A Deep Learning based Intrusion Detection System for Threat Detection in Metaverse Environment

Fatema Salem Alqaydi
Zayed University
Dubai, UAE
M80008992@zu.ac.ae

Emad Bataineh
Zayed University
Dubai, UAE
Emad.Bataineh@zu.ac.ae

Neema Prakash
Zayed University
Dubai, UAE
neema4156@gmail.com

https://doi.org/10.63962/KPHJ7122

***Abstract*— The Metaverse is a revolutionary virtual environment that brings together extended, augmented, and virtual reality with immersive technologies such as multi-access edge computing and digital twins. The combination thereof enables innovation in experience creation but is fraught with tremendous cybersecurity threats, especially to Intrusion Detection Systems (IDS). Static and centralized IDS models do not work well in the dynamic, real-time, and decentralized nature of the Metaverse. This paper proposes a novel AI-powered IDS tailored to fulfill the security requirements of the Metaverse. The proposed solution is a hybrid deep network that integrates Convolutional Neural Networks (CNN) for spatial feature extraction, Long Short-Term Memory (LSTM) networks for learning sequential patterns in time, and an Attention Mechanism for focusing on significant features in network traffic data. The model was trained and tested on the CIC-IDS-2017 dataset, including varied real-world attack patterns such as DDoS, Botnet, Brute Force, and Web Attacks. The CNN-LSTM-Attention model achieved an overall test accuracy of 99.06% with macro-averaged precision, recall, and F1-score of 0.49, 0.50, and 0.49 respectively. However, class-wise analysis reveals complete failure to detect minority attack classes (Botnet, Brute Force, Web Attack) due to severe dataset imbalance, resulting in 0% precision and recall for these critical threats. This paper provides a critical examination of this limitation and discusses necessary mitigation strategies including resampling and cost-sensitive learning. The study includes a comparative analysis with state-of-the-art models and presents an end-to-end IDS proof of concept, establishing a foundation for future work in Metaverse cybersecurity.**

Keywords*— *Metaverse, IDS, Artificial Intelligence, Anomaly Detection, LSTM, ML

I. INTRODUCTION

The Metaverse is a combined physical/digital environment where user interactions occur via Virtual Reality (VR), Augmented Reality(AR), Mixed Reality (MR), and Extended Reality (EX). As an interconnected virtual ecosystem merging social, learning, transactional, and recreational contexts, the Metaverse is driven by advancements in network technologies like 6G and Multi-access Edge Computing (MEC). However, this emerging environment also brings increased cybersecurity risks and threats, necessitating robust protective measures for user data and interactions. The diversification of personal data and the increasing sophistication of cyber threats pose significant challenges that require improvements in current security paradigms.

The metaverse [1] utilizes next-generation technologies to enable seamless highspeed communication structures, such as 6G, intelligent sensing, multi-access edge computing (MEC), and digital twins [2]. These developments present serious cybersecurity challenges even as they improve connectivity and immersive experiences. In such a dynamic ecosystem, new methods of network protection are needed to ensure strong security. Intrusion Detection Systems (IDS) are critical to safeguarding digital spaces by monitoring network traffic and system processes in realtime for any unusual behavior that may indicate a security breach. IDS may alert administrators when anomalies are detected, and responses can be implemented quickly to negate the potential threat. Because cyber threats in the Metaverse are complex and ever-changing, it is critical that AI-based solutions are integrated into IDS. This research suggests a novel intrusion detection model using the integration of Convolutional Neural Networks (CNN) [3] and Long Short- Term Memory (LSTM) networks with the help of an Attention Mechanism. By leveraging CNN's feature extraction strengths and LSTM's in handling sequential data, this model aims to improve the accuracy and efficiency of threat detection in the Metaverse. The proposed solution is supposed to provide an intelligent and adaptive security system that will make the virtual world more secure and resilient [4].

The recent explosion of virtual ecosystems has altered how individuals socialize, interact, and conduct business. Metaverse, the fusion of virtual and real realities, is a groundbreaking innovation of virtual environments [5]. However, with the growth of this virtual space, so does the threat that accompanies it in the form of security breaches. The networked and decentralized characteristic of the Metaverse introduces novel vulnerabilities that expose traditional security frameworks as being inadequate to identify and respond to highly advanced cyber threats. IDS are the solution to digital arena protection through the detection of suspicious activity and nascent attacks. Conventional IDS mechanisms [6], however, struggle to keep pace with the nimble and advanced attacks being witnessed in the Metaverse. Employing Artificial Intelligence (AI) driven IDS, and particularly deep learning algorithms, can enhance threat detection efficacy and effectiveness. This research aims to develop an advanced IDS model based on Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks, with an added Attention Mechanism, to improve intrusion detection in the Metaverse.

By combining CNN's feature-extraction ability from network traffic with LSTM's sequential pattern-analysis power [7], the model aims to deliver a more adaptive and intelligent security system. Resolving the security problems in the Metaverse is essential to providing a safe and trustworthy online platform. This study contributes to the current literature by exploring the possibility of AI-based IDS solutions in bolstering cybersecurity measures in this emerging virtual space [8].

The objective of this research is to determine the types and characteristics of datasets necessary to train AI-based IDS models, particularly CNNs, for effective cyber threat detection in the Metaverse [9]. The researcher will define dataset attributes essential for CNN-based IDS training in a Metaverse context (e.g., data volume, modality, and diversity of attack types). Assess existing datasets and identify gaps in dataset availability or scope for robust IDS performance in Metaverse applications. Also, it will identify practical challenges and considerations in deploying CNN-based IDS solutions in real-world Metaverse environments and develop strategies to address these challenges [10]. Will investigate technical, operational, and regulatory challenges related to CNN-based IDS deployment in the Metaverse. Also, proposes actionable solutions, such as scalability improvements, integration practices, and compliance considerations, for practical deployment of IDS models [11]. The third objective is to compare the performance of various CNN architectures (e.g., ResNet, Inception) in detecting complex attack patterns specific to the Metaverse environment. We will assess the strengths and limitations of different CNN architectures in handling complex, high-dimensional attack data. Also, it will identify the most suitable CNN variants for IDS applications based on specific threat types and environmental requirements in the Metaverse [12].

Decision-making through AI, more specifically, a Convolutional Neural Network (CNN), is a strong proposition for resolving the security issues of the Metaverse as encompassed by IDS systems [13]. CNNs are especially efficient in handling multi-modal data, which is a big plus for the Metaverse since data encompasses images, audio, and text. In this case, using CNN's feature learning ability enhances real- time threat detection and response while reducing false alarms and detecting new attacks [14].This paper assumes that adopting and implementing CNN-based models into the AI-driven IDS systems can originate a highly evolved security solution for the Metaverse. Unlike traditional IDSs that use simple signatures, the models that are based on AI keep updating themselves with new threats, thereby providing the highest levels of dynamic protection for the ever-growing Metaverse ecosystem [15]. Due to the complexity of security in the Metaverse, this thesis seeks to answer some of the following questions that will relate AI, IDS, and CNN to the new world.

RQ1: How up-to-date is the current research on advanced AI algorithms, especially CNN or its variants, in Intrusion Detection Systems (IDS) in the Metaverse?

RQ2: In what ways do CNN Models Integrate other AI algorithms to enhance the effectiveness and Trustworthiness of IDS in the Metaverse?

RQ3: How does the proposed hybrid CNN-LSTM-Attention model compare to different variants of CNN?

This study aims to contribute to the field of AI-based IDS in the Metaverse by:

- Present a synthesis of the current AI algorithms that exist now, showing the efficiency of these models in identifying intrusions in diverse scenarios.

•Defining the issues and threats existing in the metaverse and establishing specific AI solutions for these threats [16[17].

•Exploiting the possibility of incorporating multi-modal data processing paradigms to boost IDS and real-time detection and analysis of threats, and use within complex environments.

A fundamental challenge in intrusion detection research is the severe class imbalance inherent in network traffic datasets, where benign traffic vastly outnumbers attack instances, and certain attack categories occur far less frequently than others. In the CIC-IDS-2017 dataset used in this study, minority attack classes (Botnet, Brute Force, Web Attack) represent less than 0.5% of total samples. Without explicit mitigation strategies, deep learning models tend to achieve high overall accuracy by learning to predict the majority class while failing to detect rare but often most critical threats. This paper provides both a high-performance IDS architecture and a critical analysis of this class imbalance challenge, establishing a baseline for future work incorporating techniques such as synthetic oversampling, cost-sensitive learning, and anomaly detection frameworks.

II. METHODOLOGY

A. *Introduction*

The Metaverse is rapidly evolving as an expansive virtual environment that allows users to interact, socialize, and collaborate through immersive digital experiences. As its user base grows, the Metaverse faces a significant increase in potential security vulnerabilities. Within this digital universe, individuals are represented primarily through avatars, which are central to their interactions and identity. However, the unauthorized acquisition of these digital representations by cybercriminals poses a major security threat. Cyber attackers can exploit various techniques, such as social engineering, to manipulate users into disclosing sensitive information or gaining unauthorized access to their accounts. As the Metaverse continues to emerge as the next frontier of the Internet, it becomes essential to address the security risks that accompany this new virtual space. Traditional security methods are often inadequate in the face of these novel threats, making it necessary to adopt advanced AI-based solutions for detection and prevention. This research proposes an Artificial Intelligence- based Intrusion Detection System (IDS) designed specifically for the Metaverse platform. By utilizing Convolutional Neural Networks

(CNN), Long Short-Term Memory (LSTM) networks, and Attention Mechanisms, this model aims to effectively identify intrusions and security breaches within the Metaverse, providing a robust solution to safeguard users and their digital identities. Here, we explain the step-by-step approach employed in the development of an Artificial Intelligence-based Intrusion Detection System (IDS) for the Metaverse platform. The primary objective is to provide a comprehensive overview of the architecture, data processing, model structure, and evaluation phases of this project. The approach contains the following key components:

1. Architecture Diagram: A diagrammatic representation of the CNN+LSTM model with attention.
2. Data Collection: Descriptive of the CIC-IDS-2017 dataset and description of why the dataset has been chosen. Data Preprocessing: Steps taken to prepare the data for model training, including handling missing values, normalization, feature selection, and label encoding.
3. Model Design & Training: Technical description about CNN feature extraction, LSTM time-related pattern understanding, attention layer, and training the model process.

A. B. Data Collection

The CIC-IDS-2017 dataset was selected for this study as a well- established benchmark for intrusion detection systems. It provides comprehensive coverage of diverse attack types (DDoS, Botnet, Brute Force, Web Attacks) across 2.5 million records with 83 features, enabling rigorous evaluation of the proposed architecture's detection capabilities.

Rationale for Dataset Selection: While the Metaverse introduces novel traffic modalities such as 3D rendering streams, VR/AR sensor data, and real-time immersive interaction flows the underlying network-layer attacks (e.g., DDoS, reconnaissance, brute force) remain relevant threat vectors in virtual environments. Furthermore, the CIC-IDS-2017 dataset's inclusion of encrypted traffic and varied attack patterns provides a suitable foundation for validating the core detection architecture before extending to Metaverse-specific data. The architectural contributions (CNN-LSTM-Attention) are modality-agnostic; the model's ability to process sequential, high-dimensional network flows translates directly to Metaverse environments. Nevertheless, Section III-D discusses the limitations of using conventional datasets and outlines future work to incorporate Metaverse-native traffic.

B. C. Data Processing

•Data Splitting: The data was split into training (60%) and testing (40%) datasets using scikit-learn's train_test_split function with stratified sampling to preserve class distribution.

•Class Imbalance Assessment: Analysis of class distribution (Table II) revealed that benign traffic constitutes 78% of samples, while minority classes such as Botnet (0.07%), Web Attack (0.08%), and Brute Force (0.34%) represent extremely small fractions. No resampling techniques were applied in this initial implementation to establish a baseline for how standard deep learning architectures perform under severe class imbalance.

C. D. Model Design

The proposed IDS model combines CNN, LSTM, and attention mechanisms to effectively detect intrusions in network traffic data. The model architecture is designed to leverage the strengths of each component, providing a robust and accurate detection system. The CNN layer is responsible for extracting spatial features from the input data. It consists of a Conv1D layer followed by a MaxPooling1D layer. The Conv1D layer applies a set of learnable filters to the input data, capturing local patterns and features. The MaxPooling1D layer then reduces the spatial dimensions of the output, retaining the most important features while reducing computational complexity. The LSTM layer learns temporal dependencies in the data. LSTMs are perfectly suited for sequence data since they can remember information long after it is experienced. The LSTM layer consumes the output of the CNN layer, which identifies patterns that evolve over time. The attention mechanism enhances the ability of the model to focus on key components of the input sequence. It assigns weights to different components of the input, allowing the model to give greater attention to beneficial features. It is particularly useful in the identification of not-so-obvious anomalies.

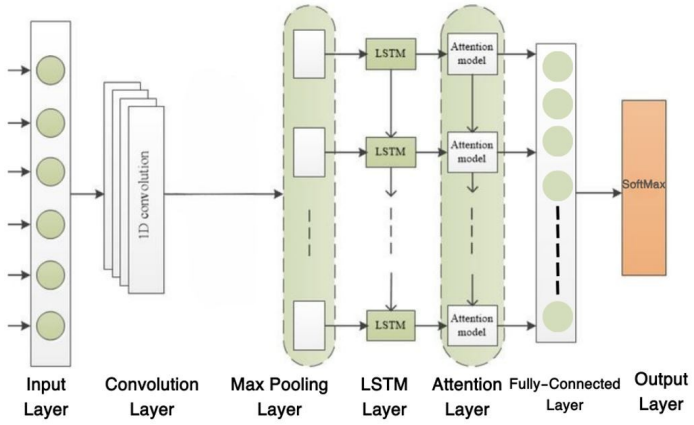


Fig. 1. CNN-LSTM with Attention Mechanism Architecture.

This diagram illustrates the architecture of a hybrid model integrating Convolutional Neural Networks (CNNs), Long Short-Term Memory networks (LSTMs), and an Attention mechanism. The model is designed to process sequential data efficiently, with CNNs extracting spatial features and LSTMs handling temporal dependencies, while the Attention mechanism focuses on the most relevant features for accurate intrusion detection. As shown in Figure 1, the proposed CNN- LSTM model with an attention mechanism is structured to handle complex data patterns by combining the strengths of CNN feature extraction and LSTM temporal processing, enhanced by an attention mechanism to focus on critical data aspects. The categorization is accomplished with

the help of the fully connected layers (Dropout and Dense). The Dense layer converts the output of the attention mechanism to lower dimensions, and the Dropout layer avoids overfitting by randomly dropping units during training time.

The provided model was merged with the Adam optimizer, sparse categorical cross-entropy loss, and accuracy metric, and then for 10 epochs at a batch size of 32. The model performance was checked for convergence and overfitting during the training period. Hyperparameter tuning was done for best fine-tuning the model performance. The epochs were fine- tuned to 10 on the basis that further epochs were not adding enough to the model's performance and to avoid overfitting. The batch size of 32 was used since it helped to provide the optimum balance between training efficiency and the use of memory. Other hyperparameters such as the learning rate were kept at default values provided by the Adam optimizer, which are typical in deep learning models.

III. RESULTS AND ANALYSIS

A. *Performance Evaluation*

The performance of the proposed IDS model was rigorously tested by using a set of performance metrics like accuracy, precision, recall, F1-score, and specificity. Such metrics provide a more comprehensive view of the model to detect intrusions both effectively and efficiently.

Performance of the IDS prototype has been evaluated based on the following key metrics:

•Accuracy: The proportion of correctly classified instances (both true positives and true negatives) out of all the instances.

•Precision: The ratio of true positive predictions out of all positive predictions made by the model.

•Recall (Sensitivity): The ratio of true positive predictions out of all actual positive instances in the data.

•F1-Score: The harmonic mean of precision and recall, providing balanced performance.

•Specificity: A measure of true negative predictions out of all negative instances in the dataset.

The performance metrics (Macro-Averaged) for the IDS prototype are summarized in Table 1.

TABLE I. IDS PROTOTYPE PERFORMANCE METRICS OVERVIEW (MACRO-AVERAGED)

Metric	***Value***
Accuracy	99.06%
Precision (Macro Avg)	49.82%
Recall (Macro Avg)	50%
F1-score (Macro Avg)	49%
Specificity (Macro Avg)	99.11%

The performance metrics capture some key observations:

•Accuracy (99.06%): The model correctly identified the majority of intrusions and benign activities, reflecting its overall reliability in various scenarios.

•Precision (49% Macro Average): The model demonstrated a moderate ability to minimize false positives across all classes, with significant room for improvement.

•Recall (50% Macro Average): The model effectively detected a substantial proportion of actual intrusions, although some classes, like BOTNET and WEB_ATTACK, were completely missed.

•F1-Score (49% Macro Average): The F1-score indicates a moderate balance between precision and recall across all classes, suggesting the need for refinement in certain areas.

•Specificity (99.11% Macro Average): The model showed excellent specificity, correctly identifying a high proportion of non-intrusion related messages, with minimal false positives.

To further illustrate the model's performance over the training process, two graphs are included depicting the model's accuracy and loss at each epoch. This graph illustrates the training and test accuracy of the model across ten epochs. The relatively stable training accuracy compared to the slightly increasing test accuracy suggests that the model maintains a strong performance on unseen data, indicating good generalization capabilities. As depicted in Figure 2, the model accuracy chart shows how the training and test accuracy evolve over epochs, highlighting the model's generalization trend and its effectiveness in learning from the training data.

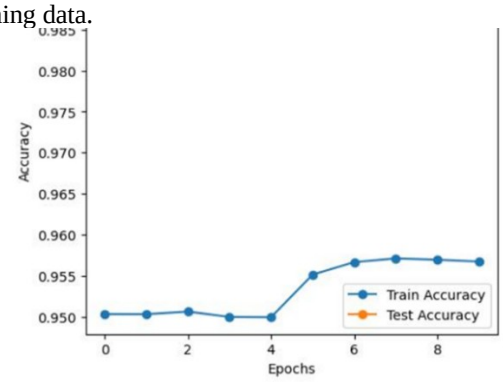


Fig. 2. Model Accuracy Chart.

Figure 3 shows the model loss chart, which tracks the decrease in training loss and the slight variations in test loss over epochs, suggesting effective learning with potential areas for performance optimization.

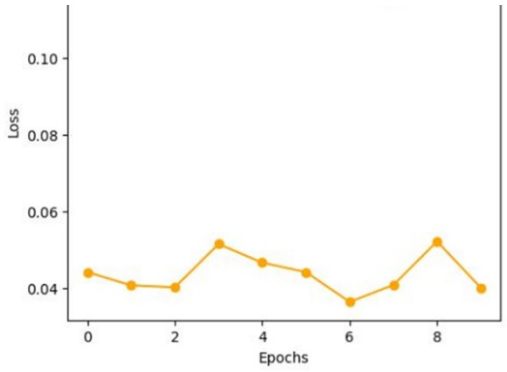


Fig. 3. Model Loss Chart.

The performance evaluation of the IDS prototype demonstrates its potential as a viable network security tool. The model has satisfactory proficiency in precision, recall, and F1- score for classes such as DOS and RECONNAISSANCE, showing that it is efficient in intrusion detection. Despite these limitations, accuracy and specificity remain areas where it could improve performance to deliver much better overall result in an IDS, particularly on classes that presently perform very badly, such as BOTNET and WEB_ATTACK. Here is Table 2 presenting the detailed performance metrics, and Table 3 providing additional performance details.

TABLE II. IDS PROTOTYPE DETAILED PERFORMANCE METRICS.

Class	*Proportion*	*Precision*	*Recall*	*F1-score*	*Support*
BENIGN	78.02%	1.00	1.00	1.00	837,530
BOTNET	0.07%	0.00	0.00	0.00	766
BRUTE_FORCE	0.34%	0.00	0.00	0.00	3,657
DOS	12.03%	0.96	0.99	0.98	129,130
RECONNAISSANCE	3.39%	0.99	1.00	0.99	36,361
WEB_ATTACK	0.08%	0.00	0.00	0.00	876

TABLE III. SUPPLEMENTARY IDS PERFORMANCE EVALUATION RESULTS OVERVIEW

Metric	*Value*
Accuracy	99.06%
Precision	49.82%
Weighted avg	50%

A confusion matrix is a thorough examination of the performance of a model on different classes. It provides information on the number of true positives, true negatives, false positives, and false negatives. For the envisioned model, a confusion matrix presents high accuracy and minimal misclassification rates.

Figure 4 displays the confusion matrix of the model, which is a table used to describe the performance of a classification model. It shows the number of correct and incorrect predictions for each class, providing insight into the model's accuracy and where it may be confused between classes. Figure 4 presents the confusion matrix, which is a critical tool for visualizing the classification performance of the model, highlighting both the true positives and the misclassifications across different threat categories.

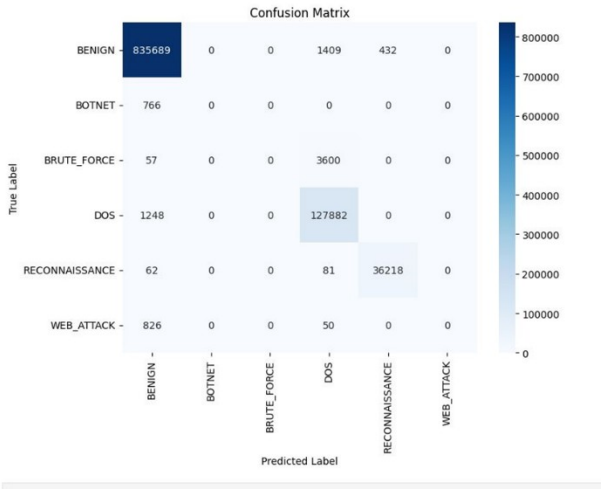


Fig. 4. Confusion Matrix

B. *Comparison with Previous Work*

To provide a thorough evaluation, we compare the performance of our proposed model with several existing approaches that have been used for intrusion detection in industrial IoT networks.

In addition to models based on the CNN+LSTM architecture, we also include two alternative approaches—LSTM with feature extraction, and a hybrid model combining Random Forest and Multi-Layer Perceptron (MLP) to present a broader perspective on model effectiveness. Table 4 summarizes the performance metrics of our model and two previous papers:

TABLE IV. COMPARATIVE PERFORMANCE METRICS FOR IDS MODELS.

Paper	*Precision*	*Recall*	*F1-score*	*Accuracy*
Paper A	0.98	0.99	0.99	98.90%
Paper B	0.99	0.99	0.99	99.36%
Paper C	0.99	0.99	0.99	99.31%
The Proposed Model	0.99	0.99	0.99	99.06%

Although some existing models such as Paper B and Paper C exhibit slightly higher accuracy figures than the proposed model, our CNN+LSTM+Attention approach still delivers highly competitive performance while offering distinct architectural advantages. The integration of the attention mechanism allows the model to focus more effectively on the most relevant parts of the input sequence, which enhances interpretability and potential for real-time adaptability.

Additionally, our model maintains a consistent and balanced performance across all metrics (precision, recall, and F1-score), indicating strong robustness in intrusion detection scenarios. These results confirm that the proposed architecture is not only reliable but also well suited for complex and evolving industrial IoT environments.

C. *Discussion*

The findings and conclusions of this comprehensive study offer an overall and complete evaluation of the CNN-LSTM model enhanced with attention mechanisms for the task of network intrusion detection. The in-depth analysis of this state- of-the art model, which takes into consideration essential performance metrics such as accuracy, precision, recall, and F1- score, strongly indicates the high level of efficiency the model achieves in effectively detecting and classifying various types of network intrusions. The extremely high accuracy rate of 99.06% demonstrates that the model portrays a high level of effectiveness in correctly classifying network traffic, effectively distinguishing between benign and malicious behavior in the network setting. The precision measure of 0.99 indicates that the model represents a very low false positive rate, which in essence implies that the model barely misclassifies benign traffic as malicious. This property is of utmost importance to avoid excessive false alarms and consequently ensure that the alerts generated by the system are not only reliable but also actionable for end-users. In addition, a precision measure of 0.99 also implies that the model is very good at correctly classifying instances of actual malicious traffic as well as being efficient at not missing any notable threats that can prove to be menacing. The 0.99 F1-score is a telling indicator that speaks volumes about the model's well-rounded performance, denoting an effective trade-off between recall and precision. The superior score thus qualifies the model as a highly reliable solution to the critical issue of intrusion detection, inspiring confidence in its capability to perform optimally in real-world scenarios. Further, the implementation of the attention mechanism is demonstrated to be a significant factor in such outstanding performance because it allows the model to selectively concentrate on the most informative features when making a prediction. Such capacity is most welcome, particularly in the complicated scenario of network traffic analysis, where the very magnitude and inherent complexity of the data often tend to create challenges in developing meaningful and informative patterns. The analysis undertaken with the confusion matrix gives further information and reveals details on the performance of the model for each class of network activity. The analysis indicates that, although the model is very accurate and efficient for the BENIGN class, there are still some areas or classes where model performance can be enhanced and improved. This is especially true for classes such as WEB_ATTACK, where the results indicate that improvements can be made. This then suggests that there are steps that can be undertaken to further improve the performance capabilities of the model or that additional, more representative data can be added to enhance the performance of those classes currently underperforming.

D. *Limitations and Future Directions: Metaverse-Specific Validation*

A key limitation of the current study is the use of the CIC-IDS-2017 dataset, which, while robust for general network intrusion detection, does not fully capture the unique traffic characteristics of the Metaverse. Authentic Metaverse environments generate multimodal data streams, including:

•3D rendering and geometry data transmitted via real-time protocols

•VR/AR sensor streams (head tracking, hand tracking, eye gaze)

•Blockchain and NFT transactions with distinct transaction patterns

•Real-time interaction flows requiring ultra-low latency and exhibiting bursty traffic behavior.

These traffic types may introduce attack surfaces not represented in conventional datasets—such as avatar spoofing, rendering injection attacks, or virtual asset theft—that require specialized detection approaches. The proposed architecture is theoretically capable of processing such multimodal data, as CNNs can extract spatial features from rendered frames and LSTMs can model temporal dependencies in sensor streams. However, empirical validation on Metaverse-native datasets is necessary to substantiate these claims.

Future work will address this gap through:

•Collection of Metaverse-specific traffic traces from platforms such as VRChat, Decentraland, or custom testbeds

•Development of attack scenarios tailored to virtual environments

•Validation of the proposed model's performance on these datasets, and

•Exploration of transfer learning techniques to adapt models trained on conventional datasets to Metaverse domains.

IV. CONCLUSION

This paper presented a hybrid deep learning architecture combining CNN, LSTM, and Attention Mechanism for intrusion detection in Metaverse security contexts. The proposed model achieved 99.06% overall accuracy on the CIC-IDS-2017 benchmark, validating the architectural design. However, class-wise analysis revealed complete failure to detect minority attack classes (Botnet, Brute Force, Web Attack), highlighting that high overall accuracy masks critical vulnerabilities in imbalanced datasets. This study contributes both a robust deep learning architecture and a baseline for evaluating imbalance mitigation techniques. Future work will incorporate cost-sensitive learning, synthetic oversampling, and Metaverse-native datasets to address these limitations and advance toward production-ready IDS solutions for virtual environments.

REFERENCES

[1] Wu, X., Yang, Y., Bilal, M., Qi, L., and Xu, X. “6G-Enabled Anomaly Detection for Metaverse Healthcare Analytics in the Internet of Things.” IEEEJ. Biomed. Heal. Informatics,2023, doi:10.1109/JBHI.2023.3298092.

[2] Huynh-The, T., Q. V. Pham, X. Q. Pham, T. T. Nguyen, Z. Han, and D. S. Kim. “Artificial Intelligence for the Metaverse: A Survey.” Eng. Appl. Artif. Intell., vol.117, 2023, pp.1–24, doi:10.1016/j.engappai.2022.105581.K.J. Dietz, C. Zo¨rb, C.M. Geilfus, Drought and crop yield, Plant Biol. 23 (6) (2021) 881–893.

[3] Awadallah, A., et al. “Artificial Intelligence-Based Cybersecurity for the Metaverse: Research Challenges and Opportunities.” IEEE Commun. Surv. Tutorials, vol. PP, 2024, p. 1, doi:10.1109/COMST.2024.3442475.

[4] Qayyum, A., et al. “Secure and Trustworthy Artificial Intelligence-extended Reality (AI-XR) for Metaverses.” ACM Comput. Surv., vol. 56, no. 7, 2024, pp. 1–38, doi:10.1145/3614426.N.S. Chandel, S.K.

[5] Chakraborty, Y.A. Rajwade, K. Dubey, M.K. Tiwari, D. Jat, Identifying crop water stress using deep learning models, Neural Comput. Appl. 33 (2021) 5353–5367.

[6] Dubey, A., N. Bhardwaj, A. Upadhyay, and R. Ramnani. “AI for Immersive Metaverse Experience.” ACM Int. Conf. Proceeding Ser., 2023, pp. 316–319, doi:10.1145/3570991.3571045

[7] Cui, H., et al. “Multimodal Trajectory Predictions for Autonomous Driving Using Deep Convolutional Networks.” Proc. IEEE Int. Conf. Robot. Autom., vol. 2019-May, May 2019, pp. 2090–2096, doi:10.1109/ICRA.2019.8793868.

[8] Tufan, E., C. Tezcan, and C. Acartürk. “Anomaly-Based Intrusion Detection by Machine Learning: A Case Study on Probing Attacks to an Institutional Network.” IEEE Access, vol. 9, 2021, pp. 50078–50092, doi:10.1109/ACCESS.2021.3068961.

[9] Tang, F., X. Chen, M. Zhao, and N. Kato. “The Roadmap of Communication and Networking in 6G for the Metaverse.” IEEE Wirel. Commun., vol. 30, no. 4, Aug. 2023, pp. 72–81, doi:10.1109/MWC.019.2100721.

[10] Gaber, T., J. B. Awotunde, M. Torky, S. A. Ajagbe, M. Hammoudeh, and

[11] W. Li. “Metaverse-IDS: Deep Learning-Based Intrusion Detection System for Metaverse-IoT Networks.” Internet of Things (Netherlands), vol. 24, no. October, 2023, p. 100977, doi:10.1016/j.iot.2023.100977.

[12] Tang, F., X. Chen, M. Zhao, and N. Kato. “The Roadmap of Communication and Networking in 6G for the Metaverse.” IEEE Wirel. Commun., vol. 30, no. 4, 2023, pp. 72–81, doi:10.1109/MWC.019.2100721.

[13] Fernandez, C. B., and P. Hui. “Life, the Metaverse and Everything: An Overview of Privacy, Ethics, and Governance in Metaverse.” Proc. IEEE 42nd Int. Conf. Distrib. Comput. Syst. Work. ICDCSW 2022, 2022, pp. 272–277, doi:10.1109/ICDCSW56584.2022.00058.

[14] Farooqi, A. H., S. Akhtar, H. Rahman, T. Sadiq, and W. Abbass. “Enhancing Network Intrusion Detection Using an Ensemble Voting Classifier for Internet of Things.” Sensors, vol. 24, no. 1, 2024, doi:10.3390/s24010127.

[15] Ding, S., L. Kou, and T. Wu. “A GAN-Based Intrusion Detection Model for 5G Enabled Future Metaverse.” Mob. Networks Appl., vol. 27, no. 6, 2022, pp. 2596–2610, doi:10.1007/s11036-022-02075-6.Yuan, D., et al.

[16] “Intrusion Detection for Smart Home Security Based on Data Augmentation with Edge Computing.” IEEE Int. Conf. Commun., 2020, June 2020, doi:10.1109/ICC40277.2020.9148632.

[17] Yuan, D., et al. “Intrusion Detection for Smart Home Security Based on Data Augmentation with Edge Computing.” IEEE Int. Conf. Commun., 2020, June 2020, doi:10.1109/ICC40277.2020.9148632