INTERNATIONAL JOURNAL OF NOV.EL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 4, April 2026 | ISSN: 2456-4184 | IJNRD.ORG

CyberShieldPro: A Lightweight Security Monitoring Solution for Small Organizations

Sahil Gurav
Department of information and Cyber Security.
Guru Nanak Khalsa College, Matunga.
Email: sahilgurav787@gmail.com

1. Abstract

Security Information and Event Management (SIEM) is used to check system activity and find possible threats. It collects data from different places and helps in understanding what is going on. But in real cases, most SIEM tools are not simple. They are costly and also need good systems to run. Because of this, small places like schools or colleges cannot use them properly. Also, too much log data is generated, so it becomes confusing to find actual issues.

In this project, a simple SIEM tool called CyberSheildPro is made. The goal was simplicity, plain and simple. It was built to function on everyday systems, not the latest and greatest. The aim was functionality, not complexity.

To understand the data, raw logs are not shown directly. Instead, simple graphs are used so it becomes easier to see what is going on. This helps because logs can be confusing.
Even if a person is not that much technical, they can still understand the output without any difficulty.

The system mainly checks activity in real time and looks at logs in a simple way. It also tries to find unusual behavior, but only at a basic level. Everything is kept simple so that it runs without putting too much load on the system.

From this project, it is clear that even a basic SIEM tool can be useful. It may not be advanced, but it can still help in small environments. It is helpful where budget and system resources are limited.

Keywords— Security Information and Event Management (SIEM), analytical visualization, log analysis, security analytics, real-time dashboards.

2. Introduction

Security Information and Event Management (SIEM) systems are mostly used in cybersecurity domain to monitor activities and detect real time threats. SIEM systems collect data from various sources of systems and platforms such as servers, applications, and network devices, which helps in understanding what is happening inside an organization's network. This makes it a lot easier to recognise and identify abnormal behavior and take quick action when required.
Although, most SIEM solutions that are available today are costly and require high end system resources, which makes them difficult to use for smaller organizations like schools and colleges. These organizations usually do not have advanced infrastructure or dedicated security teams. Also, the large number of alerts generated by SIEM systems can create confusion, because many of them turn out to be false positives.
In this project, the main aim is to develop a small-scale SIEM tool named CyberSheildPro, which is capable to run on low-end systems and be affordable for small scale organizations. The focus is on reducing false positive alerts so that users can concentrate only on real security threats. This helps in improving efficiency without increasing complexity.
As cyber-attacks are increasing day by day, relying only on traditional security methods is not enough. Even in a lightweight system like CyberSheildPro, basic techniques such as pattern analysis are used to identify

possible threats from large amounts of data. This allows faster and more effective response, even with limited resources.

The proposed system also capable of creating a simple report, which can be helpful for organizations that have basic compliance or auditing requirements. Since everything is available in one single place, users can check activities more easily without requiring more technical knowledge. Also, some repetitive work is reduced so that users do not have to do everything manually.

In the end, this project tries to showcase that SIEM tools do not always have to be complex or costly. A simple and lightweight solution like **CyberSheildPro** can still provide useful security support, especially for smaller setups such as schools and colleges where resources are limited.

---

3. Background

As the use of digital systems in organizations are increasing, the risk of cyber threats has increased too. Even small-scale organizations like schools and colleges are now utilizing networks, online platforms, and stored data, which makes them a potential target for attacks. Although, most of the organizations lacks advanced security systems or dedicated teams to monitor their networks.

SIEM (Security Information and Event Management) systems were introduced to tackle this problem by collecting logs from various sources and analyzing them to detect possible threats. These systems help in monitoring activities and recognising and identifying suspicious behavior. But in practice, most of the SIEM tools available today are mainly built for large organizations. They often come with higher costs, need better hardware to operate, and can be complicated to manage. Another issue is the number of alerts they generate. Not all of these alerts are actual threats, and many of them turn out to be false positives, which can make things confusing for users. This can lead to user confusion and an increased workload. This issue becomes even more noticeable in smaller organizations, where there may not be enough technical knowledge to handle such complex systems properly. Because of this, there is a need for a SIEM solution that is simpler to use and also more affordable.

This project is mainly about building a lightweight and ease to use SIEM tool called CyberSheildPro that can operate on low-end systems and can still handle basic security monitoring. The plan is to keep the system simple to use, reduce unnecessary alerts, and make sure that even small organizations can improve their security without spending too much or dealing with complex setups.

---

4. Literature review

4.1 Review of Literature

Even while SIEM research has advanced significantly, smaller firms continue to lag behind. The majority of research focuses on enterprise-grade systems that manage complex threats and enormous data volumes. The main advancements in SIEM technology—log analysis, alert management, visualization, and lightweight design—are reviewed in this part along with the gaps that CyberSheildPro fills for educational institutions.

4.2 The Development of SIEM Systems

In the early days of security monitoring, server logs had to be manually checked. time-consuming and prone to mistakes. Subsequently, SIM and SEM combined to create contemporary SIEM solutions that provide real-time correlation and centralized data collecting. These techniques significantly increased network visibility. The issue is that they became more complicated. Commercial SIEMs of today are unsuitable for contexts with limited resources because they are designed for huge, well-funded businesses with server farms.

4.3 Log Analysis and Event Correlation

Every SIEM starts with logs. Gather them from a variety of applications and systems, including servers, firewalls, and endpoints, and then look for questionable trends. Event correlation connects the dots—say, linking failed logins to privilege escalation attempts. Sounds straightforward, but massive log volumes

overwhelm most systems. Processing delays mount up, demanding serious computational muscle that low-end hardware just can't provide.

4.4 The Alert Fatigue Problem

Here's where SIEMs often fail: alert overload. Systems generate hundreds of warnings daily, but 70-80% turn out false positives. Security teams waste many hours chasing these false alerts. Researchers push hybrid approaches—rules plus behavioural analysis—to filter junk alerts. Trade-off? More complexity, higher resource demands, exactly what small IT teams want to avoid.

4.5 Visualization Makes SIEM Usable

Raw logs intimidate non-experts. Smart researchers often turned to dashboards, heatmaps, and timelines instead. Convert event data to visual patterns and anomalies jump out. Studies had confirmed visualization slashes analysis time by 30-50%. Catch? Sophisticated charts require hefty frontend frameworks that bog down basic systems.

4.6 Lightweight SIEM Research Gap

Most literature chases AI-powered SIEMs with machine learning and SOAR integration. Impressive detection rates, sure—but they need data centers, not classroom laptops. Open-source alternatives help, yet even ELK Stack recommends 8GB+ RAM. Schools operating decade-old Dells need different solutions: minimal footprint, dead-simple setup, actual affordability.

What CyberSheildPro Brings

Current research overlooks practical needs of small organizations. Enterprise SIEMs don't scale down. We need tools that:

- Can operate on low-end systems
- Is affordable for small scale organizations
- Reduces false positives without hard and complex configurations
- Provides simple visualization and UI for better understanding

CyberSheildPro targets exactly this space—a lightweight SIEM built for real-world constraints without sacrificing essential monitoring capabilities.

---

5. Problem Statement

When we look at current SIEM systems, there are a few practical problems that can be noticed, especially in smaller setups.

1. High Cost of SIEM tools

First, most SIEM tools are not cheap. They are usually made for big companies, so small organizations like schools or colleges may not be able to afford them easily.

2. Powerful hardware to run

Another issue is the system requirement. These tools often need good hardware to run properly. If the system is low-end, performance can become slow or unstable.

3. Complexity of setting up SIEM

Also, setting up a SIEM system is not always simple. Many tools require proper configuration, and without technical knowledge, it becomes difficult to use them effectively.

4. Increasing False Positives

One more common problem is the number of alerts generated. SIEM tools tend to produce a lot of alerts, but not all of them are real threats. This makes it harder to focus on the important ones.

5. Log Handling

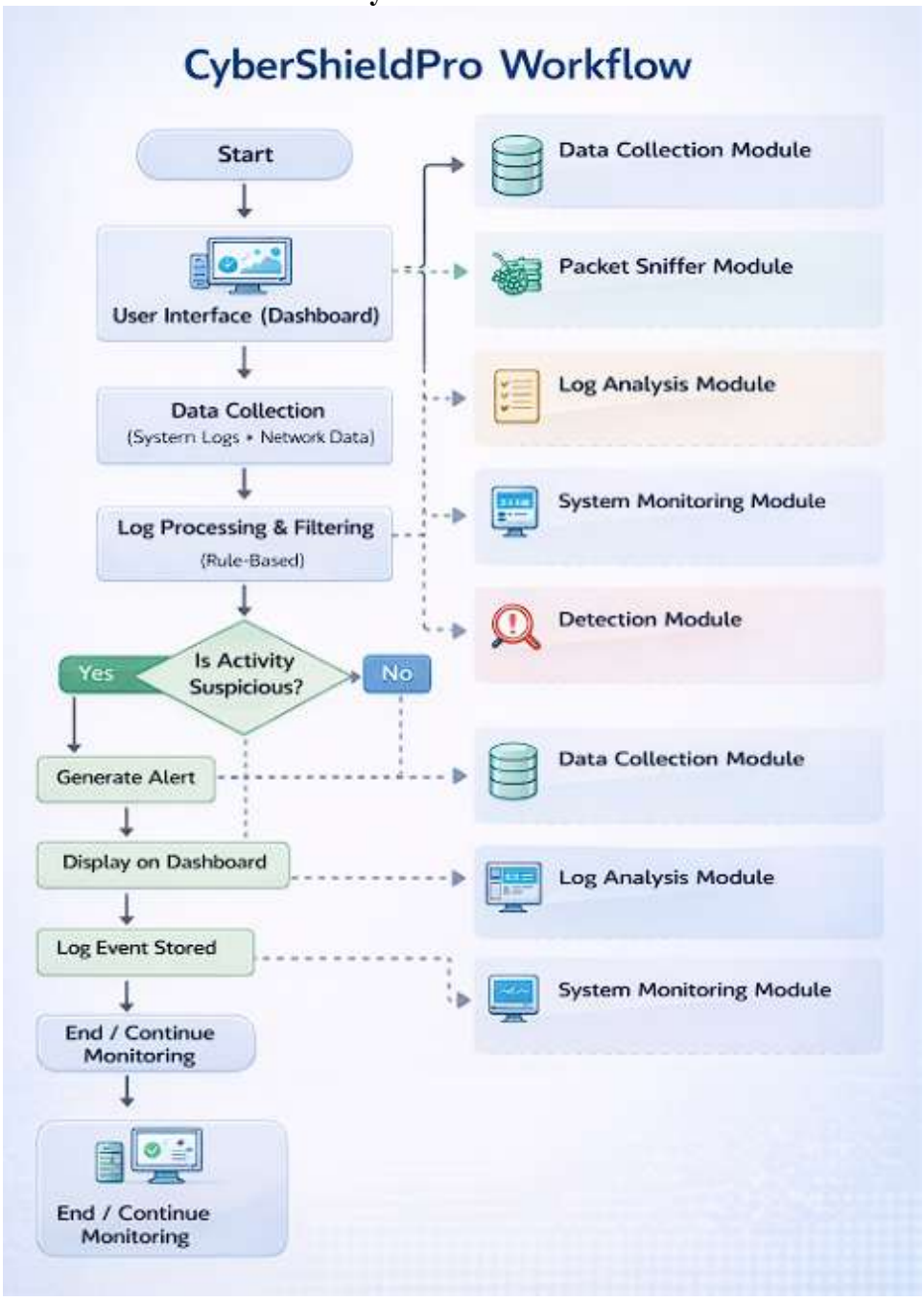
Handling log data is also not easy. Since there is a large amount of data, analysing it can take time and effort.

In addition to this, most SIEM systems are designed for large-scale environments. Because of this, they do not always fit well in smaller organizations.

Lastly, users who are new to cybersecurity may find these tools difficult to understand and operate.

6. Research Methodology

6.1 System Architecture



The architecture of CyberSheildPro is not very complicated. The idea was to keep things simple so that it can run on normal or low-end systems without any problem. Instead of adding too many advanced features, only the required parts are used.

Data Collection Module
First, the system starts with collecting data. The data collection part takes logs from system activity and network traffic. Whatever information is needed for checking comes from here.

Packet Sniffer Module
Then there is a packet sniffer. It keeps an eye on the network and captures packets. If there is any unusual communication, this module helps in noticing it. It does not go very deep, but it is enough for basic monitoring.

Log Analysis Module
After that, the logs are checked in the log analysis part. Here the system looks at the data and tries to find anything different from normal behavior. The checking is kept simple so that it does not slow down the system.

System Monitoring Module
There is also a system monitoring part which looks at what is happening inside the system. For example, file changes or processes. Sometimes problems are not from network, so this helps in that case.

Detection Module
For detection, simple rules are used. It is not using heavy models or anything like that. Just basic conditions to identify if something is suspicious. This helps in keeping the system lightweight. If something looks wrong, the system gives an alert. But too many alerts can be confusing, so only important ones are shown.

Dashboard Module
The output is then shown using a simple dashboard. Instead of showing full logs, it shows things in an easy way so that the user can understand quickly.

At the end, the interface is kept very simple. The goal was that even a beginner can use it without much difficulty.

Also, while building this, we tried to keep everything simple so that it works properly on a normal laptop without needing high resources.

6.2 Development Environment and Tools (for your SIEM)

The system is developed using Python because it is simple and easy to work with. It also supports many libraries which help in faster development.

The following tools and technologies are used:

- Python 3.10+ for overall system development
- Scapy/ socket libraries for packet sniffing
- SQLite for storing logs and alert data
- Basic visualization libraries (like matplotlib) for dashboard
- OS modules for system monitoring

The system is developed and tested on Windows, so that it works properly on normal desktop systems.

6.3 Data Source and Log Collection

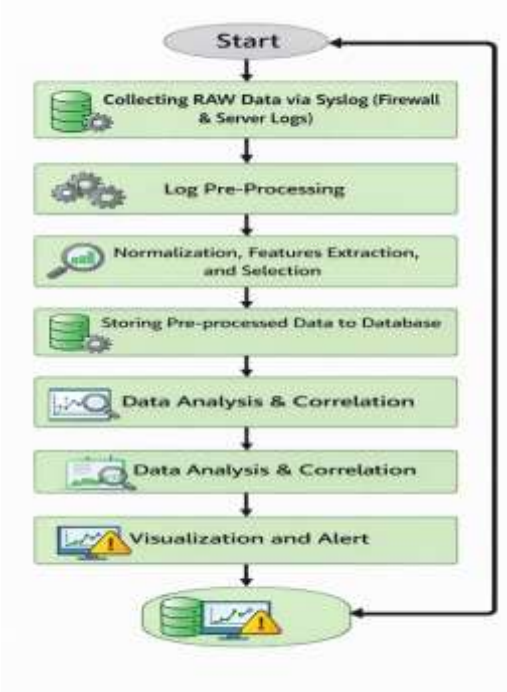
The system mainly depends on log data collected from different sources.

- Logs are collected from system activities and network traffic
- Packet sniffer captures basic network information
- System monitoring tracks file and process activity

The collected data is then stored and used for further analysis. The goal is to keep the data handling simple so that performance is not affected.

6.4 Detection Workflow

The working of the system follows a simple flow.



This process runs continuously in the background.

6.5 Testing and Evaluation

For testing, I did not follow anything very complex. The main idea was just to see how the system behaves in normal and slightly abnormal situations.
At first, I let the system run normally and observed regular activity. After that, I tried adding some simple suspicious cases manually just to check whether the system is able to catch them or not. I also kept generating logs continuously for some time to see if real-time monitoring works properly.

While doing this, I mainly focused on a few things. One was whether the system is able to detect activities correctly or not. Another thing I checked was how many unnecessary alerts are coming, because too many alerts can be confusing. I also observed CPU and memory usage since the system is supposed to run on low-end machines. Along with that, I checked how quickly the alert is generated after an activity happens.
From what I observed, the system was working fine on a normal laptop and was able to give useful alerts without slowing down too much.

6.6 Research Significance

This project is mainly done to solve some basic problems seen in existing SIEM tools.

Most tools are either too heavy or too complex, so here the idea was to keep things simple. The system is lightweight, so it can run on systems that don't have high specifications. It also tries to avoid too many unnecessary alerts, which makes it easier to understand what is actually important.

---

7. Findings

After working on the system and testing it in different situations, a few things were noticed. The testing was done in a simple way just to understand how the system behaves in real use.

7.1 Real-time monitoring

The system keeps running in the background and checks activity continuously. Because of this, when I tried some unusual actions, it was able to catch them quickly. It didn't take much time compared to normal checking methods.
For example, when some suspicious activity was created, the system picked it up almost immediately. This shows that continuous monitoring is useful because there is less delay.

7.2 Log handling

Even when logs were increasing, the system was still working fine. It didn't slow down too much. I kept it running for some time and it was stable.
The logs were getting stored properly and there was no major issue while handling them. This means the system can manage data in a simple way without needing high resources.

7.3 Detection using rules

The system uses simple rules, so it was able to detect basic suspicious patterns without much problem. It worked properly for known cases, but for completely new cases it may not always work.

Still, for normal use, this type of detection is useful because it is fast and easy to implement.

7.4 Alerts

When something was not normal, the system gave an alert. This helped in noticing issues quickly. But if alerts keep coming too much, it can get confusing sometimes.
So, the system is kept in a way that it mostly shows only important alerts. This makes it easier to understand what is actually wrong.

7.5 System performance

While running the system, CPU and memory were observed. Most of the time it stayed normal. Sometimes it went a little high, but only for a short time.
Even after running for longer duration, there was no major issue. It was working fine on a normal laptop.

7.6 Ease of use

The system is simple to use. It is not very complicated, so even a beginner can understand it. The output is also kept simple. Dashboard and alerts are easy to read, so it is clear what is happening.

7.7 Overall use

After testing, the system looks useful for small setups like schools or colleges. It may not be like big SIEM tools, but still, it does the basic work.
It can help in improving security in a simple way without needing high cost.

---

8. Technical Challenges

While building and designing this system, some practical issues came up during implementation of the same. Most of them were related to real-time working and keeping the system as simple as possible.

1. Handling real-time data
One problem I noticed was when data is being generated continuously. Sometimes logs or activity are still in use, so directly processing them was not always smooth.
Because of this, I had to make the system retry in such cases instead of failing. Basic error handling was added so that the system keeps running.

2. Managing logs
As logs keep increasing, it can become slow if not handled properly. During testing, this was noticeable when data started growing.
So, I kept the storage and processing simple. The idea was not to overcomplicate it and keep it working without slowing down.

3. Continuous monitoring
Another issue was making sure the system keeps running all the time. At first, when some processing was happening, there were small delays.
Later, this was handled by keeping monitoring separate so it continues in the background.

4. Alerts handling
Alerts were a bit tricky while working on the system. When too many alerts come at the same time, it becomes hard to understand which one is actually important.
So, the idea was to not show everything. Only useful and positive alerts are displayed so that it is easier to focus on real issues.

5. Keeping system lightweight
Since the system is made for low-end machines, performance was always in mind while building it.
I tried to keep CPU and memory usage under control. For that, some parts were kept simple so that it can run smoothly on a normal laptop without causing any noticeable slowdown.

---

9. Conclusion

This project is about making a simple SIEM system. The idea was to check if basic monitoring can be done without using heavy tools.
While working on CyberSheildPro, it was observed that system activity can be tracked and alerts can be generated in a simple way. It is not very complex, but it still works for basic needs.
Features like continuous monitoring and simple log checking were used. These were kept basic so that the system does not become heavy.
During testing, it was working fine on a normal laptop. It was able to give useful alerts and did not slow down the system much.

9.1 Key Contributions

This project contributes in a few practical ways:
1. A simple real-time monitoring system was developed to track system and network activity
2. Log collection and basic analysis were implemented in one place
3. A lightweight detection approach was used instead of complex models
4. Alerts are generated in a controlled way to reduce confusion
5. The system is designed to run on low-end machines
6. A basic dashboard and logging system were added for better understanding

9.2 Research Hypothesis Validation

From the testing results, the initial assumptions are supported.

1. Real-time monitoring helped in faster detection compared to normal checking methods
2. The system was able to run without affecting performance much
3. Alert handling was improved by reducing unnecessary alerts

These points show that the system meets its main objective of being simple and usable.

9.3 Broader Implications

This project also gives some general understanding about how SIEM systems can be used in a simple way. The data suggests that a system's usefulness doesn't always depend on its complexity. Even basic monitoring can improve security, especially in smaller settings. Also, simple tools like this can be useful for learning as well as practical use. Small organizations can still use such systems without spending too much.

9.4 Limitations

There are a few limitations in the system:
1. The system uses simple rules, so it may miss completely new or unknown threats.
2. It was tested on a basic setup, so its performance in larger environments is not clearly known.
3. Features like AI or deeper analysis are not included in the current version.
4. Network-level monitoring is limited for now.
It is mainly suitable for small setups and may not work the same way at a larger scale

10 REFERENCES

[1] Md Liakat Ali, Kutub Thakur, Helen Barker, “The Rise of Artificial Intelligence: Industry Insights and Applications in Security Information and Event Management (SIEM)”, IEEE 13th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), October 2024.

[2] Hase, Linus, FH Wedel, "The Path to Choosing a SIEM System – A Systematic Literature Review", IT-Management of Digital Age, Germany, July 2024.

[3] Mary Jane C. Samonte, Pritz Lorraine F. Dorado, John Benjamin M. Dulay, Alain Marcus M. Levya, “Enhancing Threat Detection in Financial Institutions with AI-Driven Security Information and Event Management Integration”, 4th International Conference on Computer System (ICCS), September 2024.

[4] Zeyad Safaa Younus and Mafaz Alanezi, “Detect and Mitigate Cyberattacks Using SIEM", International Conference, December 2023.

[5] Konstantinos Bezas and Foteini Filippidou, "Comparative Analysis of Open-Source Security Information & Event Management Systems (SIEMs)", International Hellenic University, Indonesian Journal of Computer Science, Volume 12, Issue 2, April 2023.

[6] Adabi Raihan Muhammad, Parman Sukarno and Aulia Arif Wardana, "Integrated Security Information and Event Management (SIEM) with IDS based on Machine Learning, 4th International Conference on Industry and Smart Manufacturing, December 2023.

[7] Aleksandar Skendžić, Bozidar Kovačić, and Branko Balon, "Management and Monitoring Security Events in a Business Organization-SIEM System", 45TH Jubilee International Convention on Information, Communication & Electronic Technology (MIPRO), May 2023.

[8] Anish Sridharan and V. Kanchana, "SIEM Integration with SOAR", International Conference on Futuristic Technologies (INCOFT), November 2022.

[9] Tim Laue, Carsten Kleiner, Kai-Oliver Detken, Timo Klecker, "A SIEM Architecture for Multidimensional Anomaly Detection", 11TH IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Poland, September 2021.

[10] González-Granadillo, González-Zarzosa, and Diaz, "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures", published in the journal Sensors, Volume 21, Issue 14, July 2021.

[11] S M Mozammal Hossain, Russell Couturier, Jeff Rusk, "Automatic Event Categorizer for SIEM", Proceedings of the 31st Annual International Conference on Computer Science and Software Engineering (CASCON), Canada, November 2021.

[12] Pejman Najafi, Feng Cheng, and Christoph Meinel, SIEMA: Bringing Advanced Analytics to Legacy Security Information and Event Management, 17th EAI International Conference on Security and Privacy in Communication Networks, September 2021.

[13] Cosmin Măcăneață, "Overview of Security Information and Event Management Systems", Informatică Economică, Volume 28, Issue 1, 2024.

[14] Skendzic, A., Kovacic, B., & Balon, B., "Management and Monitoring Security Events in a Business Organization - SIEM system", 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO), May 2022.
[15] Evgenia Novikova and Igor Kotenko , "Analytical Visualization Techniques for Security Information and Event Management", Euromicro International Conference on Parallel, Distributed and Network-based Processing, 2013.
[16] S. Sandeep Sekharan and Kamalanathan Kandasamy , "Profiling SIEM Tools and Correlation Engines for Security Analytics", International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), March 2017.
[17] Vaishali Kumar, Abhishek Yadav, and Shivam Bhorde, "Securing Systems using SIEM and FIM Tools, International Journal of Scientific Research in Science and Technology, Volume 11, Issue 3, May 30, 2024.
[18] David R. Miller, "Security Information and Event Management (SIEM) Implementation", McGraw-Hill Higher Education,2011.