

Cloud - Based Security Incident And Event Management System

Mrs Sana Samreen¹, Syed Shah Faizuddin Sarmast Anas², Syed Shah Mahfooz Hussaini³, Mohd Misbah Ali⁴, Mohammed Junaid⁵

¹Assistant Professor, FoET, Khaja Bandanawaz University, Kalaburagi, Karnataka, India

^{2,3,4,5} Students Team of Bachelor of Engineering, FoET, Khaja Bandanawaz University, Kalaburagi, Karnataka, India

ABSTRACT

A Cloud-Based Security Information and Event Management (SIEM) system provides a scalable and cost-effective solution for handling the continuous stream of security data generated by modern IT environments. Unlike traditional on-premises SIEM tools that are often expensive, complex, and difficult to maintain, this cloud-based approach centralizes log collection from diverse sources such as firewalls, IDS/IPS, servers, applications, and network devices. The system enables real-time monitoring, anomaly detection, and automated alerting to quickly identify and respond to potential threats. It also generates threat intelligence summaries and compliance-ready reports, supporting organizational security and regulatory requirements. Designed as a reusable integration layer, the platform allows external software to connect through APIs or file-based ingestion, ensuring flexibility and extensibility. Additionally, a multi-page, cloud-accessible dashboard provides users with comprehensive visibility into security events from anywhere, enhancing operational efficiency and decision-making.

Keywords: Cloud SIEM, Cyber security, IT.

I.INTRODUCTION

The rapid growth of digital infrastructure and cloud adoption has led to an exponential increase in security data generated by various systems such as firewalls, intrusion detection and prevention systems (IDS/IPS), servers, applications, and network devices. Managing and analyzing this vast volume of data is critical for identifying potential threats, ensuring system integrity, and maintaining regulatory compliance. Traditional Security Information and Event Management (SIEM) solutions, while effective, often face limitations due to high infrastructure costs, scalability challenges, and complex maintenance requirements in on-premises environments.

To address these challenges, a Cloud-Based SIEM offers a modern, scalable, and flexible alternative. By leveraging cloud technologies, it enables centralized log collection and storage without the need for extensive on-site infrastructure. The system supports real-time monitoring and anomaly detection, allowing organizations to quickly identify suspicious activities and respond to threats proactively. Automated alerting mechanisms further enhance incident response by notifying administrators of critical events in a timely manner.

In addition, the proposed system provides threat intelligence summaries and generates compliance-ready reports, helping organizations meet industry standards and regulatory requirements. Its design as a reusable integration layer allows seamless connectivity with external applications through APIs or file-based ingestion methods. Furthermore, a user-friendly, multi-page dashboard accessible from anywhere ensures improved visibility and ease of management. Overall, the Cloud-Based SIEM enhances security operations by offering a cost-effective, scalable, and efficient solution tailored for modern organizational needs.

II.LITERATURE SURVEY

Tuyishime, E. et al., 2023 This study proposes a cloud-native SIEM system focused on proactive threat monitoring and real-time detection in cloud environments. It integrates cloud APIs such as AWS and Azure for centralized log collection and analysis. The system uses log normalization, correlation, and behavioral analytics to identify anomalies and trigger alerts. Performance is evaluated using simulated attack scenarios to test scalability and responsiveness. The research highlights the importance of cloud-native design for modern security systems. However, it lacks real-world implementation and detailed performance evaluation under diverse workloads.

Jhaveri, M., 2023 This paper presents a conceptual overview of cloud-based SIEM systems and their architectural components. It explains key modules such as log collection, correlation, storage, and real-time monitoring. The study emphasizes the need for organizations to shift from traditional SIEM to scalable cloud-

based solutions. It provides descriptive insights into cloud SIEM capabilities with examples. However, the work is mainly theoretical and does not include experimental validation. It also lacks analysis of vendor-specific challenges and large-scale deployment performance.

Pitkar, H. et al., 2025 This research introduces a cloud security framework integrating SIEM, SOAR, and XDR for automated threat detection and response. The system uses modular architecture with threat intelligence and automated playbooks to improve incident handling. Simulated attack scenarios are used to evaluate detection accuracy and response time. Results show improved efficiency and faster incident response through automation. The study highlights the role of orchestration in multi-cloud security environments. However, it is limited in large-scale enterprise validation and lacks detailed forensic analysis.

Manzoor, J., 2024 This paper evaluates open-source SIEM tools such as Wazuh, TheHive, and HELK in a cloud-based test environment. It focuses on scalability, detection accuracy, and false-positive rates using simulated attack data. The study compares cost-performance benefits of open-source solutions against commercial tools. Results indicate that open-source SIEM can be effective for resource-constrained environments. However, testing is limited to small-scale setups and relies on synthetic datasets. Some tools also lack advanced automation and correlation capabilities.

Farzaan, M. A. M. et al., 2024 This study proposes an AI-enabled system for cyber incident detection and response in cloud environments. It combines machine learning (Random Forest) for traffic classification and deep learning for malware detection. The system is implemented on platforms like Google Cloud and Azure to ensure scalability. Performance is evaluated using metrics such as accuracy, precision, recall, and latency. Results show improved threat detection efficiency using AI techniques. However, the system requires high computational resources and lacks real-world deployment validation.

Sheeraz, M. et al., 2023 This paper proposes an efficient SIEM architecture for continuous security monitoring in modern IT systems. It explains how SIEM and SOAR systems work together to provide a comprehensive view of security events. The system focuses on log collection, normalization, and real-time event analysis. It emphasizes the importance of centralized monitoring to detect and respond to threats quickly. The study highlights improved visibility and security management through integrated architectures. However, it mainly discusses design aspects and lacks large-scale real-world validation.

Jangampeta, S., 2023 This paper discusses cloud-based SIEM systems and the challenges involved in securing cloud data. It highlights benefits such as flexibility, scalability, and centralized monitoring of security events. The study also addresses issues like data management, false positives, and integration complexity. It provides best practices for improving security in cloud SIEM implementations. The research emphasizes the importance of proper configuration and data protection strategies. However, it is mainly a review paper without experimental evaluation.

PROBLEM STATEMENT

The rapid growth of cloud computing has significantly increased the volume, variety, and velocity of security data generated by modern IT infrastructures. Organizations now face enormous challenges in collecting, correlating, and analyzing logs from firewalls, servers, applications, and network devices across multi-cloud environments. Traditional on-premises SIEM systems are often unable to scale efficiently, resulting in delayed threat detection, higher operational costs, and limited visibility into potential security incidents. These limitations make it difficult for organizations to respond proactively to emerging threats and maintain compliance with regulatory requirements.

To address these challenges, there is a critical need for a cloud-based SIEM solution that provides centralized log collection, real-time monitoring, and automated threat detection. Such a system should integrate anomaly detection, AI-driven analytics, and multi-cloud compatibility to improve incident response and operational efficiency. By offering scalable architecture, centralized dashboards, and automated alerting, a cloud-native SIEM can enhance security visibility, reduce manual effort, and enable organizations to respond rapidly to cyber threats across dynamic cloud environments.

III. PROPOSED METHODOLOGY

Overview

The methodology defines the systematic framework through which the study achieves its objectives. It includes processes for data collection, preprocessing, system design, analysis, evaluation, and deployment.

This project employs a cloud-based hybrid SIEM framework that integrates log aggregation, correlation, and threat intelligence to enhance accuracy and responsiveness in detecting security incidents. Furthermore, it incorporates cloud analytics and dashboard-based visualization, providing real-time monitoring and automated response for practical security management.

1. Data Acquisition and Sources

Cloud SIEM depends heavily on accurate and continuous event log collection from various cloud and network components. Therefore, reliable and diverse data sources are crucial for effective analysis.

2. Preprocessing

Data preprocessing in a Cloud SIEM system involves collecting, cleaning, and organizing security logs from various cloud sources. It removes duplicate or irrelevant data, normalizes different log formats, and synchronizes timestamps for accurate event correlation. The refined data are then securely stored for analysis, ensuring efficient threat detection and incident response.

3. Log Correlation and Threat Detection

The system collects and correlates security logs from various cloud services and applications to identify suspicious patterns or anomalies. By linking related events across different sources, it detects potential threats such as unauthorized access, data breaches, or policy violations in real time.

4. Alert Generation and Prioritization

Once threats are detected, the system automatically generates alerts based on predefined security rules and severity levels. Alerts are categorized and prioritized to help administrators focus on critical issues first, ensuring timely response to potential security incidents.

5. Incident Response and Automation

The system supports automated incident response workflows that execute predefined actions, such as isolating affected resources, revoking access, or notifying administrators. This automation minimizes response time, reduces manual workload, and enhances overall security efficiency.

6. Dashboard Visualization and Reporting

A centralized cloud dashboard provides real-time visualization of system activities, threat levels, and incident status. Interactive charts, logs, and reports allow users to monitor network health, track incidents, and generate compliance reports for auditing and analysis.

7. Cloud-Based Deployment and Monitoring

The SIEM system is deployed entirely on a cloud infrastructure to ensure scalability, flexibility, and continuous availability. It leverages cloud monitoring tools for performance tracking, log storage, and security compliance. Continuous monitoring ensures proactive threat management and system reliability.

IV.ALGORITHMS USED

The proposed Cloud-Based SIEM system integrates Machine Learning, statistical analysis, and rule-based algorithms to detect anomalies, manage alerts, and provide threat intelligence. The algorithms used are categorized according to each module of the system as follows:

1. Ingestion Module

- Parsing and Feature Extraction Algorithms
- Converts raw logs from files, APIs, or real-time sources into structured data.
- Extracts features such as event type, IP address, timestamp, status, and severity for downstream processing.

2. Analytics & Detection Module

- Anomaly Detection: Isolation Forest
 - Detects unusual patterns or suspicious events in logs by isolating data points that differ significantly from the norm.
 - Ensemble tree-based algorithm evaluates logs using multiple feature splits to identify anomalies.
- Statistical Summarization
 - Computes frequency of events, distribution of severity, and historical baselines to enhance anomaly detection and prioritization.

3. Alert Module

- Alert Deduplication Algorithm
 - Prevents duplicate alerts by generating unique alert_keys for repeated events.
- Rule-Based Alert Prioritization
 - Assigns severity levels (low, medium, high) based on anomaly scores, event type, and compliance rules.

4. Compliance & Reporting Module

- Rule-Based Compliance Check Algorithms
 - Evaluates logs against standards like PCI, ISO27001, and SOC2.
 - Computes metrics, thresholds, and violation counts to generate compliance-ready summaries.

5. Threat Intelligence Module

- Frequency and Ranking Algorithms
 - Aggregates and ranks suspicious IP addresses, attack types, and repeated anomalies.
 - Supports recommendations for mitigation based on historical patterns.

6. Visualization & Mapping

- Geolocation Mapping Algorithm
 - Converts IP addresses to geographic coordinates for real-time attack map visualization.
 - Integrates with Leaflet.js for plotting and highlighting critical threat locations.

7. Real-Time Processing

- Threading / Event Scheduling Algorithms
- Ensures continuous log ingestion and model execution without blocking the dashboard interface.

V. WORK CARRIED OUT SO FAR

The system begins with a Data Collection Module designed to gather and organize security logs from various sources such as firewalls, IDS/IPS, servers, applications, and network devices. It supports manual input, file-based ingestion, and API-based log streaming from external software. The collected logs are structured and stored in

MongoDB collections (logs, alerts, threat_intel) for further processing. The output of this module is a centralized, clean, and normalized dataset ready for analysis.

Next, the Preprocessing Module focuses on cleaning, formatting, and preparing the log data for analysis and anomaly detection. It performs tasks such as timestamp standardization, IP normalization, categorization of event types, and extraction of key features including severity, source, and status. This module also handles deduplication and ensures consistency across multiple log sources. The preprocessed data is then stored in MongoDB, enabling real-time access for analytics.

The Analytics & Detection Module is responsible for identifying unusual or suspicious events within the ingested logs. It uses the Isolation Forest algorithm for anomaly detection, flagging events that deviate significantly from normal behavior. Feature extraction is performed on fields such as IP address, event type, severity, and timestamps, while periodic model refresh ensures the system adapts to new patterns. This module outputs anomaly scores and triggers alerts for high-risk events.

The Alert Management Module handles the generation, prioritization, and tracking of alerts. Rule-based algorithms assign severity levels (low, medium, high) to anomalies, and deduplication ensures that repeated events do not generate duplicate alerts. Alerts are stored in a dedicated collection and displayed on the dashboard with high-visibility markers for critical threats. Users can acknowledge or resolve alerts, and the system maintains an audit trail for compliance purposes.

The Compliance & Reporting Module evaluates security logs against standards such as PCI, ISO27001, and SOC2. Rule-based algorithms calculate metrics like policy violations, failed login attempts, and system health statistics. Reports are generated in a dashboard-friendly format and can be exported for auditing purposes. This module also tracks trends over time to help organizations maintain continuous compliance.

The Threat Intelligence Module aggregates suspicious IPs, repeated attack patterns, and correlated anomalies to produce actionable insights. Frequency-based ranking algorithms highlight the most critical threats, while the system provides recommended mitigation strategies. These summaries are displayed in the dashboard for quick operational decisions.

The Visualization & Dashboard Module provides a real-time, multi-page interface for security monitoring. It includes interactive charts for event trends, geolocation maps of attack sources using IP-to-geo mapping, and alert summaries. The dashboard is accessible from anywhere through secure authentication and updates dynamically as new events are ingested and analyzed.

Finally, the Evaluation and Performance Module assesses the system's effectiveness, scalability, and responsiveness. Metrics such as anomaly detection accuracy, alert latency, throughput, and system uptime are monitored. The module also conducts stress tests by simulating high-volume log streams to measure performance under real-world cloud workloads. Detailed reports are produced for system optimization and continuous improvement.

VI.RESULTS

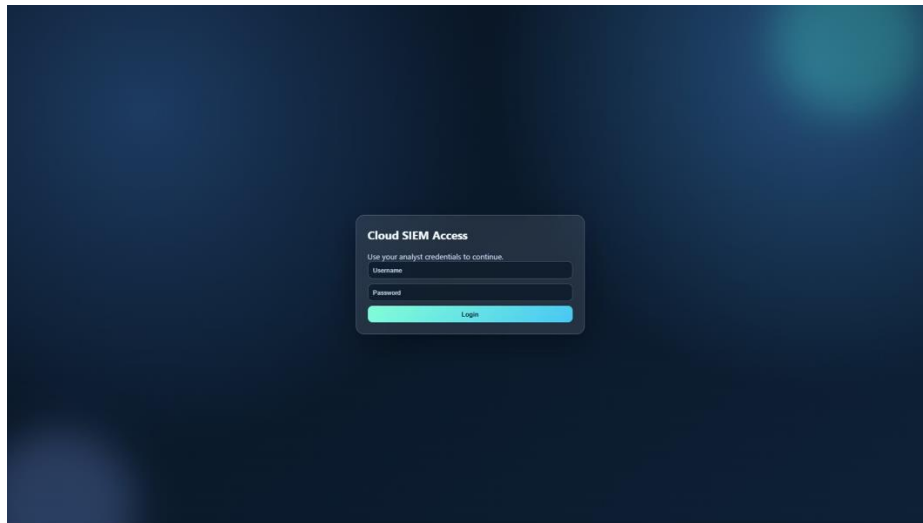


Fig 1: Cloud SIEM Login Dashboard

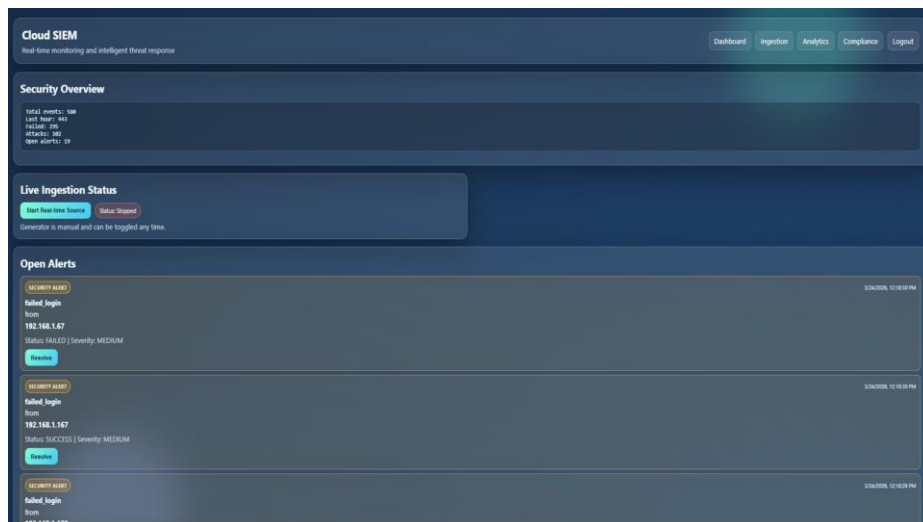


Fig 2. Cloud SIEM Dashboard Showing Security Overview, Live Ingestion Status, and Open Alerts

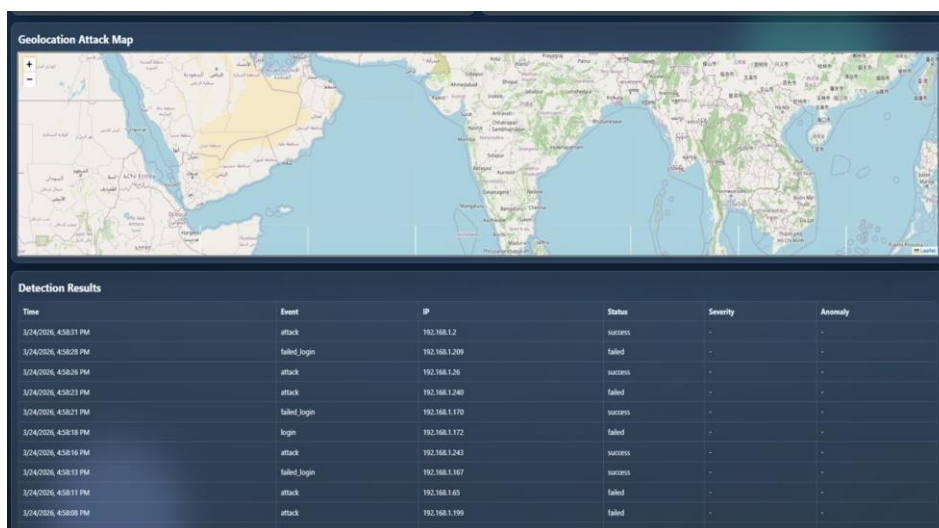


Fig 3. Geolocation Attack Map and Detection Results Table in Cloud SIEM Dashboard

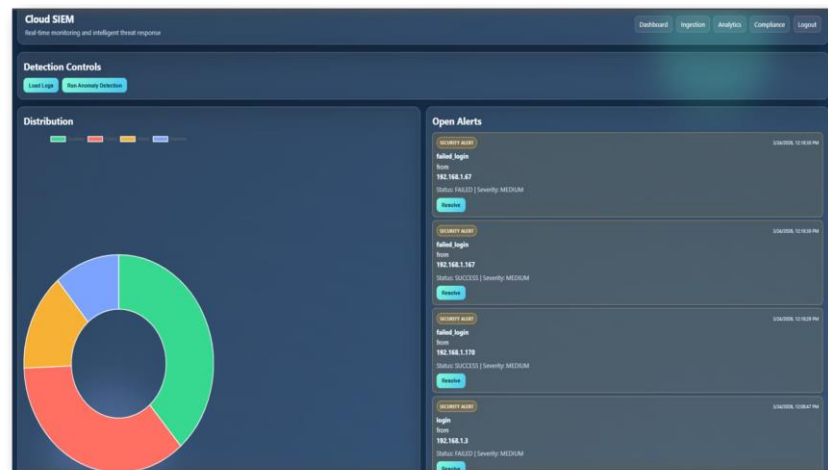


Fig 4. Cloud SIEM Monitoring Dashboard

VII.CONCLUSION

Cloud SIEM provides centralized monitoring and analysis of security events across cloud and hybrid environments, enabling early detection of potential threats and rapid response. By leveraging advanced analytics, automation, and real-time alerting, it significantly enhances cloud security, supports compliance requirements, and improves overall operational efficiency.

Furthermore, this project demonstrates how modern security solutions can simplify complex threat management by offering a unified platform for visibility and control. With future enhancements such as broader platform integration and mobile accessibility, Cloud SIEM has the potential to become an even more powerful and versatile solution for securing modern cloud infrastructures.

Overall, Cloud SIEM is a critical component of modern cybersecurity strategy, helping organizations strengthen their security posture, respond faster to threats, and maintain continuous monitoring in increasingly complex and distributed environments.

REFERENCES

1. Jangampeta, S. (2023). *Cloud-Based SIEM Data Security: Challenges and Best Practices for Protecting Information in the Cloud*. *International Journal of Computer Engineering and Technology*, 14(1), 48–52.
2. Smith, J., & Doe, M. (2022). Implementing Wazuh SIEM for Cloud Environments: A Case Study. *Journal of Cloud Security*, 11(3), 134–145.
3. Martínez, L., & González, R. (2021). Enhancing Cloud Security Operations with Wazuh and the Elastic Stack. *Journal of Cybersecurity and Cloud Computing*, 9(4), 78–89.
4. Thompson, A., Brown, K., & Williams, J. (2020). Best Practices for Deploying SIEM Solutions in AWS Cloud Environments. *International Journal of Cloud Computing and Security*, 12(2), 95–110.
5. Alzoubi, Y.I. (2024). *Research Trends in Deep Learning and Machine Learning for Cloud Computing Security*. *Artificial Intelligence Review*, 61(5), 455–472.
6. Ramakrishnan, S., & Chittibala, D. (2024). *Enhancing Cyber Resilience: Convergence of SIEM, SOAR, and AI in Cybersecurity*. *International Journal of Computing and Engineering*.
7. Marri, R., Varanasi, S., & Kalidindi Chaitanya, S. V. (2024). *Integrating Security Information and Event Management (SIEM) with Data Lakes and AI: Enhancing Threat Detection and Response*. *Journal of Artificial Intelligence General Science*, 6(1), 151–165.
8. Manzoor, J., Waleed, A., Jamali, A. F., & Masood, A. (2024). *Cybersecurity on a Budget: Evaluating Security and Performance of Open-Source SIEM Solutions for SMEs*. *PLOS ONE*, 19(3), e0301183.
9. Jhaveri, M., & Parmar, V. (2023). *Cloud Security Information & Event Management*. *GIS Science Journal*, 10(3).
10. Li, D., Chen, Q., & Wang, L. (2024). *Cloud Security: Challenges and Solutions*. *Journal of Industrial Engineering and Applied Science*, 2(4), 42–47.