Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 4 | April-2026
ISSN (O) 3107-6696

Design and Implementation of a Web-Based SIEM Framework with Secure Authentication and Interactive Threat Visualization

"An Integrated Approach for Real-Time Log Analysis, Threat Detection, and Visualization"

Prithi Jessica J (23CU0310239), Kaavya K (23CU0310383), Tharshini A (23CU0310397)
Student, Hindustan Institute of Technology Science

Dr. Monica Jenefer, Ms. P. Chandralekha
Professor, Assistant Professor
Computer Science and Engineering, Hindustan Institute of Technology and Science

---

Abstract – Security Information and Event Management (SIEM) systems play a crucial role in modern cybersecurity by enabling centralized log analysis, threat detection, and incident response. However, many existing SIEM solutions are complex, resource-intensive, and costly, making them less suitable for academic environments and small-scale deployments. This paper presents SIEM Secure, a lightweight, web- based SIEM framework designed to provide secure authentication, real-time log analysis, rule- based threat detection, and interactive visualization through an intuitive dashboard.

The proposed system adopts a three-layer architecture comprising data, processing, and presentation layers. It supports both local and remote log collection, where logs are parsed and normalized to extract key attributes such as timestamp, IP address, username, and event type. A rule-based detection engine is implemented to identify common security threats, including brute- force login attempts, suspicious access patterns, and unauthorized activities. Detected events are classified into severity levels and stored in structured JSON databases for efficient management.

The system integrates role-based authentication with SHA-256 password hashing, account lockout mechanisms, and audit logging to enhance security. Alerts generated during analysis are visualized using interactive charts and tables, enabling users to monitor system activity effectively. Additionally, a notification module provides real-time dashboard alerts and email notifications for critical incidents using SMTP configuration.

Experimental evaluation demonstrates that SIEM Secure effectively detects simulated attack patterns and provides meaningful insights through visualization. The proposed framework offers a practical, scalable, and user-friendly solution for security monitoring, particularly suitable for educational purposes and small to medium-scale environments.

Keywords- Security Information and Event Management (SIEM), Log Analysis, Threat Detection, Cybersecurity Monitoring, Rule-Based Detection, Stream lit Dashboard, Authentication Security, Alert Management, Security Visualization, Intrusion Detection System (IDS).

I. INTRODUCTION

With the rapid expansion of digital systems, cloud services, and interconnected networks, organizations generate a massive volume of system and security logs on a daily basis. These logs contain valuable information about user activities, system behavior, and potential security incidents. However, manually analyzing such large-scale and unstructured data is inefficient, time-consuming, and prone to human error. As cyber threats such as unauthorized access, brute- force attacks, and data breaches continue to increase, there is a growing need for automated solutions that can efficiently monitor, analyze, and respond to security events in real time.

Security Information and Event Management (SIEM) systems have emerged as a critical component in cybersecurity operations, providing centralized log collection, event correlation, and threat detection capabilities. Despite their importance, many existing SIEM solutions are complex, expensive, and require significant computational resources, making them less accessible for academic environments and small- scale organizations.

To address these challenges, this paper proposes SIEM Secure, a lightweight and web-based SIEM framework designed to simplify log analysis and threat detection while maintaining essential security features. The system integrates secure user

authentication, role-based access control, and an automated log processing pipeline that supports

both local and remote log sources. Using a rule- based detection engine, the system identifies suspicious patterns such as repeated failed login attempts and unauthorized access activities.

Furthermore, SIEM Secure provides an interactive dashboard built with modern visualization tools to present alerts, statistics, and system insights in a user-friendly manner. By combining usability, security, and efficient log analysis, the proposed system serves as a practical and scalable solution for cybersecurity monitoring and educational applications

II. PRELIMINARIES

The increasing dependence on digital platforms and networked systems has significantly amplified the risk of cyber threats, making cybersecurity a critical concern in modern computing environments. Organizations rely on various systems such as servers, applications, and network devices, all of which continuously generate log data. These logs serve as a primary source of information for monitoring system activities, detecting anomalies, and identifying potential security breaches. However, due to their large volume and unstructured nature, manual log analysis is inefficient and often ineffective in detecting sophisticated attacks.

Security Information and Event Management (SIEM) systems are designed to address this challenge by providing a centralized platform for log collection, normalization, analysis, and threat detection. SIEM solutions combine Security Information Management (SIM) and Security Event Management (SEM) functionalities to enable real-time monitoring and correlation of events across multiple sources. By applying predefined rules and patterns, SIEM systems can identify suspicious activities such as repeated login failures, unauthorized access attempts, and abnormal user behaviour.

A key aspect of SIEM systems is log parsing and normalization, where raw log data is converted into a structured format by extracting important attributes such as timestamps, IP addresses, usernames, and event types. This structured representation allows efficient analysis and correlation of events. Additionally, rule-based detection mechanisms are commonly used to identify known attack patterns, offering a simple yet effective approach for threat detection.

The proposed SIEM Secure system builds upon these foundational concepts by implementing a lightweight, web-based SIEM framework. It focuses on automated log analysis, rule-based threat detection, secure authentication, and interactive visualization. By integrating these components, the system provides a simplified yet practical approach to understanding real-world security monitoring and incident detection processes.

II.I KEY TECHNOLOGIES

Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) is a cybersecurity solution that provides real-time monitoring, detection, and analysis of security events across an organization's IT infrastructure. It combines Security Information Management (SIM), which handles log collection and storage, with Security Event Management (SEM), which focuses on real-time threat detection and alerting. SIEM systems collect logs from multiple sources such as servers, applications, and network devices, then analyse them using predefined rules or algorithms to identify suspicious activities. When potential threats are detected, alerts are generated for further investigation. SIEM also supports incident response, compliance reporting, and forensic analysis. Modern SIEM solutions integrate visualization dashboards and automated notifications, enabling security teams to respond quickly and efficiently to cyber threats

Security Operations Center (SOC)

The Security Operations Centre (SOC) represents the operational layer where security monitoring and incident response are performed. The Stream lit dashboard acts as a simplified SOC interface, allowing users to continuously monitor logs, analyse threats, and manage alerts in real time. Security analysts (users) can run log analysis, view detected threats, and respond by acknowledging alerts. The system simulates key SOC functionalities such as real-time alerting, incident tracking, and audit logging. Additionally, features like email notifications and dashboard

alerts ensure timely awareness of critical threats. Thus, SIEM Secure functions as a mini SOC platform, integrating monitoring, detection, visualization, and response into a single unified system.

Log Parsing and Normalization

The log parsing and normalization are essential steps in transforming raw log data into a structured format for analysis. The system reads logs from local files or remote servers and extracts key attributes such as timestamp, IP address, username, and event type. Since logs may come in different formats,

normalization ensures that all data follows a consistent structure, enabling accurate comparison and processing. This standardized data is then used by the SIEM Framework to apply detection rules and identify potential threats. Effective parsing and normalization improve detection accuracy, reduce false positives, and support meaningful visualization in the dashboard.

Rule-Based Correlation

In the SIEM Secure project, rule-based correlation is used to identify security threats by analysing patterns within normalized log data. The SIEM Framework applies predefined rules to detect suspicious activities such as multiple failed login attempts, unusual IP access, or privilege escalation. Instead of evaluating single events in isolation, the system correlates multiple related events over time to recognize potential attacks like brute force or unauthorized access. When a rule condition is met, the system generates an alert with a defined severity level. This approach enables efficient threat detection, reduces noise from irrelevant logs, and helps users focus on critical security incidents within the dashboard.

Brute-force Attack Detection

The brute-force attack detection is achieved using rule-based analysis in the SIEM Framework. The system tracks repeated failed login attempts from the same IP address or user within a short duration. When these attempts exceed a defined threshold, it is identified as a potential brute-force attack. The system then generates a high or critical alert containing details like IP address, username, and timestamp. This enables users to quickly detect unauthorized access attempts and respond effectively through the dashboard and alert management system.

Severity Classification

The severity classification is used to prioritize detected security threats based on their impact and urgency. Each alert generated by the SIEM Framework is assigned a severity level such as LOW, MEDIUM, HIGH, or CRITICAL. This classification is determined based on the type of attack, frequency of events, and potential risk to the system. For example, multiple failed logins may be HIGH, while privilege escalation attempts are CRITICAL. This helps users quickly identify and focus on the most serious threats through the dashboard, improving response efficiency and decision-making.

II.II LOG ATTRIBUTES CONSIDERED

The log attributes play a crucial role in enabling effective threat detection, correlation, and analysis. During the log parsing and normalization phase, raw log data collected from local files or remote servers is transformed into a structured format by extracting key attributes. These attributes provide meaningful information about each event and serve as the foundation for the SIEM Framework's detection engine.

The primary attribute considered is the timestamp, which records the exact date and time an event occurred. This is essential for identifying patterns over time, such as repeated login failures within a short duration. The IP address is another critical attribute, used to trace the origin of activities and detect suspicious or unauthorized access attempts from unknown or blacklisted sources. The username attribute helps monitor user behaviour and identify anomalies such as repeated failed login attempts or unusual login patterns.

The event type is also a key attribute, indicating the nature of the activity, such as login success, login failure, or system access. This helps in classifying events and applying appropriate detection rules. Additionally, the log message or description provides detailed context about the event, which can be analyzed to identify specific attack signatures or unusual behavior. The system source attribute indicates where the log originated, such as a server or application, enabling better tracking and categorization of events.

Security Information and Event Management (SIEM) systems have emerged as a critical component in cybersecurity operations, providing centralized log collection, event correlation, and threat detection capabilities. Despite their importance, many existing SIEM solutions are complex, expensive, and require significant computational resources, making them less accessible for academic environments and small- scale organizations.

To address these challenges, this paper proposes SIEM Secure, a lightweight and web-based SIEM framework designed to simplify log analysis and threat detection while maintaining essential security features. The system integrates secure user authentication, role-based access control, and an automated log processing pipeline that supports alerts ensure timely awareness of critical threats. Thus, SIEM Secure functions as a mini SOC platform, integrating monitoring, detection, visualization, and response into a single unified system.

II. III CHALLENGES AND MOTIVATION

The development of the SIEM Secure system is driven by the increasing need for efficient and real-time cybersecurity monitoring in modern digital environments. Organizations generate massive volumes of log data from various sources

Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 4 | April-2026
ISSN (O) 3107-6696

such as servers, applications, and network devices. However, manually analyzing these logs to identify potential threats is both time- consuming and prone to human error. This challenge highlights the necessity for an automated system that can intelligently process and analyze security events, which serves as the primary motivation behind this project.

One of the key challenges faced during the implementation of SIEM Secure is handling heterogeneous log formats. Logs collected from different sources may vary in structure and content, making it difficult to standardize them for analysis. To overcome this, the project incorporates log parsing and normalization techniques to ensure consistency. Another significant challenge is designing effective rule- based detection mechanisms that can accurately identify threats such as brute-force attacks while minimizing false positives and false negatives.

Real-time processing is also a critical challenge, as the system must analyze logs and generate alerts promptly without performance degradation. Additionally, ensuring secure user authentication and role-based access control is essential to prevent unauthorized access to sensitive security data. Implementing features such as account lock mechanisms, password hashing, and audit logging adds complexity but is necessary for maintaining system integrity.

Integrating multiple components such as log collection, analysis engine, alert management, visualization dashboard, and email notification system into a single cohesive platform is another major challenge. Despite these challenges, the motivation behind SIEM Secure lies in creating a practical, scalable, and user-friendly solution that demonstrates the core functionalities of a real- world SIEM system. It provides users with the ability to monitor, detect, visualize, and respond to security threats efficiently, thereby enhancing overall cybersecurity awareness and preparedness.

III. EXISTING SYSTEM

In the current cybersecurity landscape, traditional security monitoring systems and basic log management tools are widely used by organizations to track system activities and detect potential threats. These existing systems primarily focus on collecting and storing logs generated from servers, applications, and network devices. While they provide a record of events, they often lack advanced capabilities for real-time analysis, threat detection, and intelligent alerting.

Most existing systems rely heavily on manual log inspection, where security analysts must review large volumes of data to identify suspicious activities. This approach is time-consuming, inefficient, and prone to human error, especially when dealing with high-frequency log generation. Additionally, many basic systems do not support proper log normalization, leading to inconsistencies when handling logs from multiple sources with different formats.

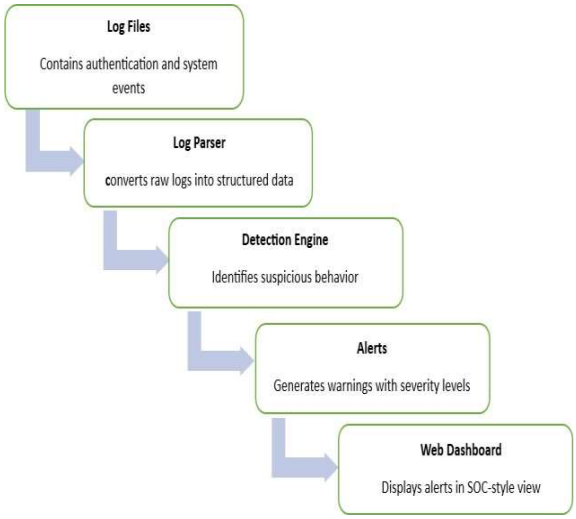
Another limitation of existing systems is the lack of effective correlation mechanisms. They often analyse events in isolation rather than identifying patterns across multiple events. As a result, complex attacks such as brute-force attempts or multi-stage intrusions may go undetected. Furthermore, traditional systems may not provide proper severity classification, making it difficult for analysts to prioritize critical threats over less significant events.

Visualization is also a major drawback in many existing solutions. Basic tools typically offer limited or no graphical dashboards, forcing users to interpret raw data without clear insights. This reduces the overall efficiency of threat analysis and decision-making. Additionally, alerting mechanisms in such systems are either absent or not robust, meaning users may not be notified promptly when critical threats occur.

Security features such as role-based access control, audit logging, and secure authentication are also often limited or missing in simpler implementations. This can lead to unauthorized access and lack of accountability within the system.

These limitations highlight the need for an advanced, integrated solution like SIEM Secure, which overcomes these challenges by providing automated log analysis, rule-based detection, real- time alerts, interactive dashboards, and enhanced security features in a unified platform.

IV. ARCHITECTURE FOR SIEM LOG ANALYZER



V. MODULES DESCRIPTION

The proposed SIEM Secure Log Analyzer system is composed of multiple modules that work together to ensure efficient log monitoring, accurate threat detection, and secure system access. These modules include authentication, log collection, detection, and correlation, each contributing to the overall functionality of the system. The authentication module secures user access, while the log collection module gathers data from local and remote sources. The detection engine identifies potential threats, and the correlation engine links related events to detect complex attack patterns. The modular design

improves scalability, maintainability, and clarity, enabling systematic and efficient processing of security events.

Authentication module

The Authentication module in the SIEMSecure project ensures secure access to the system through user registration and login functionalities. It implements password hashing using SHA-256 and enforces strong password policies. The module tracks failed login attempts and temporarily locks accounts after multiple failures to prevent unauthorized access. It also supports role-based access (Admin and Analyst) and logs all activities in the audit system for accountability and security monitoring.

Log collection module

The Log Collection module in the SIEMSecure project is responsible for gathering log data from different sources for analysis. It supports both local log files in test mode and remote log retrieval using SSH in live mode. The module ensures that logs are continuously accessible for processing by the SIEMFramework. By collecting logs from various sources, it provides the foundation for detecting security events and monitoring system activities effectively.

Detection Engine

The Detection Engine in the SIEMSecure project is the core component responsible for identifying potential security threats. It operates within the SIEMFramework by applying rule-based correlation on parsed and normalized log data. The engine detects suspicious patterns such as repeated failed logins, unusual access attempts, and privilege escalation. When a rule is triggered, it generates alerts with appropriate severity levels, enabling users to quickly identify and respond to security incidents.

Correlation Engine

The Correlation Engine in the SIEMSecure project analyzes relationships between multiple log events to identify complex security threats. Instead of evaluating events individually, it links related activities such as repeated login failures from the same IP or unusual access patterns over time. By applying rule-based correlation, the engine detects coordinated or multi-stage attacks more effectively, reduces false positives, and enhances the accuracy of threat detection within the system.

VI. METHODOLOGY

The SIEM Secure system follows a structured methodology to achieve efficient log monitoring, threat detection, and security management. The process begins with data acquisition, where logs are collected from different sources. The system supports both local log files (test mode) and remote log collection using SSH (live mode). This ensures flexibility in handling real-world and simulated environments.

Once the logs are collected, the next step is log parsing and normalization. In this phase, raw log data is processed to extract important attributes such as timestamp, IP address, username, and event type. Since logs may come in different formats, normalization ensures that all data is converted into a consistent structure, making it easier for further analysis.

After preprocessing, the detection phase is carried out using a rule-based approach. The SIEM Framework applies predefined rules to identify suspicious patterns such as repeated failed login attempts, unauthorized access, and abnormal user behavior. These rules help in detecting common cyber threats like brute-force attacks and privilege misuse.

The next step is correlation analysis, where multiple related events are linked together to identify complex or multi-stage attacks. Instead of analyzing events individually, the system examines patterns over time, improving detection accuracy and reducing false positives.

Once threats are detected, the system generates alerts with different severity levels such as LOW, MEDIUM, HIGH, and CRITICAL. These alerts are stored in a database and displayed in the dashboard for user review. Users can filter, analyze, and acknowledge alerts through the interface.

The system also includes a notification mechanism, where critical alerts trigger email notifications using SMTP configuration.

Additionally, all user activities and system events are recorded in an audit log for security and accountability.

Finally, the results are visualized using an interactive dashboard built with Stream lit and Plot Ly, providing charts, metrics, and summaries. This methodology ensures a complete workflow from log collection to threat detection, alerting, and response, making the SIEM Secure system efficient and reliable.

VI.I HYPOTHESIS

The proposed SIEM Secure system is based on the hypothesis that an automated, rule-based log analysis framework can effectively detect and manage security threats in real time while improving accuracy, efficiency, and response time compared to traditional manual monitoring systems. It assumes that by collecting logs from multiple sources, parsing and normalizing them into a structured format, and applying predefined detection rules, the system can identify suspicious activities such as brute-force attacks, unauthorized access, and abnormal user behaviors.

Another key hypothesis is that correlating multiple related events over time will significantly enhance threat detection capabilities. Instead of analyzing individual log entries in isolation, the system links patterns such as repeated login failures or unusual access sequences to detect complex or multi-stage cyberattacks. This approach is expected to reduce false positives and provide more meaningful alerts.

The project also hypothesizes that implementing severity classification for alerts will help users prioritize critical threats effectively. By categorizing alerts into levels such as LOW, MEDIUM, HIGH, and CRITICAL, the system enables faster decision-making and efficient incident response.

Furthermore, it is assumed that integrating visualization tools such as dashboards and charts will improve user understanding

of security events and system status. The inclusion of real-time notifications and email alerts is expected to enhance responsiveness to critical incidents.

Finally, the hypothesis suggests that a modular architecture, combined with secure authentication and audit logging, will ensure system scalability, maintainability, and security. Overall, the SIEM Secure system is expected to provide a reliable and efficient solution for real-time security monitoring and threat management.

VI.II SOLUTION AND APPROACH

The SIEM Secure project proposes an integrated solution for real-time security monitoring and threat detection by combining log analysis, rule- based detection, and interactive visualization within a single platform. The approach focuses on automating the entire security monitoring process, reducing manual effort while improving detection accuracy and response time.

The solution begins with efficient log collection, where the system gathers data from local files (test mode) or remote servers using SSH (live mode). This ensures flexibility in handling both simulated and real-world environments. The collected logs are then passed through a parsing and normalization process, where important attributes such as timestamp, IP address, username, and event type are extracted and standardized into a consistent format.

The core of the approach lies in the rule-based detection engine, implemented within the SIEM Framework. Predefined rules are applied to identify suspicious activities such as multiple failed login attempts, unauthorized access, and abnormal user behavior. These rules enable quick identification of common attack patterns like brute-force attacks.

To enhance detection accuracy, the system incorporates a correlation engine that links related events over time. This allows the system to detect complex or multi-stage attacks by analyzing patterns rather than isolated events, thereby reducing false positives.

Once a threat is detected, the system generates alerts with appropriate severity classification (LOW, MEDIUM, HIGH, CRITICAL). These

alerts are stored and displayed in an interactive dashboard built using Stream lit and Plotly, providing visual insights through charts and metrics. Users can filter, analyze, and acknowledge alerts directly through the interface.

Additionally, the system includes a notification mechanism, where critical alerts trigger real-time dashboard notifications and email alerts using SMTP configuration. An audit logging system records all user actions and system events to ensure accountability and traceability.

Overall, the proposed solution provides a structured and automated approach to security monitoring, enabling efficient detection, visualization, and response to cyber threats.

VII. EXPERIMENTAL RESULTS AND DISCUSSIONS

The SIEM Secure system was tested using both local log files (test mode) and simulated live environments to evaluate its performance in detecting security threats. The experimental results demonstrate that the system is capable of efficiently parsing and analyzing large volumes of log data while accurately identifying suspicious activities. During testing, common attack scenarios such as multiple failed login attempts and unauthorized access patterns were successfully detected using the rule-based detection engine.

The system generated alerts with appropriate severity levels, allowing clear prioritization of threats. Critical and high-severity alerts were effectively highlighted in the dashboard, enabling quick identification and response. The correlation engine further improved detection accuracy by linking related events, which helped in identifying patterns such as brute-force attacks over time rather than isolated incidents.

The dashboard visualization provided meaningful insights through charts and metrics, including alert distribution and attack statistics. This improved the interpretability of results compared to raw log analysis. Additionally, the alert management system allowed users to acknowledge and track incidents efficiently.

The notification system was also tested, where critical alerts triggered real-time dashboard notifications and email alerts, ensuring timely awareness. The audit log successfully recorded all user activities, enhancing accountability and traceability.

Overall, the experimental results indicate that the SIEM Secure system performs effectively in real- time log monitoring, threat detection, and alert management. The system demonstrates reliability, usability, and improved efficiency compared to traditional manual log analysis approaches.

VIII. FUTURE WORKS

The SIEM Secure system can be further enhanced by integrating advanced technologies to improve its performance and capabilities. One important improvement is the incorporation of machine learning and artificial intelligence techniques to enhance threat detection and identify unknown or zero-day attacks. Expanding log collection to include cloud services, network devices, and IoT systems will make the system more scalable and suitable for real-world environments.

Additionally, implementing real-time data processing frameworks can improve system performance when handling large volumes of logs. The system can also be upgraded with automated incident response features, such as blocking suspicious IP addresses or locking compromised accounts. Enhancing the user interface with more interactive and customizable dashboards will improve usability. Finally, adding advanced security features like multi-factor authentication and integration with external threat intelligence sources will strengthen the overall security and reliability of the system.

IX. CONCLUSION

The SIEM Secure system provides an effective solution for real-time log monitoring and threat detection. It integrates log collection, parsing, detection, and correlation to identify suspicious activities and generate alerts. The dashboard enhances visualization, while authentication and audit logging ensure system security. The notification system enables timely response to critical threats. Overall, SIEMSecure offers a simple, scalable, and efficient approach to cybersecurity monitoring and improves the effectiveness of threat detection and response.

REFERENCES

[1] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, ―Security information and event management (SIEM): Analysis, trends and usage in critical infrastructures,‖ *Sensors*, vol. 21, no. 14, pp. 1–24, 2021.

[2] N. Upadhyay, ―Machine learning in SIEM: A survey on intelligent event correlation and anomaly detection,‖ 2025.

[3] E. Hernandez and M. Song, ―A comprehensive study of security information and event management (SIEM) systems: Architectures, benefits and challenges,‖ 2019.

[4] M. Vielberth, ―Security information and event management (SIEM),‖ in *Encyclopedia of Cryptography, Security and Privacy*, Springer, 2021.

[5] S. Shaik, ―Security information and event management trends and data overload challenges,‖ *International Journal of Latest Research in Engineering and Technology*, 2025.

[6] A. P. Kotwal, ―Big data analytics in security information and event management (SIEM),‖ *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, 2024.

[7] M. H. Saju et al., ―SynRAG: Retrieval- augmented generation for SIEM query processing,‖ 2025.

[8] A. Shukla et al., ―RuleGenie: Optimizing rule- based detection in SIEM systems,‖ 2025.

[9] A. Garofalo, F. Tundis, and G. Bianchi,

―Improving SIEM capabilities for protecting critical infrastructures,‖ 2014.

[10] T. Davies et al., ―Collaborative intrusion detection systems with SIEM integration,‖ 2025.

[11] J. Zhu, Q. Fu, J.-G. Lou, H. Zhang, and J. Li,

―Tools and benchmarks for automated log parsing,‖ in *Proc. IEEE/ACM Int. Conf. Software Engineering (ICSE)*, 2019.

[12] M. Du and F. Li, ―DeepLog: Anomaly detection and diagnosis from system logs through deep learning,‖ in *Proc. ACM Conf. Computer and Communications Security (CCS)*, 2017.

[13] K. Agarwal and K. Sharma, ―Log-based anomaly detection using machine learning,‖ 2021.

[14] A. L. Buczak and E. Guven, ―A survey of data mining and machine learning methods for intrusion detection,‖ *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[15] F. Valeur, G. Vigna, C. Kruegel, and R. A. Kemmerer, ―A comprehensive approach to intrusion detection alert correlation,‖ *IEEE Trans. Dependable Secure Comput.*, vol. 1, no. 3, pp. 146–169, 2004