|  |  |
| --- | --- |
|  | |
| Journal Name: | [**Asian Journal of Research in Computer Science**](https://journalajrcos.com/index.php/AJRCOS) |
| Manuscript Number: | **Ms\_AJRCOS\_133363** |
| Title of the Manuscript: | **Enhancing Security in Private Network Communications through Advanced Encryption Gateways: Innovations, Implementations, and Performance Analysis** |
| Type of the Article | **Short communication** |

|  |  |  |
| --- | --- | --- |
| 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 paper brings big news for the science and cybersecurity communities with an adaptive encryption gateway architecture that balances performance, security, and compatibility. With dynamic algorithm selection, protocol conversion, and quantum-resistant features it tackles the biggest challenges in securing private network communications – especially in high-risk areas like healthcare, finance, and defense. Real-world case studies and empirical data make this paper practical and set the stage for future secure data transmission innovation. Overall it moves the ball forward for secure network infrastructure in a more connected and threatful digital world. |  |
| **Is the title of the article suitable?**  **(If not please suggest an alternative title)** | Yes, it's quite suitable. |  |
| 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 ok and gets the importance, architecture, evaluation and reality of encryption gateways across. However, there are a few things to improve to make it clearer and focused:  **Strengths of the Abstract:** States the problem (private networks security). Highlights the key features of the solution (encryption algorithms, protocol conversion, tunnel creation). Mentions the performance (40% throughput, 60% latency). Has empirical data, simulations and case studies which is great.  **Things to improve:** Be more specific: Add a sentence that explains what’s new about this vs existing encryption gateways. More technical depth: Hybrid encryption models are mentioned but naming the actual algorithms (e.g. AES, ChaCha20) can help. Simplify language: Consider removing “Mermaid diagrams illustrate…” from the abstract; diagrams tools are better mentioned in the main text not the abstract. Future-proofing: Add a sentence about how this contributes to future-proofing network security (e.g. quantum resilient encryption or ML-based adaptability). |  |
| Is the manuscript scientifically, correct? Please write here. | Yes, the manuscript is right and grounded in current cryptography and network security. It shows good understanding of encryption gateway architecture, encryption algorithms (e.g. AES, ChaCha20, RSA, Kyber), protocol conversion (e.g. FTP to SFTP), and secure tunnel protocols (e.g. IPsec, WireGuard). The use of empirical data, diagrams and real world case studies adds scientific credibility and practical validation to the concepts.   * Correctly distinguishes symmetric and asymmetric encryption and their trade-offs. * Uses hybrid encryption based on traffic type (bulk vs real-time). * Incorporates TEE, blockchain logging and future looking concepts like QKD. * Discusses practical implementation issues and presents scientific solutions.   In summary the paper is **technically correct**, it uses current knowledge and looks forward to emerging threats and technologies. Minor improvments could be made to explain some technical terms for a broader scientific audience but the core is solid. |  |
| **Are the references sufficient and recent? If you have suggestions of additional references, please mention them in the review form.** | Yes, its mostly relevant. Adding 2-3 well-chosen foundational and emerging topics references would make the manuscript even more robust and well-supported. |  |
| Is the language/English quality of the article suitable for scholarly communications? | Overall this is academic language but could be a bit clearer, more consistent and easier to follow.  What works well is the technical terms are correct and demonstrate a good understanding of cyber security and encryption. Most of the sentences are clear and the section headings and formatting help the reader. The diagrams support the technical content well.  However there are some areas to improve. The terms ChaCha20 and AES should be used consistently throughout the document. A few sentences are a bit long or repetitive and could be simplified. The tone could be more formal, instead of "digital Great Wall" it should be more neutral. Minor grammar and wording issues could be polished, e.g. plural and singular forms, and "prioritize" should be clarified in context. |  |
| Optional/General comments |  |  |

|  |  |  |
| --- | --- | --- |
| **PART 2:** | | |
|  | Reviewer’s comment | Author’s comment *(if agreed with the 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 detail)* |  |

**Reviewer Details:**

**Raja Chattopadhyay, USA**