Review Form 3

Journal Name:	**Journal of Engineering Research and Reports**
Manuscript Number:	**Ms_JERR_131308**
Title of the Manuscript:	**Cloud Computing and Data Security: Addressing Data Privacy Concerns in Digital Currency Transactions**
Type of the Article	**Review Article**

Review Form 3

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 addresses critical challenges at the intersection of cloud computing, data security, and digital currency transactions—a timely topic given the rapid adoption of blockchain technologies and cloud infrastructure in finance. It provides empirical insights into AI-driven fraud reduction, quantum-resistant cryptography, and regulatory frameworks, offering actionable strategies for securing digital financial ecosystems. The integration of quantitative analysis with emerging threats like adversarial AI and quantum computing makes it a valuable resource for researchers and practitioners aiming to balance innovation with security and privacy.	
Is the title of the article suitable? **(If not please suggest an alternative title)**	Suggested alternative: "Cloud Computing and Data Security in Digital Currency Transactions: Mitigating Risks Through AI, Post-Quantum Cryptography, and Regulatory Compliance."	
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 is comprehensive but could emphasize the study's limitations (e.g., reliance on future-dated data). Add: "This study highlights challenges in reconciling speculative future incidents (e.g., 2025 breaches) with current cryptographic and regulatory frameworks."	
Is the manuscript scientifically, correct? Please write here.	The manuscript is scientifically sound in its methodology and analysis. However, citing future-dated references (e.g., 2025 publications) and hypothetical incidents (e.g., the 2025 Phemex hack) undermines credibility. These should either be replaced with peer-reviewed, published works or explicitly framed as projections.	
Are the references sufficient and recent? If you have suggestions of additional references, please mention them in the review form.	References are extensive but include speculative or non-peer-reviewed sources	

Review Form 3

Is the language/English quality of the article suitable for scholarly communications?	The language is suitable for scholarly communication but has minor grammatical errors and formatting inconsistencies	
Optional/General comments	The manuscript relies heavily on future-dated references (e.g., 2025 publications) and hypothetical incidents (e.g., the 2025 Phemex hack). This undermines the credibility and scientific rigor of the study. Many references are from non-peer-reviewed sources, such as news articles (e.g., SecurityWeek, Forbes) and blog posts, which lack the academic rigor expected in scholarly research. While the methodology section outlines statistical and time-series analyses, it lacks sufficient detail on data collection, preprocessing, and validation. This makes it difficult to assess the reproducibility of the study. The manuscript contains formatting inconsistencies, such as misplaced brackets, incomplete sentences, and irregular citation styles, which detract from its professionalism. While AI and quantum computing are important, the manuscript disproportionately focuses on these topics without adequately addressing other critical security concerns, such as insider threats or social engineering attacks. The manuscript does not sufficiently discuss the limitations of the study, such as the reliance on publicly available datasets, potential biases in the data, or the speculative nature of future-dated references. While privacy-enhancing technologies like zero-knowledge proofs and homomorphic encryption are mentioned, their practical implementation challenges (e.g., computational overhead, scalability) are not thoroughly explored. The manuscript briefly mentions regulatory frameworks like GDPR and MiCA but does not provide a detailed analysis of how these regulations interact with technological advancements in cloud-based cryptocurrency systems. **While generally suitable for scholarly communication, the manuscript contains grammatical errors, awkward phrasing, and repetitive language, which could be improved through thorough editing.**	

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:	**Hemraj S L**
Department, University & Country	**Vellore Institute of Technology Bhopal University, India**