RESEARCH ARTICLE

Bridging WSN and the Metaverse: An AI-Powered Hybrid Model for Cyber Threat Mitigation

Sanchit Vashisht[1] **and Shalli Rani**[1,*]

[1] Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura 140401, Punjab, India

Abstract

Wireless Sensor Networks (WSNs) have emerged as a fundamental technology in modern digital ecosystems, enabling real-time data acquisition and communication. Their integration with the metaverse enhances immersive experiences by providing real-time environmental data, motion tracking, and networked interactions. However, the fusion of WSNs with the metaverse introduces significant security challenges, including network vulnerabilities, data privacy concerns, latency issues, and scalability constraints, which hinder seamless operation. To address these challenges, Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) techniques have been leveraged to enhance network security, optimize resource management, and improve data processing efficiency. AI-driven models facilitate anomaly detection, predictive maintenance, and real-time decision-making, making WSN-based metaverse environments more resilient and adaptive. A hybrid DL and ML model is proposed, integrating Convolutional Neural Networks (CNNs) and Bidirectional Long Short-Term Memory (Bi-LSTM) for feature extraction, followed by XGBoost for classification. The model achieves 99.64% accuracy, 96.39% balanced accuracy, 99.65% precision, 99.64% recall, and 99.73% ROC-AUC score, outperforming existing approaches. The results demonstrate its effectiveness in detecting security threats within WSN-based metaverse environments while ensuring computational efficiency and real-time attack detection.

Keywords: wireless network, 5G, AI, network virtualization, 6G.

1 Introduction

The metaverse is a rapidly evolving digital ecosystem that integrates virtual and augmented environments to create immersive, interactive experiences. It is a collective digital space where users can interact with each other and digital elements in real-time [1]. This digital universe is driven by cutting-edge technologies, including AI and Extended Reality (XR), encompassing Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR). The metaverse offers applications in various sectors such as gaming, education, healthcare, and industrial simulations, making it a transformative force in modern digital interactions [2]. AR enhances the real-world environment by overlaying digital elements such as graphics, sounds, and haptic feedback. This

Submitted: 28 February 2025
Accepted: 26 May 2025
Published: 27 June 2025

Vol. 1, **No.** 1, 2025.
10.62762/TWN.2025.750033

***Corresponding author:**
✉Shalli Rani
shallir79@gmail.com

Citation
Vashisht, S., & Rani, S. (2025). Bridging WSN and the Metaverse: An AI-Powered Hybrid Model for Cyber Threat Mitigation. *ICCK Transactions on Wireless Networks*, 1(1), 32–41.

technology enables users to experience an enriched perception of their surroundings, commonly applied in fields such as retail, education, and navigation [3]. Unlike VR, AR does not replace the physical environment but rather integrates digital elements into it, facilitating a seamless blend of the real and virtual worlds.

VR and MR are two other key components of immersive technology. VR creates a fully digital environment, isolating users from the real world and immersing them in a computer-generated setting through specialized hardware like head-mounted displays (HMDs) [4]. On the other hand, MR combines elements of both AR and VR, allowing digital objects to interact with the physical world in real time. MR is extensively used in training simulations, remote collaboration, and industrial applications, making it a crucial component of metaverse development [5]. Wireless Sensor Networks (WSN) play a critical role in bridging the physical and digital worlds within the metaverse. A WSN consists of distributed sensor nodes that monitor and transmit environmental data, facilitating real-time interactions between users and the metaverse infrastructure [6]. These networks are widely implemented in smart cities, healthcare, and industrial automation, ensuring seamless data flow and intelligent decision-making in a metaverse-driven ecosystem. In the metaverse, WSNs provide essential functionalities such as environmental monitoring, motion tracking, and networked communication, enabling users to engage more effectively with the digital space [7].

Despite its potential, integrating WSN into the metaverse presents several challenges, including network latency, security vulnerabilities, energy constraints, and scalability issues [8]. The sheer volume of data generated by sensor nodes requires robust computational frameworks to process and analyze real-time information efficiently [8]. AI, ML, and DL are revolutionizing this field by enhancing network security, optimizing energy consumption, and improving data processing capabilities. Advanced AI-driven models facilitate anomaly detection, predictive maintenance, and intelligent decision-making, allowing WSN-based metaverse environments to overcome existing limitations and provide a seamless user experience [9]. These innovations continue to shape the evolution of WSNs, ensuring their effective integration into the metaverse while addressing the complexities associated with large-scale immersive environments.

2 Literature Review

The literature review explores existing research on WSN security in the metaverse, challenges in cyber threat detection, and advancements in AI-driven models, highlighting gaps that the proposed hybrid approach aims to address. Truong et al. [10] introduced MetaCIDS, a collaborative intrusion detection system that uses blockchain and federated learning to protect the metaverse. It can identify zero-day attacks that are resistant to poisoning and SPoF. According to performance evaluation, the accuracy scores of multiclass and anomaly detection ranges from 96% to 99% in four datasets. Wang et al. [11] looks at the metaverse's architecture, enabling technologies, and challenges of safely interfacing with data. It introduces Integrated Sensing, Communication, and Computing (SCC) to overcome resource limitations and discusses SCC-based solutions, significant findings, and future research directions.

Salmi et al. [12] suggests using lightweight, DL-based IDS for detection of DoS assaults in WSNs. On the WSN-DS dataset, CNN outperformed DNN, CNN, RNN, and CNN+RNN in terms of accuracy (98.79%). Feature selection for optimization is part of future work. Saleh et al. [13] presents SG-IDS, a ML-based IDS for WSNs using GNB and Stochastic Gradient Descent (SGD) algorithms. It achieved 98% accuracy, 96% recall, and 97% F1-score on WSN-DS, with strong IoMT dataset performance. Feature selection enhances efficiency and reduces overfitting.

Moundounga et al. [14] proposes a stochastic ML-based attack detection system for WSNs using HMMs and GMMs. It achieved 94.55% accuracy, with cross-validation scores ranging from 96% to 98%, demonstrating superior performance in detecting malicious activities and routing errors. Lai et al. [15] proposes an online-learning-based DoS attack detection model for WSNs, integrating feature selection and a noise-tolerant classifier. It achieved 97.16% accuracy, outperforming traditional algorithms. Future work aims to address external factors affecting detection performance.

Moudoud et al. [16] presents MAF-DRL, a framework combining Multi-Agent Federated Learning and Deep Reinforcement Learning to secure WSNs against emerging threats. It achieved 99% accuracy, enhancing attack detection, privacy, and energy efficiency while improving resilience against adversarial attacks. Panda et al. [17] proposes the ADSVM protocol

for detecting blackhole attacks in IoT networks using SVM. It achieved 84.37% accuracy through eightfold cross-validation on a newly created IoT dataset, improving attack prediction in both static and mobile WSN scenarios.

3 Preliminaries

WSNs have become a critical component in modern digital ecosystems, including the metaverse. The integration of WSNs with metaverse environments enables real-time data acquisition, immersive interactivity, and enhanced user experiences. However, this integration comes with various challenges, including security threats, latency issues, and network reliability concerns. In this section, we explore the implementation of WSNs in the metaverse, the challenges faced, and how ML and DL techniques are leveraged to mitigate these challenges.

3.1 Implementation of WSN in the Metaverse

The integration of WSNs into the metaverse is a multi-faceted process that involves real-time data sensing, transmission, and processing to create interactive and immersive experiences [20]. WSNs plays an important part in the metaverse by enabling real-time data acquisition through sensors that monitor environmental conditions and transmit data for visualization [18]. To enhance efficiency, edge and fog computing process data at local nodes before sending it to the cloud, reducing latency and bandwidth usage. Seamless connectivity is ensured by wireless communication protocols like ZigBee, LoRa, and 5G, facilitating fast and reliable data transfer. AI-driven context awareness further enhances decision-making by analyzing sensor data for anomaly detection, predictive maintenance, and adaptive responses [19]. To ensure security, cryptographic techniques and blockchain frameworks safeguard data against cyber threats, making WSNs a secure and efficient backbone for metaverse applications.

3.2 Challenges Faced in WSN-based Metaverse

Despite the potential benefits, integrating WSNs into the metaverse introduces several challenges. Scalability is a major concern, as managing numerous sensor nodes while maintaining seamless communication is complex [21]. Energy efficiency is also critical since sensor nodes have limited battery life, requiring optimized power usage. Data security and privacy must be ensured to protect confidentiality and integrity in an interconnected environment [22]. Additionally, minimizing latency is essential for real-time processing to enhance immersive experiences and decision-making. Lastly, network congestion due to high data traffic can lead to packet loss and reduced Quality of Service (QoS), affecting overall system performance [23].

3.3 Leveraging Machine Learning and Deep Learning for WSN-based Metaverse

To address the aforementioned challenges, ML and DL techniques have been employed to enhance the efficiency, security, and intelligence of WSN-based metaverse environments. Below, three prominent models such as XGBoost, CNN, and Bi-LSTM are discussed, along with their mathematical formulations, as they are being implemented for this study.

3.4 WSN Layer (Physical Environment)

3.4.1 XGBoost

XGBoost is an ensemble model that improves prediction accuracy by minimizing loss using gradient descent techniques. The model optimizes the objective function as shown in Eq 1:

$$Obj = \sum_{i=1}^{n} L(y_i, \hat{y}_i) + \sum_{k=1}^{K} \Omega(f_k) \tag{1}$$

where $L(y_i, \hat{y}_i)$ and $\Omega(f_k)$ are the loss function and the regularization term that prevents overfitting respectively. The predictions are computed iteratively, refining weak learners to enhance model performance.

3.4.2 Convolutional Neural Network (CNN)

CNNs are widely used in image and time-series data processing due to their feature extraction capabilities. The key operation in CNNs is the convolution, calculated as Eq 2:

$$Z_{i,j} = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} X_{i+m,j+n} W_{m,n} + b \tag{2}$$

where X , W, b, and Z are the input matrix, kernel weights, bias and the output feature map respectively. CNNs use pooling layers to reduce dimensionality and fully connected layers to make predictions.

3.4.3 Bidirectional Long Short-Term Memory

Bi-LSTM enhances sequence modeling by processing information in both forward and backward directions.

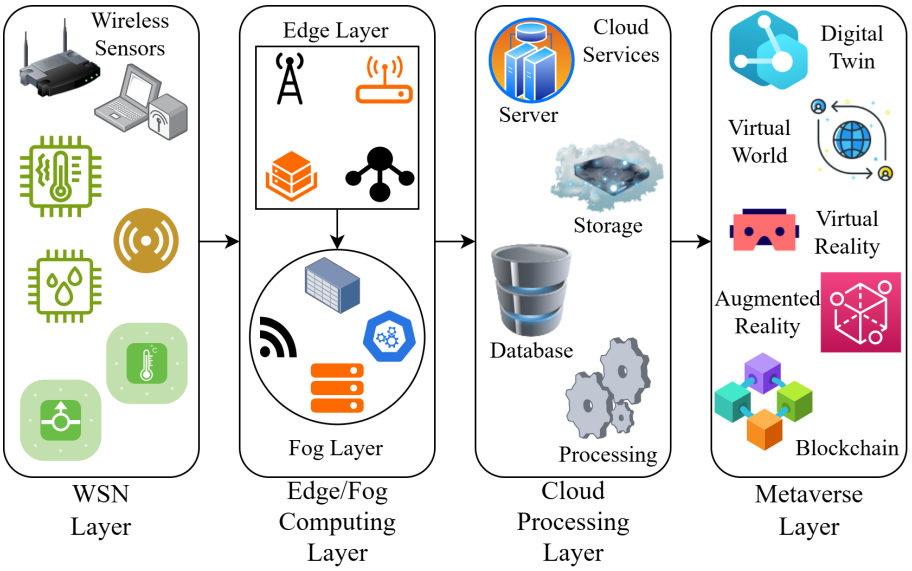

Figure 1. WSN enabled Metaverse architecture.

The LSTM cell is mathematically calculated as Eq 3:

$$\begin{aligned} f_t &= \sigma(W_f \cdot [h_{t-1}, x_t] + b_f), \\ i_t &= \sigma(W_i \cdot [h_{t-1}, x_t] + b_i), \\ \tilde{C}_t &= \tanh(W_C \cdot [h_{t-1}, x_t] + b_C), \\ C_t &= f_t * C_{t-1} + i_t * \tilde{C}_t, \\ o_t &= \sigma(W_o \cdot [h_{t-1}, x_t] + b_o), \\ h_t &= o_t * \tanh(C_t) \end{aligned} \tag{3}$$

where f_t, i_t, o_t are forget, input, and output gates respectively, controlling information flow. Bi-LSTMs process sequences bidirectionally, capturing dependencies effectively for time-series applications.

WSNs play a crucial role in metaverse environments, but their integration presents several challenges. The adoption of ML and DL techniques, including XGBoost, CNN, and Bi-LSTM, provides effective solutions for scalability, security, and real-time processing. The next sections will explore the experimental setup and evaluation of these models in WSN-based metaverse applications [24].

4 Metaverse Architecture

The metaverse is built upon a multi-layered architecture that integrates physical and digital environments to create immersive and interactive experiences. This architecture consists of several key layers, each playing a crucial role in ensuring seamless operation, data processing, and user interaction. Figure 1 illustrates the multi-layered architecture of metaverse.

The WSN layer forms the foundation of the metaverse by collecting real-world data through distributed sensor networks. These sensors monitor environmental parameters such as temperature, humidity, motion, and location. This layer ensures a continuous flow of real-time data, allowing digital twin systems to mirror physical environments accurately.

4.1 Edge/Fog Computing Layer

This layer processes data closer to the source by using edge and fog computing techniques. It reduces latency and bandwidth usage by filtering, aggregating, and preprocessing sensor data before sending it to the cloud. This enables faster decision-making and enhances real-time interactivity within the metaverse.

4.2 Cloud and AI Processing Layer

The cloud layer performs high-level data analytics, storage, and AI-driven decision-making. Machine learning models analyze large volumes of WSN data, detecting patterns and anomalies while ensuring scalability and reliability. AI algorithms help in predictive maintenance, security threat detection, and automated responses within the metaverse ecosystem.

4.3 Metaverse Layer (Digital Twin and XR Interface)

This final layer creates immersive experiences through digital twins and extended reality (XR) interfaces. The processed data from previous layers is used to render realistic and interactive virtual environments, enhancing user engagement. XR technologies such as AR, VR, and MR facilitate

seamless interactions between digital and physical worlds, making metaverse experiences highly dynamic and responsive.

5 Proposed Methodology

In this part, the suggested approach for attack detection in a WSN-based metaverse environment has been presented. The methodology leverages a hybrid DL and ML model comprising CNN, BiLSTM, and XGBoost to ensure accurate and efficient threat detection. Figure 2 depicts the steps followed in order to achieve the goal.

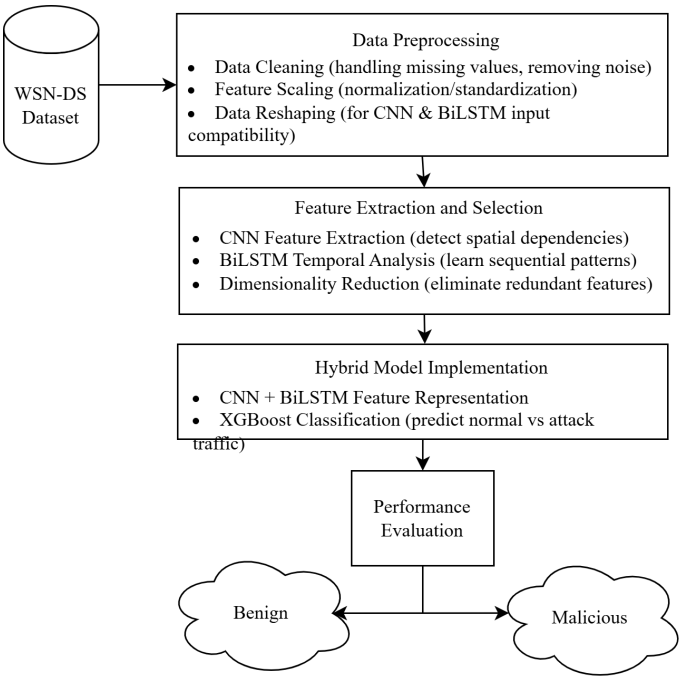

Figure 2. Proposed methodology.

5.1 Data Collection

Data collection is a crucial step in training and evaluating the proposed model. We used the WSN-DS dataset, a benchmark dataset specifically designed for detecting various attacks (e.g., DoS, blackhole, grayhole) in wireless sensor networks, to train and evaluate our hybrid model. The dataset consists of multiple features representing network traffic characteristics and labels corresponding to normal and attack classes.

5.1.1 Dataset Overview

The WSN-DS dataset [1] consists labeled network traffic data that includes normal and attack instances such as Denial-of-Service (DoS), blackhole, grayhole, and flooding attacks. The dataset provides essential attributes such as packet arrival time, packet size, transmission delays, and network connectivity metrics, which are useful for identifying suspicious patterns in network behavior.

The total dataset of 374661 is split into training and testing sets using an 80:20 ratio, ensuring that the model learns effectively while maintaining generalizability to unseen data. The training set is used for model learning, while the testing set is used for evaluation.

5.2 Pre-Processing

Before data is fed into the hybrid model, preprocessing ensures quality and consistency. First, data cleaning is performed to handle missing or irrelevant values, preventing inconsistencies. Next, feature scaling is applied through standardization to normalize numerical values, ensuring all features contribute equally to learning. Finally, the data is reshaped to fit the structured input format required by CNN and BiLSTM models, optimizing it for DL processing.

5.3 Feature Selection

Feature selection enhances the performance of the model by eliminating redundant and irrelevant attributes, ensuring that only the most relevant contribute to the detection of attacks. A CNN extracts meaningful patterns from network traffic data, capturing spatial dependencies and detecting anomalies. Meanwhile, BiLSTM analyzes sequential dependencies, identifying attack patterns that evolve over time. Finally, dimensionality reduction removes unnecessary features while preserving critical information, improving efficiency and classification accuracy.

5.4 Attack Detection

After feature extraction and refinement, attack detection is carried out using XGBoost, a highly efficient and accurate classifier. The CNN and BiLSTM models work together to generate a comprehensive feature representation of network activity. XGBoost then classifies traffic as normal or malicious based on these learned features. The model's performance is evaluated using various key metrics ensuring a thorough assessment of its effectiveness in real-time scenarios.

5.4.1 Training Time

Training time is a crucial metric that evaluates the efficiency of the model in terms of computational

[1] https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds/data

resources. It is defined as the total time taken to train the model on the given dataset. Lower training time is desirable for real-time applications. Figure 3 illustrates the training time for different models.

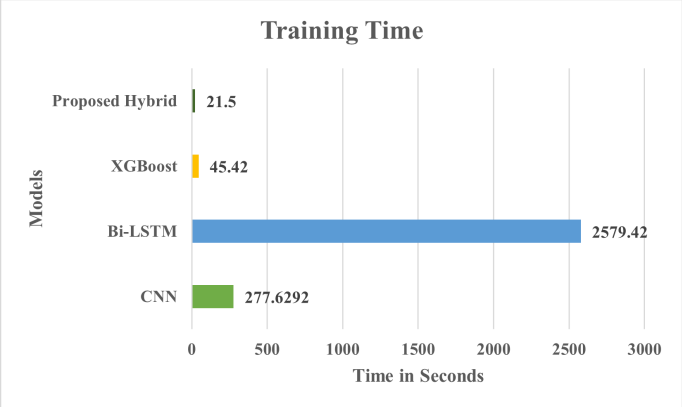

Figure 3. Training time of models.

5.4.2 Testing Time

Testing time measures the time taken by the model to make predictions on the test dataset. A lower testing time is preferred for real-time attack detection in WSN-based metaverse environments. Figure 4 presents the testing time of different models.

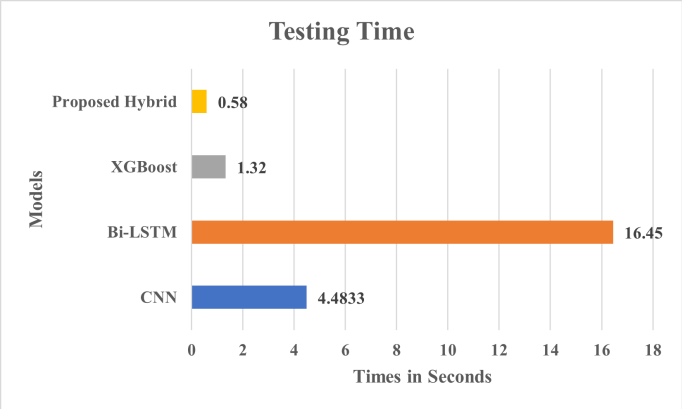

Figure 4. Testing time of models.

This hybrid approach ensures high accuracy in detecting various network attacks while maintaining computational efficiency, making it a robust solution for securing WSN-based metaverse environments. The computational efficiency of different models was evaluated based on their training and testing times. The CNN model required 277.63 seconds for training and 4.48 seconds for testing. The Bi-LSTM model had the highest computational demand, with a training time of 2579.42 seconds and a testing time of 16.45 seconds. XGBoost demonstrated significantly faster performance, requiring only 45.42 seconds for training and 1.32 seconds for testing. The proposed hybrid model outperformed all individual models in terms of efficiency, with the lowest training time of 21.5 seconds and the fastest testing time of 0.58 seconds.

6 Result and Analysis

In this part, the assessment and evaluation of the proposed hybrid model's performance. Various evaluation metrics are used to assess the efficiency and accuracy of the model in detecting attacks in a WSN-based metaverse environment.

6.1 Confusion Matrix

The confusion matrix is an essential evaluation tool that assesses the classification performance of the model. It consists of four key components: True Positives (TP), which represent correctly identified attack instances; False Positives (FP), where normal instances are mistakenly classified as attacks; True Negatives (TN), indicating correctly identified normal instances; and False Negatives (FN), where attack instances are incorrectly classified as normal. The confusion matrix helps in determining various performance metrics such as accuracy, recall, precision and F1-score. Figure 5 illustrates the confusion matrix of the proposed hybrid model.

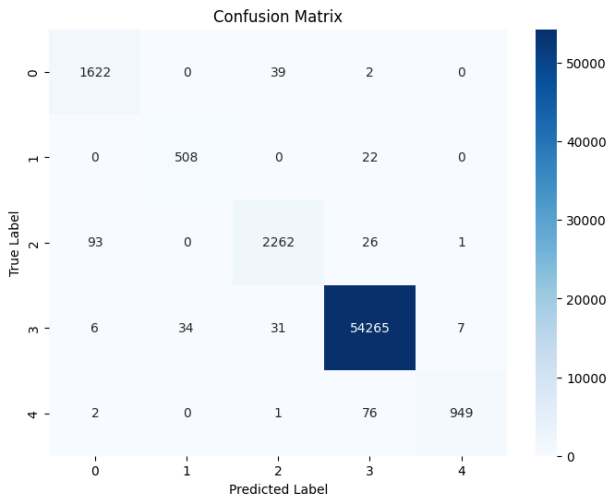

Figure 5. Confusion matrix of the proposed hybrid model.

Table 1 compares the proposed hybrid model with other models on the basis of accuracy, balanced accuracy, precision, recall and F1-score.

6.1.1 Accuracy

Accuracy is the rate of correctly predicted cases to the total cases in the dataset. It is evaluated as Eq 4:

$$ACC = \frac{TN + TP}{TN + TP + FN + FP} \tag{4}$$

Table 1. Comparison of the proposed hybrid model with other learning models

Models	Accuracy (%)	Balanced Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
CNN	98.73	92.06	98.78	98.73	98.22
Bi-LSTM	99.19	94.26	99.27	99.19	99.19
XGBoost	99.49	95.85	99.50	99.49	99.49
Proposed Hybrid	99.64	96.39	99.65	99.64	99.64

6.1.2 *Precision*

Precision measures the accuracy of positive class predictions and is given by Eq 5:

$$Precision = \frac{TP}{FP + TP} \tag{5}$$

Higher precision indicates fewer false positives.

6.1.3 *Recall*

Recall (or Sensitivity) measures the ability of the model to detect positive instances correctly, it is calculated as Eq 6:

$$Recall = \frac{TP}{FN + TP} \tag{6}$$

High recall ensures that most attack instances are correctly identified.

6.1.4 *F1-Score*

F1-score is the harmonic mean of precision and recall, balancing both metrics, it is calculated as Eq 7:

$$F1 - score = 2 \times \frac{P \times R}{P + R} \tag{7}$$

A higher F1-score indicates a better balance between precision(P) and recall(R)a. Figure 6 illustrates the comparison of different models based on their accuracy and other performance metrics.

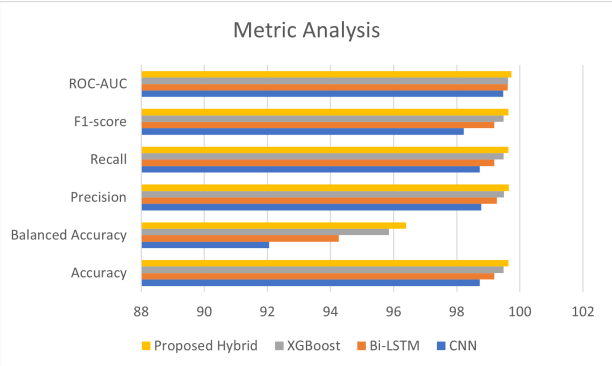

Figure 6. Comparison of models on the basis of performance matrices.

6.1.5 *ROC-AUC Curve*

The Receiver Operating Characteristic (ROC) curve plots the True Positive Rate (TPR) against the False Positive Rate (FPR).

A higher AUC value indicates better model performance. Figure 7 illustrates the ROC curve for the proposed hybrid model.

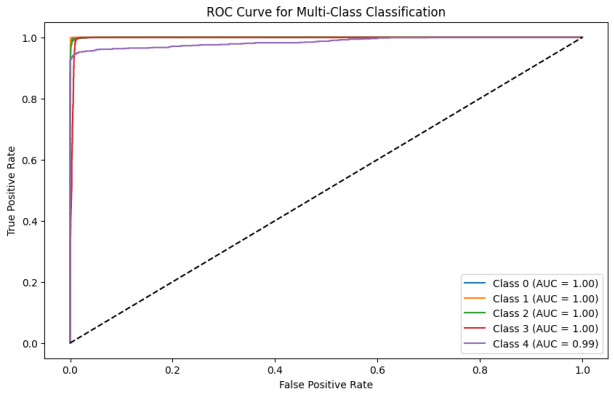

Figure 7. ROC curve of proposed hybrid model.

The ROC-AUC score, which measures the model's ability to distinguish between attack and normal instances, was evaluated for different models. The CNN model achieved an ROC-AUC of 99.47, indicating strong classification performance. The Bi-LSTM model improved slightly with an ROC-AUC of 99.62, showing enhanced capability in distinguishing attack patterns. The XGBoost model further refined this performance, achieving an ROC-AUC of 99.63, highlighting its robustness. The proposed hybrid model achieved the highest ROC-AUC of 99.73, demonstrating its superior effectiveness in accurately classifying network traffic instances.

6.1.6 *Matthews Correlation Coefficient*

Matthews Correlation Coefficient (MCC) is a balanced measure that takes into account all four confusion matrix elements. Figure 8 presents the MCC values for different models.

MCC was evaluated for different models to assess their overall classification performance, considering both true and false predictions. The CNN model achieved

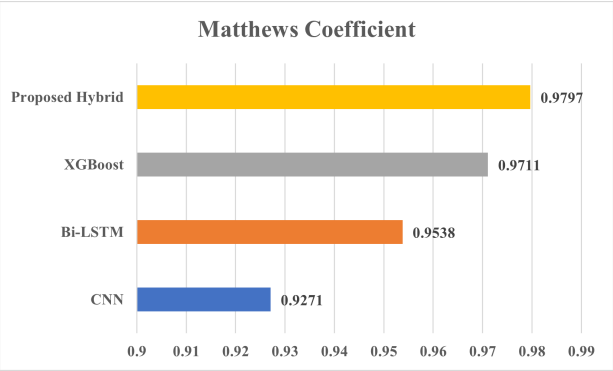

Figure 8. Matthews correlation coefficient of models.

an MCC of 0.9271, indicating strong predictive capability. The Bi-LSTM model improved upon this with an MCC of 0.9538, reflecting better-balanced classification performance. The XGBoost model further enhanced the results, achieving an MCC of 0.9711, demonstrating its robustness in distinguishing between normal and attack instances. The proposed hybrid model attained the highest MCC of 0.9797, highlighting its superior ability to maintain consistency across all classification categories.

6.1.7 Log Loss

Log Loss measures the uncertainty in probability-based classifications. Figure 9 presents the Log Loss for various models.

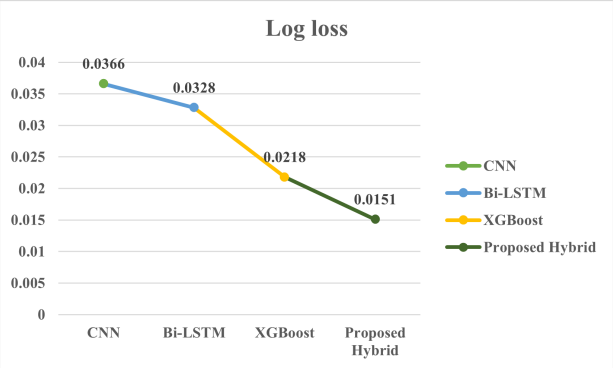

Figure 9. Logloss of models.

The log loss values of different models were analyzed to evaluate their predictive uncertainty and classification performance. The CNN model achieved a log loss of 0.0366, indicating a moderate level of uncertainty in its probability-based predictions. The Bi-LSTM model performed slightly better with a log loss of 0.0328, showing improved confidence in its classification decisions. The XGBoost model demonstrated even lower uncertainty, achieving a log loss of 0.0218. The proposed hybrid model outperformed all other models, achieving the lowest log loss of 0.0151, signifying its superior ability to generate highly confident and accurate predictions. The presented results confirm the effectiveness of the proposed hybrid CNN-BiLSTM-XGBoost model, achieving high accuracy and strong classification performance across multiple evaluation metrics.

7 Conclusion

The integration of WSNs with the metaverse has revolutionized real-time data acquisition, communication, and immersive interactions. However, this integration introduces several security challenges, including network vulnerabilities, privacy risks, latency issues, and scalability concerns. Ensuring a secure and efficient WSN-based metaverse environment requires advanced techniques capable of detecting and mitigating cyber threats in real time. To address these challenges, AI, ML, and DL have been employed to enhance network security, optimize computational efficiency, and improve decision-making. AI-driven models enable anomaly detection, predictive maintenance, and adaptive security mechanisms, making WSNs more resilient to cyber threats. By leveraging these technologies, real-time attack detection and efficient resource management can be achieved in large-scale metaverse ecosystems. A hybrid DL and ML model has been developed, integrating CNN and Bi-LSTM for feature extraction, followed by XGBoost for classification. The model demonstrates superior performance, achieving 99.64% accuracy, 96.39% balanced accuracy, 99.65% precision, 99.64% recall, 99.73% ROC-AUC score, 0.9797 MCC, and 0.0151 log loss. Additionally, the model exhibits high computational efficiency, with a training time of 21.5 seconds and a testing time of 0.58 seconds, significantly outperforming individual baseline models. These results highlight its efficiency in detecting security threats while maintaining low computational costs and real-time response capability, making it a promising solution for securing WSN-based metaverse environments. Future research can explore federated learning to enhance privacy-preserving attack detection by enabling decentralized model training across multiple WSN nodes. Additionally, integrating blockchain-based security frameworks can further strengthen data integrity and authentication within the metaverse. Advancements in edge AI can also reduce computational overhead, enabling faster decision-making and real-time threat mitigation. By incorporating these emerging technologies, the security, scalability, and adaptability of WSN-based

metaverse environments can be further improved.

Data Availability Statement

Data will be made available on request.

Funding

This work was supported without any funding.

Conflicts of Interest

The authors declare no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Murgai, V., Lolabhattu, V. R. R., Stimpson, R., Tripathi, E., & Chickala, S. (2024). Securing the metaverse: Traffic application classification and anomaly detection. In *2024 IEEE 25th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)* (pp. 111–117). IEEE. [CrossRef]

[2] Gupta, B. B., Gaurav, A., & Chui, K. T. (2023). Deep CNN Based Anomaly Detection in Centralized Metaverse Environment. In *2023 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)* (pp. 1–6). IEEE. [CrossRef]

[3] Rathore, S., & Park, J. H. (2018). Semi-supervised learning based distributed attack detection framework for IoT. *Applied Soft Computing, 72*, 79–89. [CrossRef]

[4] Liu, J., Kantarci, B., & Adams, C. (2020). Machine learning-driven intrusion detection for Contiki-NG-based IoT networks exposed to NSL-KDD dataset. In *Proceedings of the 2nd ACM workshop on wireless security and machine learning* (pp. 25–30). ACM. [CrossRef]

[5] 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. [CrossRef]

[6] Musleh, D., Alotaibi, M., Alhaidari, F., Rahman, A., & Mohammad, R. M. (2023). Intrusion detection system using feature extraction with machine learning algorithms in IoT. *Journal of Sensor and Actuator Networks, 12*(2), 29. [CrossRef]

[7] Gao, X., Shan, C., Hu, C., Niu, Z., & Liu, Z. (2019). An adaptive ensemble machine learning model for intrusion detection. *IEEE Access, 7*, 82512–82521. [CrossRef]

[8] Yu, Y., & Bian, N. (2020). An intrusion detection method using few-shot learning. *IEEE Access, 8*, 49730–49740. [CrossRef]

[9] Kurniawan, Y. I., Razi, F., Nofiyati, N., Wijayanto, B., & Hidayat, M. L. (2021). Naive Bayes modification for intrusion detection system classification with zero probability. *Bulletin of Electrical Engineering and Informatics, 10*(5), 2751–2758. [CrossRef]

[10] Truong, V. T., & Le, L. B. (2023). MetaCIDS: Privacy-preserving collaborative intrusion detection for metaverse based on blockchain and online federated learning. *IEEE Open Journal of the Computer Society, 4*, 253-266. [CrossRef]

[11] Wang, X., Guo, Q., Ning, Z., Guo, L., Wang, G., Gao, X., & Zhang, Y. (2024). Integration of Sensing, Communication, and Computing for Metaverse: A Survey. *ACM Computing Surveys, 56*(10), 1–38. [CrossRef]

[12] Salmi, S., & Oughdir, L. (2023). Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network. *Journal of Big Data, 10*(1), 17. [CrossRef]

[13] Saleh, H. M., Marouane, H., & Fakhfakh, A. (2024). Stochastic gradient descent intrusions detection for wireless sensor network attack detection system using machine learning. *IEEE Access, 12*, 3825-3836. [CrossRef]

[14] Moundounga, A. R. A., & Satori, H. (2024). Stochastic machine learning based attacks detection system in wireless sensor networks. *Journal of Network and Systems Management, 32*(1), 17. [CrossRef]

[15] Lai, T. T., Tran, T. P., Cho, J., & Yoo, M. (2023). DoS attack detection using online learning techniques in wireless sensor networks. *Alexandria Engineering Journal, 85*, 307–319. [CrossRef]

[16] Moudoud, H., Abou El Houda, Z., & Brik, B. (2024). Advancing security and trust in wsns: A federated multi-agent deep reinforcement learning approach. *IEEE Transactions on Consumer Electronics, 70*(1), 123–134. [CrossRef]

[17] Panda, N., & Supriya, M. (2023). Blackhole attack prediction in wireless sensor networks using support vector machine. In *Advances in Signal Processing, Embedded Systems and IoT* (pp. 321–331). Springer. [CrossRef]

[18] Gu, J., & Lu, S. (2021). An effective intrusion detection approach using SVM with naïve Bayes feature embedding. *Computers & Security, 103*, 102158. [CrossRef]

[19] Chakir, O., Rehaimi, A., Sadqi, Y., Alaoui, E. A. A., Krichen, M., Gaba, G. S., & Gurtov, A. (2023). An empirical assessment of ensemble methods and traditional machine learning techniques for web-based attack detection in industry 5.0. *Journal of King Saud University-Computer and Information Sciences, 35*(3), 103-119. [CrossRef]

[20] Logeswari, G., Bose, S., & Anitha, T. (2023). An intrusion detection system for sdn using machine learning. *Intelligent Automation & Soft Computing,*

35(1), 867–880. [CrossRef]

[21] Kuo, S. Y., Tseng, F. H., & Chou, Y. H. (2023). Metaverse intrusion detection of wormhole attacks based on a novel statistical mechanism. *Future Generation Computer Systems, 143*, 179–190. [CrossRef]

[22] Khan, L. U., Guizani, M., Yaqoob, I., Niyato, D., Al-Fuqaha, A., & Hong, C. S. (2024). A survey on metaverse-empowered 6G wireless systems: a security perspective. *Internet of Things, 25*, 101325. [CrossRef]

[23] Kashyap, D., & Sood, M. (2023). A Precursor to a Review of Security Scenario in Metaverse with Reference to the Security Protocols in Wireless Communication and IoT. In *The International Conference on Recent Innovations in Computing* (pp. 483–500). Springer. [CrossRef]

[24] Ali, M., Naeem, F., Kaddoum, G., & Hossain, E. (2023). Metaverse communications, networking, security, and applications: Research issues, state-of-the-art, and future directions. *IEEE Communications Surveys & Tutorials, 26*(2), 1238–1278. [CrossRef]

Sanchit Vashisht is pursuing his PhD from Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab, India. He received M.Tech. degree in Artificial Intelligence from Chitkara University, Rajpura, Punjab in 2024 and B.Tech. degree in Computer Science from Chitkara University, Rajpura, Punjab in 2022. His main area of interest and research are Metaverse, AR/VR, Internet of Things, Cybersecurity and Artificial Intelligence. (Email: Sanchit.vashisht@chitkara.edu.in)

Shalli Rani completed her Post-doc from Manchester Metropolitan University, UK in June, 2023. She is Professor in Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab, India. She has 18+ years teaching experience. She received MCA degree from Maharishi Dyanand University, Rohtak in 2004 and the M.Tech. degree in Computer Science from Janardan Rai Nagar Vidyapeeth University, Udaipur in 2007 and Ph.D. degree in Computer Applications from Punjab Technical University, Jalandhar in 2017. Her main area of interest and research are Wireless Sensor Networks, Underwater Sensor networks, Machine Learning and Internet of Things. She has published/accepted/presented more than 100+ papers in international journals /conferences (SCI+Scopus) and edited/authored five books with international publishers. She is serving as the associate editor of IEEE Future Directions Letters. She served as a guest editor in IEEE Transaction on Industrial Informatics, Wiley WCMC and Elsevier IoT Journals. She has also served as reviewer in many repudiated journals of IEEE, Springer, Elsevier, IET, Hindawi and Wiley. (Email: shallir79@gmail.com)