JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

MapX: TOOL FOR SECURE AUTOMATIC NETWORK TOPOLOGY CREATION.

Thakur Shyamnarayan Degree College
Mr. Prathrva Surve, Amit Pandey, Aditya Gupta
Assistant professor, Undergraduate Student, Undergraduate Student
Department of Information Technology
University of Mumbai, Mumbai, India

Abstract:
The rapid expansion of digital infrastructure and interconnected systems has increased the complexity of managing modern computer networks. Organizations and individuals rely on efficient network visualization to monitor, analyze, and secure their systems. However, manual network mapping is time-consuming, error-prone, and often requires advanced technical expertise. Existing tools either lack automation, require complex configurations, or do not provide secure user access mechanisms.
This paper presents the **Tool for Secure Automatic Network Topology Creation**, an intelligent and user-centric system designed to automatically detect, map, and visualize network devices in a structured graphical format. Unlike traditional network tools that rely heavily on manual configuration, this system focuses on automation, usability, and security. It provides real-time topology visualization with device identification and structured layouts, enabling users to better understand network architecture.
Index Terms— Network Topology, Network Visualization, Cybersecurity, Automation, Data Visualization, Network Monitoring

I. INTRODUCTION

Modern computer networks form the backbone of digital communication, supporting everything from personal devices to enterprise-level infrastructures. As networks grow in size and complexity, understanding their structure becomes increasingly challenging. Network topology plays a crucial role in identifying how devices are interconnected, enabling efficient monitoring, troubleshooting, and security management.
Network administrators and users often struggle to obtain a clear visual representation of their network. Without proper visualization, identifying connected devices, their relationships, and potential vulnerabilities becomes difficult. **Tool for Secure Automatic Network Topology Creation** is proposed as a solution to these challenges. It reduces manual effort, enhances accuracy, and enables users to gain immediate insights into their network structure.

II. LITERATURE REVIEW

Existing research in network management highlights the importance of visualization in simplifying complex network structures. Graph-based representations, including node-link diagrams, have been widely used to depict relationships between devices in a network. These visualizations improve understanding, enabling users to quickly identify connectivity patterns and network anomalies.
Several network topology tools provide automated scanning and mapping features. However, many of these tools are either enterprise-focused or require advanced technical knowledge for configuration. Additionally, some tools lack integration with secure authentication systems, making them less suitable for environments requiring controlled access.
Despite advancements, there is a gap in tools that combine automation, visualization, and security within a user-friendly interface. The proposed system addresses these limitations by providing an integrated solution that is both accessible and secure.

III. RESEARCH METHODOLOGY

Figure 1: High-Level Architecture

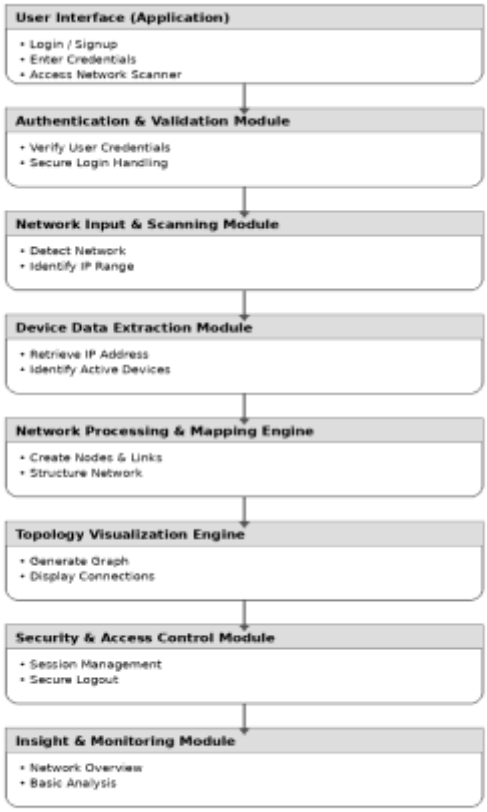


Figure 1 illustrates the high-level architecture of the network topology creation system, demonstrating the flow from user authentication to topology visualization.

The methodology follows a modular and systematic approach to ensure efficient processing and scalability. The system consists of multiple components, each responsible for a specific function.

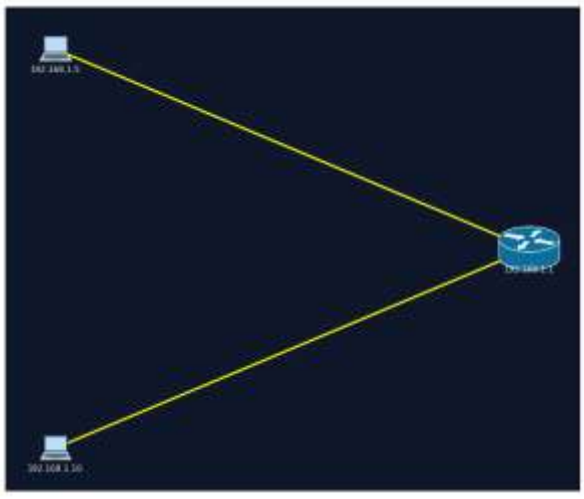
The process begins with the user accessing the application and selecting either login or signup. User credentials are securely stored and verified using a structured database system. Upon successful authentication, the user gains access to the main application interface.

The network scanning module then detects devices connected within the network. It identifies active hosts, retrieves IP addresses, and gathers relevant device information. This data is processed and structured into a format suitable for visualization.

The system architecture ensures that each component operates independently while maintaining seamless data flow. This modular design enhances maintainability, scalability, and performance.

IV. RESULTS AND DISCUSSION

The implementation of the **Tool for Secure Automatic Network Topology Creation** demonstrates significant improvements in network visualization and usability. The system successfully automates device detection and presents the network structure in a clear graphical format.



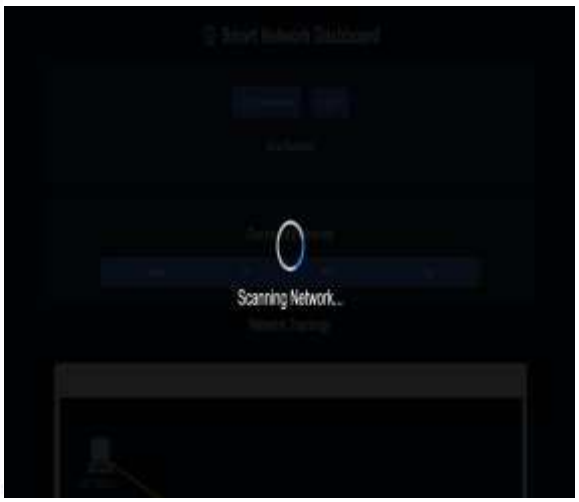


Figure 2 illustrates the main topology view, where connected devices are represented as nodes with their corresponding IP addresses. The visualization provides a high-level overview of the network, allowing users to quickly understand device relationships.

Figure 3 presents a more detailed representation, highlighting individual devices and their connections. This enables users to analyze network structure more deeply and identify potential issues such as disconnected nodes or unusual connections.



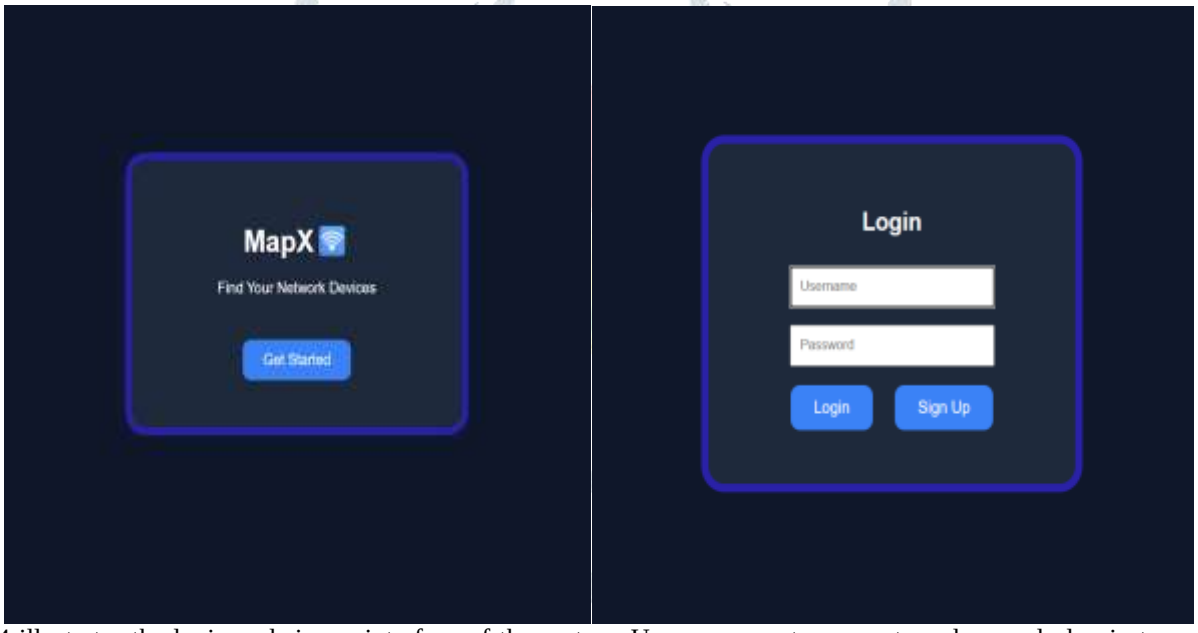


Figure 4 illustrates the login and signup interface of the system. Users can create accounts and securely log in to access the application. The interface is designed to be simple and user-friendly, ensuring accessibility.

Figure 5 demonstrates the authentication process, where user credentials are verified against the database. The system ensures secure session management by validating inputs and restricting unauthorized access.

The results indicate that the system effectively reduces manual effort in network mapping while improving accuracy. The integration of authentication mechanisms enhances security, and the visualization features improve user comprehension.

The authentication module is a critical component of the **Tool for Secure Automatic Network Topology Creation**, designed to ensure secure and controlled access to the application. It provides users with the ability to create an account (signup) and securely log in using validated credentials. The system is integrated with a database to store and verify user information, ensuring data integrity and privacy.

User Signup Process

The signup functionality enables new users to register and create an account within the system. Users are required to provide essential details such as username, email address, and password.

Upon submission, the system performs input validation to ensure:

- All required fields are completed
- Email format is valid
- Password meets security requirements

Once validated, the user credentials are securely stored in the database. Passwords are encrypted before storage to prevent unauthorized access. The system ensures that duplicate accounts are not created by verifying the uniqueness of the email or username.
Successful registration allows the user to access the login interface and use the application features.

V. CONCLUSION

This paper presented the **Tool for Secure Automatic Network Topology Creation**, an automated system designed to simplify network visualization and management. By integrating device detection, secure authentication, and graphical representation, the system provides an efficient and user-friendly solution for understanding network structures.

VI. FUTURE SCOPE

Future enhancements to the system may include real-time network monitoring, advanced device classification using machine learning, and integration with cybersecurity tools for threat detection. Additional features such as cloud-based access, multi-network support, and interactive dashboards can further improve functionality and scalability.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to faculty members, mentors, and peers for their guidance and support throughout the development of this project.

