IRJCS: International Research Journal of Computer Science
Volume 13, Issue 03, March 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.15

Network Log Analyzer for Attack Detection

Saranya N, Niga S
UG Student, Department of Computer Science and Engineering (Cyber security)
Sengunthar Engineering College (Autonomous),
Tiruchengode, India
saranyanarayanan2004@gmail.com, nigas0705@gmail.com

Prof.P.Sangeetha
Department of Computer Science and Engineering (Cyber security)
Sengunthar Engineering College (Autonomous), Tiruchengode, India
psangeetha.cse@scteng.co.in
https://orcid.org/0009-0008-7778-6546

Publication History
Manuscript Reference: IRJCS/RS/Vol.13/Issue03/CSMR26.MRCS10094
Research Article | Open Access | Double-Blind Peer Reviewed Article ID: IRJCS/RS/Vol.13/Issue03/CSMR26.MRCS10094
Received: 30, January 2026, Revised: 13, February 2026, Accepted: 28 February 2026 Published Online: 25 March 2026
https://www.irjcs.com/volumes/Vol13/iss-03/15.CSMR26.MRCS10094.pdf
Article Citation:Saranya,Niga,Prof.Sangeetha(2026),Network Log Analyzer for Attack Detection, IRJCS: International Research Journal of Computer Science, Volume 13,Issue 03 of 2026 pages 184-190
Doi:> https://doi.org/10.26562/irjcs.2026.v1303.15
BibTeX Key Prof.Sangeetha@2026 Network **Orcid:** https://orcid.org/0009-0004-9398-7488
IRJCS papers should be cited as IRJCS (International Research Journal of Computer Science, AM Publications, India 2026, ISSN 2393-9842, https://doi.org/10.26562/ijrcs.2025.v1303.15 The journal's official abbreviation is IRJCS.

Abstract: This research presents a Network Log Analyzer for Attack Detection, a system designed to monitor and analyze network log files in order to identify potential cyber attacks. In modern computer networks, various types of attacks such as brute force attempts, unauthorized access, and suspicious login activities can occur frequently. Analyzing network logs is an effective way to detect these malicious activities and improve network security. The proposed system collects and processes log files generated from network devices and servers. These logs contain important information such as IP addresses, timestamps, login attempts, and system events. The log analyzer parses the log data and applies detection rules to identify abnormal patterns that indicate possible attacks. For example, repeated failed login attempts from the same IP address can indicate a brute force attack. The system automatically analyzes the logs, detects suspicious activities, and generates alerts for the administrator. This helps network administrators monitor network behavior and respond quickly to potential threats. The results show that the proposed system can effectively identify suspicious patterns and improve the security monitoring process.Thisresearchcontributestoenhancingnetworksecuritybyproviding a simple and efficient method for log analysis and attack detection in organizational or campus networks.
Keywords: Network Security, Log Analysis, Cyber Attack Detection, Intrusion Detection, Network Monitoring, Brute Force Attack Detection, Log File Processing, Cyber security.

I. INTRODUCTION

Network log analyzer for attack detection in today's digital world, computer networks play a vital role in communication, data sharing, and organizational operations. However, the increasing use of networks has also led to a rapid growth in cyber security threats such as unauthorized access, brute force attacks, malware activities, and other malicious behaviors. These attacks can compromise sensitive information, disrupt services, and cause serious damage to network systems. Network devices and servers continuously generate log files that record various activities occurring within the system. These log files contain valuable information such as IP addresses, login attempts, timestamps, and system events. By analyzing these logs, it is possible to identify unusual patterns and detect potential security threats in the network. However, manually analyzing large volumes of log data is time-consuming and inefficient for network administrators. To address this problem, a Network Log Analyzer for Attack Detection is proposed. The main objective of this system is to automatically collect and analyze network log files in order to identify suspicious activities and possible cyber attacks. The system processes the log data, detects abnormal patterns such as repeated failed login attempts or unusual access behaviors, and alerts the administrator about potential threats. The proposed system helps improve network monitoring and security management by providing an efficient method for analyzing log files and detecting attacks at an early stage. This approach can assist organizations, educational institutions, and network administrators in maintaining a secure and reliable network environment. The proposed system integrates the Gradient Boosting algorithm with network flow analysis using the DAP dataset. It captures real-time traffic, extracts behavioral features, and employs supervised learning to distinguish normal from malicious activities. A modular architecture ensures systematic processing and scalability. Experimental results show improved detection accuracy with reduced false positives compared to conventional systems. This study contributes a robust, adaptive APT detection framework that strengthens organizational cyber security and enables proactive threat mitigation against evolving adversaries.

IRJCS: International Research Journal of Computer Science
Volume 13, Issue 03, March 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.15

The final stage presents the analysis results in a simple and understandable format. The detected attacks and suspicious activities can be displayed through reports or dashboards. This helps administrators easily monitor network security and understand the behavior of network traffic. The proposed architecture improves network security by providing an automated method to analyze log files and detect cyber attacks efficiently. In this stage, the system analyzes the processed log data to identify suspicious patterns that may indicate cyber attacks. For example, repeated failed login attempts from the same IP address within a short period may indicate a brute force attack.

II. LITERATURE REVIEW

Network security has become an important research area due to the increasing number of cyber threats and attacks on computer networks. Many researchers have proposed different techniques to monitor network activities and detect malicious behavior. One of the common approaches used in network security is the analysis of network logs, which record all activities occurring in a network system. Previous studies have shown that log analysis plays a significant role in identifying abnormal patterns and detecting cyber attacks. Network devices, servers, and applications generate log files that contain detailed information about user activities, login attempts, system errors, and network traffic. By examining these logs, security administrators can identify suspicious activities such as repeated failed login attempts, unauthorized access, and unusual traffic patterns. Several research works have also used tools such as log analyzers and packet monitoring systems to detect network attacks. These systems analyze log data and apply predefined rules or pattern recognition techniques to identify potential threats. Some researchers have focused on intrusion detection systems (IDS), which monitor network traffic and generate alerts when malicious activities are detected. However, many existing systems require complex configurations and high-level technical knowledge to operate effectively. In addition, the large volume of log data generated in modern networks makes manual analysis difficult and time-consuming. Therefore, there is a need for a simple and efficient log analysis system that can automatically monitor network logs and detect possible attacks. The proposed Network Log Analyzer for Attack Detection focuses on analyzing log files to identify suspicious activities and improve network security monitoring. This approach helps administrators quickly detect potential threats and take necessary actions to protect the network.

In addition to rule-based methods, some researchers have applied machine learning techniques for intrusion detection. Machine learning models can analyze large volumes of network data and identify abnormal patterns that may indicate new or unknown attacks. Although these methods can provide more advanced detection capabilities, they often require complex algorithms, large datasets, and high computational resources. Another important area of research involves the development of log monitoring tools such as Snort and other intrusion detection systems. These tools monitor network traffic and generate alerts when suspicious activities are detected. However, many existing tools require complex configuration and specialized technical knowledge to operate effectively. Despite the availability of various intrusion detection techniques, analyzing large volumes of log data remains a challenging task. Manual analysis of logs is time-consuming and prone to human error. Therefore, automated log analysis systems are necessary to efficiently process log data and detect cyber attacks. The proposed Network Log Analyzer for Attack Detection system aims to address these challenges by providing an automated platform for analyzing network log files and identifying suspicious activities. The system focuses on detecting abnormal patterns within log data and generating alerts to notify administrators about potential security threats. This approach helps improve network monitoring and enhances the overall security of computer networks. The cloud-based analytics layer stores processed data and runs scalable machine learning algorithms capable of identifying malicious network activities. Interactive dashboards provide real- time insights into network status, security alerts, and potential attack indicators.

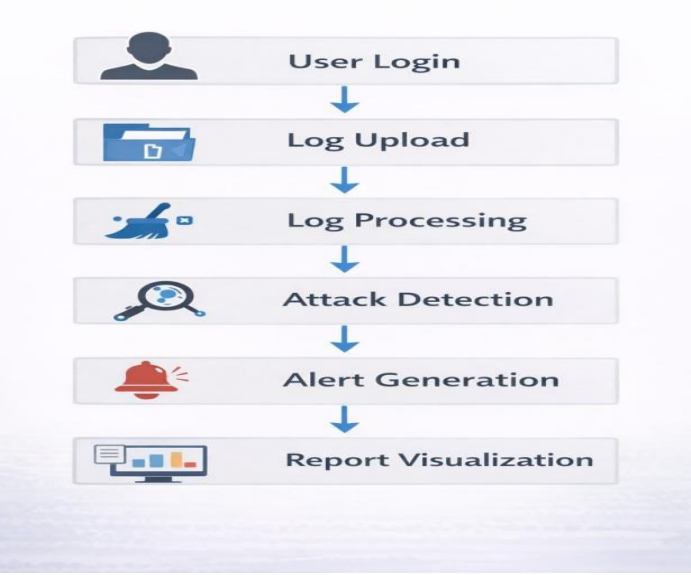

Fig.1. Architecture Diagram

ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.15

This architecture enables scalable and intelligent monitoring of enterprise networks to detect stealthy cyber threats. Several researchers have focused on developing intrusion detection systems that monitor network activities and identify potential attacks. Denning (1987) introduced one of the earliest models for intrusion detection based on monitoring system activities and detecting abnormal behavior. This model laid the foundation for many modern security monitoring systems. Later research expanded this approach by using automated techniques to analyze network logs and detect suspicious events. Log analysis has been widely used as an effective approach for detecting cyber attacks. Network devices such as routers, servers, firewalls, and operating systems continuously generate log files that record system activities. These logs contain valuable information such as login attempts, IP addresses, time stamps, and system events. By analyzing these logs, security administrators can identify suspicious activities such as repeated login failures, unusual access patterns, and unauthorized system usage. Several studies have also explored the use of rule-based detection techniques for analyzing log data. In rule-based systems, predefined rules are used to identify patterns that indicate possible security threats. For example, multiple failed login attempts from the same IP address within a short time period may indicate a brute force attack. Such rule-based approaches are widely used because they are simple to implement and effective for detecting known attack patterns.

A. User Login

The system begins with the user authentication process. In this module, the administrator logs into the system using valid credentials. This ensures that only authorized users can access the log analysis system and perform security monitoring tasks. designed to monitor and analyze network log files in order to identify suspicious activities and possible cyber attacks. The system works by collecting log data from network devices and analyzing it to detect abnormal patterns.

B. Log Upload

The first step in the system is the collection of log files generated by network devices, servers, or applications. These log files contain important information such as IP addresses, timestamps, login attempts, and system events. The collected logs act as the primary data source for analyzing network activities. After successful login, the administrator uploads the network log files into the system. These log files may be generated from network devices, servers, firewalls, or applications. The uploaded log files contain important network activity information such as IP addresses, timestamps, login attempts, and event details.

C. Log Processing

After collecting the log files, the system performs log parsing to extract relevant information from the raw log data. During this stage, unnecessary data is removed, and important fields such as IP address, date and time, login status, and event type are identified. This preprocessing step helps convert unstructured log data into a structured format for further analysis. In this stage, the system processes the uploaded log files. The raw log data is cleaned and parsed to extract useful information required for analysis. Unnecessary or irrelevant data is removed, and the log entries are organized into a structured format to simplify further analysis.

D. Attack Detection

The Once the log data is processed, the system analyzes the logs to detect suspicious activities. The system identifies abnormal patterns such as repeated failed login attempts, unusual access behavior, or multiple requests from the same IP address. For example, repeated failed login attempts from the same IP address within a short period may indicate a brute force attack. These patterns may indicate potential cyber attacks such as brute force attacks or unauthorized access attempts. Detection rules are applied to identify abnormal behaviors and possible security threats.

Security Implementation

The Network Log Analyzer for Attack Detection system is implemented as a web-based application that analyzes network log files and detects suspicious activities within the network. The system is developed using modern web technologies and consists of multiple modules that work together to process log data and identify potential cyber attacks. The implementation process involves several stages including user authentication, log file upload, log processing, attack detection, alert generation, and result visualization**.**

E. Alert Generation

There If suspicious activity is detected, the system automatically generates alerts. These alerts notify the administrator about potential security threats in the network. Early alerts allow administrators to take immediate action to prevent further damage to the system. Once suspicious activity is detected, the system generates alerts to notify the network administrator. These alerts help administrators quickly respond to potential attacks and take appropriate security actions to prevent further damage.

F. Report Visualization

These the final module presents the analysis results in the form of reports or visual charts. The system displays detected attacks, suspicious IP addresses, and other security-related information. This visualization helps administrators easily understand network activity and monitor the overall security status of the system. The proposed architecture provides an efficient and automated approach for analyzing network log files and detecting cyber attacks, thereby improving network security monitoring.

III. TECHNOLOGIES USED

1. Network Log Detection Modules

The proposed Network Log Analyzer for Attack Detection system is developed using modern web technologies to provide an efficient and interactive platform for analyzing network logs and detecting cyber attacks.

IRJCS: International Research Journal of Computer Science
Volume 13, Issue 03, March 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.15

The main technologies used in the development of the system include React, TypeScript, JavaScript, HTML, and CSS. These technologies help build a responsive user interface and support efficient data processing and visualization. Data Collection and Flow Monitoring. Network flow monitoring technologies.

II. React Framework

React is a popular JavaScript library used for building user interfaces, especially for web applications. It enables developers to create reusable UI components and manage the application interface efficiently. In the proposed system, React is used to design the main dashboard where administrators can upload log files, monitor network activity, and view analysis results.

III. Type Script

Data TypeScript is a strongly typed programming language that builds on JavaScript. It adds static typing and advanced development features, which help improve code quality and reduce programming errors. In this project, TypeScript is used to develop reliable and maintainable code for the frontend application. Using TypeScript helps developers detect errors during development rather than during runtime, making the system more stable and easier to maintain. It also improves the readability and scalability of the application.

IV. JavaScript

A JavaScript is widely used for developing dynamic and interactive web applications. It allows the system to process user actions, manage data, and communicate between the user interface and backend services. In the proposed system, JavaScript is used to handle log file uploads, process user inputs, and control system functionalities such as displaying alerts, generating reports, and updating dashboard components.

V. HTML

The HyperText Markup Language (HTML) is used to create the structure of the web application. It defines the layout of different elements such as forms, buttons, tables, and dashboards within the system. In this project, HTML is used to build the interface where administrators can log into the system, upload network log files, and view the analysis results. It acts as the foundation for presenting information in the browser.

VI. CSS

Visualization Cascading Style Sheets (CSS) is used to design and style the user interface of the application. CSS controls the appearance of web pages, including colors, fonts, layouts, and responsiveness. In the proposed system, CSS is used to create a clean and user-friendly interface for administrators. It ensures that the dashboard, reports, and alert notifications are displayed clearly and in an organized manner. These technologies help build a responsive web application that allows administrators to easily interact with the system and monitor network security. The Attack Detection Module is the core component of the system. It analyzes the processed log data to identify suspicious activities and potential cyber attacks. The system uses rule-based detection techniques to identify abnormal patterns in network activity.

VI. IMPLEMENTATIONS AND RESULTS

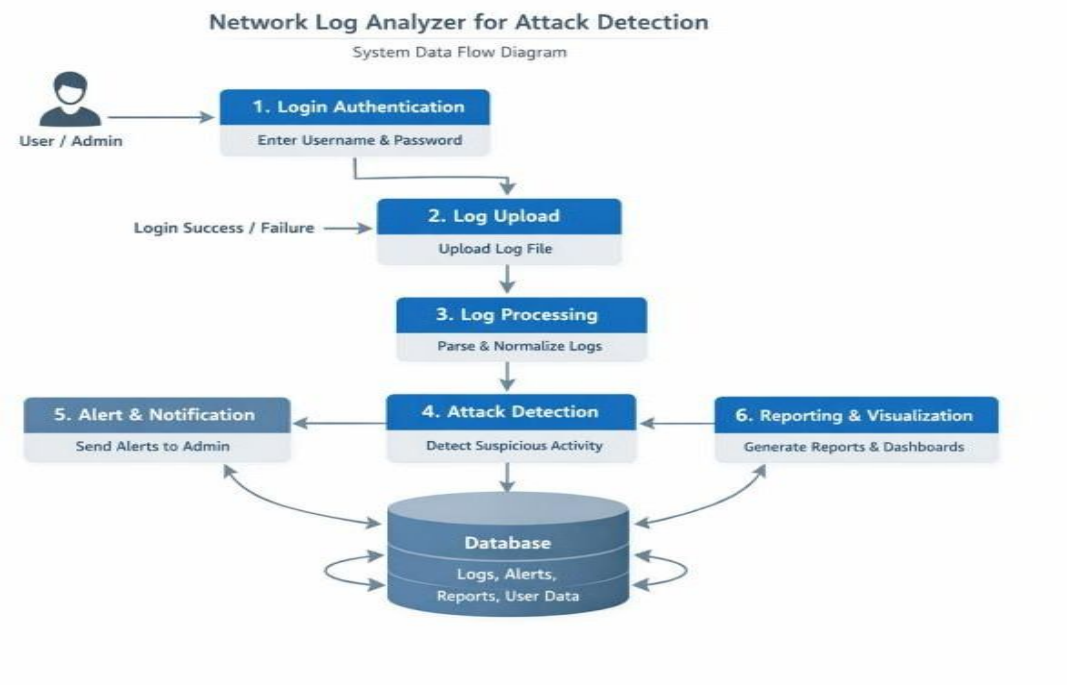

Fig.2: System Implementation

IRJCS: International Research Journal of Computer Science
Volume 13, Issue 03, March 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.15

The Network Log Analyzer for Attack Detection system is implemented as a web-based application that analyzes network log files to identify suspicious activities and potential cyber attacks. The implementation integrates modern frontend technologies to provide an efficient and user-friendly interface for network administrators. The system processes log files through several stages, including authentication, log upload, log parsing, attack detection, and result visualization.

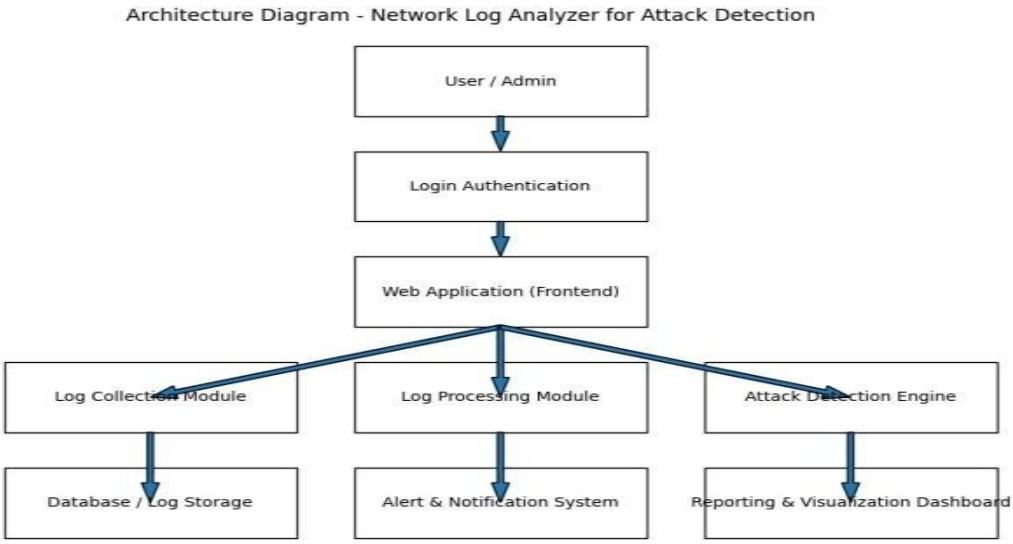

Fig.3 Use case Diagram

A Use Case Diagram represents the interaction between the users and the system. It illustrates how different actors interact with the system to perform various operations. In the proposed Network Log Analyzer for Attack Detection, the use case diagram describes the functionalities provided by the system and how the administrator interacts with these functionalities. The primary actor in the system is the Administrator**,** who is responsible for managing the log analysis process and monitoring network security activities.

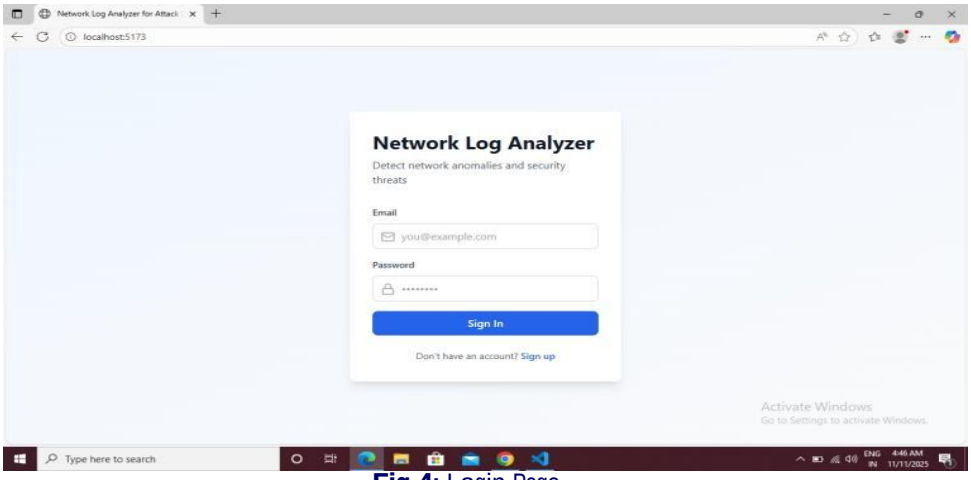

Fig 4: Login Page

The Login Page is the entry point of the Network Log Analyzer for Attack Detection system. It allows the administrator to access the system by entering a username and password. The system verifies the entered credentials to ensure that only authorized users can access the platform. If the login details are correct, the administrator is redirected to the main dashboard to upload log files and analyze network activities. This page helps maintain the security and access control of the system.

Key Considerations:

Accuracy of log data: While developing the Network Log Analyzer for Attack Detection, several important factors must be considered to ensure the system performs efficiently and securely.

Efficient log processing: Network systems generate large volumes of log data continuously, so the system must be capable of processing and analyzing these logs quickly. Proper parsing and filtering techniques should be applied to extract only relevant information.

Security and privacy of log data: The must also be maintained since log files may contain sensitive information such as IP addresses and system events. Access control and authentication mechanisms should be implemented to ensure that only authorized administrators can view or analyze the logs.

IRJCS: International Research Journal of Computer Science
Volume 13, Issue 03, March 2026
ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.15

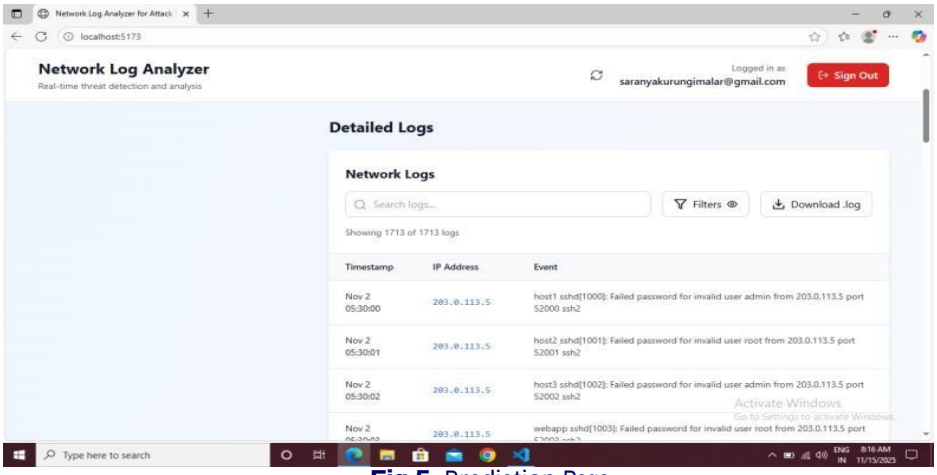

Fig 5: Prediction Page

Accuracy of attack detection: The system should be designed to minimize false positives and false negatives while detecting suspicious activities such as repeated failed login attempts or abnormal access patterns. As network traffic increases, the system must be capable of handling larger log datasets while still providing a user-friendly interface that allows administrators to easily monitor network security and respond to threats.

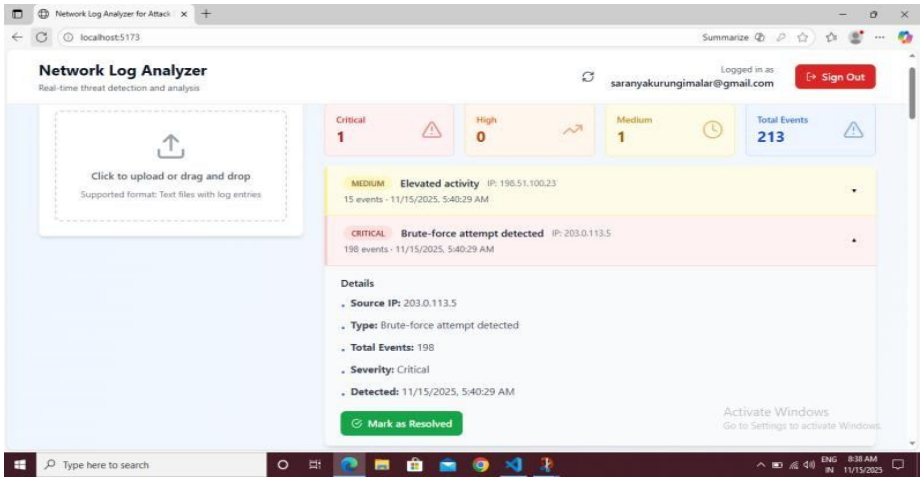

Fig 6: Threat Detection

IV. CONCLUSION

The proposed Network Log Analyzer for Attack Detection system is designed to improve network security by analyzing log files generated from network devices and servers. Log files contain important information such as IP addresses, timestamps, login attempts, and system activities, which can be used to identify suspicious behavior in the network. The proposed system processes these log files and detects abnormal patterns that may indicate cyber attacks such as brute force attacks or unauthorized access attempts. The system consists of several modules including user authentication, log file upload, log processing, attack detection, alert generation, and report visualization**.** When suspicious activity is detected, the system generates alerts and displays reports to notify the administrator. This helps administrators quickly identify security threats and take appropriate actions to protect the network. Overall, the proposed system provides an effective and reliable solution for monitoring network activities and enhancing cyber security. Once suspicious activity is detected, the system generates alerts to notify the administrator. The results are also presented through reports and visual summaries, allowing administrators to easily monitor network activity and understand security conditions.

REFERENCES

1. W.Stallings, Network Security Essentials: Applications and Standards, 6th ed. Boston, MA,USA: Pearson, 2017.
2. W.Stallings and L.Brown, Computer Security: Principles and Practice, 4th ed. Boston, MA, USA: Pearson, 2018.
3. K.Scarfone and P.Mell, “Guide to Intrusion Detection and Prevention Systems (IDPS),” National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, Special Publication 800-94, 2012.
4. B.Mukherjee, L.T.Heberlein, and K. N. Levitt, “Network intrusion detection,” IEEE Network, vol. 8, no. 3, pp. 26–41, May–Jun. 1994.
5. R.Sommer and V.Paxson, “Outside the closed world: On using machine learning for network intrusion detection,” in Proc. IEEE Symp. Security and Privacy, 2010, pp. 305–316.
6. D.Denning, “An intrusion detection model,” IEEE Transactions on Software Engineering, vol. SE-13, no. 2, pp. 222–232, Feb.1987.

ISSN: 2393-9842
https://www.irjcs.com/archives
https://doi.org/10.26562/irjcs.2025.v1303.15

7. S.Axelsson, "Intrusion detection systems: A survey and taxonomy," Dept. Computer Engineering, Chalmers Univ., Sweden, Tech. Rep., 2000.
8. M.Roesch, "Snort: Lightweight intrusion detection for networks," in Proc. USENIX LISA Conf., 1999, pp. 229–238.
9. C.Kruegel and G.Vigna, "Anomaly detection of web-based attacks," in Proc. ACM CCS, 2003, pp. 251–261.
10. A.Lazarevicet al., "A comparative study of anomaly detection schemes in network intrusion detection," in Proc. SIAM Int. Conf. Data Mining, 2003.
11. S.Northcutt and J. Novak, Network Intrusion Detection, 3rd ed. Indianapolis, IN, USA: New Riders Publishing, 2003.
12. M.Behl and A.Behl, Cyber security and Cyberwar: What Everyone Needs to Know, Oxford, U.K.: Oxford University Press, 2017.
13. J.Behl and K.Behl, Cyber security and Cyberwar: What Everyone Needs to Know, Oxford University Press, 2017.
14. T.F. Lunt, "A survey of intrusion detection techniques,"Computers&Security,vol.12,no.4, pp. 405–418, 1993.
15. S.Garfinkel and G.Spafford, Practical UNIX and Internet Security, 3rd ed. Sebastopol, CA,USA: O'Reilly Media, 2003.
16. J.Anderson, "Computer security threat monitoring and surveillance," James P. Anderson Co., Fort Washington, PA, USA, Tech. Rep., 1980.
17. R.Bace and P.Mell, "Intrusion detection systems," National Institute of Standards and Technology (NIST), Special Publication 800-31, 2001.
18. K.Julisch, "Clustering intrusion detection alarms to support root cause analysis," ACM Transactions on Information and System Security, vol. 6, no. 4, pp. 443–471, Nov. 2003.
19. S.Kent and K.Seo, "Security architecture for the Internet protocol," Internet Engineering Task Force (IETF), RFC 4301, 2005.
20. T.Liao, V.Vemuri, "Use of K-nearest neighbor classifier for intrusion detection," Computers&Security,vol.21,no.5,pp.439–448,2002.