International Journal of Advanced Multidisciplinary Research and Educational Development ISSN: **3107-6513**
Volume 2, Issue 2 | March – April 2026 | www.ijamred.com

Digital Forensic Analysis of False Login Attempts Using System Artifacts

S. Priyanga[1], V. Yogashri[2]
[1,2]Department of Computer Science, Rathinam College of Arts and Science (Autonomous), Coimbatore, Tamil Nadu, India.
[1]Corresponding Author:priyanga2006seelan@gmail.com
[2]Corresponding Author:yogashri.cs@rathinam.in

Abstract:

The rapid increase in cyber threats has made system security a critical concern for individuals and organizations. Unauthorized access attempts, particularly brute-force attacks, often involve repeated login failures that can be detected through system logs. However, manual analysis of these logs is inefficient and time-consuming. This paper presents an automated digital forensic analysis system designed to detect failed login attempts using Windows system artifacts. The system focuses on Event ID 4625 from Windows Security Logs and applies user-based, time-based, and IP-based analysis techniques to identify suspicious behaviour. Threshold-based conditions are used to classify activities into different severity levels. The proposed system generates a structured forensic report that improves investigation efficiency and reduces manual effort. The results demonstrate that the system provides accurate detection of suspicious login patterns and enhances overall cybersecurity monitoring.

Keywords *-Digital Forensics, Cybersecurity, Log Analysis, Brute Force Attack, Event ID 4625, Python*

1. Introduction

In the modern digital era, the rapid growth of information technology has significantly increased the risk of cyber threats and unauthorized access attempts. Organizations and individuals rely heavily on computer systems to store and manage sensitive data, making system security a critical concern. One of the most common methods used by attackers to gain unauthorized access is through repeated login attempts using incorrect credentials, commonly known as brute-force attacks.

Operating systems such as Windows maintain detailed security logs that record various system activities, including login attempts. Among these, Event ID 4625 specifically represents failed login attempts and provides valuable information such as username, timestamp, and source IP address. These logs play an important role in digital forensic analysis, as they help in identifying suspicious behaviour and tracing potential security threats.

However, analysing these logs manually using tools like Event Viewer is time-consuming and inefficient, especially when dealing with large volumes of data. It becomes difficult to identify patterns such as repeated login attempts or abnormal user activity without automated support. This creates a need for an efficient system that can automatically process and analyse login data.

In this paper, an automated digital forensic analysis system is proposed to detect failed login attempts using Windows system artifacts. The system extracts and processes security logs and applies user-based, time-based, and IP-based analysis techniques to identify suspicious activities. Threshold-based detection is used to classify login behaviour, and a structured forensic report is generated to support investigation.

The proposed approach improves efficiency, reduces manual effort, and enhances the accuracy of detecting unauthorized access attempts, making it a useful solution for cybersecurity monitoring and forensic analysis.

In addition, the increasing number of cyber-attacks highlights the need for efficient monitoring systems that can detect threats at an early stage. Automated forensic analysis plays a key role in strengthening system security by providing quick and accurate identification of suspicious activities.

2. Existing System

In the existing system, the analysis of login attempts is performed manually using tools such as

Windows Event Viewer. System administrators and analysts must filter logs based on specific event IDs and examine each entry individually to identify failed login attempts.

This approach has several limitations. Firstly, it is time-consuming, especially when dealing with large volumes of log data. Secondly, it requires technical expertise to interpret the log information accurately. Additionally, identifying patterns such as repeated login attempts or suspicious behavior is difficult without automated support.

The existing system also lacks a structured reporting mechanism. Analysts are required to manually compile information, which increases the chances of human error. Furthermore, there is no automatic detection of abnormal login activity, making it difficult to identify potential brute-force attacks in real time.

Due to these limitations, the existing approach is inefficient and not suitable for modern cybersecurity requirements.

3. Proposed System

The proposed system is an automated digital forensic analysis tool designed to detect and analyse failed login attempts using Windows system artifacts. The system focuses on extracting and processing security logs, specifically Event ID 4625, which represents failed login attempts.

The system uses Python to automate the process of log collection, processing, and analysis. Initially, the required security logs are extracted from the Windows Event Viewer using system commands. The extracted data is then filtered to obtain relevant information such as username, timestamp, and source IP address.

After processing the data, the system performs multiple types of analysis to identify suspicious behaviour. User-based analysis is used to detect accounts with repeated failed login attempts. Time-based analysis helps in identifying multiple login attempts within short time intervals. IP-based analysis is performed to track repeated login attempts from the same source address.

To improve detection accuracy, threshold-based conditions are applied. If the number of failed login attempts exceeds predefined limits, the system classifies the activity as suspicious or potentially malicious.

Finally, the system generates a structured forensic report that includes details such as total failed login attempts, user-wise analysis, IP-based patterns, and detected suspicious activities. This automated approach reduces manual effort, improves efficiency, and enhances the accuracy of forensic investigations.

4. Literature Survey

In recent years, several studies have focused on improving system security through log analysis and monitoring techniques. Log analysis plays a crucial role in identifying unauthorized access attempts and detecting suspicious activities within a system.

Traditional approaches rely on manual log analysis using tools such as Windows Event Viewer. While these tools provide detailed information, they require significant time and effort to analyse large volumes of data. This makes it difficult to identify patterns such as repeated login attempts within short time intervals.

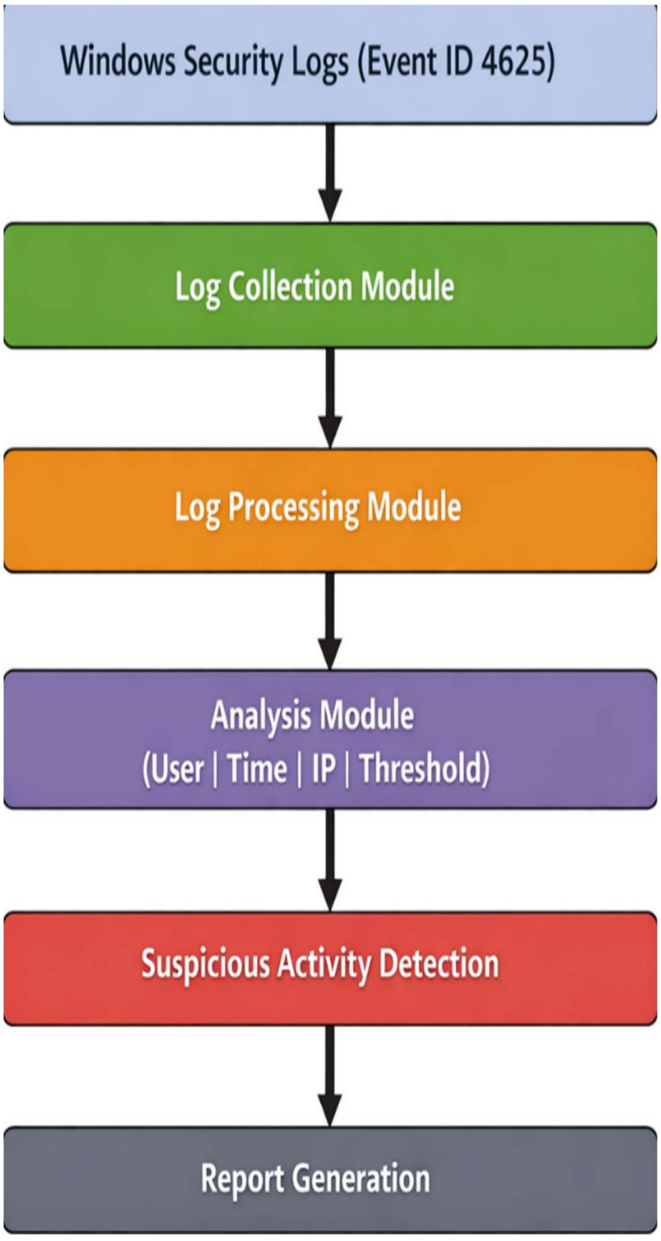
In large-scale environments, advanced systems such as Security Information and Event Management (SIEM) tools are used to monitor and analyse system logs. These tools provide automation and real-time monitoring capabilities. However, they are often expensive and require complex configuration, making them less suitable for small-scale or educational applications.

Recent research emphasizes the importance of automated log analysis systems that use rule-based and pattern-based techniques to detect suspicious behaviour. These systems improve efficiency and reduce manual effort.

The proposed system builds upon these concepts by providing a simple and cost-effective solution using Python. It focuses on analysing failed login attempts using Event ID 4625 and applies user-based, time-based, and IP-based techniques along with threshold-based detection to identify suspicious login behaviour.

5. Methodology

The proposed system follows a systematic methodology to analyse failed login attempts using Windows security logs. The entire process is divided into multiple stages, including log collection, log processing, data analysis, and report generation. Each stage plays an important role in ensuring accurate detection of suspicious login behaviour.



5.1 Log Collection

The first stage of the system involves collecting security log data from the Windows operating system. The system specifically targets Event ID 4625, which represents failed login attempts. These logs contain important details such as username, timestamp, and source IP address. The logs are extracted using system commands, ensuring that the required data is obtained efficiently without manual intervention.

5.2 Log Processing

Once the logs are collected, the next step is log processing. The raw log data contains a large amount of unstructured and irrelevant information, which needs to be filtered. The system processes the logs to extract only the required fields, such as user account name, login time, and network address. This step ensures that the data is clean, organized, and suitable for further analysis.

5.3 Analysis Techniques

After processing the data, the system performs detailed analysis using multiple techniques to identify suspicious behaviour. These techniques help in detecting patterns that may indicate unauthorized access attempts.

- **User-Based Analysis:** This method counts the number of failed login attempts associated with each user. Users with repeated login failures are identified as potential threats.
- **Time-Based Analysis:** This technique analyses login attempts based on time intervals. Multiple failed attempts within a short duration may indicate a brute-force attack.
- **IP-Based Analysis:** This method tracks login attempts originating from the same IP address. Repeated attempts from a single source are considered suspicious.
- **Threshold-Based Detection:** The system applies predefined threshold values to classify login activity. For example, more than three failed attempts may be considered suspicious, while more than six attempts may indicate a possible attack.

5.4 Report Generation

After completing the analysis, the system generates a structured forensic report. The report

includes details such as total failed login attempts, user-wise analysis, IP-based patterns, and detected suspicious activities. The report is designed to be clear and easy to understand, allowing system administrators and investigators to quickly identify potential threats and take necessary action.

6. Results and Discussion

The proposed system was tested using Windows security logs containing multiple failed login attempts. The system successfully extracted relevant information from Event ID 4625 and processed the data for further analysis. The extracted logs included details such as username, timestamp, and source IP address, which were used as the basis for detecting suspicious activities.

The results show that the system effectively identifies abnormal login patterns using different analysis techniques. Through user-based analysis, the system was able to detect user accounts with repeated login failures. These accounts were flagged as potentially suspicious, indicating possible unauthorized access attempts.

Time-based analysis played an important role in identifying rapid login attempts within short intervals. The system was able to detect patterns where multiple login failures occurred within a limited time frame, which is a common indicator of brute-force attacks. This helped in distinguishing normal user mistakes from malicious activities.

IP-based analysis further enhanced the detection capability of the system. By tracking login attempts originating from the same IP address, the system identified repeated attempts from specific sources. This allowed the system to detect suspicious behavior that may not be visible through user-based analysis alone.

The implementation of threshold-based detection improved the accuracy of classification. When the number of failed login attempts exceeded predefined limits, the system classified the activity as suspicious or potentially malicious. This approach ensured that only abnormal behavior was flagged, reducing false positives.

Compared to manual log analysis, the automated system significantly reduces the time required for investigation. Manual methods require continuous monitoring and detailed inspection of logs, whereas the proposed system performs analysis automatically and provides results in a structured format. This improves efficiency and minimizes human error.

The generated forensic report presents the results in a clear and organized manner. It includes total failed login attempts, user-wise details, IP-based patterns, and detected suspicious activities. This makes it easier for system administrators and investigators to understand login behaviour and take appropriate action.

Overall, the system demonstrates reliable and efficient performance in analysing failed login attempts. It provides an effective solution for detecting unauthorized access attempts and supports digital forensic investigations in cybersecurity environments.

6.1 Performance Analysis

The performance of the proposed system was evaluated based on its ability to detect suspicious login attempts accurately and efficiently. The system was able to process large volumes of log data without significant delay, demonstrating good performance in real-time analysis scenarios.

The use of multiple analysis techniques improved the overall detection capability. User-based analysis helped in identifying targeted accounts, while time-based analysis was effective in detecting rapid login attempts within short durations. IP-based analysis further enhanced the detection process by identifying repeated attempts from specific sources.

The system also demonstrated efficiency in reducing the time required for analysis compared to manual methods. Automated processing ensures faster detection and consistent results, making the system suitable for practical cybersecurity applications.

7. Conclusion

This paper presented an automated digital forensic analysis system for detecting failed login attempts using Windows system artifacts. The system focuses on analysing Event ID 4625 and applies multiple techniques, including user-based, time-based, and IP-based analysis, to identify suspicious login behaviour.

The proposed system successfully automates the process of log collection, processing, and analysis. By

eliminating the need for manual inspection of large volumes of log data, the system significantly reduces the time and effort required for forensic investigations. It also improves the accuracy of detection by minimizing human errors and providing consistent results.

The implementation of threshold-based detection enables the system to classify login activities into different levels of severity. This helps in identifying potential brute-force attacks and unauthorized access attempts effectively. The structured forensic report generated by the system provides clear insights into login patterns, making it easier for system administrators and investigators to understand and respond to security threats.

Overall, the system serves as a reliable and efficient solution for monitoring login activities and enhancing system security. It is suitable for use in cybersecurity environments where continuous monitoring and quick detection of suspicious behaviour are essential.

8. Future Scope

The proposed system can be further improved by implementing real-time monitoring and alert mechanisms to detect suspicious login attempts instantly. This would enable faster response to potential security threats and improve system protection.

Additional enhancements such as graphical data visualization can be incorporated to present analysis results in a more user-friendly manner. Integration with intrusion detection systems and advanced security tools can further improve the effectiveness of the system.

The system can also be extended to support other types of security events and logs, making it a more comprehensive solution for digital forensic analysis and cybersecurity monitoring.

9.References

1. Microsoft Corporation, *Windows Security Log Events Documentation*, Available: https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4625
2. Nelson, B., Phillips, A., and Steuart, C., *Guide to Computer Forensics and Investigations*, Cengage Learning, 5th Edition, 2018.
3. Casey, E., *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, Academic Press, 3rd Edition, 2011.
4. Behl, A., *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, 2017.
5. Scarfone, K., and Mell, P., *Guide to Intrusion Detection and Prevention Systems (IDPS)*, National Institute of Standards and Technology (NIST), 2007.
6. Kent, K., Chevalier, S., Grance, T., and Dang, H., *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication 800-86, 2006.
7. Stallings, W., *Network Security Essentials: Applications and Standards*, Pearson Education, 6th Edition, 2016.
8. Garfinkel, S., *Digital Forensics Research: The Next 10 Years*, Digital Investigation Journal, 2010.
9. Bejtlich, R., *The Practice of Network Security Monitoring*, No Starch Press, 2013.
10. Bishop, M., *Computer Security: Art and Science*, Addison-Wesley, 2003.
11. NIST, *Computer Security Incident Handling Guide*, Special Publication 800-61, 2012.
12. Chuvakin, A., Schmidt, K., and Phillips, C., *Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management*, Syngress, 2012.