Unique Proposed solution:

The unique proposed solution based on an AI-Enabled Secure Communication Mechanism in Fog Computing harnesses the capabilities of AI algorithms to enhance security, privacy, energy efficiency, scalability, and adaptability in fog computing environments. By combining real-time threat detection, energy optimization, privacy preservation, and integration with blockchain technology, the solution offers a comprehensive and robust approach to secure communication in fog computing, paving the way for the deployment of reliable and trustworthy IoT applications.

Energy Efficiency: Develop communication protocols and mechanisms that minimize energy consumption, considering the limited power availability of fog nodes. Utilize AI algorithms to optimize resource allocation and data routing to minimize energy usage while maintaining security and reliability.

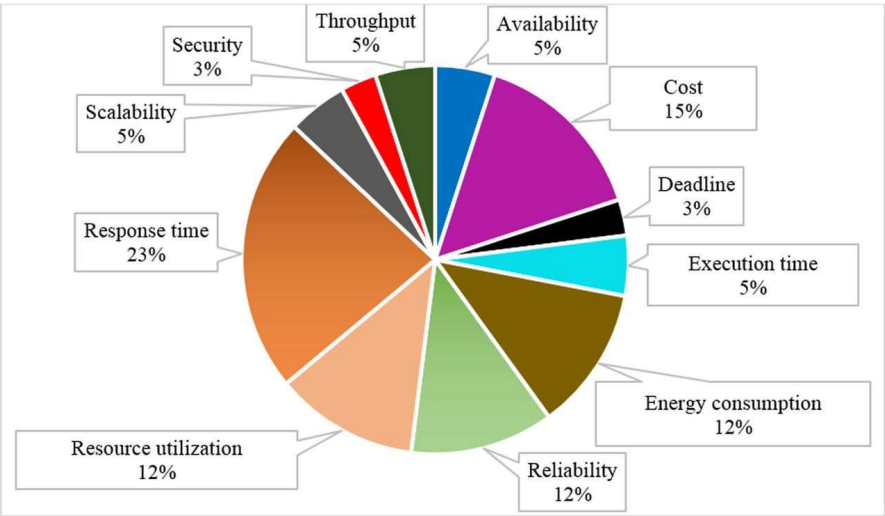
Real-time Threat Detection: Implement AI-based intrusion detection and threat mitigation techniques to identify and respond to security threats in real-time. The solution should be capable of detecting various attack types, such as DDoS attacks, unauthorized access attempts, and data tampering, while minimizing false positives and false negatives.

Scalability and Adaptability: Design the communication mechanism to be scalable, capable of accommodating a growing number of devices and fog nodes. Employ AI techniques to dynamically adapt to changes in network topology, device mobility, and workload distribution, ensuring uninterrupted communication even in highly dynamic fog computing environments.

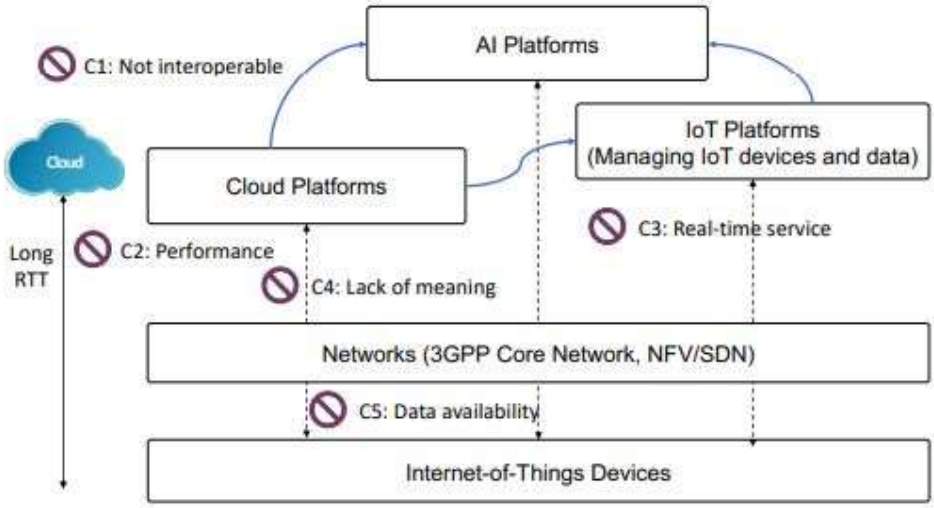
Privacy-Preserving Data Transmission: Incorporate AI algorithms to protect the privacy of sensitive data during transmission. Develop techniques for data anonymization and encryption to prevent unauthorized access and maintain confidentiality.

Resilience to Network Disruptions: Build a resilient communication mechanism that can withstand network disruptions and failures. Employ AI-based fault tolerance mechanisms to automatically recover from communication failures, reroute data traffic, and ensure continuous operation of fog computing applications.

Quality of service-aware approaches in fog computing



The objective of this project is to develop an AI-enabled secure communication mechanism specifically tailored for resource-constrained fog computing environments. The proposed solution should strike a balance between security, energy efficiency, scalability, and adaptability, ensuring reliable and secure data transmission while optimizing the utilization of available resources. By addressing these challenges, the proposed mechanism will enhance the overall security and performance of fog computing systems, enabling the deployment of robust and scalable IoT applications in real-world scenarios.


AI Platforms
C1: Not interoperable
Cloud
Cloud Platforms
IoT Platforms
(Managing IoT devices and data)
C3: Real-time service
Long
RTT
C2: Performance
C4: Lack of meaning
Networks (3GPP Core Network, NFV/SDN)
C5: Data availability
Internet-of-Things Devices