IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, July 2025
Impact Factor: 7.67

Real Port Scan Detection With Intelligent Network Backup Tool

Midhila S[1], Nisha A[2], Harikrishnan S R[3]
Midhila, MCA, CHMM College for Advanced Studies, Trivandrum, India [1]
Nisha A, MCA, CHMM College for Advanced Studies, Trivandrum, India [2]
Head of the Department, MCA, CHMM College for Advanced Studies, Trivandrum, India [3]

Abstract: *In the evolving landscape of cybersecurity, modern networks face increasingly sophisticated threats like port scans, packet drops, unauthorized access attempts, and denial-of-service attacks. Traditional mechanisms often fail to detect these in real time or preserve critical data during breaches. This paper introduces a Real-Time Port Scan Detection with Intelligent Network Backup Tool that integrates network traffic monitoring, behavior-based detection, anomaly detection using ML, and automated backups. The system identifies and mitigates port scan threats using advanced analysis and logs all incidents for forensic reporting. A smart backup mechanism ensures data preservation during attacks, minimizing data loss and improving disaster recovery. It provides real-time dashboards and proactive alert systems to support administrators in enhancing cyber resilience.*

Keywords: Cybersecurity, Port Scan Detection, Real-Time Monitoring, Intelligent Backup, Anomaly Detection, Intrusion Detection System

I. INTRODUCTION

As cyber threats grow more sophisticated, traditional security systems often fail to detect real-time intrusions like port scans or prevent data loss during attacks. Port scanning allows attackers to identify vulnerabilities, making early detection essential. Conventional tools typically rely on static rules or known signatures, which limits their effectiveness against new or stealthy threats.To address this, we propose a Real-Time Port Scan Detection with Intelligent Network Backup Tool that combines behavior- based intrusion detection, anomaly detection using machine learning, automated alerts, and dynamic data backup. This integrated system enhances threat visibility, ensures data protection during attacks, and supports real-time analysis through a centralized dashboard. It aims to deliver a proactive and resilient approach to modern network security.

II. LITERATURE REVIEW

In the domain of cybersecurity, port scanning is recognized as a common reconnaissance technique employed by attackers to identify exploitable services. Numerous research efforts have been directed towards detecting and mitigating such activities.Stallings (2017) discusses the foundations of intrusion detection systems (IDS), categorizing them into signature-based and anomaly-based methods. While signature-based detection relies on known attack patterns, it often fails against novel or obfuscated threats. This limitation has been addressed by machine learning-based anomaly detection techniques, which learn baseline network behavior and flag deviations as potential threats.Snort and Bro (now Zeek), two prominent open-source IDS platforms, implement rule-based detection and behavioral analytics. However, their ability to trigger real-time countermeasures or initiate immediate backups during an incident is limited. Tools such as OSSEC and Suricata have enhanced event logging and rule customization but lack intelligent data resilience capabilities.In Garfinkel's work [1], the importance of forensic logging in cybersecurity is emphasized, asserting that post-attack analysis is critical for system improvement and legal proceedings. The concept of the "network black box" introduced in his work serves as a metaphor for the type of forensic mechanism integrated into our proposed system.Recent studies have also explored intelligent backup strategies. Traditional periodic backups are insufficient against rapid data loss during cyberattacks. Intelligent backup systems, as discussed in [2], utilize threat-

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, July 2025
Impact Factor: 7.67

triggered mechanisms to initiate data preservation dynamically, reducing the impact of ransomware and advanced persistent threats (APTs).Furthermore, the application of machine learning for anomaly detection has been extensively researched. In [3], models such as Isolation Forest, Autoencoders, and One-Class SVMs have shown effectiveness in identifying zero-day attacks and stealth intrusions, validating the importance of ML-based detection in modern cybersecurity solutions.Despite these advances, most existing solutions operate in silos—detecting threats or preserving data, but rarely integrating both in a real-time, unified platform. This gap in the literature validates the need for a comprehensive solution like the one proposed in this paper: a real-time port scan detection system that integrates intelligent backup, forensic logging, anomaly detection, and live alerts into a single cohesive tool.

III. PROPOSED SYSTEM

The proposed system, titled Real-Time Port Scan Detection with Intelligent Network Backup Tool, is designed as an integrated cybersecurity solution that addresses the limitations of traditional intrusion detection and backup systems. It proactively monitors network traffic, detects unauthorized port scans in real-time, and safeguards critical data through automated intelligent backup mechanisms.This system employs a modular architecture where each component contributes to overall network security and data resilience. It leverages behavior-based detection and machine learning techniques to identify both known and unknown threats, while a centralized dashboard provides administrators with real-time insights and alerts.

Key Features and Capabilities:

• Port Scan Detection: Utilizes behavior analysis and ML models to detect SYN, FIN, NULL, and stealth scan attempts.
• Anomaly Detection: Detects deviations from normal traffic patterns, identifying zero-day attacks and persistent threats.
• Intelligent Backup System: Automatically triggers data backup when a security threat is detected, minimizing data loss.
• Forensic Logging: Logs detailed attack data and system activities for investigation and audit purposes.
• Real-Time Alerting: Generates alerts via in-application dashboards, enabling instant administrator response.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, July 2025
Impact Factor: 7.67

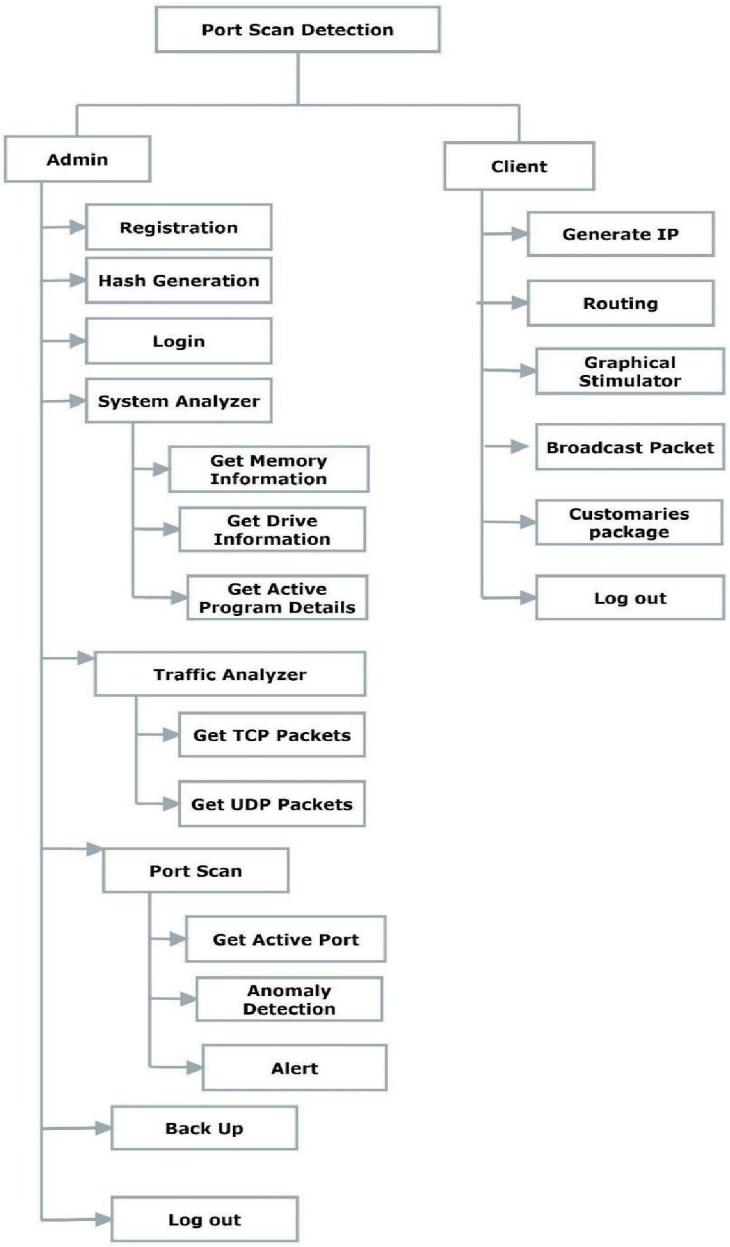

Fig 1.Subsystem of Design

IV. EXPERIMENT

To evaluate the effectiveness and functionality of the proposed system, a series of experiments were conducted in a controlled lab environment simulating real-time network conditions. The goal was to verify the system's ability to detect port scans, respond to anomalies, and initiate intelligent backup operations automatically.

1. Experimental Setup

• Operating System: Windows 10 (64-bit)
• Development Tools: Visual Studio 2019, .NET Framework
• Programming Languages: C#.NET, ML.NET

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, July 2025
Impact Factor: 7.67

• Database: Microsoft SQL Server 2022

Table 4.3.1 Login

Field Name	Data Type	Constraints	Description
uid	int	NULL	Unique identifier for the user (can be made PRIMARY KEY if needed).
username	varchar(max)	NULL	Stores the username of the user.Can be used for login/authentication.
salt	varchar(max)	NULL	Random string used to hash the password securely.
saltedpassword	varchar(max)	NULL	Hashed password combined with salt.
name	varchar(50)	NULL	Full name of the user.
phone	varchar(50)	NULL	Phone number of the user.
email	varchar(max)	NULL	Email address of the user.

OUTPUT IMAGES

Fig 2 Login Form

Fig 3.Main Form

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, July 2025
Impact Factor: 7.67

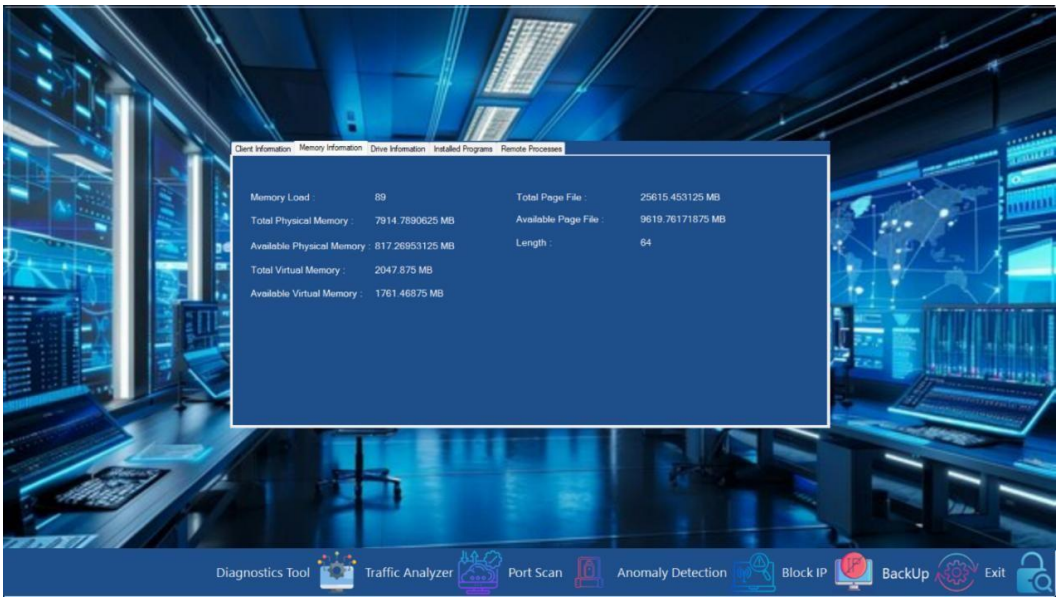

Fig 4.System Analyzer

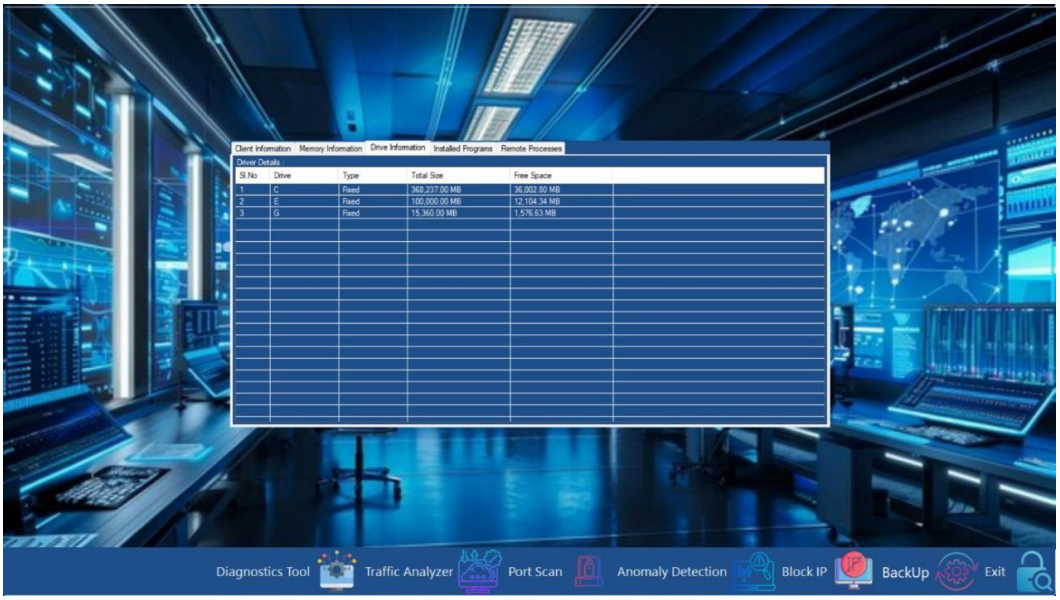

Fig 5. Drive Information

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, July 2025
Impact Factor: 7.67

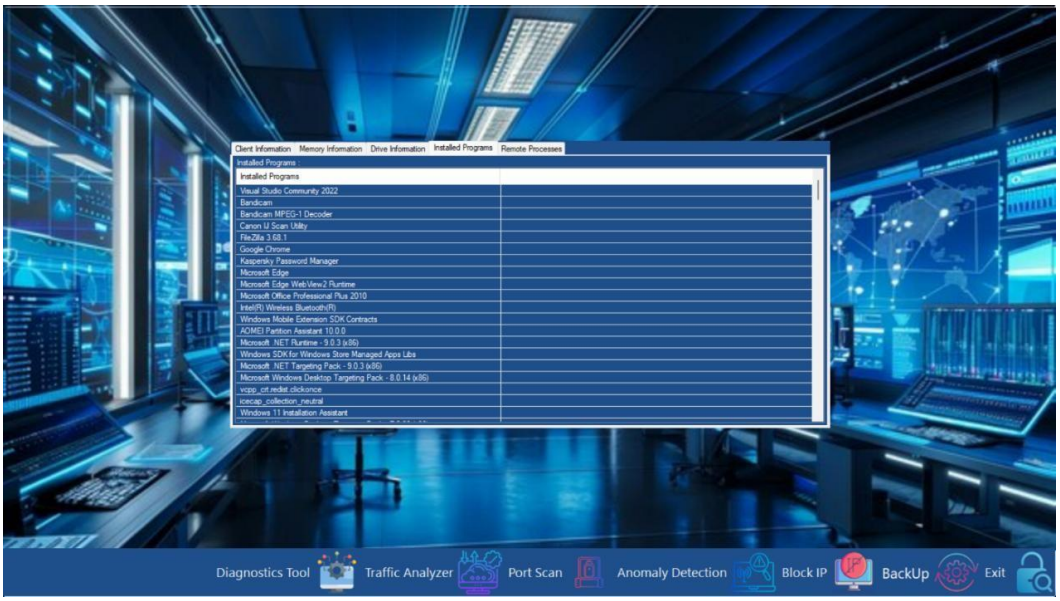

Fig 6.Software Information

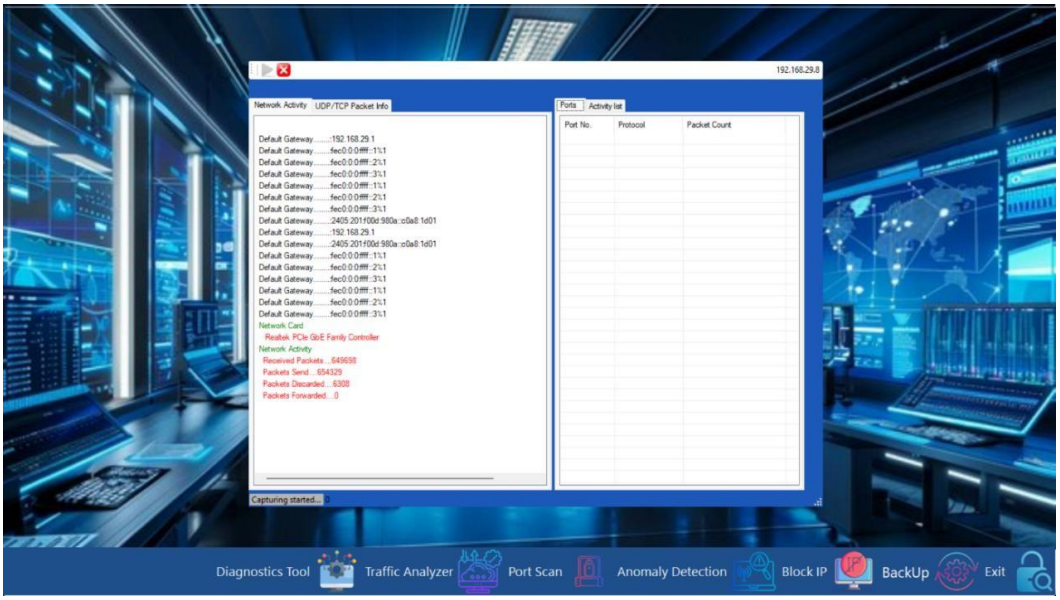

Fig 7. Monitor Ports

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, July 2025
Impact Factor: 7.67

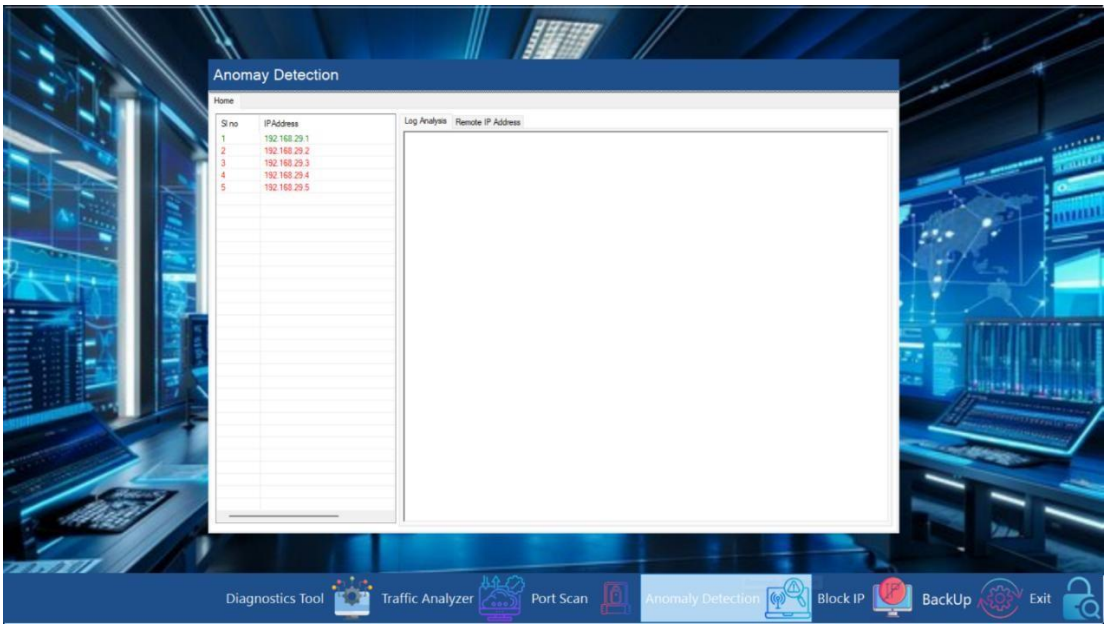

Fig 8 . Block IP

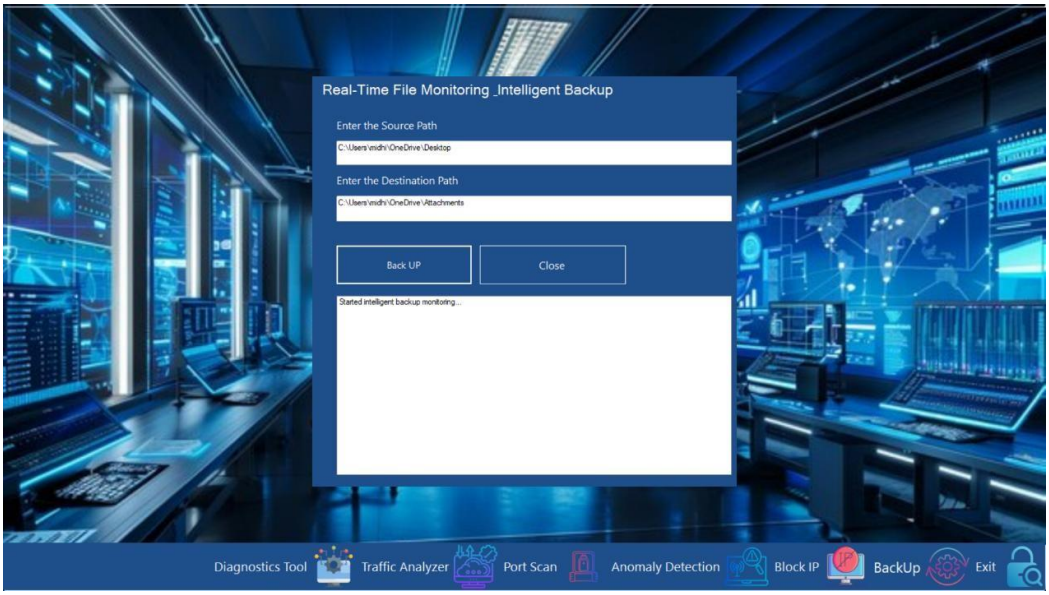

Fig 9.Backup

V. FUTURE SCOPE

To further strengthen the capabilities of the Real-Time Port Scan Detection with Intelligent Network Backup Tool, several enhancements are proposed. These include integrating AI-driven threat intelligence to adapt to zero-day vulnerabilities, enabling cloud-based dashboards for remote monitoring, and implementing self- healing mechanisms for automated response. Enhanced machine learning models like LSTM and CNN can improve anomaly detection accuracy while reducing false alerts. A built-in simulation framework would allow safe testing of attack scenarios, and

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, July 2025
Impact Factor: 7.67

a plugin-based architecture would support scalable customization. Additionally, a visual forensic replay feature can aid administrators in analyzing and understanding attack patterns more effectively.

VI. Results And Features

The tool successfully detects SYN, FIN, NULL, and stealth scans with minimal false positives. Real-time backup was triggered automatically during threat detection. Features include:

- Real-time detection of port scanning
- Automated backup upon threat detection
- Forensic logging of attack vectors
- Admin dashboard for live system analysis
- Alerting via in-app notification

VII. CONCLUSION

This system provides a unified cybersecurity solution by combining real-time intrusion detection and intelligent backup response. It enhances resilience, reduces downtime, and supports forensic investigations. Future work may include cloud integration, AI-enhanced prediction, and extended protocol analysis.

REFERENCES

[1] W. Stallings, 'Network Security Essentials', Pearson, 2017.
[2] P. Garfinkel, 'Network Forensics: Tracking Hackers through Cyberspace', O'Reilly Media.
[3] Microsoft Documentation on C# and ML.NET
[4] RFC 793 – Transmission Control Protocol
[5] OpenCV Documentation – https://opencv.org