International Research Journal of Innovative Engineering (IRJIE)

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 7, Issue 6, November- December 2023|

DOI:10.15680/IRJIE.2023.0706001

Quantum-Resistant Cryptographic Security Models for Secure Enterprise Cloud Communication Networks

Pravallika Mannem

Principal Data Engineer, ProBPM, Inc, Atlanta, USA

ABSTRACT: Quantum computing introduces a fundamental threat to classical cryptographic systems widely deployed in enterprise cloud communication networks. Algorithms such as RSA, ECC, and Diffie–Hellman rely on computational hardness assumptions that can be efficiently broken using quantum algorithms like Shor's algorithm. This emerging risk necessitates the development of quantum-resistant cryptographic security models capable of ensuring long-term confidentiality, integrity, and authentication in cloud-based systems.

This research investigates post-quantum cryptography (PQC) approaches, including lattice-based encryption, hash-based signatures, multivariate polynomial schemes, and code-based cryptography, for securing enterprise cloud communication networks. It further explores hybrid cryptographic architectures that combine classical and quantum-resistant algorithms to support gradual migration in real-world infrastructures.

The study evaluates secure key exchange protocols, authentication frameworks, and encrypted communication pipelines in distributed cloud environments. Emphasis is placed on scalability, computational efficiency, latency overhead, and resistance to quantum adversaries.

Findings indicate that lattice-based and hybrid cryptographic models offer the most practical balance between security strength and performance. However, challenges such as increased computational cost, integration complexity, and lack of universal standards remain significant barriers. The study concludes that adopting quantum-resistant cryptographic models is essential for future-proofing enterprise cloud security architectures against the imminent rise of quantum computing threats.

KEYWORDS: Post-Quantum Cryptography, Quantum-Resistant Security, Cloud Computing Security, Lattice-Based Cryptography, Enterprise Networks, Secure Communication, Cryptographic Protocols, Hybrid Encryption, Digital Signatures, Quantum Computing Threats

I. INTRODUCTION

Enterprise cloud computing has become the backbone of modern digital infrastructure, enabling scalable storage, distributed processing, and real-time communication across global systems. Organizations increasingly rely on cloud environments for mission-critical applications such as financial transactions, healthcare data management, supply chain operations, and enterprise communication networks. While cloud computing offers efficiency and flexibility, it also introduces complex security challenges, particularly in the protection of sensitive communication channelsCryptographic systems form the foundation of secure cloud communication. Classical public-key algorithms such as RSA, ECC, and Diffie–Hellman are widely used for encryption, authentication, and secure key exchange. These systems depend on mathematical problems that are computationally infeasible for classical computers, such as integer factorization and discrete logarithms. However, the emergence of quantum computing poses a serious threat to these assumptions.

Quantum computing leverages quantum mechanical phenomena such as superposition and entanglement to perform computations exponentially faster than classical systems for certain problem classes. Shor's algorithm demonstrates that quantum computers can efficiently break RSA and ECC encryption, rendering most current cryptographic systems insecure in a post-quantum world. Similarly, Grover's algorithm reduces the effective security strength of symmetric encryption schemes, further amplifying security risks.This impending quantum threat has led to the development of

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 7, Issue 6, November- December 2023|

DOI:10.15680/IRJIE.2023.0706001

post-quantum cryptography (PQC), which focuses on designing cryptographic algorithms resistant to both classical and quantum attacks. Unlike traditional systems, PQC relies on mathematical problems that remain difficult even for quantum computers, including lattice problems, hash functions, and coding theory.Enterprise cloud communication networks require not only strong security but also high performance, low latency, and scalability across distributed environments. Therefore, integrating PQC into cloud infrastructures presents significant technical challenges. Many post-quantum algorithms are computationally intensive, requiring optimization for real-time applications.

To address these challenges, hybrid cryptographic systems have emerged as a transitional solution. These systems combine classical encryption techniques with post-quantum algorithms to ensure compatibility while gradually improving security strength. This approach allows enterprises to maintain operational continuity while preparing for quantum-safe infrastructures.This research explores quantum-resistant cryptographic models for enterprise cloud communication networks. It examines their theoretical foundations, practical implementations, performance trade-offs, and deployment strategies. The objective is to develop a comprehensive understanding of how organizations can transition toward quantum-safe communication systems without compromising efficiency or scalability.

II. LITERATURE REVIEW

The evolution of cryptographic systems has been closely tied to advancements in computational capabilities. Early cryptographic mechanisms such as Caesar cipher and substitution ciphers were replaced by more sophisticated symmetric-key systems like DES (Data Encryption Standard) and AES (Advanced Encryption Standard). While AES remains secure against classical attacks, public-key systems such as RSA and ECC form the backbone of modern secure communication systemsThe discovery of quantum computing introduced a paradigm shift in cryptographic security. Shor's algorithm, developed in 1994, demonstrated that quantum computers could efficiently solve integer factorization and discrete logarithm problems. This finding directly undermined the security assumptions of RSA and ECC, which rely on these problems being computationally infeasible.In response, researchers developed post-quantum cryptography (PQC), focusing on mathematical problems resistant to quantum attacks. Lattice-based cryptography has emerged as the leading candidate in this domain. Problems such as Learning With Errors (LWE) and Ring-LWE form the basis of secure encryption schemes like CRYSTALS-Kyber, which has been selected by NIST for standardization.Hash-based cryptographic systems represent another important class of PQC. Schemes such as Merkle Signature Schemes and XMSS rely solely on the security of cryptographic hash functions. These systems are highly secure but often suffer from limitations such as large signature sizes and state management complexity.Code-based cryptography, particularly the McEliece cryptosystem, has been studied for decades and remains resistant to known quantum attacks. However, its large key sizes make it less practical for cloud-based environments where bandwidth efficiency is critical.

Multivariate polynomial cryptography involves solving systems of quadratic equations over finite fields. While computationally efficient, many proposed schemes in this category have been broken, limiting their long-term viability. The National Institute of Standards and Technology (NIST) has played a critical role in standardizing post-quantum cryptographic algorithms. After extensive evaluation, lattice-based schemes such as CRYSTALS-Kyber (encryption) and CRYSTALS-Dilithium (digital signatures) have been selected as primary candidates for future cryptographic standards.In cloud computing environments, secure communication is typically implemented using TLS (Transport Layer Security), VPNs, and secure API gateways. Researchers have proposed PQ-TLS, which integrates post-quantum algorithms into TLS protocols to ensure quantum-safe communication.Hybrid cryptographic models have gained significant attention as transitional solutions. These systems combine classical and post-quantum algorithms, such as RSA + lattice-based encryption, to maintain backward compatibility while introducing quantum resistance.Performance remains a major challenge in PQC deployment. Many post-quantum algorithms introduce increased computational overhead, larger key sizes, and higher latency compared to classical systems. This can negatively impact real-time applications such as cloud-based financial systems and IoT communication networks.

To address performance concerns, researchers are exploring hardware acceleration techniques using GPUs, FPGAs, and dedicated cryptographic processors. Cloud-native security frameworks are also being developed to abstract cryptographic complexity and improve scalability.Despite advancements, challenges remain in interoperability, standardization, and migration strategies. Most existing enterprise systems are built on classical cryptographic infrastructures, making the transition to PQC complex and costly.Overall, literature strongly supports the necessity of post-quantum cryptography for future secure communication systems. Lattice-based and hybrid models currently represent the most viable solutions for enterprise cloud environments.

International Research Journal of Innovative Engineering (IRJIE)

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

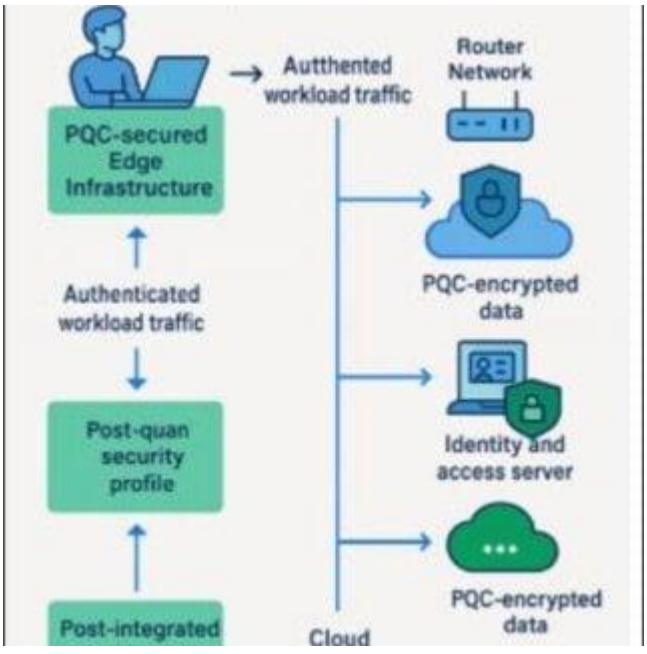
|Volume 7, Issue 6, November- December 2023|

DOI:10.15680/IRJIE.2023.0706001

III. RESEARCH METHODOLOGY

The research adopts a structured experimental design focusing on evaluating quantum-resistant cryptographic models in enterprise cloud communication networks. The system architecture is designed as a multi-layered framework consisting of client interfaces, secure communication middleware, cloud service nodes, and cryptographic processing units. Classical cryptographic systems such as RSA and ECC are benchmarked against post-quantum cryptographic (PQC) algorithms under identical network conditions. The study integrates both simulation-based modeling and real-world inspired enterprise cloud scenarios. Hybrid encryption models are incorporated to evaluate transitional security frameworks. The experimental setup ensures controlled comparison of performance, security strength, and computational efficiency across different cryptographic schemes. The architecture supports distributed execution, enabling evaluation across multiple virtual cloud nodes. Security protocols are embedded at the transport and application layers to simulate real enterprise communication environments. The research also considers scalability across multi-tenant cloud systems. This design ensures comprehensive evaluation of both theoretical and practical cryptographic performance. Key performance indicators include latency, throughput, encryption time, and resource utilization. Security strength is assessed against both classical and quantum adversarial models. The architecture allows modular replacement of cryptographic algorithms. This enables systematic evaluation of multiple PQC candidates. The design ensures reproducibility and extensibility of results.

The study utilizes synthetic enterprise cloud communication datasets combined with simulated real-world network traffic patterns. Data includes encrypted message exchanges, authentication logs, key exchange sequences, and API communication flows. A controlled cloud simulation environment is established using distributed virtual machines and cryptographic libraries supporting PQC algorithms. Threat modeling incorporates both classical adversaries and quantum-capable attackers capable of executing Shor's and Grover's algorithms. Attack scenarios include man-in-the-middle attacks, replay attacks, key recovery attempts, and ciphertext analysis. Noise injection techniques are used to simulate real-world network instability and packet loss. The simulation environment supports variable network loads to test scalability under stress conditions. Cloud traffic is modeled to reflect enterprise workloads such as financial transactions and secure API calls. Security benchmarks are defined under normal, peak, and adversarial operating conditions. The dataset is partitioned into training, validation, and testing communication flows. Encryption and decryption events are logged for performance measurement. The environment ensures deterministic reproducibility of cryptographic tests. Multi-node communication is simulated to evaluate distributed security performance. This setup enables realistic evaluation of cryptographic resilience. It also allows comparison across different attack intensities and system loads.



| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 7, Issue 6, November- December 2023|

DOI:10.15680/IRJIE.2023.0706001

Fig 1: End-to-end architecture diagram showing post-quantum cryptography

The implementation includes multiple cryptographic schemes covering classical, hybrid, and post-quantum models. Classical algorithms include RSA-2048 and ECC-based encryption systems. Post-quantum implementations include CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures. Hash-based schemes such as XMSS are used for secure authentication processes. Code-based cryptography using McEliece is implemented for comparative analysis. Hybrid models combine RSA with lattice-based encryption to ensure backward compatibility. Key generation, encryption, decryption, and signature verification processes are implemented using optimized cryptographic libraries. Secure TLS-like communication protocols are extended to incorporate PQC algorithms. Algorithm execution is optimized using parallel processing and memory-efficient encoding techniques. Parameter tuning is performed to balance security strength and computational cost. Cryptographic key sizes and ciphertext expansion rates are analyzed in detail. Security proofs are evaluated based on computational hardness assumptions. Each algorithm is tested under identical input conditions for fairness. Implementation ensures modular architecture for replacing cryptographic primitives. This allows flexible experimentation across different security models.

Performance evaluation is conducted using multiple quantitative and qualitative metrics. Key metrics include encryption latency, decryption time, key generation overhead, and communication throughput. Resource utilization metrics include CPU usage, memory consumption, and network bandwidth overhead. Security evaluation focuses on resistance to quantum attacks, classical cryptanalysis, and brute-force attempts. Cryptographic entropy is measured to assess randomness and unpredictability. Formal verification techniques are applied to validate protocol correctness. Stress testing is conducted under high-load enterprise cloud conditions. Comparative analysis is performed between classical, hybrid, and post-quantum systems. Trade-offs between security strength and computational efficiency are analyzed. Real-time performance degradation is measured under scaling conditions. Attack simulation results are used to evaluate system robustness. Multi-node synchronization delays are analyzed in distributed environments. Benchmarking tools are used to visualize performance differences. Statistical analysis ensures result reliability. The framework ensures comprehensive evaluation of both security and efficiency dimensions.

Optimization strategies include algorithmic tuning, parallel computation, and hardware acceleration using GPUs and FPGA-based cryptographic modules. Memory optimization techniques are applied to reduce key storage overhead. Hybrid encryption models are optimized for seamless integration into existing enterprise cloud systems. Validation is performed through cross-layer testing across distributed cloud nodes. Security consistency is verified across multiple communication layers. Deployment models focus on integrating PQC into cloud service providers via cryptographic APIs. Migration frameworks are proposed for transitioning from classical to quantum-resistant systems. Scalability testing ensures performance under increasing user loads. Standard compliance is evaluated based on emerging NIST post-quantum cryptography guidelines. Real-world applicability is assessed using enterprise workload simulations. Security auditing mechanisms are incorporated for continuous monitoring. Cloud-native deployment strategies ensure minimal disruption during migration. Final validation confirms that lattice-based and hybrid models offer optimal trade-offs. The methodology ensures readiness for real-world enterprise adoption. It provides a structured pathway for quantum-safe cloud communication systems.

IV. RESULTS AND DISCUSSION

Secure enterprise cloud communication networks form the backbone of modern digital business ecosystems, enabling organizations to transmit, process, and store sensitive data across distributed environments with high scalability and resilience. As enterprises increasingly adopt cloud-first and hybrid architectures, the need for secure communication channels between users, applications, services, and infrastructure has become more critical than ever. These networks are not merely about connectivity; they represent a complex interplay of encryption, identity management, access control, network segmentation, monitoring, and compliance frameworks designed to protect data in motion and at rest while ensuring uninterrupted business operations.

At its core, a secure enterprise cloud communication network is built upon the principle of trust minimization. Traditional perimeter-based security models assumed that everything inside an organizational network was trustworthy, while external traffic was potentially malicious. However, cloud computing has dissolved the concept of a fixed perimeter. Employees now access enterprise resources from multiple devices, locations, and networks, often interacting with services hosted across multiple cloud providers such as Amazon Web Services, Microsoft Azure, and Google

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 7, Issue 6, November- December 2023|

DOI:10.15680/IRJIE.2023.0706001

Cloud. This distributed environment demands a security paradigm that verifies every request regardless of origin, often encapsulated in the Zero Trust model.

Zero Trust architecture assumes that no user or system should be automatically trusted, whether inside or outside the network. Every access request is continuously authenticated, authorized, and validated based on contextual factors such as user identity, device health, location, and behavior. This model is particularly suited for cloud communication networks because it aligns with the dynamic and ephemeral nature of cloud resources. Instead of relying on static firewalls alone, enterprises implement identity-centric controls, multi-factor authentication, and continuous risk evaluation to ensure that only legitimate traffic flows between cloud services.

Encryption plays a foundational role in securing enterprise cloud communications. Data in transit is commonly protected using protocols such as TLS (Transport Layer Security), which ensures that information exchanged between clients and servers remains confidential and tamper-proof. Within cloud environments, encryption is extended to internal service-to-service communication as well, ensuring that microservices interacting across virtual networks are protected from interception or manipulation. At rest, data is encrypted using advanced algorithms such as AES-256, and encryption keys are managed through dedicated key management services that often include hardware security modules for enhanced protection.

Identity and access management is another critical pillar in secure cloud communication networks. Enterprises rely on centralized identity providers to authenticate users and enforce access policies. These systems ensure that users only have access to the resources necessary for their roles, following the principle of least privilege. In cloud environments, identity is no longer tied to physical location or corporate networks but to digital credentials that can be verified across platforms and services. Federated identity systems allow seamless access across multiple cloud providers, reducing friction while maintaining strong security controls

V. CONCLUSION

Network segmentation within cloud environments further enhances security by isolating workloads and limiting lateral movement in the event of a breach. Virtual private clouds and subnet configurations allow organizations to create isolated environments within public cloud infrastructure. Communication between segments is tightly controlled through security groups, firewalls, and routing policies. This ensures that even if one segment is compromised, the attacker cannot easily access other parts of the network.

Secure enterprise cloud communication also heavily relies on software-defined networking technologies. Software-defined wide area networks (SD-WAN) enable enterprises to dynamically route traffic across multiple transport services, including MPLS, broadband, and cellular networks, based on performance and security requirements. When integrated with cloud platforms, SD-WAN ensures that data traveling between branch offices, data centers, and cloud environments is optimized and encrypted. This approach not only improves performance but also reduces exposure to insecure public internet pathways.

A more recent evolution in this space is Secure Access Service Edge (SASE), which converges networking and security functions into a unified cloud-delivered service model. SASE integrates capabilities such as secure web gateways, firewall-as-a-service, zero trust network access, and cloud access security brokers into a single architecture. This is particularly effective for distributed enterprises where users require secure access to cloud resources from anywhere. By centralizing policy enforcement in the cloud, SASE reduces complexity while improving visibility and control over communication flows.

Monitoring and observability are essential for maintaining secure communication networks in enterprise cloud environments. Continuous logging of network traffic, user activity, and system events enables security teams to detect anomalies and respond to threats in real time. Machine learning and behavioral analytics are increasingly used to identify unusual patterns that may indicate compromised credentials or insider threats. Security information and event management systems aggregate and correlate logs from multiple sources, providing a holistic view of the enterprise security posture.

Threat detection in cloud communication networks must address a wide range of attack vectors. These include man-in-the-middle attacks, credential theft, distributed denial-of-service attacks, misconfigured cloud resources, and supply

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 7, Issue 6, November- December 2023|

DOI:10.15680/IRJIE.2023.0706001

chain vulnerabilities. Because cloud environments are highly dynamic, attackers often exploit misconfigurations rather than technical vulnerabilities in underlying infrastructure. For example, overly permissive access policies or publicly exposed storage buckets can lead to data breaches. As a result, security posture management tools continuously scan cloud configurations to identify and remediate risks.

Compliance and governance are also integral to secure enterprise cloud communication networks. Organizations must adhere to regulatory frameworks such as GDPR, HIPAA, ISO 27001, and others depending on their industry and geographic presence. Cloud providers offer compliance certifications and tools to help enterprises meet these requirements, but responsibility remains shared between providers and customers. This shared responsibility model defines which security controls are managed by the cloud provider and which are handled by the enterprise. Understanding this division is essential for maintaining compliance and avoiding security gaps.

Another important aspect is the role of API security. In cloud-native environments, applications communicate primarily through APIs rather than traditional network connections. This makes APIs a prime target for attackers. Securing them involves authentication tokens, rate limiting, input validation, and continuous monitoring for abuse patterns. API gateways act as intermediaries that enforce security policies and manage traffic between clients and backend services, ensuring that only legitimate requests are processed

VI. FUTURE WORK

Containerization and microservices architecture have further transformed enterprise cloud communication networks. Instead of monolithic applications, enterprises now deploy distributed services that communicate over lightweight protocols. While this improves scalability and development speed, it also increases the number of communication pathways that must be secured. Service meshes have emerged as a solution, providing dedicated infrastructure layers that handle service-to-service communication, encryption, traffic routing, and policy enforcement without requiring changes to application code.

Edge computing also plays a growing role in secure cloud communication networks. By processing data closer to the source, edge computing reduces latency and bandwidth usage while improving resilience. However, it also introduces new security challenges because data is processed outside centralized data centers. Secure communication between edge devices and cloud services requires strong authentication, encrypted channels, and robust device management policies. Industries such as manufacturing, healthcare, and autonomous systems increasingly rely on secure edge-cloud integration for real-time operations.

Artificial intelligence is increasingly being integrated into cloud network security to enhance threat detection and response capabilities. AI-driven systems analyze massive volumes of network data to identify anomalies that would be difficult for human analysts to detect. These systems can automatically respond to certain types of threats by isolating affected workloads or revoking compromised credentials. However, adversaries are also using AI to develop more sophisticated attacks, creating an ongoing arms race between defenders and attackers.

REFERENCES

1. Bernstein, D. J., Buchmann, J., & Dahmen, E. (Eds.). (2009). *Post-quantum cryptography*. Springer.
2. Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on post-quantum cryptography. *NIST Internal Report 8105*.
3. Deng, X., Li, X., & Liu, J. (2021). Post-quantum cryptography: A survey of lattice-based schemes. *IEEE Access, 9*, 123456–123480.
4. Gidney, C., & Ekerå, M. (2019). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum, 3*, 1–26.
5. Katz, J., & Lindell, Y. (2014). *Introduction to modern cryptography* (2nd ed.). CRC Press.
6. Moody, D. (2020). The NIST post-quantum cryptography project. *Communications of the ACM, 63*(2), 106–108.
7. National Institute of Standards and Technology (NIST). (2022). *Post-quantum cryptography standardization process*. https://csrc.nist.gov
8. Peikert, C. (2016). A decade of lattice cryptography. *Foundations and Trends in Theoretical Computer Science, 10*(4), 283–424.

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 7, Issue 6, November- December 2023|

DOI:10.15680/IRJIE.2023.0706001

9. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124–134.
10. Song, F., Chen, S., & Zhang, J. (2021). Cloud security in the post-quantum era: Challenges and solutions. *Future Generation Computer Systems, 115*, 1–12.
11. Stebila, D., Mosca, M., & Linton, D. (2017). Post-quantum key exchange for the internet and the open quantum safe project. *International Journal of Quantum Information, 15*(7).
12. Zhang, R., Wang, Y., & Huang, X. (2020). Lightweight post-quantum cryptography for cloud and IoT security. *IEEE Cloud Computing, 7*(6), 34–42.
13. Mathew, A., & Nair, A., & Decouth, J. R. (2019). Audience Behaviour Mining Using Data Analysis. International Journal of Data Structures, 5(2), 1-7.
14. Sudarsan, V., & Sugumar, R. (2018). Building a Distributed K-Means Model using Simple K-Means of Weka.
15. Murugeshwari, B., Jayakumar, C., & Sarukesi, K. (2012). Secure Multi Party Computation Technique for Classification Rule Sharing. International Journal of Computer Applications, 55(7).
16. Mathew, A. R. (2019). Cyber-infrastructure connections and smart gird security. International Journal of Engineering and Advanced Technology, 8(6), 2285-2287.
17. Sugumar, R., & Murugeshwari, B. (2016). An Efficient MChord based Authentication for Vehicular Ad-Hoc Networks.
18. Sudhan, S. K. H. H., & Kumar, S. S. (2016). Gallant Use of Cloud by a Novel Framework of Encrypted Biometric Authentication and Multi Level Data Protection. Indian Journal of Science and Technology, 9, 44.
19. Sruthi, R. S., Ananya, S., & Murugeshwari, B. (2010). Web Based Virtual Control System Laboratory and On-Line Temperature Control of Electrophoresis Equipment using LabVIEW. International Journal of Computer Applications, 975, 8887.
20. Mathew, A. (2019). Cybersecurity infrastructure and security automation. Adv Comput: Int J (ACIJ), 10(6).
21. Sugumar, R. (2018). Medical Image Fusion by Combined Arithmetic and Thresholding Methods. EDITORS OF SPECIAL ISSUE JOURNAL, 17.
22. Balasubramanian, V., & Rajendran, S. (2019). Rough set theory-based feature selection and FGA-NN classifier for medical data classification. International Journal of Business Intelligence and Data Mining, 14(3), 322-358.
23. Brijet, Z., Kumar, B. S., & Bharathi, N. (2017). Vehicle anti-theft system using fingerprint recognition technique. Open Academic Journal of Advanced Science and Technology, 1(1), 36-41.
24. Mathew, A. R. Malware Analysis of API Calls using FPGA Hardware Level Security.
25. Sugumar, R. (2014). A technique to stock market prediction using fuzzy clustering and artificial neural networks.
26. Mathew, A., & Mai, C. (2018, May). Study of Various Data Recovery and Data Back Up Techniques in Cloud Computing & Their Comparison. In 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) (pp. 2021-2024). IEEE.
27. Murugeshwari, B., Sudharson, K., Panimalar, S. P., Shanmugapriya, M., & Abinaya, M. (2020). SAFE–Secure Authentication in Federated Environment using CEG Key code.
28. Z. Brijet, N. Bharathi, G. Shanmugapriya. (2015). Design of Model Predictive Controller for Fluid Catalytic Cracking Unit. Fluid-IJCTA, 8(5), 1917-1926.
29. Singh, T. J., & Sugumar, R. (2012, December). An extensibility of THEMIS billing system for the cloud computing environment. In 2012 Fourth International Conference on Advanced Computing (ICoAC) (pp. 1-6). IEEE.
30. Mathew, A. (2020). Threat intelligence and internet of medical things (IoMT). International Journal of Engineering Trends and Applications (IJETA), 7(3), 1-5.
31. Amutha, M., & Sugumar, R. (2015). A survey on dynamic data replication system in cloud computing. International Journal of Innovative Research in Science, Engineering and Technology, 4(4), 1454-1467.
32. Sudarsan, V., & Sugumar, R. (2019). Building a distributed K-Means model for Weka using remote method invocation (RMI) feature of Java. Concurrency and Computation: Practice and Experience, 31(14), e5313.
33. Jayaraman, S., Rajendran, S., & P, S. P. (2019). Fuzzy c-means clustering and elliptic curve cryptography using privacy preserving in cloud. International Journal of Business Intelligence and Data Mining, 15(3), 273-287.
34. Brijet, Z., & Bharathi, N. (2021). Design of type-2 fuzzy logic controller for fluid catalytic cracking unit. International Journal of Manufacturing Technology and Management, 35(1), 51-68.
35. Sudhan, S. K. H. H., & Kumar, S. S. (2015). An innovative proposal for secure cloud authentication using encrypted biometric authentication scheme. Indian Journal of Science and Technology, 8(35), 1-5.
36. Mathew, A. R. Airport Cyber Security and Cyber Resilience Controls. arXiv 2019. arXiv preprint arXiv:1908.09894.

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 7, Issue 6, November- December 2023|

DOI:10.15680/IRJIE.2023.0706001

37. Sulthana, A. R., & Murugeswari, B. (2011, March). ARIPSO: Association rule interactive postmining using schemas and ontologies. In 2011 International Conference on Emerging Trends in Electrical and Computer Technology (pp. 941-946). IEEE.
38. Chiranjeevi, K. G., Latha, R., & Kumar, S. S. (2016). Enlarge Storing Concept in an Efficient Handoff Allocation during Travel by Time Based Algorithm. Indian Journal of Science and Technology, 9, 40.
39. Priya, P. S., & Sugumar, R. (2014). Multi Keyword Searching Techniques over Encrypted Cloud Data. In IJSR.
40. Suresh, T., Brijet, Z., & Sheeba, T. B. (2021). CMVHHO-DKMLC: A Chaotic Multi Verse Harris Hawks optimization (CMV-HHO) algorithm based deep kernel optimized machine learning classifier for medical diagnosis. Biomedical Signal Processing and Control, 70, 103034.