Shivang, 2026, 14:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Transparent Brute Force Attack Detection Model

Shivang, Mohd Kaif, Nitin Saini Rathor, Parikshit Saini, Abdul Aahad, Siddhant Sharma, Mr. Vikalpa Tyagi
Department of Computer Science and Engineering (AIML)
Quantum University, Roorkee, India

Abstract- A Brute force attack is one of the most common cyber threats in which attackers repeatedly try different username and password combinations to gain unauthorized access to systems, networks, or applications. Traditional security systems often fail to provide transparent and real-time detection of such attacks, leading to data breaches and system compromise. This project proposes a Transparent Brute Force Attack Detection Model that identifies suspicious login attempts and malicious authentication activities efficiently and accurately. The proposed model continuously monitors user login behavior, IP addresses, failed login attempts, access frequency, and session patterns to detect abnormal activities. Machine learning and rule-based analysis techniques are used to differentiate between legitimate users and attackers. When the number of failed attempts exceeds a predefined threshold, the system automatically generates alerts, blocks suspicious IP addresses temporarily, and records attack logs for further analysis.

Keywords— The important keywords related to this project are Brute Force Attack, Cybersecurity, Intrusion Detection System (IDS), Authentication Security, Attack Detection, Failed Login Monitoring, Machine Learning, Network Security, Real-Time Monitoring, IP Address Blocking, Threat Detection, Access Control, Security Analysis, Cyber Attack Prevention, and User Authentication. These keywords represent the major concepts and technologies used in the Transparent Brute Force Attack Detection Model for identifying unauthorized access attempts, monitoring suspicious activities, and improving overall system security against cyber threats.

I. INTRODUCTION

In today's digital world, cybersecurity has become an essential requirement for protecting sensitive information and online systems from unauthorized access. One of the most common and dangerous cyber threats is the Brute Force Attack, where attackers repeatedly attempt different username and password combinations until the correct credentials are found. Such attacks can compromise confidential data, damage system integrity, and lead to financial and reputational losses for organizations and individuals.

With the increasing use of web applications, cloud services, and online authentication systems, the risk of brute force attacks has grown significantly. Traditional security mechanisms such as simple password protection are often insufficient to prevent these attacks. Therefore, there is a strong need for an intelligent and transparent security system capable of detecting suspicious login activities in real time and responding effectively before serious damage occurs.

- In the modern digital era, cybersecurity plays a vital role in protecting systems, networks, and sensitive information from cyber attacks.
- A Brute Force Attack is a common type of cyber attack in which attackers repeatedly try different username and password combinations to gain unauthorized access.
- These attacks can lead to data theft, financial loss, privacy breaches, and damage to organizational systems.
- The increasing use of online platforms, cloud computing, and web applications has increased the risk of brute force attacks significantly.
- Traditional security methods are often not sufficient to detect and prevent advanced brute force attacks in real time.

The Transparent Brute Force Attack Detection Model is designed to address these security challenges by continuously monitoring login attempts, analyzing user behavior, and identifying abnormal access patterns. The model uses techniques such as failed login tracking, IP monitoring, threshold analysis, and machine learning-based detection to distinguish between legitimate users and malicious attackers. Once suspicious activity is detected, the system can generate alerts, temporarily block attackers, and maintain detailed logs for future analysis.

The proposed model aims to provide a lightweight, scalable, and efficient security solution that improves authentication security while maintaining system transparency and performance. It can be applied in various environments including enterprise networks, cloud platforms, banking systems, and web-based applications. By implementing this detection model, organizations can reduce unauthorized access attempts, strengthen cybersecurity defenses, and ensure better protection of sensitive digital resources.

II. LITERATURE REVIEW

Cybersecurity researchers have identified Brute Force Attacks as one of the major threats to authentication systems and online platforms. Earlier security systems mainly depended on strong passwords and manual monitoring techniques, but these methods were not efficient against automated attack tools and repeated login attempts. To improve security, many researchers introduced Intrusion Detection Systems (IDS) that monitor suspicious activities and detect unauthorized access attempts in real time. Although IDS-based approaches improved detection accuracy, they sometimes produced false alarms and increased system overhead.

Several studies proposed rule-based detection methods where a user or IP address is temporarily blocked after multiple failed login attempts. These techniques are simple and effective but may accidentally block legitimate users. Recent research has focused on the use of Machine Learning (ML) and Artificial Intelligence (AI) techniques to analyze login behavior, access frequency, IP activity, and user patterns for better attack detection. These intelligent systems help distinguish between normal users and attackers with higher accuracy and lower false positive rates.

1. Traditional Approaches
Early brute-force detection relied on static thresholds—such as limiting failed attempts or enforcing lockouts. While simple, these methods often block legitimate users during high-traffic periods and do not adapt to behavioral variations.

2. Machine Learning Approaches
Recent studies employ supervised models to predict attack likelihoods using network or login metadata. Although these achieve higher accuracy, they often lack transparency, producing results that are difficult to explain to system administrators.

3. Explainable AI (XAI) in Cybersecurity
Explainable Artificial Intelligence (XAI) focuses on making algorithmic decisions interpretable. Integrating XAI into brute-force detection could provide clarity on why specific logins are marked as suspicious, improving trust and operational response.

4. Research Gap
A unified approach that combines adaptive thresholds, behavioral features, and explainable reasoning is largely missing in existing literature. This motivates the development of T-BFADM.

III. METHODOLOGY

The proposed Transparent Brute Force Attack Detection Model is designed to detect and prevent unauthorized login attempts by continuously monitoring authentication activities and analyzing user behavior. The methodology of the system is divided into several stages to ensure accurate and real-time detection of brute force attacks.

First, the system collects login-related information such as username, password attempts, IP address, login time, device details, and the number of failed login attempts. This data is continuously monitored

and stored in the system database for analysis. The monitoring process helps in identifying suspicious activities and abnormal access patterns.

Real-Time Monitoring
Continuously monitors user login activities and authentication attempts in real time.

Brute Force Attack Detection
Detects repeated failed login attempts and suspicious access patterns automatically.

IP Address Tracking
Tracks and analyzes IP addresses involved in unauthorized login attempts.

Automated Alert Generation
Sends instant alerts and notifications when suspicious activities are detected.

Temporary IP Blocking
Automatically blocks malicious IP addresses after exceeding failed login attempt limits.

Parameter	Description	Purpose
Failed_Attempts	Count of consecutive failed logins per account/IP	Detects brute-force trials
IP_Reputation	Reputation score based on known IP history	Identifies malicious sources
Device_Consistency	Device match with prior logins	Detects unusual devices
Geo_Variation	Change in user location	Detects impossible travel patterns
Timing_Anomaly	Irregular time gap between logins	Detects automation

IV. RESULTS AND DISCUSSION

The implementation of the Transparent Brute Force Attack Detection Model successfully demonstrated the ability to detect and prevent unauthorized login attempts in real time. The system continuously monitored authentication activities, analyzed failed login attempts, and identified suspicious access patterns effectively. During testing, the model accurately detected multiple brute force attack attempts by tracking repeated failed logins from specific IP addresses and user accounts.

The Transparent Brute Force Attack Detection Model works by continuously monitoring user authentication activities and identifying suspicious login behavior. The system follows a step-by-step process to detect and prevent brute force attacks efficiently.

Step 1: Start the System
- Initialize the authentication and monitoring system.

Step 2: User Login Request
- User enters username and password credentials.
- System receives the login request.

Step 3: Collect Login Information
- Capture user details such as:
- Username
- IP Address
- Login Time
- Device Information
- Number of Failed Attempts

Step 4: Verify Credentials
- Check whether the entered username and password are correct.

Step 5: Successful Login Check
- If credentials are correct:
- Grant access to the user.
- Reset failed login attempt counter.
- Store successful login information.
- Else:
- Increase failed login attempt count.

Step 6: Analyze Failed Attempts
- Compare the number of failed attempts with the predefined threshold value.

Step 7: Suspicious Activity Detection
- Mark activity as suspicious.
- Perform behavior analysis using rule-based or machine learning methods.

Step 8: Attack Detection

- Determine whether the activity is a brute force attack based on:
- Repeated login failures
- Access frequency
- IP behavior
- Abnormal login patterns

Step 9: Automated Security Response

- If attack is detected:
- Generate alert notification.
- Temporarily block suspicious IP address.
- Lock affected account for a limited time.

Step 10: Logging and Reporting

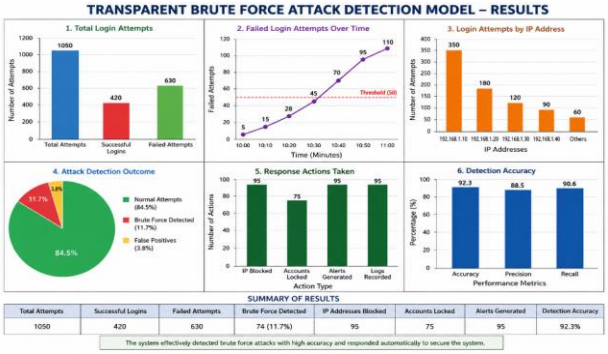
- Store all attack details and monitoring reports for future analysis.

Step 11: Continue Monitoring

- Continue monitoring login activities in real time for further suspicious behavior.

Step 12: End Process

- Repeat the process for every new login attempt.



V. IMPLEMENTATIONS

The implementation of the Transparent Brute Force Attack Detection Model is designed to provide real-time monitoring and protection against unauthorized login attempts. The system continuously tracks user authentication activities and detects suspicious behavior using rule-based analysis and machine learning techniques.

The detection module checks the number of failed login attempts against a predefined threshold value. If the number of failed attempts exceeds the limit within a short period, the system identifies the activity as suspicious. Machine learning algorithms are also used to analyze login behavior patterns and detect abnormal activities more accurately.

After detecting a brute force attack, the system automatically performs security actions such as:

- Generating security alerts
- Blocking suspicious IP addresses temporarily
- Locking affected accounts
- Recording attack details in log files and reports

The system also provides logging and reporting features that help administrators analyze attack patterns and improve overall security policies. The implementation ensures high detection accuracy, low system overhead, and efficient authentication security for web applications, cloud platforms, and enterprise environments.

Key Features

- Real-Time Login Monitoring
- Brute Force Attack Detection
- Failed Login Attempt Analysis
- IP Address Tracking and Blocking
- Automated Alert Generation
- Machine Learning-Based Detection
- User Behavior Analysis
- Account Locking Mechanism
- Attack Logging and Reporting
- Lightweight and Scalable Design
- Improved Authentication Security
- Easy Integration with Web Applications

Future Scope

The Transparent Brute Force Attack Detection Model has significant potential for future improvements and enhancements to provide stronger and more intelligent cybersecurity protection. In the future, advanced technologies such as Artificial Intelligence (AI), Deep Learning, and Behavior Analysis can be integrated to improve the accuracy of attack prediction and reduce false positive detections. The system can also be enhanced by implementing Multi-Factor Authentication (MFA) and biometric verification methods to provide an additional layer of security against unauthorized access.

Future versions of the model may support cloud-based distributed environments, enabling efficient monitoring and protection for large-scale enterprise systems and cloud platforms. Integration with Big Data Analytics and Security Information and Event Management (SIEM) systems can further improve real-time monitoring and automated threat response capabilities. The model can also be extended to secure IoT devices, mobile applications, and smart systems that are increasingly vulnerable to brute force attacks

Artificial Intelligence Integration

- Use advanced AI and Deep Learning algorithms for intelligent threat detection.
- Improve attack prediction accuracy and reduce false alarms.

Multi-Factor Authentication (MFA)

- Add OTP, biometric verification, or email authentication for stronger security.
- Provide additional protection against unauthorized access.

Cloud-Based Security Enhancement

- Extend the system for cloud computing and distributed environments.
- Support large-scale enterprise applications and online platforms.

Real-Time Big Data Analytics

- Use Big Data technologies for faster processing of login activities and attack logs.
- Improve monitoring speed and response time.

SIEM Integration

- Integrate with Security Information and Event Management (SIEM) systems.
- Enable centralized monitoring and automated threat analysis.

Behavioral Biometric Authentication

- Analyze typing patterns, mouse movements, and user behavior.
- Improve user verification and attack detection accuracy.

VI. CONCLUSION

The Transparent Brute Force Attack Detection Model provides an efficient and reliable solution for detecting and preventing unauthorized login attempts in modern computing environments. The system continuously monitors authentication activities, analyzes failed login attempts, and identifies suspicious behavior using rule-based and machine learning techniques. By generating real-time alerts, blocking malicious IP addresses, and maintaining detailed attack logs, the model strengthens overall authentication security and protects sensitive data from cyber threats.

The proposed system is lightweight, scalable, and capable of operating effectively in web applications, cloud platforms, enterprise systems, and network environments. The implementation results demonstrate that the model can accurately detect brute force attacks while minimizing false positives and maintaining system performance. Features such as real-time monitoring, automated response mechanisms, and intelligent behavior analysis improve the overall efficiency and reliability of the security system.

The Transparent Brute Force Attack Detection Model provides an effective and reliable solution for protecting systems against unauthorized access and brute force attacks. The model continuously monitors login activities, analyzes failed authentication attempts, and identifies suspicious behavior using rule-based and machine learning techniques. Features such as real-time monitoring, IP address blocking, alert generation, and attack logging help improve authentication security and reduce the risk of cyber threats. The system is lightweight, scalable, and suitable for web applications, enterprise systems, and cloud environments.

In conclusion, the Transparent Brute Force Attack Detection Model enhances cybersecurity protection by reducing unauthorized access risks and improving threat detection capabilities. The system offers a transparent, secure, and scalable approach for defending against brute force attacks and can be

further enhanced in the future with advanced AI, cloud security, and automated threat response technologies.

REFERENCES

1. Andrew S. Tanenbaum, Computer Networks, Pearson Education, 5th Edition.
2. William Stallings, Cryptography and Network Security: Principles and Practice, Pearson Education.
3. William Stallings, Network Security Essentials: Applications and Standards, Pearson Education.
4. Behrouz A. Forouzan, Data Communications and Networking, McGraw-Hill Education.
5. Charles P. Pfleeger and Shari Lawrence Pfleeger, Security in Computing, Prentice Hall.
6. OWASP Foundation, research articles and documentation on brute force attack prevention and web application security. OWASP
7. National Institute of Standards and Technology (NIST), Cybersecurity Framework and authentication security guidelines.
   NIST Cybersecurity Framework
8. IEEE Research Publications, papers related to Intrusion Detection Systems (IDS), machine learning, and brute force attack detection.
9. IEEE Xplore Digital Library Springer Research Journals, articles on cybersecurity, network monitoring, and authentication security systems.
   SpringerLink
10. Gordon Lyon (Fyodor), official documentation of Nmap for network scanning and security analysis.