SMART INDIA HACKATHON 2024

SCADA-Map

- **Problem Statement ID** - SIH1708
- **Problem Statement Title -** Tool for secure automatic network topology creation
- **Theme -** Miscellaneous
- **PS Category -** Software
- **Team ID -** 5900
- **Team Name -** DenQueue

DenQueue

SCADA-Map

❖ Detailed Explanation

- ❖ **Secure Topology Discovery:**
  Leverages EIGRP routing data for accurate and real-time network mapping.
  Eliminates the security risks associated with CDP/LLDP, ensuring a more robust and protected network infrastructure.
- ❖ **AI-Powered Anomaly Detection:**
  Employs AI-driven models to continuously analyze network traffic and device behavior.
  Proactively identifies suspicious activities, unauthorized devices, and potential security threats.
- ❖ **AI/ML Authentication:**
  Utilizes AI/ML technology to verify device identities and ensure only authorized devices can access the network.
  Enhances security and prevents unauthorized access, safeguarding critical SCADA infrastructure.
- ❖ **Scalability for Large Networks:**
  Designed to accommodate vast networks, spanning thousands of kilometers.
  Offers distributed architecture for local enforcement of security while maintaining centralized control.
- ❖ **Real-Time Visualization and Alerts:**
  Provides an interactive web-based interface for real-time monitoring of network topology and device status.
  Generates instant alerts for anomalies or unauthorized access attempts, enabling prompt response and efficient network maintenance.

❖ How It Addresses The Problem

- **Accurate Device Identification:**
  Avoids insecure protocols like CDP/LLDP.
  Uses syslog, EIGRP for reliable device and connection information.
- **Real-Time Network Topology:**
  Provides up-to-date network maps.
  Uses routing protocols for instant updates, aiding troubleshooting and security.
- **Network Security Across Large Areas:**
  Combines AI anomaly detection and ML-based device authentication.
  Dynamically segments the network to isolate threats and prevent unauthorized access.

DenQueue

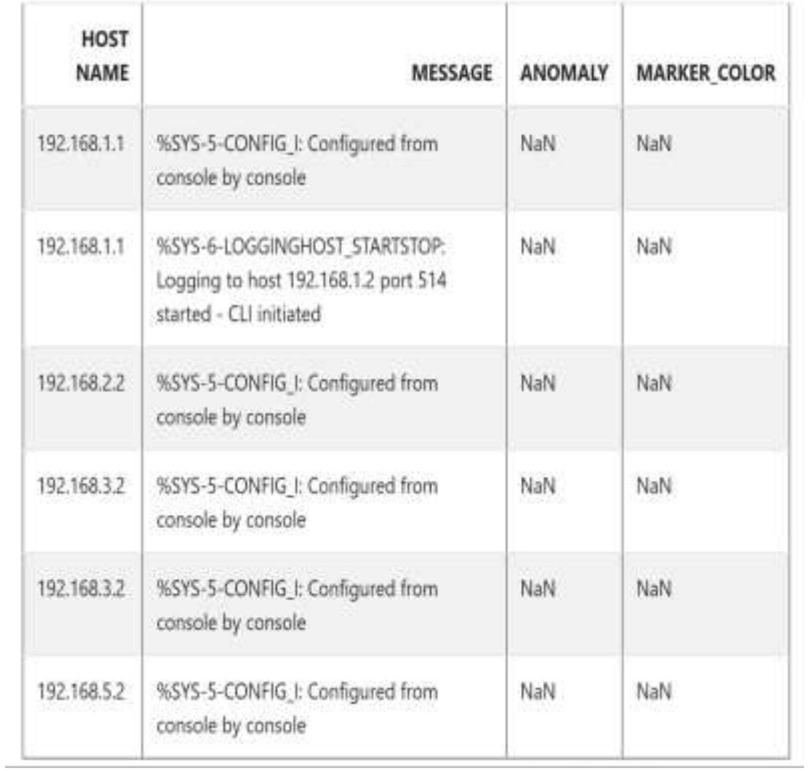
TECHNICAL APPROACH

SMART INDIA HACKATHON 2024

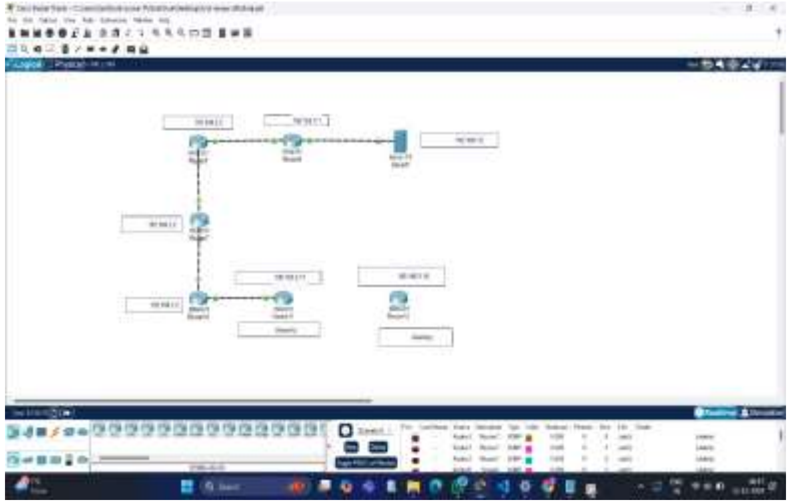
TECH STACK

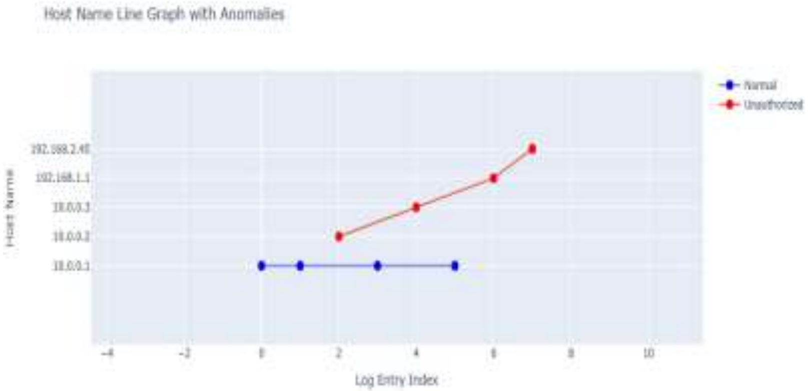
- **Front-End**: HTML, CSS, JavaScript, D3.js
- **Back-End**: Python
- **Libraries&Tools**: Pandas, Networks
- **Security Tech:** EIGRP, syslog
- **AI/ML:** sklearn, TfdfVectorizer, MultinomialNB
- **Algorithm:** Naïve Bayes Classifier
- **Simulation:** Cisco Packet Tracer

FLOWCHART



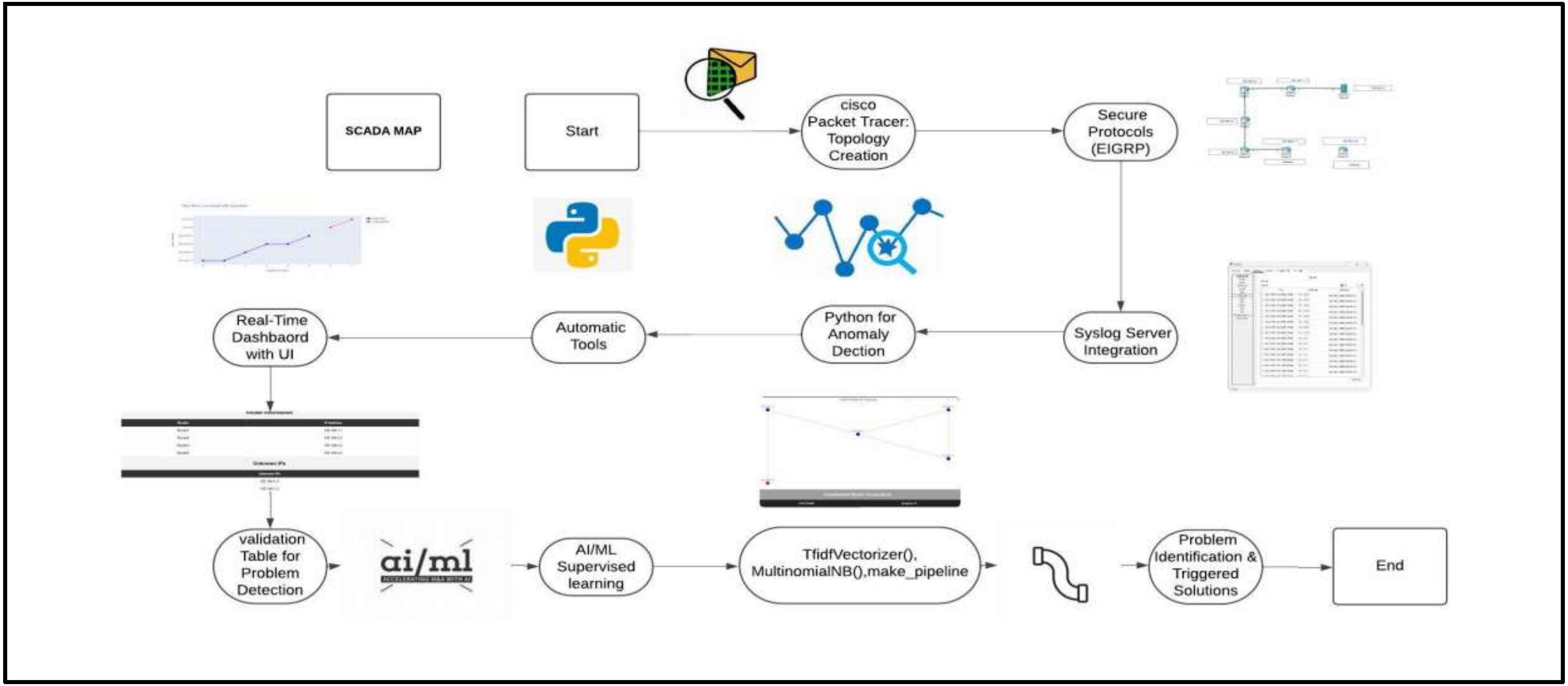
HOST NAME	MESSAGE	ANOMALY	MARKER_COLOR
192.168.1.1	%SYS-5-CONFIG_I: Configured from console by console	NaN	NaN
192.168.1.1	%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.2 port 514 started - CLI initiated	NaN	NaN
192.168.2.2	%SYS-5-CONFIG_I: Configured from console by console	NaN	NaN
192.168.3.2	%SYS-5-CONFIG_I: Configured from console by console	NaN	NaN
192.168.3.2	%SYS-5-CONFIG_I: Configured from console by console	NaN	NaN
192.168.5.2	%SYS-5-CONFIG_I: Configured from console by console	NaN	NaN





Host Name Line Graph with Anomalies

WORKFLOW:



SCADA MAP

Start

cisco Packet Tracer: Topology Creation

Secure Protocols (EIGRP)

Syslog Server Integration

Python for Anomaly Dection

Automatic Tools

Real-Time Dashbaord with UI

validation Table for Problem Detection

AI/ML Supervised learning

TfidfVectorizer(), MultinomialNB(),make_pipeline

Problem Identification & Triggered Solutions

End

DenQueue

FEASIBILITY AND VIABILITY

SMART INDIA HACKATHON 2024

Feasibility:

Feasibility Analysis:

- Utilizes free, open-source technologies, making it affordable and practical to implement.
- Can be simulated in virtual environments (Cisco Packet Tracer) removing the need for physical hardware during development.

Potential Challenges and Risks:

- Managing real-time network mapping and device identification across extensive geographic distances.
- Incorporating advanced security like blockchain without negatively affecting performance.

Strategies for Overcoming Challenges:

- Implement distributed systems for real-time data collection and accurate mapping over large networks.
- Ensure blockchain and AI integration are streamlined to maintain high security without slowing down the system.

Established Protocols

- Utilizes familiar protocols like EIGRP, ensuring smooth integration into existing networks.

Viability:

Cost-Effective:

- Built using open-source technologies (Python, Naïve Bayes Classifier) to reduce implementation costs.
- Can be developed in virtual environments avoiding the need for physical hardware.

Scalability:

- Designed for large-scale networks, with a distributed architecture that handles networks spanning thousands of kilometers.
- Real-time updates using syslog and routing data (EIGRP) ensure accurate network maps.

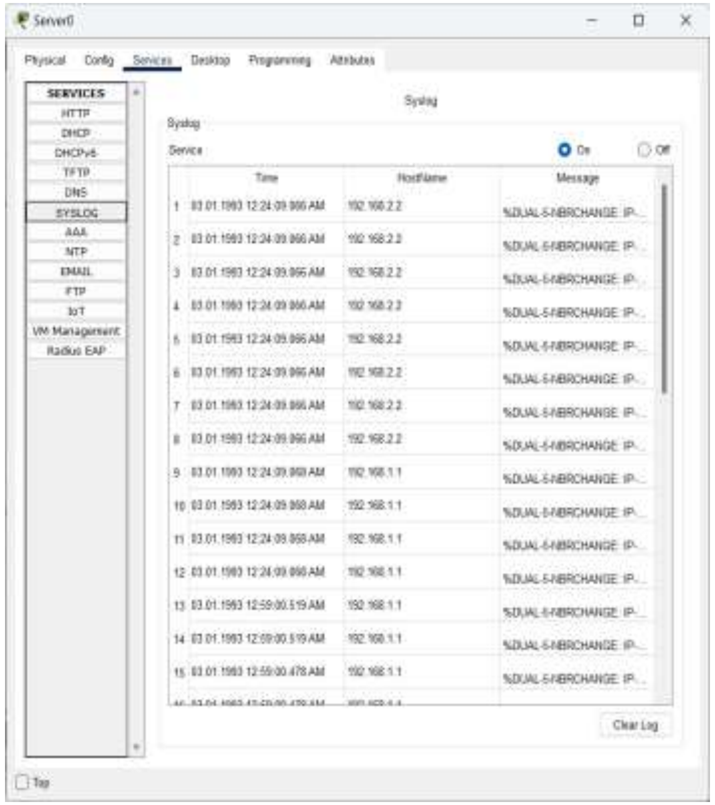
High Security:

- AI-powered anomaly detection identifies security threats in real-time, ensuring proactive threat mitigation.
- AI/ML based device authentication secures access to critical infrastructure without compromising performance.

Real-Time Monitoring:

- A web-based interface provides real-time network visualization and alerts, ensuring quick responses to security incidents.

Syslog Server:



Syslog

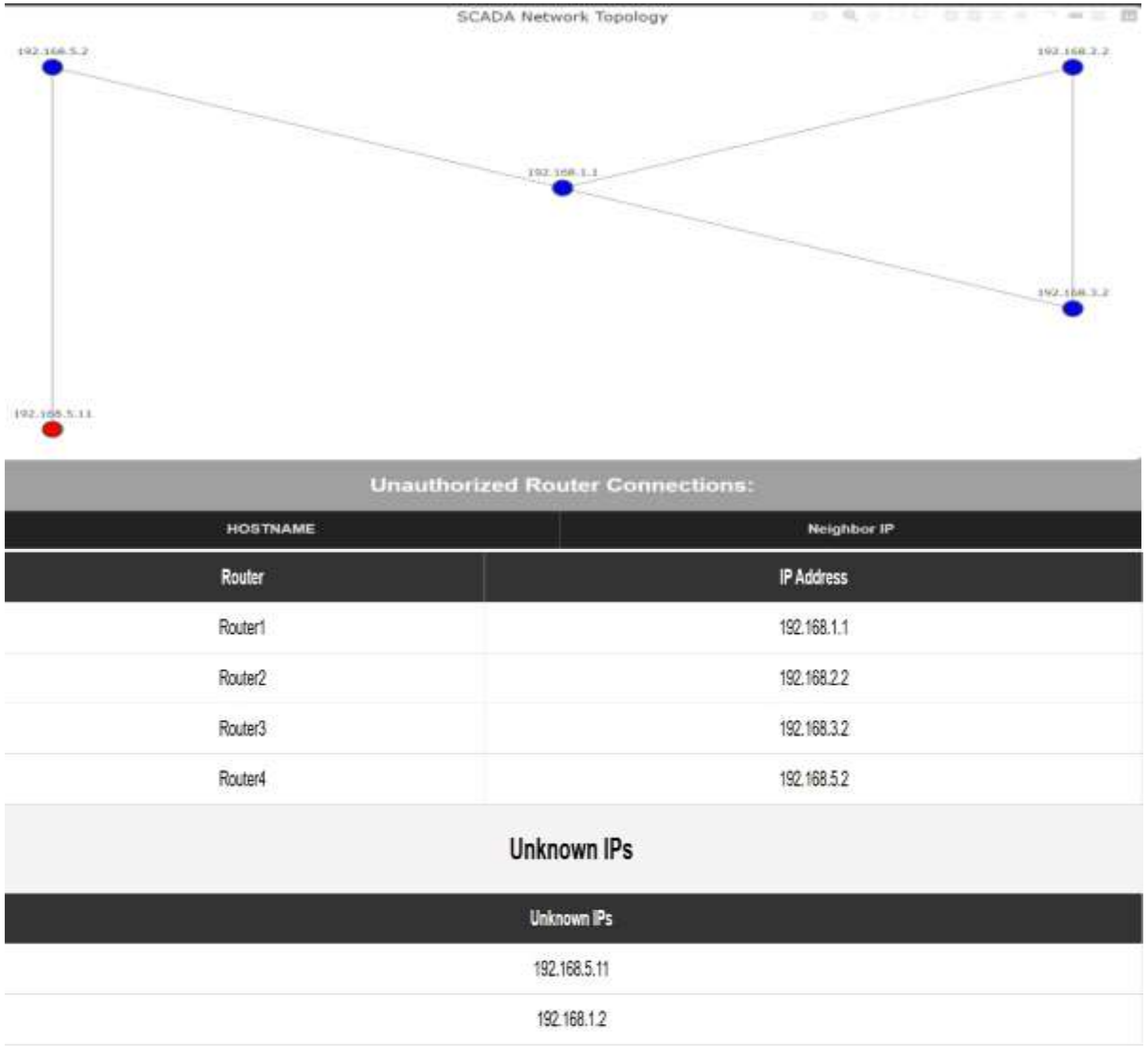
Syslog

Service ● On ○ Off

	Time	HostName	Message
1	03.01.1993 12:24:09.866 AM	192.168.2.2	%DUAL-5-NBRCHANGE: IP-...
2	03.01.1993 12:24:09.866 AM	192.168.2.2	%DUAL-5-NBRCHANGE: IP-...
3	03.01.1993 12:24:09.866 AM	192.168.2.2	%DUAL-5-NBRCHANGE: IP-...
4	03.01.1993 12:24:09.866 AM	192.168.2.2	%DUAL-5-NBRCHANGE: IP-...
5	03.01.1993 12:24:09.866 AM	192.168.2.2	%DUAL-5-NBRCHANGE: IP-...
6	03.01.1993 12:24:09.866 AM	192.168.2.2	%DUAL-5-NBRCHANGE: IP-...
7	03.01.1993 12:24:09.866 AM	192.168.2.2	%DUAL-5-NBRCHANGE: IP-...
8	03.01.1993 12:24:09.866 AM	192.168.2.2	%DUAL-5-NBRCHANGE: IP-...
9	03.01.1993 12:24:09.868 AM	192.168.1.1	%DUAL-5-NBRCHANGE: IP-...
10	03.01.1993 12:24:09.868 AM	192.168.1.1	%DUAL-5-NBRCHANGE: IP-...
11	03.01.1993 12:24:09.868 AM	192.168.1.1	%DUAL-5-NBRCHANGE: IP-...
12	03.01.1993 12:24:09.868 AM	192.168.1.1	%DUAL-5-NBRCHANGE: IP-...
13	03.01.1993 12:59:00.519 AM	192.168.1.1	%DUAL-5-NBRCHANGE: IP-...
14	03.01.1993 12:59:00.519 AM	192.168.1.1	%DUAL-5-NBRCHANGE: IP-...
15	03.01.1993 12:59:00.478 AM	192.168.1.1	%DUAL-5-NBRCHANGE: IP-...

IMPACT AND BENEFITS

IMPACT	BENEFITS
Enhanced Network Security: Ensures the SCADA network is protected from unauthorized access and potential cyber-attacks.	**Improved Efficiency**: Automates topology discovery, reducing manual work and improving response times for network issues.
Real-Time Monitoring: Provides continuous, up-to-date visibility into network topology, helping reduce downtime and improve maintenance efficiency.	**Cost-Effective Solution**: Uses open-source tools and requires no additional hardware, making it a budget-friendly option.
Scalability for Large Networks: Capable of handling networks across thousands of kilometers, supporting large-scale infrastructure.	**Secure Device Authentication**: Blockchain integration ensures only authorized devices access the network, bolstering security.
Proactive Threat Detection: AI-driven anomaly detection enables faster identification of threats, leading to quicker responses and minimized risk.	**User-Friendly Interface**: Real-time visualization and alerts via an interactive web-based UI simplify network management for administrators.



Unauthorized Router Connections:

HOSTNAME	Neighbor IP

Router	IP Address
Router1	192.168.1.1
Router2	192.168.2.2
Router3	192.168.3.2
Router4	192.168.5.2

Unknown IPs

Unknown IPs
192.168.5.11
192.168.1.2

DenQueue

RESEARCH AND REFERENCES

SMART INDIA HACKATHON 2024

Reference:

- This paper outlines the vulnerabilities of SCADA networks and their critical role in infrastructure, emphasizing security risks and solutions . Available at Science Direct- 🔗 link
- A detailed analysis of EIGRP features and the security implications for routing in critical networks like SCADA. Available at Cisco- 🔗 link
- A review of SNMPv3's security features, including encryption and authentication, suitable for secure network topology discovery. Available Research gate- 🔗 link

Research:

❖ **Research Paper:** Security of Industrial Control Systems and SCADA Networks

This paper discusses the vulnerabilities in SCADA systems and how modern tools and technologies address these vulnerabilities.

Our Team Members

SUDHARSAN.K
Front- end Developer,
UI/UX Designer

RANJITH.R
Back-End Developer,
AI & ML Developer

SELVA VISHNU.G
Database Manager

YASHRITHA.S
AI & ML Developer

SRIVARSHA.V.S
AI & ML Developer

TEAM LEAD

SANTHOSH KUMAR.P
Network Security
MAIL ID: santhoshpalanisamy292@gmail.com