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

"Cloud-Based Web Traffic Analysis and Live Security Monitoring Dashboard for Institutional Web Portals: A Case Study of AIIMS Jammu"

Faizan Muntazir[1], Mr. Deepak Kumar[2]
M. Tech Scholar, Assistant Professor
Sri Sai College of Engineering & Technology Badhani(Ptk)

ABSTRACT

Healthcare institutions increasingly rely on cloud-hosted web portals to deliver online services and manage operational systems such as AIIMS Jammu Website, Hospital Management Information Systems (HMIS) and Human Resource Management Systems (HRMS). These applications generate continuous web traffic and remain exposed to various security threats, making real-time monitoring essential. This work describes the development of a cloud-based web traffic analysis and live security monitoring dashboard implemented for institutional web portals at AIIMS Jammu. The system processes access and security logs from cloud-hosted applications and presents critical security insights, including traffic trends, suspicious request activity, attack hit statistics, abnormal access behavior, and source-based traffic distribution, through a centralized dashboard interface. A practical and rule-driven approach is employed to recognize potential attack patterns based on traffic behavior and predefined thresholds, without relying on experimental or predictive models. The dashboard enhances visibility into cloud traffic activity, assists administrators in identifying security incidents promptly, and contributes to improved monitoring and protection of healthcare web applications in a real-world institutional environment.

Keywords: Cloud Computing, Web Traffic Analysis, Security Monitoring Dashboard, Cybersecurity, Attack Pattern Analysis, Healthcare Web Portals, HMIS, HRMS

Introduction

Healthcare as an industry is undergoing rapid digital transformation, with cloud computing playing a significant role in improving healthcare service delivery. Cloud-based platforms enable healthcare institutions to host institutional websites, Hospital Management Information Systems (HMIS), and Human Resource Management Systems (HRMS), allowing centralized data access, remote services, and efficient coordination among stakeholders. The ability of cloud infrastructure to support scalability, availability, and real-time access has made it a preferred choice for managing healthcare applications and operational data. However, hosting critical web portals on the cloud also exposes healthcare organizations to continuous web traffic, including unauthorized access attempts, malicious requests, and other cyber threats, making security monitoring a critical requirement.

Healthcare web portals handle sensitive operational and administrative information, and any compromise can affect service continuity and institutional credibility. Cloud environments are dynamic in nature, where traffic patterns change frequently and traditional static security mechanisms are often insufficient to provide timely visibility into emerging threats. As a result, there is a growing need for continuous monitoring mechanisms that can observe cloud-hosted web traffic and identify abnormal or suspicious behavior in real time. Effective security monitoring focuses on analyzing access logs, request patterns, traffic frequency, and error responses to detect potential attack attempts and misuse of web applications.

This paper proposes a practical methodology for cloud-based web traffic analysis and live security monitoring tailored for healthcare institutions. The focus is on designing and implementing an interactive dashboard capable of aggregating and visualizing web traffic and security events, allowing IT administrators to detect abnormal behavior, track attack patterns, and respond to threats in real time. By leveraging cloud capabilities alongside automated monitoring and visualization techniques, this approach strengthens the security posture of healthcare web portals while maintaining system usability and operational efficiency. Furthermore, the implementation highlights the potential of combining cloud computing, data analytics, and real-time visualization to address evolving cybersecurity challenges in the healthcare domain. The presented solution not only ensures timely threat detection but also supports continuous improvement in security processes, making it highly relevant for healthcare organizations seeking to safeguard sensitive information in an increasingly complex digital environment.

Continuous monitoring solutions based on centralized log analysis and visualization enable administrators to gain real-time insight into cloud traffic behavior. By aggregating web server and security logs and presenting them through an interactive dashboard, security teams can observe attack hits, traffic anomalies, repeated access attempts, and source-based request patterns as they occur. Such dashboards do not interfere with application functionality but instead provide situational awareness and support timely administrative response to potential security incidents. In this paper, the

authors present a practical approach for cloud-based web traffic analysis and live security monitoring through a centralized dashboard, highlighting its relevance for healthcare institutions in strengthening the security oversight of institutional web portals in an evolving cloud environment.

The dynamic nature of cloud environments adds complexity to maintaining security. Web traffic in these systems can fluctuate rapidly due to user activity, automated requests, or malicious attempts to exploit vulnerabilities. Traditional static security mechanisms, such as firewall rules or manual log reviews, are often insufficient to detect emerging threats or abnormal traffic patterns in real time. Healthcare institutions are therefore increasingly seeking proactive solutions that provide continuous monitoring, anomaly detection, and threat analysis for cloud-hosted applications. Continuous monitoring systems analyze server logs, application requests, access patterns, and error messages to identify suspicious behaviors, including repeated access attempts, unusual geographic origins of traffic, or attempts to exploit system vulnerabilities. By detecting such anomalies promptly, security teams can intervene before a minor breach escalates into a full-scale security incident, thereby protecting sensitive patient data and maintaining institutional credibility.

S. No	Author(s) & Year	Title / Study	Key Contributions / Findings	Relevance to This Work
1.	Seyed Salar Sefati1,2,3*, Bahman Arasteh3,4,5, Octavian Fratu1,2,6 and Simona Halunga1,2,6 (2025)	SSLA: A Semi-Supervised Framework for Real-Time Injection Detection and Anomaly Monitoring in Cloud-Based Web Applications	Semi-supervised learning, Graph Convolutional Networks (GCN), similarity graphs	Injection attack detection and anomaly monitoring in cloud web apps
2	Rawan Rouf Abdullah (2024)	Real-Time Intrusion Detection System Based on Web Log File Analysis	Rule-based log analysis, pattern matching, thresholds	Intrusion detection using web server logs
3.	Lenka Benova (2023)	Using Logstash for Real-Time Log Analysis in Cloud-Based Applications	Logstash, ELK stack (Elasticsearch, Kibana	Log ingestion and real-time processing in cloud systems
4.	Anish Kumar Sargun Kumar (2022)	Comprehensive Analysis and Evaluation of Anomalous User Activity in Web Server Logs	Offline analysis, statistical & anomaly detection methods	Statistical evaluation of anomalous user behavior
5.	Li et al., *Journal of Medical Systems* (2023)	Systems (2023) Cloud-based healthcare system architecture and security challenges	Identifies security risks and need for continuous monitoring in healthcare cloud systems	Provides architectural and security background that justifies the need for a real-time security monitoring dashboard in healthcare portals
6.	Anish Kumar Alshammari et al., IEEE Access (2023)	Security challenges and solutions in cloud healthcare applications	Discusses threats, vulnerabilities, and security requirements in healthcare clouds	Supports the motivation for implementing continuous web traffic monitoring and security analysis
7.	Ahmed et al., *IEEE TNSM* (2023)	Real-time web traffic monitoring and security analysis	Demonstrates importance of live traffic analysis for detecting abnormal behavior	Closely aligns with real-time traffic monitoring objectives of the proposed dashboard
8.	Zhou et al., Computers & Security (2024)	Threshold-based anomaly detection in cloud web traffic	Proposes lightweight rule/threshold-based detection techniques	Validates the use of rule-based and threshold-based anomaly detection implemented in the proposed system
9.	Patel & Shah, *IJIS* (2024)	Rule-based detection of abnormal web traffic	Shows effectiveness of non-ML detection methods	Supports the PHP-MySQL based lightweight, rule-based detection approach used in the dashboard

Literature Review

Problem Statement

The rapid adoption of cloud computing by healthcare institutions has transformed the way institutional web portals

and operational systems are deployed and accessed. Cloud infrastructure is now widely used to host official institutional websites, Hospital Management Information Systems (HMIS), and Human Resource Management Systems (HRMS) due to its scalability, availability, and ease of remote access. While these advantages improve operational efficiency and service delivery, they also increase exposure to continuous and diverse web traffic originating from both legitimate users and potential malicious sources. As a result, cloud-hosted healthcare web applications face persistent security risks that require constant monitoring and timely response.

Healthcare web portals operate in a highly dynamic environment where traffic patterns change frequently, making it difficult to distinguish between normal usage behaviour and potentially harmful activity. Unauthorized access attempts, automated scanning, repeated request flooding, and abnormal access to restricted resources can occur at any time and may go unnoticed if not monitored in real time. Although cloud-hosted systems generate extensive web server and security logs, these logs are often stored in isolated formats and reviewed only after incidents occur. The lack of centralized analysis and live visibility into traffic behavior limits the ability of administrators to detect ongoing attack activity and assess the security posture of institutional web portals promptly.

Traditional security mechanisms commonly used in healthcare environments focus on static rule enforcement or periodic audits, which are insufficient in cloud settings where threats evolve continuously, and traffic volumes are high. Without a real-time monitoring mechanism, administrators must rely on delayed log analysis or manual inspection, leading to slow detection of abnormal behavior and delayed response to security incidents. This gap in visibility can result in service disruption, system misuse, or increased vulnerability to repeated attack attempts, particularly for critical systems such as HMIS and HRMS that support daily institutional operations.

Furthermore, healthcare institutions often manage multiple cloud-hosted applications simultaneously, making decentralized monitoring impractical and inefficient. The absence of a unified view of web traffic and security events across institutional portals creates challenges in understanding attack trends, identifying repeated access patterns, and correlating security events across systems. Administrators require a centralized and intuitive mechanism that consolidates traffic data and presents actionable insights in an easily interpretable format.

Therefore, the core problem addressed in this study is the lack of a practical, centralized, and real-time security monitoring solution for cloud-hosted healthcare web portals. There is a clear need for a system that can continuously analyze cloud-based web traffic, identify abnormal or suspicious access behavior, and visually present attack patterns and security statistics through a live dashboard. Addressing this problem is essential for improving situational awareness, enabling timely administrative response, and strengthening the overall security oversight of institutional web applications in a healthcare environment.

System Architecture and Dashboard Explanation

The proposed system architecture as per (Fig 1.1) for the cloud-based web traffic analysis and live security monitoring dashboard is designed to provide a comprehensive view of the web activities and potential security threats across institutional portals, including AIIMS Jammu, HMIS, and HRMS. At the foundation, the Web Portals act as the primary data sources, generating logs of user interactions, server requests, API calls, and system events. These logs are continuously collected and transmitted to the Log Collection Layer, which acts as a secure intermediary to aggregate, normalize, and structure data from multiple portals. By centralizing log collection (as per Fig 2.2), the system ensures that raw traffic data is captured efficiently and consistently, forming the basis for detailed analysis and monitoring.

Once collected, the data is processed through the Data Processing & Analytics Engine, which performs real-time analysis and anomaly detection. This layer is designed to filter out irrelevant information, detect unusual access patterns, spikes in traffic, repeated failed login attempts, and other security anomalies. Advanced AI algorithms can be incorporated at this stage to learn normal portal behavior, detect deviations, and flag potential security threats automatically. This intelligent analysis reduces the reliance on manual inspection and allows healthcare administrators to proactively monitor security while maintaining compliance with HIPAA regulations. The processed data is stored in a MySQL database, ensuring that historical trends, attack patterns, and portal-specific metrics are readily accessible for reporting and future analysis.

The Dashboard Backend, developed using PHP and MySQL, serves as the central hub for managing and delivering processed data to the user interface. It handles data queries, authentication, and role-based access controls, ensuring that only authorized personnel can access sensitive information. The Dashboard Frontend built using HTML, CSS, JavaScript, and Bootstrap, provides a user-friendly and interactive visualization of web traffic statistics, security alerts, and portal-specific performance metrics. Features such as line graphs, bar charts, heatmaps, and geo-location maps allow users to quickly understand portal activity, detect unusual patterns, and evaluate the severity of potential threats. Additionally, real-time counters, trend indicators, and alert banners make the dashboard suitable for operational monitoring and immediate response.

To enhance responsiveness and security, the architecture includes a Notifications Layer for automated alerts via email or integrated messaging systems. This ensures that anomalies or suspicious activities are communicated instantly, enabling prompt mitigation. The system is designed to be modular and scalable, with the potential for further integration of AI-based threat detection, predictive analytics, and DevSecOps principles for automated compliance and infrastructure management. By combining real-time monitoring, automated threat detection, and robust cloud-based architecture, the system not only improves the operational oversight of healthcare portals but also strengthens security, maintains HIPAA compliance, and provides administrators with actionable intelligence to safeguard sensitive patient and institutional data.

System Architecture (Fig 1.1)

Advance Detection System

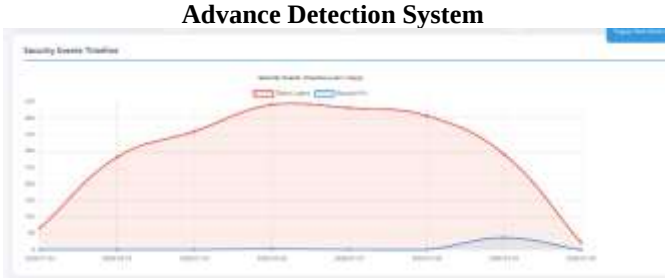

Figure (1.2)

Figure (1.3)

Methodology

The methodology employed in this study adopts a practical, system-implementation-driven approach to monitor and analyze cloud-hosted healthcare web portals through continuous web traffic observation and live security visualization. The primary objective of the methodology is to provide real-time visibility into traffic behavior and potential security events affecting institutional web portals, rather than to develop predictive or experimental security models. The methodology is designed to be scalable, non-intrusive, and suitable for operational use in a healthcare institutional environment.

1. Study Environment and System Architecture

The study is conducted on cloud-hosted institutional web portals of AIIMS Jammu, including the official institutional website, Hospital Management Information System (HMIS), and Human Resource Management System (HRMS). These applications are deployed on cloud infrastructure and are single IP address within a short time frame, abnormal spikes icators of suspicious activity. Threshold values are defined based on observed normal traffic behaviour and institutional access patterns. When these thresholds are exceeded, the activity is marked for attention on the monitoring dashboard.

5. Classification of Traffic Events

Based on the observed analysis results, traffic events are categorized into normal and suspicious activity. Normal traffic

6. Dashboard Design and Visualization Strategy

The security monitoring dashboard is designed to provide a clear and intuitive representation of traffic and security data. Visualization elements include time-series charts, summary counters, bar graphs, and tabular views. These elements

7. Real-Time Update and Monitoring Mechanism

To support continuous monitoring, the system processes incoming log data in near real time. Dashboard metrics and visual components are refreshed dynamically as new traffic data is analysed. Visual indicators highlight abnormal

accessible over the internet to authorized users, staff, and the general public. Due to their online exposure, the portals receive continuous web traffic from multiple sources, making them vulnerable to unauthorized access attempts and malicious activity.

The overall system architecture consists of three major components: log generation at the web server level, centralized log processing, and a live security monitoring dashboard. Web server access logs generated by cloud-hosted applications serve as the foundational data source. These logs are securely transferred to a centralized processing module, where traffic analysis is performed before visualization on the dashboard interface.

2. Data Collection Mechanism

Data collection is based on continuous acquisition of web server access logs generated by the cloud-hosted portals. These logs capture detailed request-level information for every incoming HTTP request. The parameters collected include timestamp, source IP address, requested resource or URL, HTTP method, response status code, and request size. Log collection is implemented in a passive manner, ensuring that there is no performance impact or disruption to normal portal operations. The system supports log collection from multiple portals simultaneously, allowing unified monitoring of institutional websites, HMIS, and HRMS. Log files are periodically fetched or streamed from the cloud environment and stored in a centralized repository for further processing and analysis.

3. Log Pre-Processing and Normalization

Raw log data often contains redundant, incomplete, or non-security-relevant entries. Therefore, a pre-processing phase is applied to prepare the data for analysis. During this stage, unnecessary fields are removed, malformed entries are filtered, and relevant security-related attributes are extracted. The extracted attributes are normalized into a consistent structure to ensure uniform analysis across different portals. Time-based ordering of log entries is maintained to support chronological analysis of traffic behavior. This normalization process enables efficient aggregation, comparison, and visualization of traffic data while preserving essential security information.

4. Web Traffic Behaviour Analysis

Traffic analysis is performed using a rule-based and threshold-driven approach to observe patterns that may indicate suspicious or abnormal behavior. The analysis focuses on identifying deviations from normal traffic characteristics rather than predicting future attacks. Key indicators used for analysis include request frequency per source, access repetition, response status trends, and request distribution over time.

patterns or sudden changes in traffic behaviour, allowing administrators to observe ongoing security events as they occur. The real-time update mechanism ensures timely visibility of potential security incidents while maintaining low system overhead and minimal resource consumption.

8. Evaluation and Validation Approach

The effectiveness of the proposed system is evaluated through observational validation under real operational conditions. The evaluation focuses on the system's ability to provide accurate and timely visualization of traffic behaviour, clarity of dashboard presentation, and usefulness in supporting administrative decision-making. Rather than using experimental benchmarking or performance metrics, the evaluation emphasizes practical usability, responsiveness, and relevance in a healthcare institutional context. Feedback from administrative observation is used to assess the system's operational effectiveness.

9. Methodological Scope and Limitations

The methodology is limited to monitoring, analysis, and

visualization of web traffic and security events for cloud-hosted healthcare portals. It does not include automated intrusion prevention, predictive analytics, machine learning-based detection, or regulatory compliance enforcement. The focus remains on enhancing real-time visibility and situational awareness through a centralized dashboard.

Results and Discussion

This section presents the outcomes obtained from implementing the cloud-based web traffic analysis and live security monitoring dashboard for institutional web portals at AIIMS Jammu. The discussion focuses on observed traffic behavior, dashboard performance, and the practical usefulness of the system in monitoring security-related events across cloud-hosted applications such as the institutional website, HMIS, and HRMS.

1. Real-Time Traffic Visibility

After deployment, the dashboard successfully provided continuous real-time visibility into incoming web traffic across all monitored portals. Administrators were able to observe live traffic counts, request trends, and time-based activity patterns without manual log inspection. The centralized view eliminated the need to access individual server logs, significantly simplifying traffic monitoring and improving situational awareness.

Traffic patterns observed during normal operational hours showed consistent request distribution from legitimate users, while off-peak hours revealed reduced but steady background traffic. These observations helped establish baseline traffic behaviour for institutional portals.

2. Detection of Abnormal Traffic Patterns

The dashboard effectively highlighted abnormal traffic behavior using predefined thresholds and rule-based indicators. Instances of repeated access attempts from specific IP addresses, sudden traffic spikes, and frequent error responses were clearly visible through visual indicators and charts. Such patterns, while not automatically classified as confirmed attacks, served as early warning signs for potential misuse or malicious activity.

The visualization of attack hit trends over time enabled administrators to identify recurring patterns, such as repeated scanning attempts or high-frequency requests targeting specific URLs. This insight supported timely investigation and preventive administrative actions.

3. Source-Based Traffic Analysis

Source IP distribution analysis revealed valuable insights into traffic origins. The dashboard displayed the concentration of requests from specific IP addresses or network ranges, helping administrators distinguish between distributed legitimate traffic and concentrated suspicious access. This feature proved useful in identifying repeated access behaviours from the same sources within short time intervals. Portal-wise traffic comparison further allowed administrators to understand which systems—such as HMIS or HRMS—were receiving higher volumes of suspicious requests, supporting focused monitoring of critical applications.

4. Dashboard Usability and Interpretation

The dashboard interface proved effective in presenting complex traffic and security data in a simplified and interpretable format. Visual elements such as graphs, counters, and tables allowed administrators to quickly assess the security posture without requiring advanced technical expertise. Time-based filtering and portal-wise views enhanced the analytical capability of the system.

The live update mechanism ensured that changes in traffic behavior were reflected promptly, enabling near real-time observation of security events. This reduced dependency on delayed log reviews and improved responsiveness to potential incidents.

5. Operational Impact

From an operational perspective, the implemented system improved the efficiency of security monitoring activities. Administrators could identify suspicious behavior early, prioritize attention based on visual indicators, and maintain continuous oversight of institutional web portals. The system functioned as a decision-support tool rather than an enforcement mechanism, aligning well with institutional operational requirements.

The non-intrusive nature of the dashboard ensured that normal application performance remained unaffected while providing continuous monitoring capabilities.

6. Discussion

The results demonstrate that centralized cloud traffic analysis combined with live dashboard visualization can significantly enhance security awareness for healthcare institutional web portals. Unlike traditional approaches that rely on manual or delayed log analysis, the proposed system offers immediate insight into traffic behaviour and emerging security concerns. The findings highlight the importance of practical monitoring solutions that focus on visibility and usability rather than complex automation. In a healthcare environment where system availability and reliability are critical, such dashboards provide a balanced approach to security oversight without introducing operational complexity.

Conclusion and Future Scope

This work presented a cloud-based web traffic analysis and live security monitoring dashboard developed for healthcare institutional portals such as AIIMS Jammu website, HMIS, and HRMS. The system demonstrates how web server access logs can be effectively utilized to provide real-time visibility into traffic behavior, suspicious activities, and potential security threats in cloud-hosted healthcare environments. The proposed solution adopts a lightweight and practical implementation using PHP and MySQL, making it easy to deploy on existing institutional infrastructure without requiring complex machine learning models or heavy log-processing frameworks. By employing rule-based and threshold-driven analysis, the system successfully identifies abnormal traffic patterns such as repeated requests, unusual access frequency, and suspicious source behavior. The interactive dashboard enables administrators to monitor portal-wise traffic statistics, detect anomalies, and respond to incidents promptly.

Overall, the system improves operational security awareness, supports continuous monitoring, and enhances the administrative decision-making process. Its centralized design allows multiple healthcare portals to be monitored from a single interface, making it particularly suitable for large institutions with multiple cloud-based services. While the proposed system provides an effective real-time monitoring solution, several enhancements can further extend its capabilities. In the future, machine learning–based anomaly detection models can be integrated to complement the existing rule-based approach, enabling detection of more complex and previously unseen attack patterns. Predictive analytics may also be incorporated to forecast abnormal traffic trends and potential threats before they escalate. The system can be expanded to support multi-cloud and hybrid cloud environments, allowing centralized monitoring across different cloud platforms. Integration with automated alerting and incident response mechanisms such as email, SMS, or ticketing systems can further reduce response time. Additionally, tighter integration with DevSecOps pipelines can enable automated log ingestion, security checks, and compliance verification during application deployment and updates.

Future work may also include enhanced role-based access control, detailed audit reporting, and compliance mapping aligned with healthcare security guidelines. These improvements would strengthen the system's applicability, scalability, and long-term

usability, making it a robust security monitoring solution for modern cloud-based healthcare institutions.

References

1. X. Li, Y. Zhang, and J. Chen, "Cloud-Based Healthcare Information Systems: Architecture, Security, and Challenges," Journal of Medical Systems, vol. 47, no. 6, 2023.
2. M. Alshammari, A. Alzahrani, and S. Alqahtani, "Security Challenges and Solutions for Healthcare Applications in Cloud Computing," IEEE Access, vol. 11, pp. 45890–45905, 2023.
3. S. Ahmed, M. Rahman, and M. Hossain, "Real-Time Web Traffic Monitoring and Security Analysis in Cloud Environments," IEEE Transactions on Network and Service Management, vol. 20, no. 3, pp. 2101–2113, 2023.
4. L. Zhou, H. Wang, and Y. Xu, "Threshold-Based Web Traffic Analysis for Anomaly Detection in Cloud Systems," Computers & Security, vol. 134, 2024.
5. D. Patel and K. Shah, "Rule-Based Detection Techniques for Abnormal Web Traffic in Cloud Applications," International Journal of Information Security, vol. 23, no. 1, pp. 77–91, 2024.
6. A. Gupta and N. Kaur, "Centralized Security Monitoring of Hospital Web Portals Using Cloud Dashboards," International Journal of Medical Informatics, vol. 179, 2024.
7. T. Chen, D. Liu, and S. Park, "Design and Implementation of Real-Time Monitoring Dashboards for Cloud Applications," IEEE Software, vol. 41, no. 2, pp. 78–86, 2024.
8. P. Reddy, S. Verma, and M. Rao, "Cybersecurity Threats and Monitoring Strategies in Hospital Information Systems," Health Informatics Journal, vol. 30, no. 1, 2024.World Health Organization (WHO),
9. Cybersecurity in Digital Health: Policy and Implementation Guidance, WHO Press, 2023. European Union Agency for Cybersecurity (ENISA), Cloud Security for Healthcare Digital Infrastructure, ENISA Report, 2024.
10. Seyed Salar Sefati1,2,3*, Bahman Arasteh3,4,5, Octavian Fratu1,2,6 and Simona Halunga1,2,6 (2025) "SSLA: A Semi-Supervised Framework for Real-Time Injection Detection and Anomaly Monitoring in Cloud-Based Web Applications"
11. Rouf Abdullah (2024), "Real-Time Intrusion Detection System Based on Web Log File Analysis"
12. Lenka Benova (2023), "Using Logstash for Real-Time Log Analysis in Cloud-Based Applications"
13. Anish Kumar Sargun Kumar (2022), "Comprehensive Analysis and Evaluation of Anomalous User Activity in Web Server Logs"
14. L. Zhou, H. Wang, and Y. Xu, "Threshold-Based Web Traffic Analysis for Anomaly Detection in Cloud Systems," Computers & Security, vol. 134, 2024.
15. D. Patel and K. Shah, "Rule-Based Detection Techniques for Abnormal Web Traffic in Cloud Applications," International Journal of Information Security, vol. 23, no. 1, pp. 77–91, 2024.
16. A. Gupta and N. Kaur, "Centralized Security Monitoring of Hospital Web Portals Using Cloud Dashboards," International Journal of Medical Informatics, vol. 179, 2024.
17. T. Chen, D. Liu, and S. Park, "Design and Implementation of Real-Time Monitoring Dashboards for Cloud Applications," IEEE Software, vol. 41, no. 2, pp. 78–86, 2024.