Review Form 3

Journal Name:	Asian Journal of Research in Computer Science
Manuscript Number:	**Ms_AJRCOS_131267**
Title of the Manuscript:	**The synergistic Role of Machine Learning, Deep Learning, and Reinforcement Learning in Strengthening Cyber Security Measures for Crypto Currency Platforms**
Type of the Article	

PART 1: Comments

	Reviewer's comment **Artificial Intelligence (AI) generated or assisted review comments are strictly prohibited during peer review.**	**Author's Feedback** *(Please correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)*
Please write a few sentences regarding the importance of this manuscript for the scientific community. A minimum of 3-4 sentences may be required for this part.	This manuscript presents a novel AI-driven cybersecurity framework for cryptocurrency platforms, integrating Machine Learning (ML), Deep Learning (DL), and Reinforcement Learning (RL) for fraud detection and smart contract security. Given the rising cybersecurity threats in decentralized finance (DeFi) and blockchain ecosystems, this study contributes significantly to the development of automated, adaptive security mechanisms. The research not only enhances fraud detection accuracy and adaptability but also provides insights into scalability, regulatory challenges, and AI ethics in financial security applications. This work is relevant to researchers, cybersecurity professionals, and financial institutions looking to enhance transaction security and risk mitigation in blockchain-based environments.	
Is the title of the article suitable? **(If not please suggest an alternative title)**	The current title, "The Synergistic Role of Machine Learning, Deep Learning, and Reinforcement Learning in Strengthening Cyber Security Measures for Cryptocurrency Platforms," is descriptive but too broad and lengthy. A more precise and engaging alternative could be: "AI-Driven Cybersecurity for Cryptocurrency: Integrating Machine Learning, Deep Learning, and Reinforcement Learning" This title maintains clarity, conciseness, and relevance while highlighting the core contributions of the study.	
Is the abstract of the article comprehensive? Do you suggest the addition (or deletion) of some points in this section? Please write your suggestions here.	The abstract provides a broad overview of the research but lacks a concise summary of key findings and performance improvements. It should include: A quantitative comparison of the proposed model with existing cybersecurity methods. A brief mention of real-world applicability and computational efficiency. The limitations of the approach and potential future directions. A more structured abstract would improve clarity and better communicate the impact of the research to readers.	
Is the manuscript scientifically, correct? Please write here.	The manuscript is scientifically sound in terms of methodology and experimental validation. However, there are areas that need improvement: Hyperparameter selection and computational complexity of the AI models should be better justified. Reinforcement Learning (RL) reward function design is not thoroughly analyzed, which could impact model effectiveness. A detailed comparison with existing hybrid AI-based cybersecurity frameworks is necessary to establish novelty.	
Are the references sufficient and recent? If you have suggestions of additional references, please mention them in the review form.	The manuscript cites relevant literature, but some recent works on AI-driven fraud detection, blockchain security, and RL in cybersecurity (published in 2022-2024) should be included. Suggested additional references: • Transformer-based fraud detection in financial transactions. • Federated learning for decentralized blockchain security.	

Review Form 3

	- Adversarial AI in cybercrime and fraud detection. Updating references would strengthen the literature review and positioning of the study.	

Review Form 3

Is the language/English quality of the article suitable for scholarly communications?	The manuscript is understandable but requires improvements in readability and scholarly tone. Some sections contain repetitive phrases, overly long sentences, and minor grammatical errors. Editing for conciseness, coherence, and technical precision would enhance clarity and engagement for an academic audience.	
Optional/General comments	1. The abstract lacks clarity on how different AI techniques (ML, DL, RL) contribute uniquely to cybersecurity in cryptocurrency platforms. The sentence "The study applies anomaly detection, supervised machine learning (Logistic Regression), comparative performance analysis (Random Forest), and regression analysis (OLS) to evaluate fraud trends..." (Page 1) should briefly explain why these specific methods were chosen over alternative techniques such as transformer-based models or hybrid AI approaches. 2. The introduction discusses the threat landscape but does not clearly highlight the research gap addressed by this study. The sentence "As decentralized finance (DeFi) and blockchain-based transactions gain adoption, cybercriminals exploit vulnerabilities..." (Page 2) should explicitly state how existing AI-based solutions fall short and how this study offers improvements. 3. The related works section lacks comparative analysis of recent cybersecurity AI frameworks used in blockchain. The paragraph "Sarker et al. (2024) posits that traditional cybersecurity frameworks, which rely on rule-based methodologies, lack the adaptability..." (Page 3) should compare this study's approach with recent hybrid AI-driven threat detection models to establish novelty. 4. The methodology does not clearly justify why Logistic Regression was used instead of more advanced classification techniques. The sentence "A Logistic Regression model is trained on the SolidiFI-Benchmark dataset to classify smart contracts as secure (y=0) or vulnerable (y=1)." (Page 10) should be expanded to discuss why non-linear models (e.g., deep neural networks, XGBoost) were not considered. 5. The dataset selection process is not well explained. The sentence "Data was sourced from Elliptic Bitcoin Dataset, SolidiFI-Benchmark, CryptoScamDB, and CipherTrace AML Reports, ensuring comprehensive coverage of fraud detection, anomaly identification, and security model evaluation." (Page 12) should provide insights into data preprocessing steps, handling of missing values, and class balance for robust evaluation. 6. The study lacks an ablation study to show the contribution of different components in the model's performance. The sentence "Experimental results show that the proposed models outperform traditional security frameworks in fraud detection." (Page 15) should include comparisons between baseline models with and without reinforcement learning (RL) to validate the impact of the RL component. 7. The deep learning section does not explain the computational complexity of the proposed models. The paragraph "Deep Learning has played a transformative role in fraud prevention by identifying intricate cyber threat patterns." (Page 16) should discuss training time, resource requirements, and feasibility for real-time fraud detection. 8. The reinforcement learning (RL) methodology lacks clarity on how reward functions were designed to optimize security outcomes. The sentence "The Actor–Critic RL algorithm achieved a high success rate in cyber-attack defense simulations." (Page 18) should explain how reward shaping techniques were used to prevent suboptimal policy learning. 9. The section discussing smart contract vulnerabilities does not include an empirical evaluation of AI-driven auditing techniques. The sentence "ML algorithms are adopted to analyze smart contract code, allowing for early detection of vulnerabilities before exploitation occurs." (Page 20) should provide quantitative results comparing AI-based auditing with traditional static code analysis tools. 10. The discussion overstates the model's effectiveness without addressing its limitations. The	

	sentence "Our results demonstrate that AI-driven security significantly reduces fraud cases in cryptocurrency transactions." (Page 22) should include a discussion on false positive rates, adversarial AI risks, and potential bias in fraud detection models. 11. The regulatory challenges section does not adequately discuss the impact of data privacy laws (e.g., GDPR, CCPA) on AI-driven fraud detection in cryptocurrency platforms. The sentence "Governments and financial authorities are tightening oversight of cryptocurrency security practices..." (Page 24) should explore the balance between AI surveillance and user privacy concerns. 12. The paper does not evaluate whether the AI models can scale with increasing transaction volumes. The paragraph "AI-based models provide real-time fraud detection capabilities." (Page 26) should discuss how latency, throughput, and computational efficiency were tested under high-volume transactions. 13. The study lacks a clear analysis of why AI-based models are preferable to traditional heuristic-based rule systems. The sentence "AI-driven models reduce false positives in fraud detection while improving real-time adaptability." (Page 27) should include specific accuracy and precision trade-offs compared to rule-based systems. 14. The future work section is too generic and does not propose concrete next steps. The sentence "Future research should explore integrating reinforcement learning to enhance AI adaptability." (Page 28) should specify how self-supervised learning, federated learning, or quantum-resistant AI can improve cybersecurity. 15. The conclusion does not summarize practical deployment challenges of the proposed AI cybersecurity framework. The paragraph "The study recommends integrating reinforcement learning to enhance AI adaptability, implementing standardized AI compliance frameworks..." (Page 30) should outline barriers to adoption, including high implementation costs and regulatory uncertainty.	

PART 2:

	Reviewer's comment	**Author's comment** *(if agreed with reviewer, correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)*
Are there ethical issues in this manuscript?	*(If yes, Kindly please write down the ethical issues here in details)*	

Reviewer Details:

Name:	**V. Gokula Krishnan**
Department, University & Country	**Saveetha School of Engineering, SIMATS University, India**