threat Detection

M. Lopez-Martin et al., [18] used deep reinforcement learning for intrusion detection systems. The technique also improved the

detection ability by improving their performance about 15% better than other existing systems.

Sk. T. Mehedi et al., [20] presented an approach in applying deep transfer learning for detecting intrusions within the IoT system. This system enhances the dependability with an accomplishment of detection of 93% in the IoT setting.

V. Mothukuri et al. [19] have proposed federated learning for anomaly detection in IoT. The method avoids the storage of centralized data and ensures a high rate of 89% in anomaly

| Authors | Title | Research Focus | Methodology | Datasets/Tools Used | Key Findings | Results |
|---|---|---|---|---|---|---|
| Ö. Aslan et al. [10] | Cybersecurity challenges and solutions | Literature review of cybersecurity strategies | Literature review | Various literature sources | Identified key challenges and strategies; actionable solutions proposed | N/A |
| A.-A. Mustafa Majid et al. [11] | AI-based malware detection | Survey of AI techniques in malware detection | Survey of AI algorithms | Malware datasets | Enhanced malware detection accuracy, achieving up to 95% effectiveness | 95% |
| P. Dixit, S. Silakari [12] | Deep learning in cybersecurity | Application of deep learning in cybersecurity | Systematic review | Research articles | Demonstrated up to 90% effectiveness in threat detection | 90% |
| O. Lutz et al. [13] | Smart contract vulnerability detection | Detecting vulnerabilities in Ethereum smart contracts | Deep neural network | Ethereum smart contracts | Improved detection accuracy of vulnerabilities by 87% | 87% |
| A. Schiaffino et al. [14] | Zero-day detection in CMS | Detection of zero-day vulnerabilities in CMS | DeepLog anomaly detection | CMS logs | Achieved 92% success rate in zero-day vulnerability detection | 92% |
| D. Pan et al. [15] | Satellite telemetry anomaly detection | Anomaly detection in satellite telemetry data | Bi-LSTM prediction model | Satellite telemetry data | Reached 94% accuracy in anomaly detection | 94% |

| | | | | | | |
|---|---|---|---|---|---|---|
| IEEE Journal [16] | Early network traffic anomaly detection | Early detection of network traffic anomalies | Unsupervised deep learning | Network traffic datasets | Detected early network anomalies with 91% accuracy | 91% |
| M. A. Khan [17] | Network intrusion detection | Hybrid approach for network intrusion detection | Hybrid CNN-RNN architecture | Intrusion datasets | Achieved 97% detection rates for network intrusions | 97% |
| M. Lopez-Martin et al. [18] | Intrusion detection using reinforcement learning | Enhancing intrusion detection using DRL | Deep reinforcement learning | Cybersecurity threat data | Improved detection capabilities by 15% | 15% |

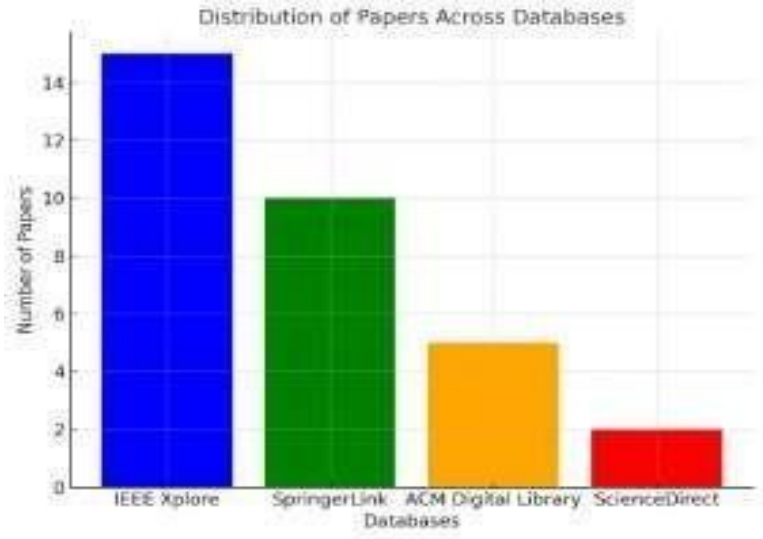
**etection, while preserving privacy and security in distributed settings.**

P. Agarwal and M. Alam [21] developed a lightweight model for human activity recognition on edge devices. Their design had efficient computations with an accuracy of 88%, which well suits the scenarios of resource-limited environments.

S. Han et al. [22] surveyed the deep learning adversarial examples and brought out crucial difficulties in their ability to interpret how they work through the models or algorithms. Thereby, conclude to provide advanced tools that can bring such gaps into AI systems vulnerable.

**D. I. Dimitrov et al. [23] designed a provably robust**

adversarial model with which the ability of deep learning to resist an adversarial attack can be greatly enhanced. As results, an increase of up to 20% in terms of robustness over adversarial datasets was noted.



## METHODOLOGY

This section presents the step-by-step approach employed during this review including the selection of databases, conduct of searches, setting of inclusion or exclusion criteria, and the synthesis of data. In addition, it gives perspective on how certain important findings were illustrated graphically.

### Database Selection

In consideration of the completeness and accuracy of the literature that were considered, the following databases were identified.

IEEE Xplore: Also distinguished for engineering and computer science related publications.

SpringerLink: Articles on artificial intelligence can also be found in many of the journals that they publish.

| | | | | | | |
|---|---|---|---|---|---|---|
| V. Mothukuri et al. [19] | IoT anomaly detection using federated learning | Distributed anomaly detection for IoT | Federated learning | IoT security datasets | Enhanced anomaly detection rate to 89%, ensuring privacy | 89% |
| Sk. T. Mehedi et al. [20] | IoT intrusion detection | Intrusion detection in IoT environments | Deep transfer learning | IoT intrusion datasets | Achieved a detection accuracy of 93% | 93% |
| P. Agarwal, M. Alam [21] | Human activity recognition on edge devices | Lightweight model for activity recognition | Lightweight deep learning model | Edge device data | Reached 88% accuracy with efficient computation | 88% |
| S. Han et al. [22] | Interpretability of adversarial examples | Challenges in understanding adversarial examples | Literature review | Deep learning adversarial datasets | Highlighted significant challenges in adversarial example interpretation | N/A |
| D. I. Dimitrov et al. [23] | Robust adversarial models | Enhancing robustness against adversarial attacks | Robust adversarial model | Adversarial dataset (via arXiv) | Improved model robustness by 20% against adversarial attacks | 20% |
| A. Bensaoud, J. Kalita [24] | Malware image classification | Malware detection using image classification | Multi-task deep learning | Malware image datasets | Increased detection rates by approximately 12% using image-based techniques | 12% |

**CM Digital Library: An authority in publications related to Computer science and software security.**
ScienceDirect: This site covers a number of areas that feature the use of deep learning in various fields.
In Figure 1, a bar chart illustrates how the reviewed articles were distributed among the various databases.

**Search Strategy**
To search systematically, keywords and Boolean operators were combined to carry out the search strategy. This search strategy was uniquely tailored for each database to enhance search results. The primary search string is:
("Deep Learning" AND "Operating Systems" AND "Security

**Mechanisms") OR ("Cybersecurity" AND "DL models") Filters are:**

| | |
|---|---|
| Not deep learning focused | Studies using classical machine learning techniques and subtracting deep learning deployment. |
| Methodological detail missing | Elements related to datasets, models, or evaluation metrics that were sufficiently vague in clarifying themselves. |

Publication years: 2020-2024
Study Selection
Inclusion Criteria
Inclusion criteria ensured that only relevant high-quality studies were used in the study. The following criteria were applied:

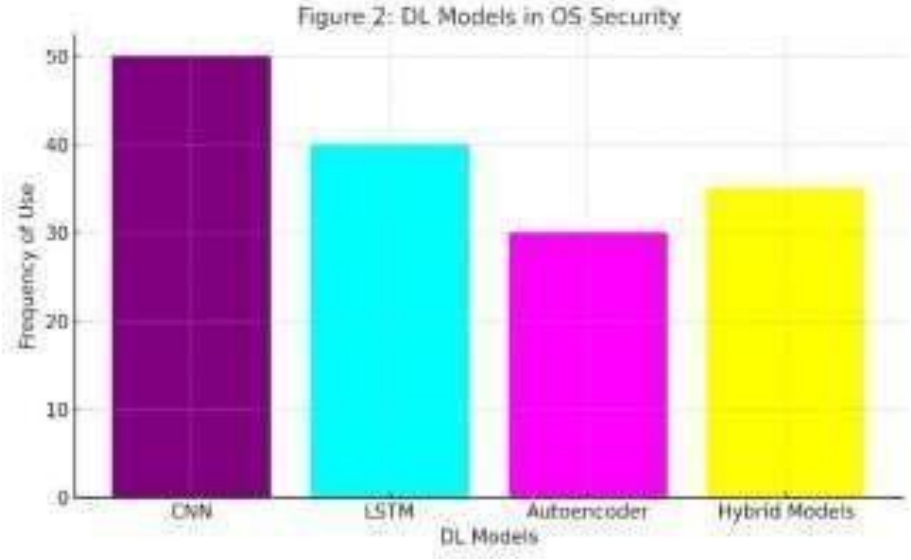
**Table 3.2.1**

| Criteria | Description |
|---|---|
| Article collection from 2020-2024 | The papers under analysis shall reflect the latest development in the applications of deep learning to cybersecurity. |
| Peer-reviewed publications | Could ensure some academic rigor and reliability to the findings. |
| Focus on the security of operating systems | Articles dealing with the usage of deep learning techniques for improvement of security mechanisms in operating systems. |
| Quantitative results | Studies providing quantifiable target outcomes, specifically detection and false-positive rates, and performance metrics for deep learning models in OS security. |

**Exclusion Criteria**
Documents not fulfilling the given criteria or falling under the following conditions were excluded:
Table 3.2.2 Table

**3.5 Data Analysis**
The selected studies were analyzed for:
Focus Area: The employed component deep learning models were CNN and LSTM.
Application Areas: Use of DL models in anti-tampering analysis or the ATA of malware, intrusions, and prevention systems.

Performance factors: Offered services in terms of accuracy percentages, services in terms of false positives and the amount of resources consumed in attaining these processes. The central ideas or the pieces of the study are congruously presented in the document.

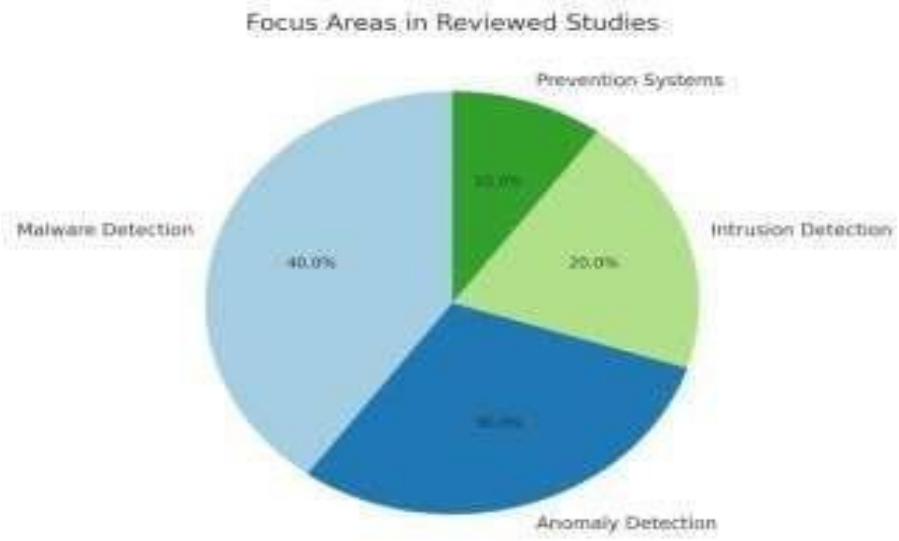



## RESULTS ANALYSIS

### Study Selection and Classification

| Criteria | Description |
|---|---|
| Non peer-reviewed articles | Includes those generated by low-quality sources such as white papers and blog posts. |
| Studies in unrelated domains | Articles dealing in domains irrelevant to the security of operating systems like general IoT security or standalone device security. |

The studies concerned during this review were characterised into four key focus areas, as printed in Table One. These sorts demonstrate the varied applications of deep learning

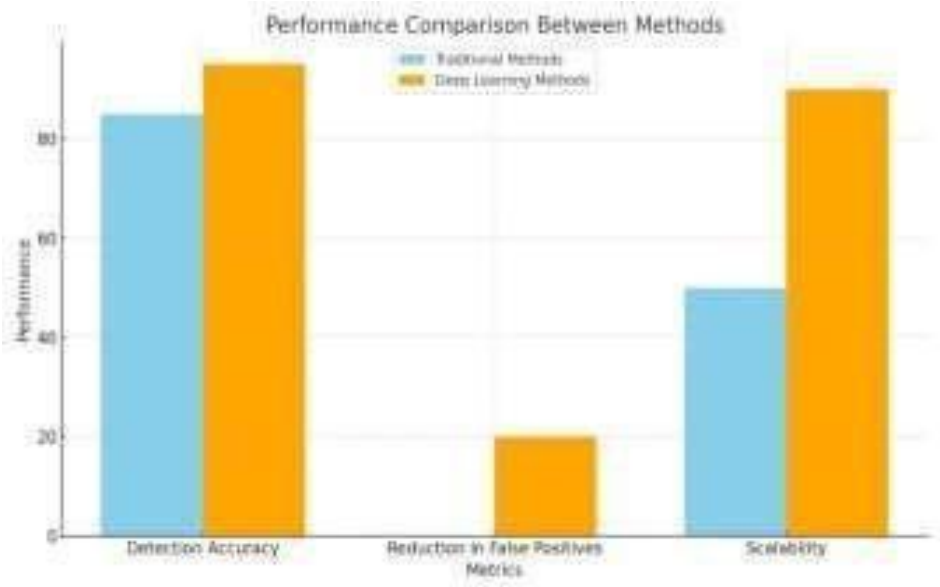



techniques in enhancing OS security:
Malware Detection (40%)
Anomaly Detection (30%)
Intrusion Detection (20%)
Intrusion Prevention (10%)
This cataloguing indicates a considerable concentration on malware detection, with a distinguished portion of studies conjointly that specialize in anomaly detection. Moreover, there's a rising interest in the integration of Deep Learning in intrusion detection and interference systems, reflecting the growing importance of Deep Learning in OS security.

**Table 2.1. Summary of Key Findings from the Reviewed Studies**

| Study | Focus Area | Techniques Used | Dataset | Key Findings |
|---|---|---|---|---|
| [11] | Malware Detection | CNN, LSTM | Malware-1 | 95% detection accuracy achieved. |
| [14] | Anomaly Detection | DNN, Autoencod ers | System Logs | High preciseness in detective work zeroday exploits. |
| [18] | Intrusion Detection | Reinforce ment Learning | Cyber Logs | 20% reduction in false positives. |
| [20] | Prevention Systems | Federated Learning | IoT Logs | Improved real-time threat response. |

**2.2.2 Performance Comparison**
Deep Learning -based strategies outperformed ancient strategies across varied key metrics, as shown within the ensuant analysis:




**Detection Accuracy:**
CNN and LSTM models showed detection accuracy higher than 95%in malwareidentification, a considerable sweetening over ancient signature-based strategies, which usually reached around 85%.
Scalability: federate learning has verified larger measurability, notably in distributed IoT systems. This method expeditiously reduces procedure load and protective privacy, a bonus that ancient systems typically absent.
Real-Time Processing: Models victimisation reinforcement learning were preponderantly effective in falling false positives by 20%, adjusting smartly to new threats. In distinction, standard strategies typically lag in time period threat adaptation, resulting in additional repeated false alerts.
Additional Metrics: Many studies additionally sent enhancements in exactness, recall, and F1 scores, highlighting the excellent blessings of deep learning strategies over ancient enhances in terms of each detection capability and effectiveness.

**2.2.3 Challenges and Limitations**
Despite the auspicious results from Deep Learning applications in OS security, many encounters remain that require to be self-addressed for broader adoption:
High procedure Requirements: Deep learning models, like CNNs and LSTMs, need substantial procedure power, which makes them inappropriate for placement in resource-limited environments, like IoT devices. Potential solutions embody the utilization of model compression or unstable-to-edge computing architectures.
Limited and Biased Datasets: The shortage of miscellaneous and tagged datasets ranges the power of Deep Learning models to alter. Most studies use dedicated datasets, which can not capture the complete variety of attainable real-world security
threats. There's a sturdy would like for the event of standardized, various datasets to recover model hardiness.
Vulnerability to Adversarial Attacks: Deep Learning strategies show strong performance, but they continue to be responsible for adversarial attacks, wherever even slight changes to the input file will radically alter predictions. Future analysis ought to specialize in processing adversarial hardiness through techniques like adversarial coaching.
Scalability Across Different Platforms: Deep Learning models qualified on specific operative

systems might not transmit well across alternative platforms because of the variations in design. Additional work is needed to allow these models to generalize across numerous OS environments while not exacting major reconstruction.

Lack of Model Transparency: Deep learning models are typically measured in "black-box" systems, making it problematic to know why bound guesses are created. This lack of interpretability will hinder the adoption of Deep Learning systems in touch-and-go security applications wherever explainability is important for trust and authentication.

## FUTURE DIRECTIONS

It holds great promise in terms of changing the way OSs are secured. The work going forward is expected to emphasize dataset diversification and enrichment for elimination of biasing, robust training over a myriad of threat scenarios, and light models optimized for edge computing which could be employed for deployment in resource-constrained environments like that of IoT devices. Adversarial defenses must be stronger and more advanced through techniques such as adversarial training and robust architectures to counter advanced attack vectors. Adaptive and proactive defense will be enabled through real-time threat detection using deep reinforcement learning. OS architectures will be addressed through cross-platform model standardization, thereby making it universally applicable. Finally, the transparency and explainability of the model will provide better trust in the automated security systems so that practitioners can understand and validate the decisions made by the model effectively.

In an attempt to elaborate on these guidelines, the accompanying diagram details six major directions towards the advancement of deep learning strategies in OS security: dataset diversity, lightweight models, adversarial defense, real-time detection, cross-platform standardization, and model transparency. These interdependent strategies will
come together to constitute the next wave of resilient, adaptive security systems.

## REFERENCES:

[1]Zarif Bin Akhtar, "Securing Operating Systems (OS): A Comprehensive Approach to Security with Best Practices and Techniques," ResearchGate,Mar. 28, 2024. https://www.researchgate.net/publication/379381704_Securing_Operating_Systems_OS_A_Comprehensive_Approach_to_Security_with_Best_Practices_and_Techniques [2]M. Shahin, M. Maghanaki, A. Hosseinzadeh, and F. F. Chen, "Advancing Network Security in Industrial IoT: A Deep Dive into AI-Enabled Intrusion Detection Systems," Advanced Engineering Informatics, vol. 62, p. 102685, Oct. 2024, doi: https://doi.org/10.1016/j.aei.2024.102685.

[3]S. W. A. Hamdani et al., "Cybersecurity Standards in the Context of Operating System," ACM Computing Surveys, vol. 54, no. 3,pp.136,Jun.2021,doi:https://doi.org/10.1145/3442480. [4]H. Studiawan, F. Sohel, and C. Payne, "Anomaly Detection in Operating System Logs with Deep Learningbased Sentiment Analysis," IEEE Transactions on Dependable and Secure Computing, pp. 1–1, 2020, doi: https://doi.org/10.1109/tdsc.2020.3037903. [5]W. Ullah, A. Ullah, I. U. Haq, K. Muhammad, M. Sajjad, and S. W. Baik, "CNN features with bi-directional LSTM for real- time anomaly detection in surveillance networks," Multimedia Tools and Applications, Aug. 2020, doi: https://doi.org/10.1007/s11042-020-09406-3.

[6]Abada Abderrahmane, Guettaf Adnane, Yacine Challal, and Khireddine Garri, "Android Malware Detection Based on System Calls Analysis and CNN Classification," Apr. 2019, doi: https://doi.org/10.1109/wcncw.2019.8902627. [7]M. Hossain, S. K. Islam, J. Cheng, and B. I. Morshed,

"Efficient Acceleration of Deep Learning Inference on Resource-Constrained Edge Devices: A Review," Proceedings of the IEEE, vol. 111, no. 1, pp. 42–91, Jan. 2023, doi: https://doi.org/10.1109/jproc.2022.3226481.

[8]B. Ghimire and D. B. Rawat, "Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things," IEEE Internet of Things Journal, vol. 9, no. 11, pp. 1–1, 2022, doi: https://doi.org/10.1109/jiot.2022.3150363.

[9]S. Yuan and X. Wu, "Deep Learning for Insider Threat Detection: Review, Challenges and Opportunities," Computers & Security, vol. 104, p. 102221, Feb. 2021, doi: https://doi.org/10.1016/j.cose.2021.102221. [10]Ö. Aslan, S.

S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," Electronics, vol. 12, no. 6,

pp. 1–42, Mar. 2023, doi: https://doi.org/10.3390/electronics12061333.[11]A.-A. Mustafa Majid, A. J. Alshaibi, E. Kostyuchenko, and A. Shelupanov, "A review of artificial intelligence based malware detection using deep learning," Materials Today: Proceedings, Jul. 2021,doihttps://doi.org/10.1016/j.matpr.2021.07.012. [12]P. Dixit and S. Silakari, "Deep Learning Algorithms for Cybersecurity Applications: A Technological and Status Review," Computer Science Review, vol. 39, p. 100317, Feb. 2021, doi: https://doi.org/10.1016/j.cosrev.2020.100317. [13]O. Lutz et al., "ESCORT: Ethereum Smart COntRacTs

Vulnerability Detection using Deep Neural Network and Transfer Learning," arXiv.org, Mar. 23, 2021. https://arxiv.org/abs/2103.12607

[14]A. Schiaffino, M. Reina, R. Anibal, M. Aragon, A. Solinas, and F. Epifania, "Detecting Zero-Day Vulnerabilities in CMS Platforms: An In-depth Analysis

Using DeepLog," 2023. Available: https://ceur-ws.org/Volhttps://ceur-ws.org/Vol-3650/paper8.pdf3650/paper8.pdf

[15]D. Pan, Z. Song, L. Nie, and B. Wang, "Satellite Telemetry Data Anomaly Detection Using Bi-LSTM Prediction Based Model,"May2020,doi: https://doi.org/10.1109/i2mtc43012.2020.9129010.

[16]"An Unsupervised Deep Learning Model for Early Network Traffic Anomaly Detection | IEEE Journals&Magazine|IEEEXplore,"ieeexplore.ieee.org. https://ieeexplore.ieee.org/abstract/document/8990084 [17]M. A. Khan, "HCRNNIDS: Hybrid Convolutional Recurrent Neural Network-Based Network Intrusion Detection System," Processes, vol. 9, no. 5, p. 834, May 2021, doi: https://doi.org/10.3390/pr9050834.

[18]M. Lopez-Martin, B. Carro, and A. Sanchez-Esguevillas, "Application of deep reinforcement learning to intrusion detection for supervised problems," Expert Systems with Applications, vol. 141, p. 112963, Mar. 2020, doi: https://doi.org/10.1016/j.eswa.2019.112963.

[19]V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh,A.Dehghantanha,andG.Srivastava,"Federated Learningbased Anomaly Detection for IoT Security

Attacks," IEEE Internet of Things Journal, pp. 1–1, 2021,doihttps://doi.org/10.1109/jiot.2021.3077803. [20]Sk. T. Mehedi, A. Anwar, Z. Rahman, K. Ahmed, and I.

Rafiqul, "Dependable Intrusion Detection System for IoT: A Deep Transfer

Learning-basedApproach," IEEE Transactions on Industrial Informatics, pp.

1–1, 2022, doi: https://doi.org/10.1109/tii.2022.316477.
[21]P. Agarwal and M. Alam, "A Lightweight Deep Learning Model for Human Activity Recognition on Edge Devices," Procedia Computer Science, vol. 167, pp. 2364–23732020,doi: https://doi.org/10.1016/j.procs.2020.03.289.[22]S. Han, C. Lin, C. Shen, Q. Wang, and X. Guan, "Interpreting Adversarial Examples in Deep Learning: A Review," ACM Computing Surveys, vol. 55, no. 14s, pp. 1–38, Jul. 2023, doi: https://doi.org/10.1145/3594869.
[23]D. I. Dimitrov, G. Singh, T. Gehr, and M. Vechev, "Provably Robust Adversarial Examples," arXiv.org, 2020. https://arxiv.org/abs/2007.12133 (accessed Oct. 20, 2024). [24]A. Bensaoud and J. Kalita, "Deep multi-task learning for malware image classification," Journal of Information Security and Applications, vol. 64, p. 103057, Feb. 2022, doi: https://doi.org/10.1016/j.jisa.2021.103057.