IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

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

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 2, 2025

A Deep Learning Approach For Detecting Malicious Activities For Mobile Edge Security

Navya Sri Chilukoti [1], Jem Alekya [2], Dandugula Shreenidhi [3], P Sudharsan[4]

[1,2,3]UG Scholar, Department of Computer Science and Engineering, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100

[4]Assistant Professor, Department of Computer Science and Engineering, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100

[1]kps2791892@gmail.com

Abstract:

Mobile edge computing (MEC) is an evolving paradigm that brings computation and data storage closer to the user, aiming to improve the performance of mobile applications. However, with the rise of these technologies, malicious activities targeting mobile edge systems have become a significant concern. Malicious activities in mobile edge security include attacks such as data breaches, denial of service (DoS), and intrusion attempts, which exploit vulnerabilities in the infrastructure and impact the integrity, availability, and confidentiality of the system. Historically, mobile edge security was addressed using signature-based detection methods and rule-based systems. These systems relied on predefined patterns of known attacks, which could only recognize threats for which signatures had been previously created. These approaches were limited in their ability to detect new or evolving attack strategies. Over time, the increasing sophistication of cyber-attacks necessitated the exploration of more advanced techniques. The introduction of machine learning (ML) algorithms to security systems has significantly changed the landscape of mobile edge security by enabling systems to detect and prevent both known and unknown attacks in real-time. Machine learning models, particularly those leveraging deep learning techniques, are capable of learning complex patterns in data and adapting to new threats as they arise. The motivation to develop an advanced solution stems from the need to overcome the shortcomings of earlier detection systems, particularly their inability to handle novel or evolving attacks. The growing reliance on mobile edge computing for critical applications has made it essential to develop robust security solutions capable of ensuring data protection and system reliability.

Keywords: Mobile Edge Computing, Deep Learning, Machine Learning, Malicious Activities, Integrity, Reliability, Availability, Mobile Edge Security, Cyber Attacks, Detection Systems, Data, Rule-Based Systems, Signature Based Detection Methods, Learning Models, Learning Techniques.

1.INTRODUCTION

The Research focuses on detecting and mitigating malicious activities within mobile edge security environments by leveraging advanced machine learning techniques. The solution utilizes various classifiers such as Decision Trees, Random Forests, and Deep Neural Networks (DNN) to identify potential security threats. By processing datasets from mobile edge systems, the project enables real-time detection of attacks, ensuring improved system performance and data protection. The integration of deep learning models enhances the accuracy of threat detection, enabling the system to adapt to new and evolving attack patterns.

Additionally, visualization tools such as ROC curves and confusion matrices provide detailed insights into the classifier performance, assisting in better decision-making for security enhancement. The primary challenge in the mobile edge security domain is the increasing sophistication and frequency of malicious activities, such as data breaches, denial-of service attacks, and intrusions. Traditional security systems, which rely on static signatures and predefined rules, often fail to detect new or evolving threats. These systems have high false-positive rates and cannot adapt quickly enough to the dynamic nature of cyber-attacks. The problem is further compounded by the growing volume of data and the complexity of the edge environments, making manual monitoring and threat detection inefficient. Thus, there is a clear need for an intelligent, automated system capable of identifying both known and unknown malicious activities in real time. The motivation behind this research stems from the limitations of conventional security systems and the need for a more effective approach to address the challenges posed by mobile edge computing environments. The increasing dependency on mobile edge applications for critical services requires a robust security framework to protect against malicious activities. Furthermore, these traditional methods required frequent updates and manual intervention, which made them less efficient in dynamic environments.

2. LITERATURE SURVEY

[1] R. Braden discusses the fundamental requirements for internet host communication layers, providing an early framework for secure data transmission. The report outlines critical security considerations necessary for maintaining the integrity and confidentiality of communications, which serve as the foundation for modern mobile edge security mechanisms. The study highlights vulnerabilities in host-based communication that can be exploited by malicious entities, necessitating advanced security measures. [2] M. Korczy´nski and A. Duda introduce Markov chain fingerprinting to classify encrypted traffic, an approach that enhances threat detection without decrypting data. This method is particularly relevant for mobile edge security as it enables anomaly detection while preserving user privacy. Their research demonstrates the effectiveness of probabilistic models in distinguishing between normal and malicious activities within encrypted network streams, a crucial aspect in preventing security breaches. [3] B. Anderson and D. McGrew propose a machine learning-based approach to identifying encrypted malware traffic using contextual flow data. The study emphasizes the limitations of traditional signature-based detection and highlights the need for adaptive techniques that can analyze traffic behavior in real time. Their work underscores the importance of leveraging AI-driven models to enhance security at the edge of the network, where conventional methods struggle to provide timely threat identification. [4] E. Rescorla presents an update on the Transport Layer Security (TLS) protocol, detailing improvements in encryption standards that enhance security for mobile and edge computing environments. The paper addresses vulnerabilities in earlier versions of TLS and introduces mechanisms that mitigate risks associated with data interception and manipulation. The research is instrumental in securing communication channels against sophisticated cyber threats in edge networks. 4 [5] C.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025

Xu et al. conduct a comprehensive survey on regular expression matching techniques for deep packet inspection, highlighting their application in network security. Their findings reveal the efficiency and accuracy of different matching algorithms in detecting malicious activities. The study also explores hardware accelerated solutions that improve the performance of real-time security systems, making them more suitable for mobile edge environments where low latency is critical. [6] C. Meyer and J. Schwenk provide a chronological analysis of SSL/TLS attacks, examining the weaknesses exploited in previous breaches. Their work is crucial in understanding the evolution of security threats and the necessity for continuous improvement in cryptographic protocols. The study emphasizes the role of proactive security measures in preventing similar attacks in mobile edge networks. [7] Y. Zhao et al. investigate exception-triggered DoS attacks on wireless networks, revealing vulnerabilities that can disrupt edge computing operations. Their research discusses the impact of such attacks on network availability and proposes countermeasures to mitigate the risk. The findings highlight the importance of robust real-time. concern. security frameworks capable of identifying and preventing denial-of-service threats in [8] J. Salowey et al. explore session resumption mechanisms in TLS to enhance security without maintaining server-side state. The study demonstrates how these mechanisms improve authentication efficiency while minimizing the risks associated with session hijacking. Their work contributes to the development of lightweight security solutions for mobile edge computing, where resource constraints are a major concern. [9] R. Hummen et al. tailor end-to-end IP security protocols for the Internet of Things (IoT), addressing the challenges posed by limited processing capabilities in edge devices. The research introduces optimized security mechanisms that balance performance with protection, ensuring secure communication in IoT-driven edge networks. Their findings support the need for scalable security solutions that can adapt to diverse mobile edge computing environments. [10] B. Anderson, S. Paul, and D. McGrew analyze how malware utilizes TLS for encrypted communication without requiring decryption. Their research presents a 5 method to identify malicious patterns in encrypted traffic, demonstrating the potential of machine learning in security applications. The study reinforces the importance of behavioral analysis techniques in detecting cyber threats in mobile edge environments.[11] Ni et al presented a convolutional neural network-based "Malware Classification Using Sim-Hash and CNN" (MCSC). They decompile the infecting code and utilize the grayscale pictures that arise to identify malware families. To transform comparable viral code into hash values, locality-sensitive hashing (LSH) is utilized. The hash values are then transformed into grayscale pictures for neural network training. They claim that their technology detects malware at a rate of 98% or higher.[12] Zhao et al describe MalDeep as a deep learning-based malware detection system that analyzes at the malware's binary file. Convolutional neural networks are used to categorize the pathogen once the binary file is transformed to a grayscale picture. One of their system's most impressive features is its 99% detection rate for dangerous malware.[13] A deep learning algorithm for malware detection that makes use of subtle system calls was developed by Zhang et al. Cuckoo sandbox monitors the specified program in order to obtain system call information and use it to train neural networks. Their method detects malware with 95% accuracy using simply system calls.[14] Zhang et al created a convolutional neural network model for detecting malware that decompiles the software into its component pieces to get op-codes and API 133 calls. Each binary is organized, and the API frequency vectors and PCA-initialized opcode bigram matrices are constructed.

These data are used to train a convolutional neural network (CNN) and a backpropagation neural network (BPNN) to include features. Their malware detection technology has a 95% accuracy rate.[15] Zhong and Gu demonstrated a multi-tiered deep learning strategy for picking significant characteristics from static and dynamic feature sets. It generates cluster sub-trees by grouping comparable qualities together using the K-means algorithm. It decides if an application is dangerous or safe by merging the outputs of the deep learning models in the tree. [16] The ransomware detection approach presented by Zhang et al converts ransom ware family names and op-code information into numerical tensors in order to train a neural network. Their approach employs self-attentional convolutional neural networks (SA-CNN). One disadvantage is that the accuracy is just about 90%. Deep learning has become a prominent technique to protect Windows systems against malware, with convolutional neural networks applied extensively. Accuracy rates up to 99% have been achieved by researchers in detecting new malware samples. But challenges like improving detection of ransomware illustrate that continued advancement of deep learning systems can further enhance malware detection on the Windows platform. [17] In, Yuxin and Siyi developed a deep belief network approach for malware detection that extracts opcode sequences from malware executable. A PE parser is used in their system to convert the PE file into a set of machine instructions. A feature extractor finds high-classification-power n-gram sequences and utilizes them to represent the PE file as an n-gram vector. This data is sent into a malware detection system that employs neural networks. Their approach detects dangerous malware with a 98% success rate. [18] Yue suggests this loss function for malware photo identification using deep convolutional networks by combining softmax regression and entropy loss. They argue that their loss function appropriately handles the challenges raised by datasets with significantly variable malware family distributions.

3. PROPOSED METHODOLOGY

The proposed system aims to enhance the detection of malicious activities in mobile edge computing environments by leveraging advanced machine learning techniques. This approach involves the collection and preprocessing of a comprehensive dataset containing various malicious activity records. Initially, the dataset undergoes preprocessing steps, including the removal of null values and label encoding, to ensure data quality and consistency. Subsequently, the system employs the Random Forest Classifier algorithm as a benchmark to evaluate its performance in identifying malicious patterns. Building upon this, a Deep Neural Network (DNN) algorithm is proposed to improve detection accuracy and adaptability. Finally, a performance comparison between the Random Forest and DNN models is conducted to assess the efficacy of the proposed system in accurately identifying and mitigating malicious activities within mobile edge computing frameworks.

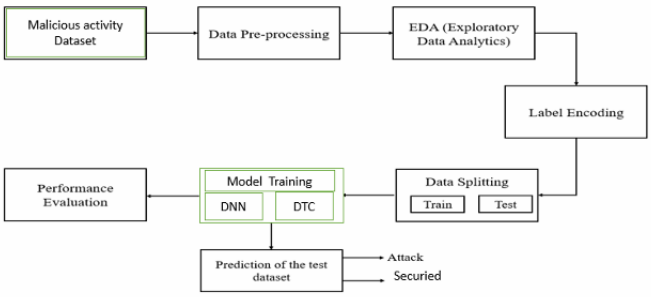

Figure 1: Block diagram.

The proposed methodology typically includes the following key components:

- The initial phase involves the collection of a comprehensive dataset encompassing various types of malicious activities pertinent to mobile edge computing environments. This dataset serves as the foundation for training and evaluating the 9 machine learning models. It includes records of different attack vectors, system vulnerabilities, and anomalous behaviors observed in mobile edge networks. The diversity and richness of this dataset are crucial for

developing a robust detection system capable of identifying a wide range of malicious activities.

- Once the dataset is compiled, preprocessing steps are undertaken to prepare the data for model training. This involves the removal of null or missing values to prevent inconsistencies that could affect model performance. Label encoding is applied to convert categorical variables into numerical formats suitable for machine learning algorithms. These preprocessing steps ensure that the dataset is clean, structured, and ready for effective training of the models.
- In this step, the Random Forest Classifier algorithm is utilized to establish a baseline for detecting malicious activities. Random Forest is an ensemble learning method that constructs multiple decision trees during training and outputs the mode of the classes for classification tasks. It operates by creating a 'forest' of uncorrelated decision trees dimensionality. whose collective output is more accurate than that of any individual tree. This algorithm is known for its robustness and ability to handle large datasets with higher dimensionality.
- Building upon the baseline, a Deep Neural Network (DNN) is proposed to enhance detection capabilities. DNNs are a class of neural networks with multiple layers between the input and output layers, capable of modeling complex patterns in data. The architecture typically consists of an input layer, multiple hidden layers, and an output layer, with each layer comprising numerous interconnected neurons. The network learns by adjusting the weights of these connections through backpropagation during training, enabling it to capture intricate data representations and improve detection accuracy.
- The final step involves a comparative analysis of the performance between the Random Forest Classifier and the Deep Neural Network models. Key metrics such as 10 accuracy, precision, recall, and F1-score are evaluated to determine the effectiveness of each model in detecting malicious activities. This comparison provides insights into the advantages of employing deep learning techniques over traditional machine learning methods in the context of mobile edge security.
- The dataset is divided into training and testing subsets to facilitate model evaluation. Commonly, a split ratio of 80:20 is used, where 80% of the data is allocated for training and 20% for testing. Preprocessing steps include normalization to scale numerical features, ensuring that each feature contributes equally to the model's learning process. Additionally, techniques such as data augmentation may be applied to address class imbalances, thereby enhancing the model's ability to generalize to unseen data.
- Model building involves selecting appropriate algorithms, tuning hyperparameters, and training the models on the preprocessed dataset. For the Random Forest Classifier, parameters such as the number of trees and maximum depth are optimized. prevent overfitting and ensure generalization. 4.3.1 Existing Algorithm In the case of the Deep Neural Network, the architecture is designed by determining the number of layers, neurons per layer, activation functions, and learning rate. The models are trained iteratively, with performance monitored on the validation set to prevent overfitting and ensure generalization.
- Random Forest is an ensemble learning method that constructs multiple decision trees during training to perform tasks such as classification and regression. For classification, the output is determined by the majority vote of the individual trees, while for regression, it is the average of their predictions. This approach enhances predictive accuracy and controls overfitting by combining the outputs of various trees.

Advantages:

- Automatic Feature Extraction: CNNs autonomously learn to identify important features directly from raw data, eliminating the need for manual feature engineering.
- Parameter Efficiency: Through weight sharing and local connectivity, CNNs significantly reduce the number of parameters compared to fully connected networks, enhancing computational efficiency.
- Translation Invariance: The architecture of CNNs allows them to recognize features regardless of their position in the input data, providing robustness to translations and distortions.
- Scalability: CNNs can be scaled to handle high-dimensional data, making them suitable for complex tasks involving large datasets.

Disadvantages:

- Computational Complexity: Training multiple decision trees can be computationally intensive, especially with large datasets and a high number of trees.
- Memory Consumption: The requirement to store numerous trees can lead to high memory usage, which may be a constraint when working with limited resources.
- Less Interpretability: Unlike single decision trees, where the decisionmaking path is straightforward, Random Forests combine multiple trees, making it difficult to understand the specific reasons behind each prediction.
- Slower Prediction Time: Due to the ensemble of trees, making predictions can be slower compared to simpler models, which may be a limitation in real time applications.

4. EXPERIMENTAL ANALYSIS

The design of error messages is an important part of the user interface design. As user is bound to commit some errors or other while designing a system the system should be designed to be helpful by providing the user with information regarding the error he/she has committed. This application must be able to produce output at different modules for different inputs.

Figure 2: Sample Images

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 2, 2025

Figure3: Enhanced Image 1

Figure 4: Enhanced Image 2

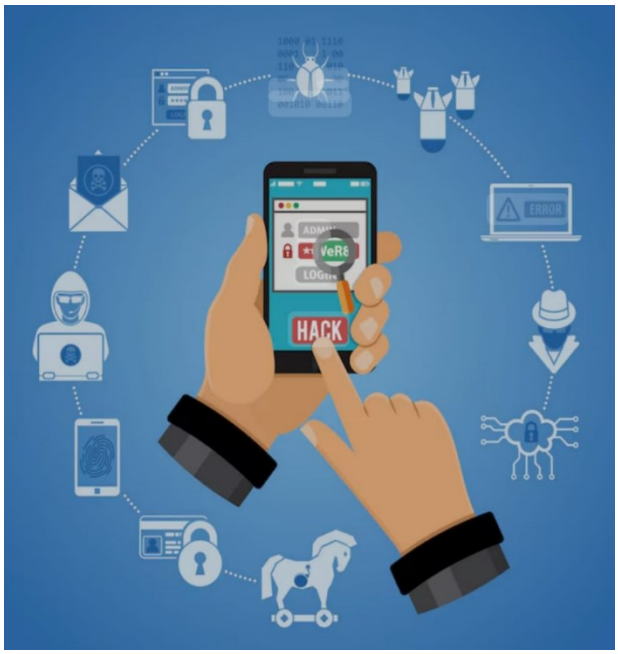

Figure 5: Enhanced Image 3

Figure 5 shows An architectural block diagram offers a high-level view of a system's structure, showcasing the main components and their interactions. It represents how major modules, such as data sources, processing units, and evaluation components, are organized and how they communicate with each other to accomplish the system's objectives. This diagram helps in understanding the overall design and flow of the system.

5. CONCLUSION

The integration of deep learning (DL) into mobile edge computing (MEC) has significantly enhanced the security and efficiency of mobile networks. By leveraging the computational power of edge devices, DL models can process data locally, reducing latency and conserving bandwidth. This localized processing is particularly advantageous for real-time applications such as intrusion detection and threat analysis, where swift responses are crucial. Moreover, the adaptability of DL algorithms enables them to learn from evolving attack patterns, providing robust Défense mechanisms against sophisticated cyber threats. The deployment of DL in MEC environments presents several challenges. Edge devices often have limited computational resources, which can constrain the complexity of DL models that can be effectively implemented. Additionally, ensuring the privacy and security of data networks. 11.2 Future Scope processed at the edge is paramount, as these devices are susceptible to various vulnerabilities. Addressing these challenges requires ongoing research and the development of optimized DL models tailored for resource-constrained environments. Despite these hurdles, the potential benefits of integrating DL into MEC for enhanced security are substantial, paving the way for more resilient and efficient mobile networks.

The research on "A Deep Learning Approach for Detecting Malicious Activities in Mobile Edge Security" highlights the significance of advanced threat detection mechanisms in modern computing environments. Traditional security methods, such as rule-based and signature-based systems, struggle to detect zero-day attacks, encrypted threats, and evolving cyber threats. The increasing reliance on mobile edge computing for critical applications necessitates robust, adaptive, and intelligent security solutions.

This study demonstrates how machine learning and deep learning techniques enhance security in mobile edge environments. The use of classifiers such as Decision Trees, Random Forests, and Deep Neural Networks (DNNs) significantly improves threat detection accuracy. These models enable real-time analysis of security threats, reducing false positives and allowing for automated identification of new attack patterns. The comparison between traditional Random Forest classifiers and DNNs highlights the superior adaptability of deep learning models, making them more effective in dynamic threat landscapes.

REFERENCES

[1] Upadhyay, A.; Alaküla, M.; Márquez-Fernández, F.J. Characterization of Onboard Condition Monitoring Techniques for Stator Insulation Systems in Electric Vehicles—A Review. In Proceedings of the IECON 2019—45th Annual Conference of the IEEE Industrial Electronics Society, Lisbon, Portugal, 14–17 October 2019; Volume 1, pp. 3179–3186. 67 .

[2] Xian, R.; Wang, L.; Zhang, B.; Li, J.; Xian, R.; Li, J. Identification Method of Interturn Short Circuit Fault for Distribution Transformer Based on Power Loss Variation. IEEE Trans. Ind. Inform. 2003, 20, 2444–2454.

[3] Faiz, J.; Nejadi-Koti, H.; Valipour, Z. Comprehensive Review on Inter-turn Fault Indexes in Permanent Magnet Motors. IET Electr. Power Appl. 2017, 11, 142–156.

[4] Wang, Z.; Yang, J.; Ye, H.; Zhou, W. A Review of Permanent Magnet Synchronous Motor Fault Diagnosis. In Proceedings of the 2014 IEEE Conference and Expo Transportation Electrification Asia-Pacific (ITEC Asia-Pacific), Beijing, China, 31 August–3 September 2014; pp. 1–5.

[5] Wu, C.; Guo, C.; Xie, Z.; Ni, F.; Liu, H. A Signal-Based Fault Detection and Tolerance Control Method of Current Sensor for PMSM Drive. IEEE Trans. Ind. Electron. 2018, 65, 9646–9657.

[6] Wang, X.; Wang, Z.; Xu, Z.; Cheng, M.; Wang, W.; Hu, Y. Comprehensive 34, 6669–6684. Diagnosis and Tolerance Strategies for Electrical Faults and Sensor Faults in Dual Three-Phase PMSM Drives. IEEE Trans. Power Electron. 2018,

[7] Orlowska-Kowalska, T.; Wolkiewicz, M.; Pietrzak, P.; Skowron, M.; Ewert, P.; Tarchala, G.; Krzysztofiak, M.; Kowalski, C.T. Fault Diagnosis and Fault-Tolerant Control of PMSM Drives–State of the Art and Future Challenges. IEEE Access 2022, 10, 59979–60024.

[8] Akrad, A.; Hilairet, M.; Diallo, D. Design of a Fault-Tolerant Controller Based on Observers for a PMSM Drive. IEEE Trans. Ind. Electron. 2011, 58, 1416–1427.

[9] Dai, X.; Gao, Z. From Model, Signal to Knowledge: A Data-Driven Perspective of Fault Detection and Diagnosis. IEEE Trans. Ind. Inform. 2013, 9, 2226–2238.

[10] Mansouri, B.; Idrissi, H.J.; Venon, A. Inter-Turn Short-Circuit Failure of PMSM Indicator Based on Kalman Filtering in Operational Behavior. In Proceedings of the Annual Conference of the PHM Society, Scottsdale, AZ, USA, 21–26 September 2019; Volume 11. 68

[11] Namdar, A.; Samet, H.; Allahbakhshi, M.; Tajdinian, M.; Ghanbari, T. A Robust Stator Inter-Turn Fault Detection in Induction Motor Utilizing Kalman Filter-Based Algorithm. Measurement 2022, 187, 110181.

[12] Lee, D.; Park, H.J.; Lee, D.; Lee, S.; Choi, J.-H. A Novel Kalman Filter Based Prognostics Framework for Performance Degradation of Quadcopter Motors. IEEE Trans. Instrum. Meas. 2023, 73, 1–12.

[13] Chang, C.-C.; Cheng, T.-H. Motor-Efficiency Estimation and Control of Multirotors Comprising a Cooperative Transportation System. IEEE Access. 2023, 11, 36566–36578.

[14] Hasan, A.; Tahavori, M.; Midtiby, H.S. Model-Based Fault Diagnosis Algorithms for Robotic Systems. IEEE Access 2023, 11, 2250–2258.

[15] El Sayed, W.; Abd El Geliel, M.; Lotfy, A. Fault Diagnosis of PMSG Stator Inter-Turn Fault Using Extended Kalman Filter and Unscented Kalman Filter. Energies 2020, 13, 2972.

[16] Mahmoudi, A.; Jlassi, I.; Cardoso, A.J.M.; Yahia, K.; Sahraoui, M. Inter Turn Short-Circuit Faults Diagnosis in Synchronous Reluctance Machines, Using the Luenberger State Observer and Current's Second-Order Harmonic. IEEE Trans. Ind. Electron. 2021, 69, 8420–8429.

[17] Guezmil, A.; Berriri, H.; Pusca, R.; Sakly, A.; Romary, R.; Mimouni, M.F. Detecting Inter-Turn Short-Circuit Fault in Induction Machine Using High-Order Sliding Mode Observer: Simulation and Experimental Verification. J. Control Autom. Electr. Syst. 2017, 28, 532–540.

[18] Bouakoura, M.; Naït-Saïd, M.-S.; Nait-Said, N. Incipient Inter-Turn Short Circuit Fault Estimation Based on a Faulty Model Observer and Ann Method for Induction Motor Drives. Recent Adv. Electr. Electron. Eng. Former. Recent Pat. Electr. Electron. Eng. 2019, 12, 374–383.

[19] Vasilios, I.C. Detection of PMSM Inter-Turn Short-Circuit Based on a Fault-Related Disturbance Observer. Int. J. Simul. Syst. Sci. Technol. 2020, 21, 31.1–31.7 Guo, Chunle, et al. "Zero-reference deep curve estimation for low-light image enhancement." Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. 2020.