The SCADA-Map project, proposed for Smart India Hackathon 2024, aims to develop a secure tool for automatic network topology creation, particularly designed for SCADA (Supervisory Control and Data Acquisition) systems. These systems are critical for industries such as power distribution, water management, and manufacturing, which require continuous, secure, and efficient network monitoring. The tool addresses the increasing security risks in these networks by combining several advanced technologies such as SNMPv3, ARP/MAC tables, NetFlow, EIGRP, AI-based anomaly detection, and blockchain-based device authentication. These elements are carefully integrated to provide real-time, accurate, and secure network topology mapping.

The key features of the SCADA-Map solution include:

**Secure Topology Discovery**: Utilizes SNMPv3 for secure device communication, ARP/MAC tables for connection mapping, and NetFlow and EIGRP for network traffic analysis and routing. This ensures accurate and secure network discovery without relying on older, insecure protocols like CDP/LLDP.

**AI-Powered Anomaly Detection**: Employs AI models built on TensorFlow and Scikit-learn to monitor network traffic and device behavior, proactively identifying potential threats or unauthorized activities. This AI-driven monitoring helps mitigate cyber-attacks by raising alerts as soon as anomalies are detected.

**Blockchain-Based Device Authentication**: Uses blockchain technology to verify device identities, ensuring that only authorized devices can access the network. This adds an extra layer of security to prevent unauthorized access or compromised devices from infiltrating the system.

**Scalability**: The system is designed to scale across large networks, such as those spanning thousands of kilometers. It supports a distributed architecture, allowing for local security enforcement while maintaining centralized monitoring. This makes it suitable for managing extensive SCADA networks in industries like energy and water distribution.

**Real-Time Visualization and Alerts**: Provides a web-based interface for real-time visualization of the network topology. The interface displays up-to-date maps, device status, and instant alerts for any unauthorized access attempts or anomalies detected by the AI system.

The technical stack for this solution includes:

**Front-End**: HTML, CSS, JavaScript, and D3.js for the real-time visualization of network topology.

**Back-End**: Python as the core programming language.

**Libraries & Tools**: PySNMP for SNMP communication, Scapy for packet manipulation, and NetFlow for traffic analysis.

**Security**: Blockchain, OAuth 2.0, JWT for secure authentication, and SSL/HTTPS for encrypted data transmission.

**AI/ML**: TensorFlow and Scikit-learn for anomaly detection and threat identification.

The project also considers feasibility and potential challenges, such as handling large volumes of network traffic and ensuring the scalability of the blockchain-based device authentication system. Strategies for overcoming these challenges include optimizing data processing, customizing blockchain protocols, and refining AI models through continuous training on real-world data.

The SCADA-Map project offers several impactful benefits:

**Enhanced Network Security**: Ensures that unauthorized devices and malicious actors are blocked from accessing the network, protecting the SCADA infrastructure from potential cyber-attacks.

**Increased Efficiency**: Automates the process of network topology discovery, reducing manual efforts and improving response times for network issues.

**Real-Time Monitoring**: Continuously updates network topology and generates instant alerts, helping administrators to react quickly to potential problems.

**Cost-Effective Solution**: Utilizes open-source tools and requires no additional hardware, making it an affordable solution for large-scale networks.

**Proactive Threat Detection**: AI-driven monitoring enables early detection of security threats, allowing for quick mitigation and reducing the risk of major breaches.

**User-Friendly Interface**: The real-time web interface simplifies network management for administrators, providing intuitive controls and real-time data visualization.

In conclusion, the SCADA-Map tool offers a robust, secure, and scalable solution for automating network topology discovery and monitoring for SCADA systems. With its integration of AI, blockchain, and secure networking protocols, the tool provides comprehensive protection for large networks, ensuring continuous and secure operation of critical infrastructure systems.