AOI :10.100.234513.0236
13th international conference on Microelectronics Circuits and Systems, Micro2026

A Machine Learning Based Framework for Detection and Prevention of Brute-Force Attacks

Shivansh Ojha, Azath M., Ashwin Gupta

School of Computer Science and Engineering
Galgotias University, Greater Noida, India
Corresponding Author: ojha.shivansha135@gmail.com

ABSTRACT

Brute-force attacks are the most common type of attacks to gain unauthorized access. The use of some of the most common brute-forcing tools includes "Hydra", "John the Ripper", "Hashcat" and "Aircrack-ng". These are some automated tools that are used nowadays to crack username and password through continuous attempt to guess the credentials using a file which is called a wordlist. A wordlist contains all the possible list of words and combination of letters, numbers or characters that could be the username or password. The traditional way of rate limiting or account lockout policy is mostly futile against new technological advancements of Brute-Force attacks that closely imitate legitimate user conduct. "Anomaly detection refers to the problem of finding patterns in data that do not conform to expected behaviour."[6] This research proposes a Brute-force Prevention Framework that uses Machine-Learning to prevent attacks. A dataset of 50,000 authentication logs was generated, that contained legitimate user logs as well as attackers. It uses the mechanism of differentiating through different factors that include number of failed attempts, time interval between attempts, IP address and session behaviour. It uses authentication logs and typical user conduct to differentiate between a legitimate user and an intruder who is trying to brute-force credentials to gain unauthorized access. Multiple classification algorithms were used, in which Random Forest model achieved highest accuracy with staggering 96.4%, 94% precision and only 4.3% false positives. After experimental analysis, we found out that machine learning models keep improving their detection accuracy to the point where the chances of trespassing become minimal. This project provides an intelligent and adaptive solution for securing systems against these types of attack.

Keywords—Brute-force attacks, Machine Learning, Authentication Security, Intrusion Detection.

I. INTRODUCTION

In this era of technological advancements and surge of digital services, security and privacy of one's personal information has become a major requirement. Today's world heavily relies on Internet, with almost two third of total population of the world thriving on social media. Personal data and information of millions of people depend upon the security frameworks that are used to keep that data secure. Despite these advancements in cryptography and other security mechanisms, Brute-Force attacks continue being a serious threat to every Internet Service that requires the user to create an account and store their data. Most common type of attack, and yet still widely used by malicious agents to pose a severe threat to the internet society indicates that we are still technically behind on security sector of this digital world.

Brute-Force attacks are carried out by automated tools that require a wordlist to guess the login credentials of a user. This type of tool keeps on trying different sets of username and password combination until it succeeds to discover valid credentials. Weak and Re-used credentials further escalate the risk. Traditional methods of stopping these attacks include rate-limiting and account lockout policies which are useful against basic attacks but fail to make any impact against advanced brute-forcing tools that imitate legitimate user actions. "Account lockout mechanisms can introduce denial-of-service vulnerabilities if not carefully implemented."[5] This is where Machine learning comes into play, a framework trained to learn from past data and behaviour pattern. This type of framework can detect even smallest of anomaly that are caused by brute-force attacks, differentiating between a legitimate user and an intruder. This research focuses on development and evaluation of machine learning based framework that can mitigate the treat of brute-force attacks efficiently. The previous machine-learning based intrusion detection models detect unusual network traffic rather than authentication logs. This lack of targeted detection, make a research gap. This research bridges that gap by evaluating authentication log data using classification framework. "Authentication systems should be designed to resist online guessing attacks, including brute-force and credential stuffing attempts."[4]

II. OBJECTIVES

Main objectives of this research are:-

- To identify how brute-force mechanism works.
- To develop a Machine learning-based detection system.

ISBN: 978-81-985770-0-9

- To identify and extract relevant security patterns and features.
- To test different machine learning techniques and algorithms for detection of these attacks.
- To prevent these attacks in real-time automatically.
- To improve detection accuracy while reducing false positives.

III. LITERATURE REVIEW

Earlier the intrusion detectors heavily relied on signature-based mechanisms, which required updates every now and then, also inconsistent and ineffective against zero-day attacks [1] (exploitation of a vulnerability unknown to the developer). Better detection mechanisms were also introduced but were ineffective against intelligent intruders. The recent studies indicate that machine learning based frameworks can be a game changer in detection and prevention of these attacks. Learning techniques like Decision Trees, Support Vector Machines, and Random Forests have been widely used for anomaly detection. These studies also indicate that analysis of login patterns provides better detection accuracy than static rules. Many researchers have emphasised the effectiveness of group learning methods that helps in reduction of false positives and enhancing generalization. Still, many existing systems focus mainly on detection of these attacks rather than prevention in real time. This study aims to bridge that gap by combining detection and prevention in one unified framework.

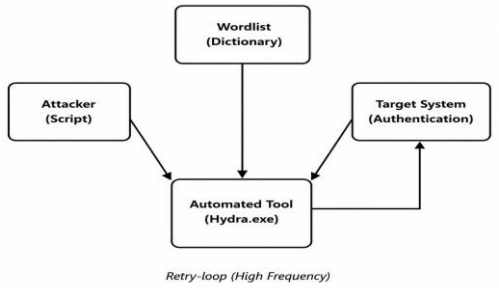

Fig. 1. The workflow of how a brute-force attack is conducted using automated tools that utilize wordlists to test credentials until a valid one is discovered.

IV. METHODOLOGY

A. *Dataset Preparation*

The data of 50,000 authentication logs were processed to remove the irrelevant data, delete an incomplete row if not critical, resizing all numbers to a specific scale. The dataset is then categorized as follows:

- Legitimate login conduct
- Brute-force attack conduct

60% of these logs contain legitimate user which include occasional Failed login attempts. The remaining 40% are brute-force attacks that are done with the help of automated scripts that attempt credential combinations at high frequency rate.

B. *Feature Selection*

This is performed to enhance model performance and reduce overfitting. This helps as model act on basis of more important information rather and filtering the trash. "Precision is the proportion of predicted positives that are correctly real positives, while recall is the proportion of real positives that are correctly predicted."[8]

TABLE I
FEATURE EXTRACTED

Feature	Description
Failed Login Counts	Number of attempts in last 5 minutes.
Time Between Attempts	Interval between consecutive login tries
IP Address Change	Number of IPs used
Username Attempt Frequency	Attempt per username
Login Session Duration	Time spent before log out.

C. *Machine Learning Algorithm*

The learning algorithms evaluated are as follows [3]:

- Logistic Regression
- Decision Tree Classifier
- Random Forest Classifier
- Support Vector Machine

TABLE II
MACHINE LEARNING ALGORITHMS USED

Algorithm	Purpose
Logistic Regression	Binary classification
Decision Tree	Pattern-based detection
Random Forest	Ensemble attack detection
Support Vector Machine	Margin-based classification

It is noticed that grouping methods exhibit better performance due to their ability of handling complex patterns. "Random forests are an ensemble learning method for classification and regression that operate by constructing a multitude of decision trees."[7]

Mathematical Model

$$P(y = 1 \mid x) = 1 / (1 + e^{-(w^T x + b)}) \quad (1)$$

where,

x = feature vector
b = bias term
w = learned weight

ISBN: 978-81-985770-0-9

V. SYSTEM ARCHITECTURE

A. Data Collection Module

This module is responsible for collecting the auto logs from servers, applications or network devices. The data include: Username, Timestamp, Source IP address, Login success or failure, Session duration.

B. Extraction Module

The raw logs are executed to make up meaningful features like: Attempt count of failed login, Time gap between the attempts, Frequency of attempts, Behaviour of IP address, Failed to successful login ratio.

C. Machine Learning Engine

In this module, the features that have been made up are introduced to the learning models which have been trained to differentiate the login behaviour between normal or malicious.

D. Detection Module

The trained model examines login attempts in real time and recognises attacks based on learned pattern.

E. Prevention Module

After attack detection, the framework automatically prevents the intruder to try more attempts using IP Blocking, CAPTCHA, or Account lockout.

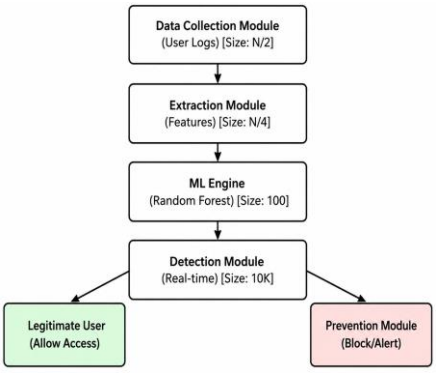

Fig. 2. The machine learning framework which is proposed. The data pipeline that moves from raw log collection to feature extraction to the Random Forest-based detection engine, which classifies them into categories such as malicious or legitimate in real time.

VI. EXPERIMENTAL RESULTS AND EVALUATION

The evaluation of machine learning performance is based on detection accuracy and precision, recall, and F-1 score. After an experimental research, it is observed that Random Forest achieves the highest accuracy. The system productively detects high as well as low-frequency brute-force attacks. This experiment was performed using Python with scikit-learn library on system with Intel i5 processor and 16 GB RAM. Random Forest training time was 2.4 seconds and average inference latency per login attempt was approx. 3 milliseconds.

VII. PREVENTION STRATEGY

After attack detection, the system initiates automated responses including:

- Temporary or permanent IP address blocking
- Repeated anomaly triggers account lockout
- Enforcement of CAPTCHA
- System Administrators are alerted

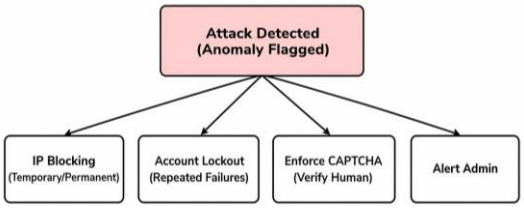

Fig. 3. This is the fully automated response logic that detects an anomaly that devises different strategies on based of the anomaly and finally alerts the administrator about the attack.

VIII. ADVANTAGES OF PROPOSED SYSTEM

- It is self-learning detection and prevention system.
- High detection accuracy
- Reduced false positives
- Scalability for real-time environments
- Capability to detect unknown attack patterns

IX. LIMITATIONS AND FUTURE SCOPE

The quality and diversity of training data decides the performance of system [2]. The future advancements may include: Better learning models for improved detection and prevention accuracy, Real-time distribution in cloud environments, SIEM platforms integrations, Using Federated Learning for detection while maintaining privacy. "Federated learning enables multiple parties to collaboratively train a machine learning model without sharing their raw data."[9]

X. RESULTS

TABLE III
COMPARISON TABLE

Model	Accuracy	Precision	Recall	F1-score
Logistic Regression	91.2%	89.5%	90.1%	89.8%
SVM	93.0%	92.2%	91.8%	92.0%
KNN	90.6%	88.9%	89.5%	89.2%
Random Forest	96.4%	95.1%	96.0%	95.5%

ISBN: 978-81-985770-0-9

TABLE IV
BASELINE COMPARISON

Method	Detection Rate	False Positive Rate
Rate Limiting Only	72%	18%
Account Lockout	81%	22%
Proposed ML System	96.4%	4.3%

XI. CONCLUSION

This study exhibits that brute-force prevention using machine learning in real time is much more effective than the traditional-used methods. The experimental results demonstrated that Random Forest does better than any other classifier, achieving 96.4% accuracy with a low false positive rate. Through learning authentication user behaviour patterns, it eliminates the static methods that require human intervention for preventing the attacks. This automated framework that detects and prevents in real-time overall strengthens the data security and prevents day to day cyber-attacks that shake up one's life.

REFERENCES

[1] NIST, Digital Identity Guidelines: Authentication and Lifecycle Management (SP 800-63B), National Institute of Standards and Technology, Gaithersburg, MD, USA, 2017, p. 32.

[2] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in Proc. IEEE Symp. Security and Privacy, Oakland, CA, USA, 2010, pp. 305–316.

[3] S. K. B. Sangeetha, S. K. Mathivanan, M. Azath, R. Beniwal, N. Ahmad, W. Ghribi, and S. Mallik, "Advanced segmentation method for integrating multi-omics data for early cancer detection," Egyptian Informatics Journal, vol. 29, p. 100624, 2024.

[4] M. Azath and T. Kiros, "Statistical machine translator for English to Tigrigna translation," International Journal of Scientific & Technology Research, vol. 9, no. 1, pp. 2095–2099, Jan. 2020, ISSN 2277-8616.

[5] F. Pedregosa et al., "Scikit-learn: Machine learning in Python," Journal of Machine Learning Research, vol. 12, pp. 2825–2830, 2011.

[6] P. Kairouz et al., "Advances and open problems in federated learning," Foundations and Trends® in Machine Learning, vol. 14, no. 1–2, pp. 1–210, 2021.

[7] M. Getahun, M. Azath, D. P. Sharma, A. Tuni, and A. Adane, "Efficient energy utilization algorithm through energy harvesting for heterogeneous clustered wireless sensor network," Wireless Communications and Mobile Computing, vol. 2022, Art. no. 4154742, 2022, doi: 10.1155/2022/4154742.

[8] M. Zekiwos, M. Azath, and A. Bruck, "Deep learning-based image processing for cotton leaf disease and pest diagnosis," Journal of Electrical and Computer Engineering, vol. 2021, Article ID 9981437, 10 pages, 2021, doi: 10.1155/2021/9981437.

[9] Faiz, M., Mounika, B. G., Akbar, M., & Srivastava, S. (2024). Deep and machine learning for acute lymphoblastic leukemia diagnosis: a comprehensive review. ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal, 13, e31420-e31420.

[10] Narayan, V., Srivastava, S., Mishra, V. K., Faiz, M., Sharma, S., Balyan, V., & Gupta, G. (2025). Multivariate Lifetime Prediction Model for Energy Efficient Region-Based Wireless Sensor Network. IET Wireless Sensor Systems, 15(1), e70015.

[11] Faiz, M., & Daniel, A. K. (2022). Threats and Challenges for Security Measures on the Internet of Things. Law, state & telecommunications review/revista de direito, estado e telecomunicações, 14(1).

[12] G. Nemomsa and M. Azath, "Designing a predictive model for antiretroviral regimen at the antiretroviral therapy center in Chiro Hospital, Ethiopia," Journal of Healthcare Engineering, vol. 2021, Art. no. 1161923, 2021, doi: 10.1155/2021/1161923.

[13] Narayan, V., Srivastava, S., Mishra, V. K., Faiz, M., Sharma, S., Balyan, V., & Gupta, G. (2025). Multivariate Lifetime Prediction Model for Energy Efficient Region-Based Wireless Sensor Network. IET Wireless Sensor Systems, 15(1), e70015.

[14] Alotibi, N., & Alshammari, M. (2023). Deep learning-based intrusion detection: A novel approach for identifying brute-force attacks on FTP and SSH protocol. International Journal of Advanced Computer Science and Applications, 14(6).

Cite this article as:

Shivansh Ojha, Azath M. and et. al."A Machine Learning Based Framework for Detection and Prevention of Brute-Force Attacks" Proceedings of 13th international conference on Microelectronics, Circuits and Systems, Micro2026.

Displayed as online on 06th July 2026.

Link:http://actsoft.org/science/micro2026-pro/34-micro2026.pdf

ISBN: 978-81-985770-0-9