ISSN: 2320-5407
International Journal of Advanced Research
Publishers Name: Jana Publication and Research LLP
www.journalijar.com

REVIEWER'S REPORT

Manuscript No.: IJAR-53884 **Date: 17/09/2025**

Title: Homomorphic Encryption-Enabled Deep Learning Model for Intelligent Cyber Threat Detection

Recommendation:
Accept as it is .....
Accept after minor revision.....
Accept after major revision .....
Do not accept (*Reasons below*) .....

Reviewer Name: **Dr. GULNAWAZ GANI**

Detailed Review Report

The article *"Homomorphic Encryption-Enabled Deep Learning Model for Intelligent Cyber Threat Detection"* addresses an important problem in cybersecurity: detecting malicious activities in IoT-enabled networks while preserving privacy and ensuring secure authentication. The abstract (lines 3–17) is clear and informative, summarizing the motivation, methodology, and main findings with metrics such as 97.36% accuracy, 89.78% precision, and a low false positive rate of 2.17%. However, it could be strengthened by briefly explaining how homomorphic encryption is integrated into the model and what makes the Extended Physics-Informed Neural Network (EPINN) unique compared to other deep learning architectures. The keywords (lines 18–19) are relevant but could include "Homomorphic Encryption" explicitly to improve indexing and search visibility.

The introduction (lines 20–41) effectively explains the growing threat of cyberattacks, particularly in financial and banking sectors. It highlights the sensitivity of stored data (lines 28–33) and the challenges of implementing cyber-attack detection due to limited resources and high false positive rates (lines 34–36). These points establish the relevance of the work. Nonetheless, the introduction could benefit from a clearer research gap—specifically, why existing deep learning models without encryption are insufficient and how the proposed solution bridges this gap. The review of AI and machine learning for automated detection (lines 37–41) is useful but remains general; citing more recent studies (2022–2024) on privacy-preserving cyber detection would strengthen the state-of-the-art context.

The related works section (lines 42–88) is comprehensive, covering a range of models including DBN (lines 43–45), DNN (lines 47–50), LSTM (lines 51–54), RNN (lines 55–59), CNN (lines 61–65), GNN (lines 66–70), and hybrid feature reduction techniques for WSNs (lines 82–88). The comparisons are rich in metrics (accuracy, precision, specificity), but the narrative is dense and could be better organized with a small table summarizing each approach, dataset, and key limitation. The discussion of signature-based systems (lines 71–80) is also relevant but repeats some points on misclassification and scaling (lines 79–81). Consolidating these overlapping observations would improve clarity.

The proposed methodology (lines 89–103) presents a multi-stage pipeline involving data preprocessing, TF-IDF-based feature extraction, dimensionality reduction via Multi-Kernel PCA, and classification with

ISSN: 2320-5407
International Journal of Advanced Research
Publishers Name: Jana Publication and Research LLP
www.journalijar.com

REVIEWER'S REPORT

EPINN, followed by a Verifiable Ring Signature-based Authentication Protocol and BFV encryption. This is a strong framework that integrates privacy and detection. However, Figure 1 (line 122) and the accompanying description are too brief. The authors should describe in more detail how the homomorphic encryption interacts with EPINN during training and inference, and whether encryption affects model latency or resource requirements.

The subsections on data preprocessing (lines 104–120) and feature extraction (lines 123–150) are well explained and demonstrate a clear understanding of challenges in IoT environments. The description of TF-IDF (lines 130–146) and its equations (lines 137–142) is precise and mathematically correct. Still, it would be valuable to explain why TF-IDF, a text-based feature extraction method, is optimal for network traffic logs, and whether other approaches like word embeddings or autoencoders were considered. The PCA section (lines 151–157) could also specify how many components were retained and how variance was measured.

The classification section (lines 158–187) introduces EPINN and its structure diagram (lines 163–174, Figure 2 line 168), which is innovative. However, the text reads more like a general explanation of physics-informed neural networks rather than describing the specific configuration used in this paper. Details such as the number of layers, activation functions, learning rate, and training epochs should be added. The integration of the signature-based authentication protocol and BFV encryption (lines 179–187) is one of the paper's main contributions but is described only briefly; clarifying how this hybrid model outperforms conventional encryption or authentication methods would enhance the impact.

The results and discussion section (lines 189–211) reports implementation details, including hardware (lines 191–192) and dataset source (lines 193–195). The confusion matrix (lines 197–204) and training accuracy vs. loss curves (lines 206–211) indicate robust performance. Yet, the section does not compare the proposed model's metrics directly with those of baseline models mentioned in related works. Adding a comparative table or graph would clearly demonstrate performance gains. Furthermore, discussing computation time, scalability, and memory footprint would make the results more practical for real-world deployment.

The conclusion (lines 212–220) effectively summarizes the proposed system's strengths—high accuracy, low false positives, privacy preservation—but it lacks a discussion of limitations. Future work should address potential challenges such as computational overhead introduced by encryption, scalability to larger datasets, and real-time deployment. Adding 2–3 specific recommendations (e.g., using lightweight encryption schemes or federated learning to improve scalability) would make the conclusion more forward-looking.

Finally, the references (lines 221–268) are extensive and relevant, covering recent literature on deep learning, IoT security, and cyberattack detection. However, citation styles are inconsistent (some include full journal details, others do not), and a few references are outdated (pre-2020) despite newer work existing on privacy-preserving deep learning. Standardizing the style (APA or IEEE) and updating sources would increase professionalism.

Overall, this paper presents a promising and timely approach combining deep learning with homomorphic encryption for secure cyber threat detection. With clearer articulation of the research gap, more detailed methodological parameters, stronger comparisons with baselines, and a discussion of computational trade-offs, it has the potential to make a strong contribution to the field. **Recommendation: Minor Revisions.**