**MULTI-HYPERVISOR-BASED AUTHORIZATION AND DOS ATTACK MITIGATION FRAMEWORK USING LC-WTRNN TECHNIQUE**

* Justify the use of the Hamming Code Quantum Cryptography (HC-QC) for encryption in terms of its computational efficiency and error correction capabilities compared to other quantum cryptographic methods.
* Provide detailed explanations of how KLDS-KAnonymity mitigates privacy risks compared to traditional anonymization methods like T-Closeness and L-Diversity.
* Elaborate on how the HellBhatt Tiger Hashing Algorithm (HB-THA) ensures scale invariance in hash tree creation, with comparative references to other hashing algorithms.
* Add clarity on how the preprocessing steps, such as Missing Value Imputation and Data Deduplication, impact the integrity of the final dataset for attack classification.
* Highlight how the proposed system outperformed the existing models in reducing false positives and negatives, with specific examples or confusion matrix insights.
* Expand on the significance of the reduced training time (36,849 ms) for LC-WTRNN and its implications for real-time applications.
* Defend the security improvement of HC-QC (98.65%) compared to Elliptic Curve Cryptography (ECC) or RSA, citing specific vulnerabilities addressed.
* Discuss the applicability of the LC-WTRNN model in other domains beyond hypervisor DoS attack mitigation, supporting generalizability.
* Offer a comparative analysis of the anonymization time (986 ms) achieved with KLDS-KAnonymity and its potential real-world implications for privacy-sensitive applications.
* Explain the rationale behind using the Boltzmann Binomial Entropy (BBE) in the BBE-WSOA, particularly in mitigating premature convergence.
* Develop the comparison section to discuss the limitations of Deep Belief Networks (DBNs) and Restricted Boltzmann Machines (RBMs) for DoS detection.
* Data encryption and hashing performance should be evaluated using metrics that align with the objectives of security and integrity