International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 01 | Jan - 2026 SJIF Rating: 8.586 ISSN: 2582-3930

Secure Login Monitoring Using an Authentication-Focused SIEM Architecture

Abirami DS[1], Akshaya A[2], Shri Akshaya K[3] Sweetha M[4]

Department of Computer Science And Engineering, Avinashilingam Institute for Home Science And Higher Education for Women, Coimbatore.

Abstract - Security threats targeting authentication systems have increased significantly with the expansion of digital platforms. Traditional login mechanisms are often vulnerable to brute-force attacks and unauthorized access, especially in small and medium-scale organizations lacking advanced security infrastructure. This project presents an Open-Source Security Information and Event Management (SIEM) based employee login and monitoring system designed to enhance authentication security and real-time threat detection. The system is developed using HTML and JavaScript for the frontend, Node.js for backend processing, and MongoDB for secure data storage. A key feature of the system is its brute-force attack detection mechanism, which automatically locks user accounts after multiple failed login attempts and generates instant SMS and email alerts using Twilio. By integrating log analysis, automated alerts, and secure authentication practices, the proposed system provides a cost-effective, scalable, and reliable security solution suitable for educational institutions and small enterprises.

Key Words: SIEM, Authentication Security, Brute-Force Detection, Log Monitoring, Open-Source Security

1.INTRODUCTION

In modern organizational environments, information systems play a vital role in daily operations and data management. As dependency on digital platforms grows, organizations become increasingly exposed to cybersecurity threats such as phishing, credential theft, and brute-force login attacks. Weak authentication mechanisms can lead to unauthorized access, data breaches, and operational disruptions. Therefore, implementing secure monitoring and detection mechanisms has become essential.

Security Information and Event Management (SIEM) systems provide centralized monitoring by collecting and analyzing logs from multiple sources to identify suspicious activities. While commercial SIEM solutions offer advanced features, their high cost and complex infrastructure requirements make them unsuitable for small and medium-sized organizations. This project focuses on developing a lightweight and open-source SIEM-based authentication monitoring system that ensures security, transparency, and affordability.

2. LITERATURE REVIEW

Security Information and Event Management (SIEM) systems have historically been employed to gather, store, and correlate security logs produced by diverse sources, including network devices, servers, and applications. Initial SIEM solutions primarily concentrated on centralized log aggregation and rule-based alerting systems. Although these systems enhanced visibility into security incidents, they frequently necessitated extensive manual setup and expert involvement, rendering them complex and expensive for small and medium-sized enterprises [8]. Recent research indicates that traditional SIEM platforms face challenges with scalability and real-time responsiveness due to the rapidly growing volume of security logs.

González-Granadillo et al. [8] point out that many current SIEM solutions function in a passive manner, analyzing logs after a significant delay, which diminishes their effectiveness against swiftly evolving threats. Furthermore, the intricate nature of configuring correlation rules often leads to elevated false-positive rates, thereby diminishing the practical usability of these systems.

Authentication security has become a significant challenge in contemporary web applications, as attackers increasingly take advantage of weak login mechanisms through brute-force and credential-stuffing attacks. Sommer and Paxson [5] contend that traditional intrusion detection systems are ill-equipped for detailed authentication analysis due to their emphasis on network-level events rather than application-level behavior. Consequently, numerous login-based attacks go undetected until a system compromise occurs.

Table 1: Group Statistics

Category	User Type	N	Mean Login Attempts	Std. Deviation	Std. Error Mean
Overall	Normal Users	148	2.41	1.12	0.092
Overall	Suspicious Users	52	4.86	1.58	0.219

Numerous scholars have investigated machine learning-based intrusion detection methods to enhance the capabilities of Security Information and Event Management (SIEM) systems. Maseer et al. [6] illustrated that anomaly detection through machine learning can significantly boost the accuracy of attack detection; however, these methods typically necessitate extensive training datasets and considerable computational power. This requirement complicates their implementation in lightweight environments where swift responses and simplicity are crucial.

Furthermore, integrated approaches combining SIEM and intrusion detection have been suggested to enhance threat visibility. Muhammad et al. [6] introduced a unified SIEM-IDS framework that is capable of real-time analysis, yet their system mainly addresses network-level threats and lacks specific features for enforcing account-level controls, such as the automation of account freezing. In a similar vein, Debar et al. [5] point out that while AI-enhanced SIEM analytics improve detection capabilities, many solutions do not provide immediate containment actions at the authentication level.

Recent studies in authentication security emphasize the necessity of automated response mechanisms to mitigate the impact of attacks. Barber et al. [6] show that monitoring user login patterns and implementing adaptive access controls can significantly bolster system resilience. Nevertheless, the majority of current systems depend on post-incident alerts instead of real-time prevention, which creates a significant gap in proactive authentication protection.

The literature reviewed indicates that current SIEM systems are either excessively complex, resource-demanding, or inadequately focused on security at the authentication level. There is a distinct requirement for a lightweight, authentication-focused SIEM framework that offers real-time login monitoring, automated account safeguarding, and prompt user notifications. These shortcomings drive the development of CipherNexus, which seeks to fill the identified research void by integrating centralized log analysis with automated response mechanisms specifically designed for authentication security.

3.EXISTING SYSTEM & RESEARCH GAP

Organizations across various sectors continue to depend significantly on conventional username and password-based authentication methods as their primary means of access control.

Although these methods are straightforward to implement and widely utilized, they are characterized by a lack of real-time monitoring, contextual awareness, and automated incident response capabilities. Consequently, they render systems vulnerable to a broad spectrum of security threats, including brute-force attacks, credential stuffing, phishing, and social engineering-based intrusions [8]. Attackers can repeatedly attempt to log in using compromised or guessed credentials without triggering immediate alerts, which allows unauthorized access to remain undetected for prolonged periods.

Another significant drawback of basic authentication systems is the lack of centralized and intelligent log analysis. Login attempts, whether successful or unsuccessful, are frequently recorded in isolated logs that are either reviewed manually or not reviewed at all. This fragmented methodology considerably hinders threat detection and obstructs security teams from recognizing suspicious patterns, such as abnormal login frequency, access from atypical locations, or repeated failures across multiple accounts [5]. In the absence of automated correlation and anomaly detection, early signs of compromise are often overlooked.

In order to tackle these challenges, there is an increasing demand for a robust authentication framework that incorporates continuous monitoring, real-time anomaly detection, and automated response functionalities. This system ought to continuously assess login behaviors, recognize deviations from standard usage patterns, and autonomously initiate defensive measures such as freezing accounts, sending alert notifications, or enforcing multi-factor authentication. The deployment of a smart and proactive authentication solution is crucial for diminishing attack surfaces, shortening response times, and protecting organizational data from the ever-evolving landscape of cyber threats [6].

4.PROPOSED SYSTEM

The proposed system, Cipher Nexus, is a Security Information and Event Management (SIEM) framework that emphasizes authentication. It is designed to monitor, analyze, and respond to suspicious login activities in real time. In contrast to traditional authentication methods that merely validate user credentials, Cipher Nexus considers every login attempt as a security event and conducts ongoing analysis to identify abnormal behavior. Recent research underscores the necessity for modern SIEM platforms to transition from passive log storage to proactive security analytics and automated response systems [8], [5].

Cipher Nexus consolidates login events generated from web-based systems and organizes them within a structured log repository. Each authentication attempt is assessed according to established security rules, including thresholds for failed logins and the status of accounts. When unusual patterns, such as multiple failed attempts, are identified, the system promptly initiates mitigation measures. This approach is consistent with current research that highlights the importance of real-time threat detection and swift responses to minimize the impact of attacks [6].

The proposed system automatically suspends compromised accounts once a specified failure threshold is surpassed and alerts the legitimate user through a notification mechanism. This strategy effectively narrows the opportunity for brute-force and credential-stuffing attacks. Research on authentication security suggests that automated controls at the account level significantly enhance system resilience against unauthorized access [6],[5]. By concentrating on authentication logs, Cipher Nexus offers a streamlined yet powerful SIEM solution that is well-suited for small and medium enterprises.

4.1. OBJECTIVE

The primary objective of this project is to develop a secure employee authentication system integrated with Security Information and Event Management (SIEM) features. The system aims to monitor login activities in real time, detect brute-force attacks through intelligent login attempt analysis, generate automated alerts for suspicious behavior, ensure secure storage and management of user credentials, and provide a scalable, cost-effective open-source security solution suitable for small and medium-scale organizations.

4.2 OVERVIEW

This phase explains the internal architecture and functional design of the proposed Secure Open Source SIEM-based Employee Authentication and Monitoring System, referred to as the CipherNexus. The system was developed using a modular design philosophy, wherein each component was implemented as an independent unit while remaining logically interconnected with other modules.

Such a modular architecture significantly enhances system scalability, eases long-term maintenance, and improves functional clarity, all of which are essential requirements for modern SIEM solutions. Each module is designed with a clearly defined responsibility, ensuring separation of concerns. Through well-coordinated interaction among these modules, the system delivers comprehensive security monitoring, intelligent analysis, timely threat correlation, and efficient automated response across diverse operational environments in large-scale, distributed, and mission-critical enterprise deployments.

4.3 SYSTEM ARCHITECTURE

The architecture of the Cipher Nexus system is constructed with a modular and scalable framework, as depicted in Fig. 1. This architecture is composed of five key components: User Interface, Backend Server, Authentication Engine, Log Storage, and Alert Engine. Contemporary SIEM architectures prioritize modular design to enhance scalability and performance, a principle that is evident in the proposed system [8].

The User Interface Layer facilitates secure login and provides users with access to the dashboard. It captures user credentials and presents account status along with security alerts. The Backend Server, developed using Node.js and Express.js, handles authentication requests and implements security protocols. Studies indicate that server-side validation and centralized processing are vital for preserving the integrity of authentication [8].

The Authentication Engine is responsible for validating user credentials through secure password hashing methods and assesses login attempts in accordance with security policies. All authentication activities are directed to the Log Storage Module, which is implemented using MongoDB Atlas, allowing for efficient storage and retrieval of structured security logs. Centralized log repositories are essential in modern SIEM systems for effective forensic analysis [8].

The Alert Engine oversees the results of log analysis and activates real-time alerts upon the detection of suspicious activities. When an account is frozen, an alert notification is dispatched to the user, ensuring prompt awareness of potential security threats. Such automated alerting systems are widely acknowledged as critical elements of modern SIEM platforms [5], [6].

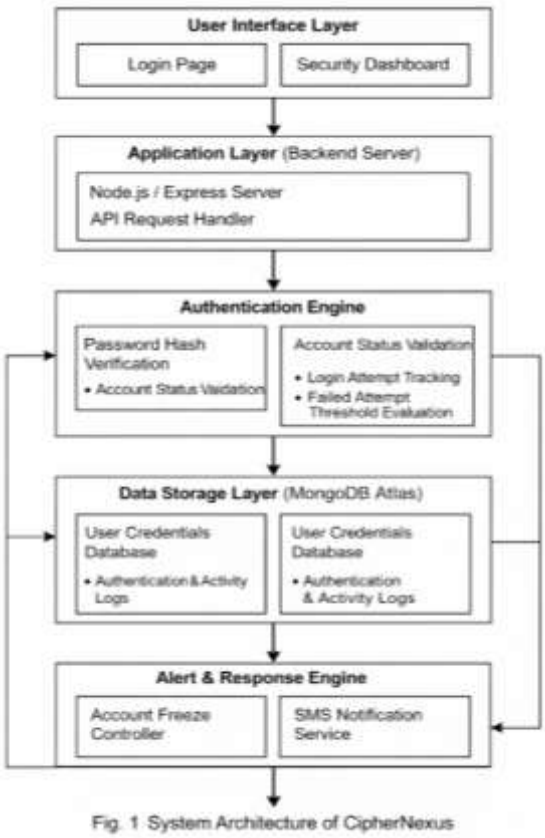

Fig. 1 System Architecture of CipherNexus

4.4 MODULE DESCRIPTION

4.4.1 Authentication Module

The Authentication Module serves as the primary access control component of the system. It is responsible for verifying user identity and regulating access to protected system resources.

Key Functions:

- Processes employee registration and login requests
- Secures user passwords using bcrypt-based cryptographic hashing
- Validates credentials during authentication attempts
- Creates and manages user sessions
- Records and tracks unsuccessful login attempts

Security Enforcement:

- All authentication attempts are continuously monitored
- An account is automatically locked for a period of three hours after three consecutive failed login attempts
- This mechanism effectively mitigates brute-force and credential-stuffing attacks

Input: User identifier and password
Output: Authenticated user session or enforced account lock

By implementing strict access validation and monitoring, this module ensures that only legitimate users can access the dashboard, while minimizing the risk of repeated unauthorized attempts.

4.4.2 Log Collection Module

The Log Collection Module functions as the centralized data acquisition layer of the SIEM framework. It captures and stores all security-relevant events that are generated during system operation.

Types of Logs Captured:

- Successful authentication events
- Failed login attempts
- Account lock and unlock events
- Session start and end timestamps
- Alert initiation record

Storage Mechanism:

- Log records are stored in MongoDB Atlas using a structured document schema
- Each log entry includes attributes such as timestamp, user identifier, event category, and status

4.4.3 Log Analysis Module

The Log Analysis Module evaluates the collected logs to detect abnormal behavior and potential security threats.

Analysis Methods:

- Threshold-based evaluation for repeated authentication failures
- Rule-driven event correlation
- Temporal analysis of login behavior patterns

Illustrative Scenario:

- Multiple failed authentication attempts occurring within a limited time window are identified as a probable brute-force attack

SIEM Functionality:

- Transforms raw log data into meaningful security insights
- Provides the logical basis for triggering alerts and enforcing security controls

This module enables the early identification of threats, thereby reducing the likelihood of escalating security incidents.

4.4.4 Alert Engine Module

The Alert Engine is responsible for initiating immediate responses when suspicious activities are detected.

Alert Triggers:

- Three consecutive failed login attempts
- Activation of account lock status
- Detection of abnormal authentication behavior

Notification Channels:

- SMS notifications delivered using the Twilio API
- Email alerts sent to registered users

The Alert Information Includes:

- Details of suspicious login activity
- Account lock confirmation
- Instructions for contacting system support in case of unauthorized access

By delivering timely alerts, the system minimizes response delays and improves overall security awareness.

4.4.5 Dashboard Module

The Dashboard Module offers a graphical interface that allows authenticated users to monitor account activity and system status.
Dashboard Features:

- Display of employee profile information
- Visualization of login history and recent actions
- Graphical representation of authentication trends
- Real-time indication of security status

Access Restrictions:

- Dashboard access is granted only after successful authentication
- Locked or unauthorized accounts are denied access

The dashboard improves situational awareness, which is a fundamental objective of SIEM.

4.5 System Workflow

The system workflow illustrates how the individual modules collaborate to deliver secure authentication and monitoring.

Workflow Sequence:

1. **User Access Initiation**
1. The employee navigates to the login interface
2. **Authentication Request Submission**
1. Credentials are forwarded to the Authentication Module
3. **Credential Validation**
1. Password verification is performed using bcrypt hashing
2. A valid session is created upon successful authentication
4. **Event Logging**
1. Each login attempt is recorded by the Log Collection Module
5. **Log Evaluation**
1. Logs are analyzed for suspicious patterns
2. Failed attempts are correlated and counted
6. **Alert Activation**
1. Threshold violations trigger the Alert Engine
2. SMS and email notifications are dispatched
7. **Dashboard Access**
1. Authenticated users are redirected to the dashboard
2. Activity history and security logs are displayed
8. **Account Lock Handling**
1. Locked users are denied access
2. The system redirects them to an account lock notification page

4.6 Module Interaction Description

Although each module operates independently, the system functions as a unified security pipeline. The Authentication Module initiates all user interactions, whereas the Log Collection Module continuously captures events. The Log Analysis Module evaluates security relevance, the Alert Engine responds to threats, and the Dashboard Module presents processed insights to users.

This coordinated interaction represents a lightweight SIEM architecture that is suitable for small- and medium-scale organizational environments.

4.6 Importance of Modular Architecture

- Facilitates system scalability and future enhancement
- Supports seamless integration of AI-based analytics and MFA mechanisms
- Reduces overall system complexity
- Conforms to modern SIEM architectural principles

5. IMPLEMENTATION

The Cipher Nexus system employs a web-based architecture that seamlessly integrates frontend interfaces with a secure backend and a centralized database. The frontend is crafted using HTML, CSS, and JavaScript to guarantee a responsive and user-friendly experience. The backend logic is constructed with Node.js and Express.js, facilitating the efficient management of authentication requests and security workflows.

MongoDB Atlas serves as the primary data storage solution for maintaining user credentials and authentication logs. Cloud-based NoSQL databases are commonly utilized in SIEM systems due to their scalability and capacity to manage substantial volumes of log data [9]. The system adheres to a modular implementation strategy, which permits the independent enhancement of authentication logic, log analysis, and alert mechanisms.

5.1 Algorithms

The algorithmic workflow implemented in CipherNexus is structured to facilitate ongoing surveillance and automated reactions to authentication-related security threats. The procedure initiates with the Login Monitoring Algorithm, which considers each authentication attempt as a security event and logs it along with pertinent attributes such as the timestamp, user identity, and authentication status. By persistently monitoring both successful and unsuccessful login attempts, the system formulates a behavioral profile for each user. Comparable rule-based monitoring strategies have proven effective in identifying brute-force and credential-stuffing attacks within contemporary SIEM environments [10], [12].

Upon the detection of anomalous behavior, control transitions to the Account Freeze Algorithm, which assesses the number of consecutive failed attempts against a predetermined security threshold. Should the threshold be surpassed, the user account is automatically suspended to avert further unauthorized access. Subsequently, the Alert Trigger Algorithm is activated to inform the legitimate user regarding the potential security incident. This systematic enforcement of monitoring, restriction, and notification guarantees swift threat containment and user awareness. Fig. 2 depicts the cohesive workflow of these algorithms, illustrating how automated response mechanisms bolster authentication security and diminish system vulnerability to recurrent attacks [11], [14].

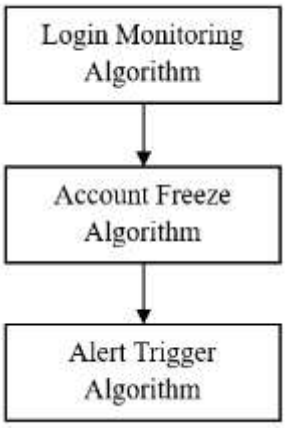

Fig. 2 Algorithm Flow Diagram

Algorithm 1: Login Monitoring Algorithm

Step 1: Accept login credentials from the user interface

Step 2: Check account status (active or frozen)

Step 3: Authenticate credentials through hashed password comparison

Step 4: Document login attempt with timestamp and status

Step 5: Relay event to log analysis module

Algorithm 2: Account Freeze Algorithm

Step 1: Obtain failed login count for the user

Step 2: Assess failure count against a predefined threshold

Step 3: If the threshold is surpassed, change account status to frozen

Step 4: Reject additional login attempts

Algorithm 3: Alert Trigger Algorithm

Step 1: Identify account freeze event

Step 2: Create alert message containing security details

Step 3: Dispatch notification to the registered user

Step 4: Record alert event for auditing purposes

Rule-based security algorithms, such as those based on threshold detection, continue to be effective in thwarting brute-force attacks, particularly in systems focused on authentication [12], [10].

5.2 Security Mechanisms

Cipher Nexus employs a variety of security mechanisms to provide strong protection against attacks that exploit authentication vulnerabilities. Passwords are safeguarded through cryptographic hashing methods, ensuring that unencrypted credentials are never stored. The secure storage of credentials is a critical aspect of contemporary authentication systems [13].

To prevent brute-force attacks, there is a continuous monitoring of failed login attempts, coupled with the enforcement of account freezing policies. Studies show that automated response systems significantly diminish the success rates of attacks by restricting repeated authentication attempts [14], [9]. Mechanisms for session management guarantee that authenticated users can maintain secure sessions without risking the exposure of sensitive data.

All logs related to authentication are securely stored and shielded from unauthorized access, facilitating forensic investigations and compliance audits. The centralized and secure storage of logs is acknowledged as an essential characteristic of effective Security Information and Event Management (SIEM) systems [10], [11]. The integration of these security mechanisms enables Cipher Nexus to deliver a dependable and intelligent framework for monitoring authentication.

6.RESULTS, CONCLUSION AND FUTURE SCOPE

6.1 Results and Analysis

This section discusses the outcomes observed during the implementation and testing of the proposed CipherNexus. The evaluation was conducted in a controlled environment to assess the functional correctness, security effectiveness, and usability.

6.1.1 Authentication and Login Evaluation

The authentication mechanism reliably validated legitimate users using Bcrypt-secured credentials stored in MongoDB. Authorized users were successfully redirected to the dashboard without noticeable delays.

Observed Outcomes:

- Correct credentials resulted in successful authentication
- Incorrect credentials were rejected and logged
- Sessions were created exclusively for authenticated users

These results confirm that the access-control mechanism effectively prevents unauthorized entry.

6.1.2 Brute-Force Mitigation and Account Locking

Repeated incorrect login attempts were simulated to assess system resilience.

Key Findings:

- Accounts were automatically locked after three consecutive failed attempts
- Additional login attempts during the lock period were blocked
- Users were clearly informed about the lock status

This behavior demonstrates the strong enforcement of authentication security policies consistent with SIEM standards.

6.1.3 Log Collection and Monitoring Performance

All authentication-related events, including login successes, failures, account locks, and alert triggers, were accurately recorded in MongoDB. The logs were stored in a structured format to enable efficient querying and analysis.

The centralized logging capability confirms the effectiveness of the proposed system as a lightweight SIEM log management solution.

6.1.4 Alerting and Notification Results

Suspicious activities immediately activated an alert engine. Both SMS and email notifications were successfully delivered, clearly informing users of potential unauthorized access.

This real-time alerting mechanism significantly reduces the incident response time.

6.1.5 Dashboard Visualization Analysis

The dashboard accurately displays user information, login history, and security status. This visualization capability improves transparency and situational awareness for authenticated users.

6.1.6 Overall System Performance

The system exhibited a stable performance with minimal resource consumption. Response times remained consistent even after repeated authentication attempts, indicating their suitability for small- and medium-scale organizational use.

6.2 Conclusion

This study successfully presents the design and implementation of a secure open-source SIEM-based employee authentication and monitoring system. The proposed solution effectively addresses critical security challenges, including unauthorized access, brute force attacks, and delayed incident detection.

By integrating secure authentication, centralized logging, intelligent log analysis, and automated alerting, this system establishes a strong security foundation. The adoption of open-source technologies, such as Node.js, MongoDB, and Twilio, ensures cost efficiency, flexibility, and scalability.

The experimental results confirm that the system achieves its core objectives of secure access control, timely threat detection, and SIEM-aligned monitoring, making it a practical solution for organizations with limited resources.

6.3 Future Scope

Although the current system delivers essential SIEM functionality, several enhancements can further improve its capabilities.

6.3.1 Machine Learning-Based Anomaly Detection

Future implementations can integrate machine learning techniques to analyze behavioral patterns and detect anomalies, such as unusual login times, abnormal access locations, and sudden spikes in authentication failures. This approach can reduce the number of false positives and enhance the detection accuracy.

6.3.2 Multi-Factor Authentication

Incorporating MFA through OTPs, biometric verification, or authenticator applications provides an additional layer of security and significantly reduces the risk of credential compromise.

6.3.3 Enterprise-Level SIEM Integration

The system can be extended to interface with enterprise SIEM platforms such as ELK Stack, Wazuh, and OSSEC, enabling advanced correlation, compliance reporting, and large-scale monitoring.

6.3.4 Cloud-Native Deployment

Deploying the solution using containerization and cloud orchestration technologies, such as Docker and Kubernetes, would improve scalability, fault tolerance, and availability.

6.3.5 Automated Incident Response

Future enhancements may include SOAR-based automation, enabling predefined response actions, such as forced password resets or administrative alerts, to be triggered automatically.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to the faculty members of the Department of Computer Science and Engineering for their continuous guidance, encouragement, and valuable suggestions throughout the course of this work. We are especially thankful to our project guide for providing insightful feedback and technical direction that significantly contributed to the successful completion of this research.

We also acknowledge our institution for providing the necessary resources and a conducive environment to carry out this study. Finally, we extend our appreciation to all those who directly or indirectly supported us during the development and documentation of the **CipherNexus** system.

REFERENCES

1. González-Granadillo, G., González-Zarzosa, S., Díaz, R.: Security information and event management systems: Analysis, trends, and challenges. *Sensors* **21**(14) (2021) Art. no. 4759. DOI: 10.3390/s21144759
2. Debar, H., Zahid, S.M., Wankar, R.: AI-driven analytics in SIEM systems for enhancing intrusion detection and policy enforcement. *Journal of Cybersecurity and Privacy* **4**(2) (2024) 143–160. DOI: 10.3390/jcp4020143
3. Muhammad, A.R., Sukarno, P., Wardana, A.A.: Integrated SIEM and intrusion detection system for real-time cyber threat analysis using machine learning. *Procedia Computer Science* **222** (2023) 339–346. DOI: 10.1016/j.procs.2022.12.339
4. Barber, J., Chen, M., Wang, L.: Enhancing authentication security using machine learning-based behavioral analysis. *IEEE Transactions on Information Forensics and Security* **18** (2023) 4172–4184. DOI: 10.1109/TIFS.2023.3284759
5. Maseer, N., Iqbal, M., Khan, A.A.: Benchmarking machine learning algorithms for anomaly-based intrusion detection systems. *IEEE Access* **9** (2021) 22351–22370. DOI: 10.1109/ACCESS.2021.3056614
6. Sommer, R., Paxson, V.: Machine learning for network intrusion detection: Limitations and opportunities. *IEEE Security & Privacy* **17**(5) (2019) 32–39. DOI: 10.1109/MSEC.2019.2928342
7. Sabahi, A., Movaghar, A.: Intrusion detection: A survey of modern challenges and solutions. *International Journal of Computer Networks and Communications* **11**(3) (2019) 1–14. DOI: 10.5121/ijcnc.2019.11301
8. Sulaiman, M.A.B.M., Hassan, R., Kama, N.: SIEM network behaviour monitoring framework using deep learning for enterprise networks. *International Journal of Electrical and Computer Engineering* **11**(6) (2021) 5134–5143. DOI: 10.11591/ijece.v11i6.pp5134-5143
9. Tendikov, N., Ivanova, D., Stoyanov, P.: Security information and event management data acquisition and analysis methods using machine learning principles. *Computer Science Review* **51** (2024). DOI: 10.1016/S2590-1230(24)00509-7
10. Kolias, C., Kambourakis, G., Stavrou, A., Voas, J.: DDoS in the IoT: Mirai and other botnets. *Computer* **51**(7) (2018) 80–84. DOI: 10.1109/MC.2017.201
11. Manzoor, J., Waleed, A., Jamali, A.F., Masood, A.: Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. *PLOS ONE* **19**(3) (2024) e0301183. DOI: 10.1371/journal.pone.0301183
12. Bezas, K., Filippidou, F.: Comparative analysis of open-source security information and event management systems (SIEMs). *Indonesian Journal of Computer Science* **12**(2) (2023) 443–468.
13. Mokalled, H., Catelli, R., Casola, V., Debertol, D., Meda, E., Zunino, R.: The applicability of a SIEM solution: Requirements and evaluation. In: *Proc. IEEE 28th Int. Conf. on Enabling Technologies* (WETICE) (2019) 132–137. DOI: 10.1109/WETICE.2019.00036
14. Özdemir Sönmez, F., Günel, B.: Evaluation of security information and event management systems for custom security visualization generation. In: *Proc. Int. Congress on Big Data, Deep Learning and Fighting Cyber Terrorism* (IBIGDELFT) (2018) 38–44. DOI: 10.1109/IBIGDELFT.2018.8625291
15. Cinque, M., Cotroneo, D., Pecchia, A.: Challenges and directions in security information and event management (SIEM). In: *Proc. IEEE Int. Symp. on Software Reliability Engineering Workshops* (ISSREW) (2018) 95–99. DOI: 10.1109/ISSREW.2018.00024