Advancements in Deep Learning: Implications for Cybersecurity and Beyond – A Literature Review

Richie Imafidon[1]
Anjum Razzaque[2*]
[1,2*] School of Computer Sciences, College of Business and Technology,
Western Illinois University, Macomb, Illinois, USA
Emails: ar-imafidon@wiu.edu[1], a-razzaque@wiu.edu[2]

Abstract

Within the ever-evolving realm of cybersecurity, advanced technologies, such as deep learning, are crucial in countering the dynamic nature of malware threats. This research initiative embarks on an initial literature review phase aimed at unraveling the intricate role of deep learning in detecting malware. By scrutinizing various dimensions such as architectures, strengths, and limitations, this study lays a robust foundation for probing the application of Convolutional Neural Networks (CNNs) in image-based detection, focusing on fundamental concepts. Furthermore, this ongoing research delineates its current trajectory and outlines a proposed future research plan within this manuscript. This plan serves as a guiding beacon for readers, particularly those venturing into this research domain for the first time, offering a structured deductive top-down research approach inspired by the methodology in this study.

Keywords: Architecture; Deep Learning; Malware; Neural Networks.

1.0 Introduction

In cybersecurity, advanced technologies like deep learning are vital against evolving malware threats. This manuscript portrays this study's initial literature review research stage, where it aims to explore deep learning's role in malware detection, covering architectures, strengths, and limitations. It lays the groundwork for Convolutional Neural Networks (CNNs) in image-based detection, focusing on key concepts. Integrating advanced technologies is crucial in the ever-evolving cybersecurity landscape to bolster defenses against dynamic and complex malware threats. Technology is necessary to combat such threats, highlighting the shortcomings of traditional approaches in addressing modern cyber challenges effectively.

The cybersecurity industry has undergone a significant shift, necessitating the integration of advanced technologies to counter evolving malware threats effectively. Traditional methods, once effective, now encounter limitations against sophisticated modern cyber threats. Artificial intelligence (AI) cannot autonomously detect and resolve every potential malware incident. However, combining bad and good behavior modeling becomes a potent weapon against even the most advanced malware (Faruk et al., 2021). The role of technology in combating malware threats is critical due to the relentless growth in their complexity and volume. Machine learning

techniques offer promise in malware analysis and detection, particularly against stealthy threats that are challenging to detect with traditional methods (Yoo et al., 2021). Additionally, AI has shown the potential to enhance cybersecurity, particularly in malware detection (Computers Nationwide., 2024). Visual analysis technology has also advanced malware identification, highlighting technological advancements' significance (Singh et al.,2020). Hardware-based malware detection schemes are advocated for protecting vulnerable software with robust hardware implementations, offering lower bug defect density due to their simplicity. Furthermore, behavior analysis and advanced methodologies are deemed more effective than traditional signature-based methods for detecting malware (Singh et al., 2021), emphasizing the importance of leveraging advanced technological methods. In cybersecurity, cloud computing is pivotal in protecting computer systems from various cyberattacks, particularly malware attacks (Ahmad et al., 2021). Hybrid security models are proposed to combat malware threats, considering IT systems' nature and business objectives. Mathematical modeling is suggested to control, prevent, and safeguard computer networks from malware intrusions, underscoring technology's role in addressing this issue. Recent literature has seen the vitality of the emergence of deep learning, a subset of machine learning. Deep learning emerges as a transformative force in the broader realm of cybersecurity. It embraces dynamic, self-learning models capable of adapting to evolving threats by autonomously learning complex patterns from vast datasets, diverging from rule-based methods. Deep learning's impact extends across fields like computer vision and medicine, surpassing previous machine learning techniques (Voulodimos et al., 2018). Its ability to learn data representations with multiple levels of abstraction enables hierarchical feature representation, benefiting domains like neuroimaging interpretation in medicine (Voulodimos et al., 2018). Deep learning also excels in design tasks such as de novo drug design and molecular dynamics simulation (Krishnan et al., 2021). Technology advancements have propelled deep learning's ascent, facilitating integration into diverse applications like musculoskeletal disease diagnosis and drug design. Access to abundant objective data and publicly available deep neural networks have further fueled its proliferation (Chung et al., 2018). Deep learning's profound impact spans from computer vision to medicine and beyond, driven by its capability to learn intricate data representations, fostering its widespread adoption and success in various applications.

Deep learning offers adaptive solutions for malware detection, harnessing neural networks to identify complex patterns. Inspired by the brain's neural networks, it enhances cybersecurity with proactive techniques (Mijwil et al., 2022). Its integration into edge computing enables dynamic maintenance (Wang et al., 2020). In healthcare, it aids in Alzheimer's disease classification and COVID-19 detection (Rong & Ailian, 2022). Deep learning's role extends to the AI life cycle, enhancing edge computing with dynamic maintenance (Rong & Ailian, 2022). Surveys attest to its advancements in edge computing (Wang et al., 2020). Overall, deep learning offers adaptive solutions across domains, from cybersecurity to healthcare and edge computing to cognitive dysfunction classification.

Convolutional Neural Networks (CNNs) are pivotal in deep learning, excelling in visual analysis and data processing tasks like image recognition. They've revolutionized image tasks,

approaching human-level performance. U-shaped Fully Convolutional Neural Networks (FCNs) notably excel in medical image segmentation. CNNs extend beyond image tasks, facilitating object recognition and scene analysis in virtual and augmented reality (Sineglazov & Boryndo, 2022). They excel in feature extraction, benefiting object detection and classification (Chen & Cheung, 2023). Moreover, CNNs enhance vehicle classification and brain MR image analysis (Agafonova et al., 2020). CNNs are indispensable in image-based tasks, spanning image recognition, segmentation, virtual reality, medical imaging, and more. Their advancements in handling complex image processing tasks underscore their fundamental role in artificial intelligence and computer vision.

The literature review highlights the critical role of advanced technologies like deep learning and CNNs in addressing evolving malware threats and advancing diverse fields. However, further exploration through a comprehensive literature review is necessary to delve deeper into their applications, challenges, and potential advancements, ensuring a thorough understanding and effective utilization in cybersecurity and other domains, hence the need for such a paper. Looking ahead, Section 2 offers an additional critique of the discussed topics. Section 3 delves into the research methodology, while the final section comprehensively discusses the concepts. It also introduces a proposition for future research, acknowledging that this study is still in progress.

2.0 Literature Review

We first delve into comprehending a broader exploration of neural network architectures to appreciate the current literature review better. To accurately portray neural network architectures in cybersecurity, we explore the applications of CNNs, Recurrent Neural Network (RNN), and Long Short-Term Memory (LSTM) networks. These models show promise in various cybersecurity applications (Shahin et al., 2022; Alharbi et al., 2021; Ma & Liu, 2021). For example, LSTM architectures have been fine-tuned for Industrial IoT datasets, demonstrating practical effectiveness (Shahin et al., 2022). Additionally, LSTM combined with conditional random fields aids cybersecurity entity recognition (Ma & Liu, 2021). CNN and RNN architectures, particularly CRNN, perform well in cybersecurity (Jung & Chung, 2020). RNN-LSTM models excel in human activity recognition, highlighting their superiority (Albaba et al., 2020). Proposals for cybersecurity systems integrating deep neural networks aim to tackle complex challenges. The significance of these architectures is emphasized by the demand for proactive security and the scarcity of labeled data, prompting adversarial active learning frameworks (Kabanda, 2020).

The next milestone in this critique of our literature review is to describe the significance of deeper learning in the context of cybersecurity. Deep learning is a pivotal role player in cybersecurity, excelling in intrusion detection, malware classification, and cyber-attack detection (Alghamdi, 2020; Sarker et al., 2020). Its efficacy extends to IoT security, even detecting new malware variants and zero-day attacks (Kabanda, 2020). Integration with cybersecurity bolsters threat detection, particularly in adversarial environments (Biggio, & Roli, 2018). Additionally,

deep learning enhances cybersecurity education, addressing the demand for skilled professionals (Tang et al., 2019). Its applications extend to knowledge graph improvement, semantic triple extraction, and cybersecurity awareness (Chien et al., 2021).

Subsequently, it is imperative to critique the types of architectures: CNNs, Recurrent Neural Networks (RNNs), Long Short-Term Memory Networks (LSTMs), etc. The neural network architectures to be explored include Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) networks. CNNs excel in image recognition tasks, automatically learning spatial features. RNNs effectively model sequential data in speech and music tasks. LSTMs, a type of RNN, handle long-term dependencies. CNNs are vital in computer vision, while RNNs, including LSTMs, are suited for sequential data tasks. Now, we explore the applications of various neural networks in malware detection. Neural network architectures like CNNs and LSTMs show potential in this area. CNNs effectively learn malicious behavior from raw bytes (Lin & Yeh, 2022). LSTMs excel in sequential data analysis, enhancing malware detection (Girones, 2023). CNNs also successfully classify obfuscated malware (Dhanya et al., 2023) and convert malware executables into grayscale images for classification (Lin & Yeh, 2022). Additionally, deep learning approaches, including CNN-based transfer learning models, address IoT device malware detection needs (Naeem et al., 2022). LSTM models are used for Android malware detection (Fallah & Bidgoly, 2022). Hybrid networks combining convolutional and recurrent layers are proposed for malware classification (Catak et al., 2020). A new malware classification framework based on deep learning algorithms has been introduced, showing promise (Aslan & Yilmaz, 2021). CNNs are employed for intelligent malware classification via network traffic and data augmentation, outperforming traditional algorithms (Jasim & Farhan, 2023).

Different neural networks have strengths and limitations, thus demanding the need for comparative analysis of architectures, hence the next aim of this rhetoric. To conduct a comparative analysis of Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) in malware detection, we must assess their respective strengths and limitations. CNNs excel in image classification and object recognition, making them ideal for tasks reliant on spatial data dependencies, such as image-based malware detection. Architectures with smaller filter kernels and deeper layers enhance training speed for specific applications. Conversely, RNNs, including LSTM, are adept at processing sequential data and capturing long-term dependencies (Dang et al., 2020). In malware detection, they prove valuable in analyzing time-series data, revealing patterns indicative of malware presence. However, standard RNNs face challenges with the gradient-vanishing problem, impacting their ability to capture long-term dependencies (Chen et al., 2018). Consideration of each architecture's limitations is crucial. CNNs may encounter difficulties manually setting the effective receptive field size (Tabernik et al., 2020), while large CNN models like VGG16 and ResNet pose computational and memory challenges (Zhang et al., 2019). Similarly, RNNs, including LSTM, struggle with capturing long-term dependencies due to their innate permutation invariance (Qin et al., 2019).

3.0 Methodology

This ongoing deductive research takes a top-down approach, starting with a general theory or hypothesis and then seeking to validate it through specific observations or data. Currently, an in-progress study is in its initial stages; it delves into the frontiers of deep learning, exploring its transformative potential in cybersecurity and beyond. The journey began with a comprehensive exploration of scholarly journals and conferences, comprehended by insight assembled from relevant textbooks and courses.

As we embark on the next phase, the focus shifts to empirically processing vast malware datasets, harnessing big data techniques to derive image representations. This manuscript represents a significant milestone in our pursuit of cutting-edge advancements and sets the stage for further groundbreaking discoveries.

4.0 Discussion and Conclusion

While this is a literature review phase of this ongoing research, it is imperative to discuss and justify such research's relevance, a justification that can be perceived from the lens of CNN. The focus on Convolutional Neural Networks (CNNs) for malware detection is justified by their proficiency in image-based tasks, which is crucial in malware detection. Widely recognized for their efficacy in vision-based applications, CNNs, like Android malware detection, streamline learning without reverse engineering processes (Almomani et al., 2022). Their superior performance in tasks like image classification makes them ideal for malware detection (Prima & Bouhorma, 2020). CNNs' use in secure network programs highlights their relevance in malware detection (Naeem et al., 2022). Literature also showcases CNNs' success in image-based Windows malware classification, reinforcing their role in malware detection (Ravi & Alazab, 2023). Their integration significantly reduces model execution time, enhancing practicality in malware-related tasks (Lad & Adamuthe, 2020). Integration in current malware detection pipelines underscores CNNs' relevance and applicability in this domain (Szegedy et al., 2015). The extensive literature on CNNs' proficiency in image-based tasks, superior performance, and practical advantages in reducing execution time justifies their exploration in malware detection.

CNNs have gained extensive traction and proven their efficacy in image-based malware detection, encompassing various malware types like IoT, Android, and Windows. For Android malware detection, Kim implemented a CNN-based system (Kim et al., 2021), while Naeem et al. utilized CNNs for malware identification using images generated from space-filling curves within apps (Naeem et al., 2022). Ravi et al.'s literature survey underscores CNNs' success in image-based Windows malware classification (Ravi & Alazab, 2023).

Yadav et al. proposed CNNs for Android malware detection by converting decompiled APKs into images (Yadav et al., 2022), showcasing CNNs' versatility in handling diverse malware forms. Integration with transfer learning and attention modules enhances malware detection and family classification for IoT devices (Wang et al., 2021), while Ye et al. achieved high detection

accuracy using CNNs and intelligent optimization algorithms for malware image detection (Ye et al., 2022). Effectively extracting features from various malware images, whether grayscale images or representations of malicious code, CNNs have been utilized for classification based on visual similarities between malware samples of the same family (Zhao et al., 2020). Gibert et al. proposed CNNs for classifying malware represented as images, leveraging visual similarities (Gibert et al., 2018). Singh et al. combined CNN features with handcrafted features for Android malware image classification, highlighting the potential of integrating CNNs with other techniques for enhanced performance (Singh et al., 2021).

The literature review endorses Convolutional Neural Networks (CNNs) for malware detection. Studies show their effectiveness in classification, including transfer learning (AlGarni et al., 2022), attention-based approaches (Ravi & Alazab, 2023), and explainable AI for IoT malware (Naeem et al., 2022). They're also used for static malware (VGG16 (Edie, 2021). Attention mechanisms aid in polymorphic malware detection (Ganesan et al., 2021), and converting malware binaries to images improves CNN detection (Awan et al., 2021). The literature strongly supports CNNs in enhancing security against evolving threats (Aslan & Yilmaz, 2021).

Finally, Figure 1 depicts the journey ahead for our evolving research, a beacon guiding our path and inspiring fellow scholars embarking on similar ventures in this dynamic domain.

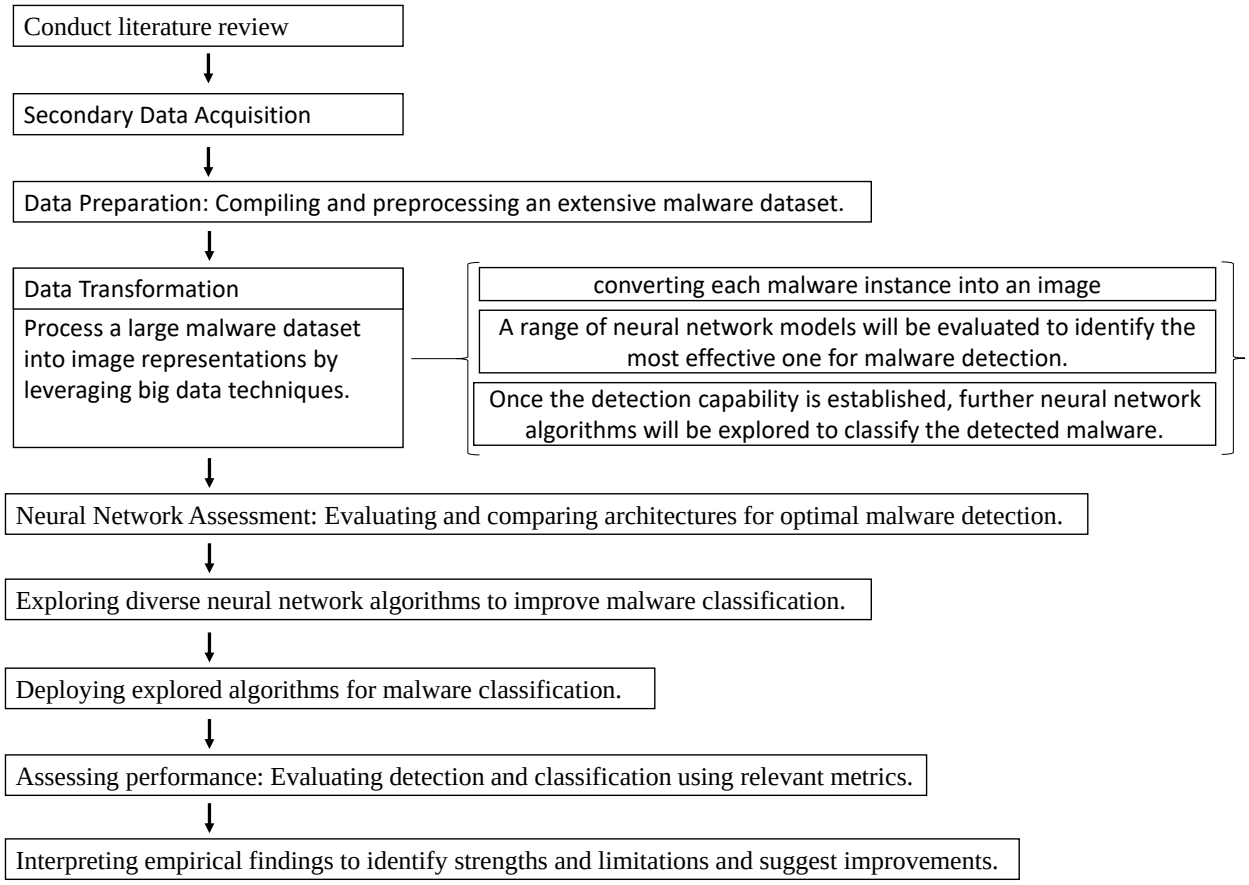

Figure 1. Current and future research trajectory

References

Awan, M. J., Masood, O. A., Mohammed, M. A., Yasin, A., Zain, A. M., Damaševičius, R., & Abdulkareem, K. H. (2021). Image-based malware classification using VGG19 network and spatial convolutional attention. *Electronics*, *10*(19), 2444.

Agafonova, Y., Gaidel, A., Surovtsev, E., & Kapishnikov, A. (2021, September). Segmentation of meningiomas in MRI of the brain using deep learning methods. In *2021 International Conference on Information Technology and Nanotechnology (ITNT)* (pp. 1-4). IEEE.

Albaba, M., Qassab, A., & YILMAZ, A. (2020). Human activity recognition and classification using of convolutional neural networks and recurrent neural networks. *International Journal of Applied Mathematics Electronics and Computers*, *8*(4), 185-189.

Alghamdi, M. I. (2020). Survey on Applications of Deep Learning and Machine Learning Techniques for Cyber Security. *International Journal of Interactive Mobile Technologies*, *14*(16).

Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2021). Cyber security in IoT-based cloud computing: A comprehensive survey. *Electronics*, *11*(1), 16.

AlGarni, M. D., AlRoobaea, R., Almotiri, J., Ullah, S. S., Hussain, S., & Umar, F. (2022). An efficient convolutional neural network with transfer learning for malware classification. *Wireless Communications and Mobile Computing*, *2022*, 1-8.

Alharbi, A. M., Al-Yami, A., & Deokar, A. (2021). Ensemble Learning Methods for Malware Detection: A Comparative Study. In International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems (pp. 91-102). Springer, Cham.

Almomani, I., Alkhayer, A., & El-Shafai, W. (2022). An automated vision-based deep learning model for efficient detection of android malware attacks. *IEEE Access*, *10*, 2700-2720.

Aslan, Ö., & Yilmaz, A. A. (2021). A new malware classification framework based on deep learning algorithms. *Ieee Access*, *9*, 87936-87951.

Biggio, B., & Roli, F. (2018, October). Wild patterns: Ten years after the rise of adversarial machine learning. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 2154-2156).

Catak, F. O., Yazı, A. F., Elezaj, O., & Ahmed, J. (2020). Deep learning based Sequential model for malware analysis using Windows exe API Calls. *PeerJ Computer Science*, *6*, e285.

Chung, S. W., Han, S. S., Lee, J. W., Oh, K. S., Kim, N. R., Yoon, J. P., ... & Kim, Y. (2018). Automated detection and classification of the proximal humerus fracture by using deep learning algorithm. *Acta orthopaedica*, *89*(4), 468–473.

Chen, L. C., Zhu, Y., Papandreou, G., Schroff, F., & Adam, H. (2018). Encoder-decoder with atrous separable convolution for semantic image segmentation. In *Proceedings of the European conference on computer vision (ECCV)* (pp. 801-818).

Chen, Y., & Cheung, N. M. (2023). The emergence of neural network and its application in image recognition. In Advances in Machine Learning and Artificial Intelligence (pp. 19-38). Springer, Cham.

Chien, K. L., Zainal, A., Ghaleb, F. A., & Kassim, M. N. (2021, January). Application of Knowledge-oriented Convolutional Neural Network For Causal Relation Extraction In South China Sea Conflict Issues. In *2021 3rd International Cyber Resilience Conference (CRC)* (pp. 1-7). IEEE.

Computers Nationwide. (2024). Artificial Intelligence & Cyber Security. Retrieved from https://computersnationwide.com/artificial-intelligence-cyber-security/

Dang, L., Pang, P., & Lee, J. (2020). Depth-wise separable convolution neural network with residual connection for hyperspectral image classification. *Remote Sensing*, *12*(20), 3408.

Dhanya, K. A., Vinod, P., Yerima, S. Y., Bashar, A., David, A., Abhiram, T., ... & Kumar, G. (2023). Obfuscated Malware Detection in IoT Android Applications Using Markov Images and CNN. *IEEE Systems Journal*.

Edie, Z. Z. (2021). Malware Detection System Based On Deep Learning Technique. *Iraqi Journal of Information and Communication Technology*, *1*(1), 33-44.

Fallah, S., & Bidgoly, A. J. (2022). Android malware detection using network traffic based on sequential deep learning models. *Software: Practice and Experience*, *52*(9), 1987-2004.

Faruk, M. J. H., Shahriar, H., Valero, M., Barsha, F. L., Sobhan, S., Khan, M. A., ... & Wu, F. (2021, December). Malware detection and prevention using artificial intelligence techniques. In *2021 IEEE International Conference on Big Data (Big Data)* (pp. 5369-5377). IEEE.

Ganesan, S., Ravi, V., Krichen, M., Sowmya, V., Alroobaea, R., & Soman, K. P. (2021, January). Robust malware detection using residual attention network. In *2021 IEEE international conference on consumer electronics (ICCE)* (pp. 1-6). IEEE.

Gasmi, M. S., Gasmi, M., & Mohammed, F. (2019). Using Recurrent Neural Network and CNN for Cyber Security Entity Recognition. Procedia Computer Science, 148, 264-271.

Gibert, D., Mateu, C., & Planes, J. (2018, September). An end-to-end deep learning architecture for classification of malware's binary content. In *International Conference on Artificial Neural Networks* (pp. 383-391). Cham: Springer International Publishing.

Girones De La Fuente, A. (2023). *Enhancing Malware Detection in Executable Files using LSTM and BiLSTM-based Deep Learning Models with Word Embedding* (Doctoral dissertation, Politecnico di Torino).

Jasim, A. D., & Farhan, R. I. (2023). Intelligent malware classification based on network traffic and data augmentation techniques. *Indonesian Journal of Electrical Engineering and Computer Science*, *30*(2), 903-908.

Jung, S. H., & Chung, Y. J. (2020). Sound event detection using deep neural networks. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *18*(5), 2587-2596.

Kabanda, G. A. B. R. I. E. L. (2020). Performance of Machine Learning and other Artificial Intelligence paradigms in Cybersecurity. *Oriental journal of computer science and technology*, *13*(1), 1-21.

Krishnan, S. R., Bung, N., Vangala, S. R., Srinivasan, R., Bulusu, G., & Roy, A. (2021). De novo structure-based drug design using deep learning. *Journal of Chemical Information and Modeling*, *62*(21), 5100-5109.

Lad, S. S., & Adamuthe, A. C. (2020). Malware classification with improved convolutional neural network model. *International Journal of Computer Network & Information Security*, *12*(6), 30-43.

Ma, L., & Liu, W. (2021, November). An Enhanced Method for Entity Trigger Named Entity Recognition Based on POS Tag Embedding. In *2021 IEEE 7th International Conference on Cloud Computing and Intelligent Systems (CCIS)* (pp. 89-93). IEEE.

Mijwil, N. A., Zedan, H., Almomani, O. R., Al-zyadat, M., & Musa, S. (2022). Deep Learning and Its Applications: A Review. In Proceedings of the 2nd International Conference on Big Data and Internet of Things (pp. 347-354). Springer, Cham.

Naeem, H., Alshammari, B. M., & Ullah, F. (2022). Explainable artificial intelligence-based IoT device malware detection mechanism using image visualization and fine-tuned CNN-based transfer learning model. *Computational Intelligence and Neuroscience*, *2022*.

Prima, B., & Bouhorma, M. (2020). Using transfer learning for malware classification. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, *44*, 343-349.

Ravi, V., & Alazab, M. (2023). Attention-based convolutional neural network deep learning approach for robust malware classification. *Computational Intelligence*, *39*(1), 145-168.

Rong, Z., & Ailian, Z. (2022). The Study of Deep Learning for Edge Computing Applications. In 2022 IEEE 7th International Conference on Intelligent Computing and Signal Processing (ICSP) (pp. 81-85). IEEE.

Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). Intrudtree: a machine learning based cyber security intrusion detection model. *Symmetry*, *12*(5), 754.

Shahin, M., Chen, F. F., Bouzary, H., Hosseinzadeh, A., & Rashidifar, R. (2022). A novel fully convolutional neural network approach for detection and classification of attacks on industrial IoT devices in smart manufacturing systems. *The International Journal of Advanced Manufacturing Technology*, *123*(5-6), 2017-2029.

Sineglazov, V., & Boryndo, I. (2022). Hand Gestures Recognition and Tracking Within Virtual Reality using Hybrid Convolutional Neural Networks.

Singh, J., Thakur, D., Ali, F., Gera, T., & Kwak, K. S. (2020). Deep feature extraction and classification of android malware images. *Sensors*, *20*(24), 7013.

Singh, J., & Singh, J. (2021). A survey on machine learning-based malware detection in executable files. *Journal of Systems Architecture*, *112*, 101861.

Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S., Anguelov, D., ... & Rabinovich, A. (2015). Going deeper with convolutions. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 1-9).

Tabernik, D., Kristan, M., & Leonardis, A. (2020). Spatially-adaptive filter units for compact and efficient deep neural networks. *International Journal of Computer Vision*, *128*(8-9), 2049-2067.

Tang, Z., Liu, X., Chen, Y., & Yang, B. (2019, September). The Role of Multiple Representations and Representational Fluency in Cryptography Education. In *Proceedings of the 20th Annual SIG Conference on Information Technology Education* (pp. 75-80).

Voulodimos, A., Doulamis, N., Doulamis, A., & Protopapadakis, E. (2018). Deep learning for computer vision: A brief review. *Computational intelligence and neuroscience*, *2018*.

Wang, C., Zhao, Z., Wang, F., & Li, Q. (2021). A novel malware detection and family classification scheme for IoT based on DEAM and DenseNet. *Security and Communication Networks*, *2021*, 1-16.

Wang, X., Han, Y., Leung, V. C., Niyato, D., Yan, X., & Chen, X. (2020). Convergence of edge computing and deep learning: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *22*(2), 869-904.

Yadav, P., Menon, N., Ravi, V., Vishvanathan, S., & Pham, T. D. (2022). A two-stage deep learning framework for image-based android malware detection and variant classification. *Computational Intelligence*, *38*(5), 1748-1771.

Ye, G., Zhang, J., Li, H., Tang, Z., & Lv, T. (2022). Android malware detection technology based on lightweight convolutional neural networks. *Security and Communication Networks*, *2022*.

Yoo, S., Kim, S., Kim, S., & Kang, B. B. (2021). AI-HydRa: Advanced hybrid approach using random forest and deep learning for malware classification. *Information Sciences*, *546*, 420-435.

Zen, H., & Sak, H. (2015, April). Unidirectional long short-term memory recurrent neural network with recurrent output layer for low-latency speech synthesis. In *2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. 4470-4474). IEEE.

Zhang, X., Zhou, X., Lin, M., & Sun, J. (2018). Shufflenet: An extremely efficient convolutional neural network for mobile devices. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 6848–6856).