Journal of Al-Turath University College (JATUC)
Open Access Journal
ISSN: 2074-5621
https://jatuc.uoturath.edu.iq/

Adaptive Brute Force Attack Detection Based On Behavioral Profiling And Machine Learning

Uqba bn Nafaa Mohammed*

Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq.

**Correspondence email*: uqba80@uomustansiriyah.edu.iq

KEYWORDS
Adaptive threshold; Anomaly detection; Behavioral analysis; Brute force Attack; cybersecurity

ABSTRACT
In addition to the growing use of digital services, brute force accesses are now popular ways of breaching the security of the information and integrity of the system. Traditional detection systems, such as simple threshold-based systems, have a large false positive rate and will not react to legitimate user behavior, particularly to low-rate stealthy attacks. The paper proposes an intelligent and dynamic brute force login attempt identification system that is composed of behavioral analytics, machine learning (Isolation Forest and LSTM), and adaptive thresholding. As experimental results on synthetic and real authentication log datasets show, the proposed framework works: In synthetic datasets (60 attacks injected), the hybrid framework was able to identify all attacks with Recall = 1.0, Precision = 0.92 and F1-Score = 0.96, with a larger decrease in false positives than the approaches of using only static thresholds. The model obtained Recall = 1.0, Precision = 0.92 and F1-Score = 0.96 on 10,000-login attempt logs with 34 known attacks and high-frequency and low-rate stealthy attacks. Overfitting was also prevented using cross-validation, feature normalization, and dropout of LSTM, and early stopping and strong generalization was demonstrated to unseen data. The proposed framework contributes an efficient, scalable, and context-sensitive framework for the real-time detection of brute force attacks, and it demonstrates a significant enhancement over the traditional techniques and a foundation for an intelligent system in intrusion detection in the future.

الكلمات المفتاحية
هجوم القوة الغاشمة؛ الأمن السيبراني؛ تعلم الآلة؛ التحليل السلوكي؛ العتبة التكيفية؛ كشف الشذوذ

الملخص
بالإضافة إلى التوسع المتزايد في استخدام الخدمات الرقمية، أصبحت هجمات القوة الغاشمة (Brute Force) من الأساليب الشائعة لاختراق أمن المعلومات وسلامة الأنظمة. تعاني أنظمة الكشف التقليدية، مثل الأنظمة المعتمدة على العتبات الثابتة البسيطة، من ارتفاع معدل الإنذارات الكاذبة، كما أنها لا تتفاعل بشكل فعّال مع سلوك المستخدم الشرعي، خصوصًا في الهجمات الخفية منخفضة المعدل. تقترح هذه الورقة نظامًا ذكيًا وديناميكيًا للتعرّف على محاولات تسجيل الدخول باستخدام هجمات القوة الغاشمة، يعتمد على التحليل السلوكي وتقنيات تعلم الآلة (مثل Isolation Forest وLSTM) بالإضافة إلى العتبات التكيفية. تُظهر النتائج التجريبية على مجموعات بيانات مصطنعة وحقيقية لسجلات المصادقة فعالية الإطار المقترح؛ إذ في مجموعات البيانات المصطنعة (مع إدخال 60 هجومًا)، تمكّن الإطار الهجين من اكتشاف جميع الهجمات بمعدل استدعاء (Recall) قدره 1.0، ودقة (Precision) بلغت 0.92، وقيمة F1-Score مقدارها 0.96، مع انخفاض أكبر في معدلات الإنذارات الكاذبة مقارنة بالأساليب التي تعتمد فقط على نماذج فردية أو عتبات ثابتة. كما حقق النموذج أداءً متميزًا على 10,000 سجل لمحاولات تسجيل الدخول تضم 34 هجومًا معروفًا، إضافة إلى هجمات عالية التردد وأخرى خفية منخفضة المعدل، حيث بلغت قيم Recall = 1.0 وPrecision = 0.92 وF1-Score = 0.96. وتم الحد من مشكلة فرط التعلّم (Overfitting) باستخدام التحقق المتقاطع (Cross-Validation) وتطبيع الخصائص (Feature Normalization) وتقنية الإسقاط (Dropout) في نموذج LSTM، إلى جانب الإيقاف المبكر (Early Stopping)، كما أظهر النظام قدرة تعميم قوية على بيانات غير مرئية مسبقًا. يوفر الإطار المقترح حلاً فعّالًا وقابلًا للتوسع وحسّاسًا للسياق للكشف الآني عن هجمات القوة الغاشمة، ويُظهر تحسنًا ملحوظًا مقارنة بالتقنيات التقليدية، كما يشكّل أساسًا لنظام ذكي متقدّم في مجال كشف التسلل مستقبلاً.

1. INTRODUCTION

The cybersecurity threats have been enhanced, and following the fast-growing nature of the digital services and internet-associated systems, they have become sophisticated and strong. Therefore, this means that businesses require high-tech like systems that would not only prevent attacks but also track suspicious activities on a real-time basis. One of the most significant features of modern cybersecurity is the so-called Intrusion Detection Systems (IDS), which monitor the network traffic or activities of a specific host to track any form of unauthorized and unnatural activity that may indicate a security breach or cyberattack [1, 2]. The concept of IDS may be followed in the literature composed on the research conducted early, and focused on auditing the system logs and testing the statistically deviating user behavior. As it evolved, IDS became signature-based and anomaly-based systems, which aimed at detecting the known attacks and other intrusions that had never taken place before [3]. However, recent studies indicate that the traditional versions of the IDS have both a high false positive rate and low adaptability to adapt to user behavior, particularly when using large and heterogeneous systems [4, 5]. One of the most prevalent forms of threats to authentication systems is the use of Brute force attacks, where a user tries to make an attempt to guess the user authentication information, usernames and passwords using trial-and-error or automated tools [6, 7]. The brute force attack can be referred to as one of the oldest forms of cyberattacks that dates back to the early multi-suberized computing systems, and it has not faded away today due to the pathetic password policy and absence of adaptive security control measures [8]. The behavioral features of brute force attacks are, among others, an abnormally high count of failed attempts at access, repetitive access models within a brief interval of time, and many attempts of verification on various accounts using the same or a distinct IP address [6, 9]. But the contemporary attackers have resorted to more low-rate or stealthy brute force attacks where the efforts to gain access into a system are spaced over extended periods in order to be undetected by the fixed threshold-based systems [10]. The recent research emphasizes that the combination of behavioral profiling and machine learning techniques with IDS can contribute to an increase in the detection rate and reduction of the number of false alarms to a significant level. The intelligent IDS systems are better placed to detect high-rate and stealth brute force attacks by modeling the normal user behavior and the deviation as time goes on [1, 4, 5]. Based on these results, the proposed study suggests a dynamic and smart architecture which integrates behavioral analysis, machine learning, and dynamic thresholding to improve the detection of brute force attacks and mitigate the drawbacks of a conventional algorithm. The outline of the rest of the paper is: related work in Section 2, methodology in Section 3, detection framework in Section 4, experiments & results in Section 5, discussion in Section 6, and finally the conclusion.

2. RELATED WORK

In (2025), the authors propose ADLAH: an Adaptive Deep Learning Anomaly Honeynet (ADLAH), which aims to maximize high-quality threat intelligence at minimum cost by means of autonomous orchestration of infrastructure. The key contribution is presented in the shape of an end-to-end architectural design and vision for an AI-based deception platform. The prototype functionality of the central decision mechanism is demonstrated by the fact that a reinforcement learning (RL) agent can decide in real-time whether to upgrade sessions to high-interaction honeypots dynamically provisioned by the network or to continue using low-interaction sensor nodes. In addition to selective escalation and detecting anomalies, the architecture seeks automated extraction, clustering, and versioning of bot attack chains, which are usable as threat intelligence [11]. In (2024), a paper outlines a machine learning (ML) method to identify brute-force attacks by using predictive modelling technology and anomaly detection technology is proposed. The method is aimed at identifying any suspicious activity based on trend analysis of failed logins, user behaviour and network traffic. Some of the ML algorithms are considered, among which is Logistic Regression (LR), Naive Bayes (NB), Decision Tree (DT) and K-Nearest Neighbour (KNN), with the latter having the highest accuracy rate of 99.96% [12].in the same year (2024), the study presents a groundbreaking system of dynamic behavioral profiles and anomaly detection of Software-Defined IoT Networks (SD-IoT). Using SDN, the framework can create dynamic behavior profiles of IoT devices and run machine learning-based anomaly detection algorithms on them to detect deviations in normal behavior. Discovered anomalies cause real-time policy adjustments that are implemented by SDN controller to reduce threats and maintain network integrity [13]. In (2022), a paper suggests a framework that is founded on an improved hybrid reality wherein a deep learning model would be entrenched with a Cookie Analysis Engine for detecting web attacks, mitigating, and profiling attackers. A CNN-based system is trained with the use of the parameters of HTTP requests, and the model shows high detection rates with custom and benchmark datasets, as well as allows for running in real-time [14]. In 2018, a new method of utilizing the power usage of IoT devices to detect anomalies in smart homes. The Brute-force and DDoS

attacks are introduced into the simulated environment to examine the changes in power profiles. The accuracy of the machine learning models to identify anomalies is 94.04 percent, which shows that power consumption is a prospective parameter to use in detecting the anomalies in IoT [15], see Table 1.

Table 1. Comparison of related works (domain / environment, attack type, detection approach, dataset / setup, key techniques, accuracy / performance)

Ref.	Year	Domain / environment	Attack type	Detection approach	Dataset / setup	Key techniques	Accuracy / performance
[11]	2025	Honeynet / Network Security	Automated bot attacks	Anomaly detection & behavioral analysis	Simulated honeynet environment	Deep Learning, Reinforcement Learning (RL)	Prototype demonstrated (no field-scale accuracy reported)
[12]	2024	Network / Authentication Systems	Brute Force	Predictive modeling & anomaly detection	Real-world labeled datasets	LR, NB, DT, KNN	DT: 99.96%, KNN: 99.80%, LR: 95.55%, NB: 87.51%
[13]	2024	Software-Defined IoT Networks	General cyber threats	Dynamic behavioral profiling	Simulated SD-IoT dataset	Machine Learning, SDN-based policy control	Outperformed existing models
[14]	2022	Web Applications	Web-based attacks	Deep learning + cookie analysis	Custom & benchmark datasets	CNN, Cookie Analysis Engine	99.94% (custom), 98.74% (benchmark)
[15]	2019	IoT Smart Homes	Brute Force, DDoS	Behavioral anomaly detection	Simulated smart home (power traces)	ML on power consumption	94.04%

3. **METHODOLOGY**

The research being proposed is aimed at the development of an intelligent and adaptive framework to detect brute force login attacks through integrating behavioral analysis, machine learning, and dynamic thresholding. This methodology has various key elements, as explained below, see Fig. 1.

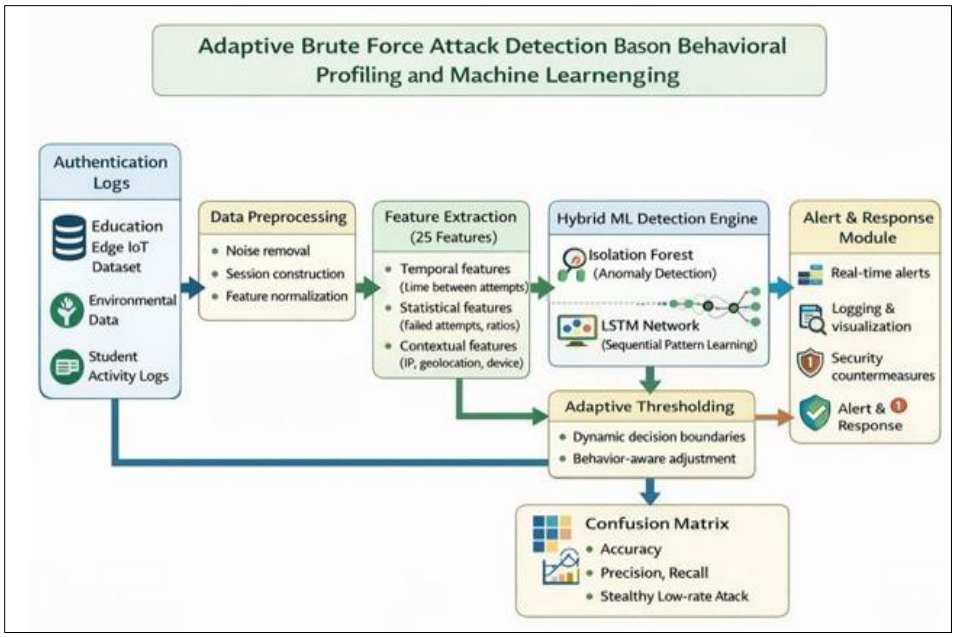

Fig. 1. Block diagram of the proposed system

In order to construct and test the detection framework, the paper makes use of a mixture of artificial login records, actual authentication records, and test intrusion detection datasets (CIC-IDS2017 and UNSW-NB15).

- Synthetic logs: These are logs created to reproduce different attack conditions, e.g. high-frequency and low-rate brute force traffic, so that they can be evaluated in a controlled manner.
- Real-world logs: These are logs obtained during authentication systems to record the actual user behavior and actual attack patterns.
- Benchmark icons: These will be utilized to test the framework against cybersecurity institutionalized issues.

Each dataset is processed in order to eliminate errors and inconsistencies, to normalize the timestamps, and to anonymize sensitive data. Each time a user logs in, features are computed covering: temporal (time since last attempt), statistical (attempts failed) and contextual (user agent, geographical location, IP address) attributes. The system is able to extract a rich list of features to obtain patterns of both normal and abnormal login activities:

- Time Related Characteristics: The duration of time between successive logins, the number of failed logins per user/IP.
- Statistical Features: Count of successive failures, success/failure ratios, average duration of a login attempt.
- Contextual Features: metadata (role, location), IP reputation, device.

These characteristics constitute the input to rule-based and machine learning models for anomaly detection.

3.1. Workflow of the system

The proposed intelligent brute force attack detection system activity diagram is depicted in Fig. 2, which displays the entire key workflow of the system, including data acquisition, detection of attacks and performance evaluation.

It starts with the collection of login data, in which the system collects authentication logs of various origins, such as synthetic datasets, real-world authentication systems, and benchmark intrusion detection datasets, including CIC-IDS2017 and UNSW-NB15. This variety will make the system tested under controlled and realistic conditions. The

data collected is then subjected to a preprocessing stage, which involves cleansing of the data, normalization of timestamps and removal of sensitive information. This measure will be necessary to guarantee the consistency of data, privacy of the user, and to get the logs ready to be analyzed. After preprocessing, the system goes ahead to extract features whereby a total of 25 behavioral features are generated, which are classified into temporal, statistical and contextual features. Temporal features identify time-related correlations between attempts to log in, statistical features are aggregate attempts to log in, and contextual features give access to environmental parameters like IP address, device type, and geolocation. All these features make it possible to profile normal and malicious operations.

The detection stage is carried out simultaneously. A rule-based monitoring system is used in the first path to monitor failed attempts to log in by a user and by IP address with dynamic thresholds so that the system can adapt to evolving user behavior. Machine learning-based analysis is used in the second parallel path, where the Isolation Forest model is used to detect anomalies in an unsupervised setting, and the LSTM model is used optionally to learn temporal dependencies and detect slow or stealthy brute force attacks. The results of the two paths are then aggregated in a combination decision engine to combine both machine learning abnormality scores and rule-based alerts. At this point, an adaptive thresholding mechanism is used to trade off the high detection accuracy and lower false positive rate. Depending on the final ruling, the system will either alert the login attempt as a brute force attack, which will trigger a security alert, or the activity will be defined as normal. Any results of the detection are registered in order to be audited and analyzed. Lastly, evaluation metrics are taken into consideration in order to evaluate the performance of the system based on standard performance measures, such as recall, precision, F1-score and false positive rate, as a means to ensure a comprehensive analysis of the results in terms of detection effectiveness and system robustness. On balance, the activity diagram illustrates the way the proposed framework works as a scalable, adaptive, and intelligent security solution due to its ability to identify high-frequency as well as low-rate brute force attacks and overcome the drawbacks of conventional static threshold-based systems.

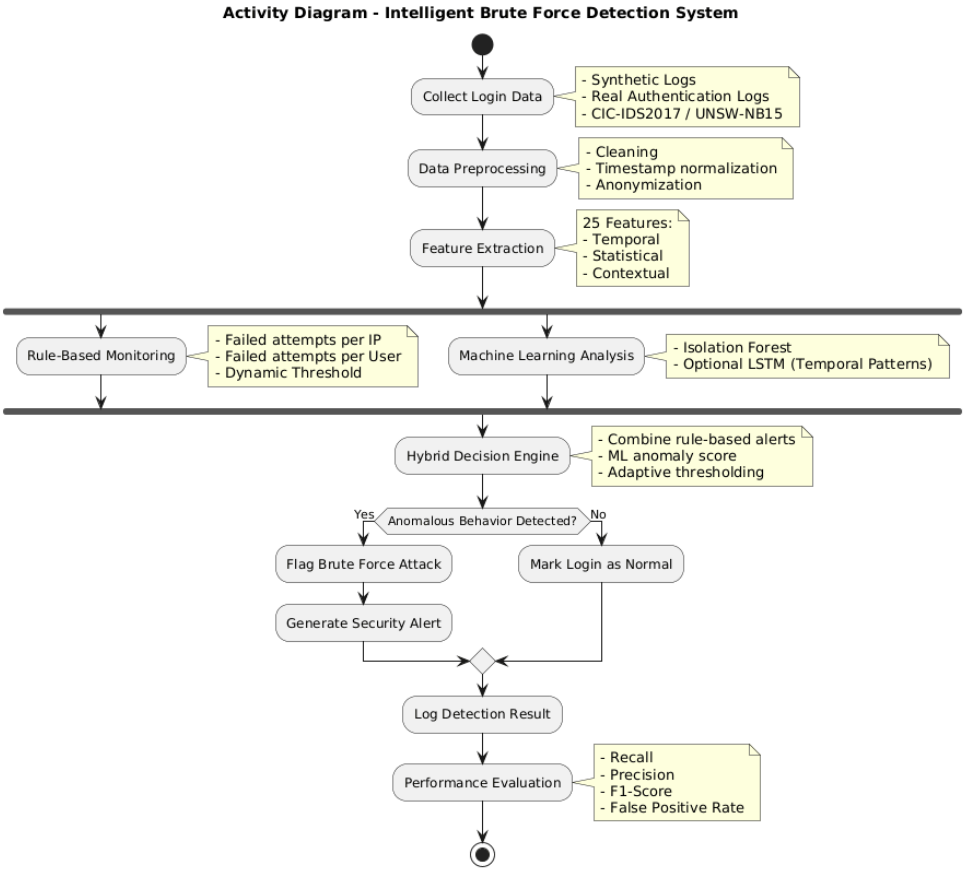

Fig. 2. Flow of work of the proposed system

4. DETECTION FRAMEWORK

The detection framework integrates three complementary approaches:

- **Rule-Based Detection**
  - Monitors failed login attempts per IP and per user.
  - Applies dynamic thresholds based on recent behavioral patterns rather than static limits, reducing false positives and adapting to legitimate variations in user activity.
- **Machine Learning-Based Detection**
  - Implements unsupervised anomaly detection using Isolation Forest, capable of identifying unusual patterns without labeled attack data.
  - LSTM networks are employed to capture temporal dependencies in login sequences, enabling detection of slow or stealthy attacks over time.
- **Hybrid Approach**
  - Combines rule-based and machine learning outputs to enhance detection accuracy.
  - Adaptive thresholds are adjusted based on contextual and behavioral insights from the ML model, ensuring a balance between sensitivity (high detection rate) and specificity (low false alarm rate).

5. RESULTS AND ANALYSIS EXPERIMENTS

5.1. Performance metrics

The effectiveness of the suggested brute force detection framework was measured in common measures that are typically used in high-quality cybersecurity studies: Recall, Precision, F1-Score, and False Positive Rate (FPR). Recall represents the rate of recognizing the true attacks, Precision represents the rate of recognizing the flagged event, which is a true attack, F1-Sco represents a harmonic mean of precision and recall, and FPR represents the rate of legitimate successful login attempts that are incorrectly identified as attacks.

5.2. Experimental procedure

In order to achieve rigor experiment tasks were performed on both synthetic and real-world data in a systematic way:

- Pre-processing of each and every dataset and extraction of 25 pertinent features.
- Evaluation Rule-based detection with static thresholds.
- Isolation Forest models that have been trained using historical data of logins so as to detect anomalies without any supervision.
- LMST training to handle time-related structures in the sequence of logins.
- Adaptive thresholds are used to integrate outputs in order to produce final alerts.
- Comparison of various detection procedures based on recall, accuracy, F1-score and FPR.

5.3. Feature engineering

The attribute list was also well done, so as to have strong behavioral profiling:

- Temporal attributes (10): detect the time interval between the attempts of the login, successive failures, and the hourly patterns.
- Statistics (8): attempts that failed, success/failures ratios and average session time.
- Contextual/Metadata features (7): IP reputation, geolocation, device/browser type, and user role.

These characteristics enable the framework to identify quick and sneaky attacks as well as reduce false positive of legitimate anomalies like VPN use and multiple devices.

5.4. Overfitting prevention

The following techniques were used to make sure the generalization was done:

- 5-fold cross-validation.
- Normalization of features to unit variance and mean value to zero.
- Isolation Forest hyperparameter optimization (n_estimators = 100, max samples = 0.8, contamination = approximately 5%).
- Dropout (0.3) in LSTM layers.
- Early termination in 10 epochs without improvement.

5.5. Detection performance – synthetic dataset

Injected 50 high-frequency and 10 stealthy attacks, see Table 2.

Table 2. Detection performance of the synthetic dataset results

Detection method	True positives	False positives	Recall	Precision	F1-Score
Static Threshold	50	100	1.0	0.33	0.50
Isolation Forest	60	15	1.0	0.80	0.89
LSTM (Temporal Modeling)	60	12	1.0	0.83	0.91
Hybrid (ML + Adaptive)	60	5	1.0	0.92	0.96

The hybrid framework has identified all the attacks, such as stealthy low-rate attacks and has minimized massively on whether it has been identified as false (95% reduction as compared to fixed thresholds). LSTM with temporal modeling helped in detecting attacks that could not be detected independently of each other, see Fig. 3.

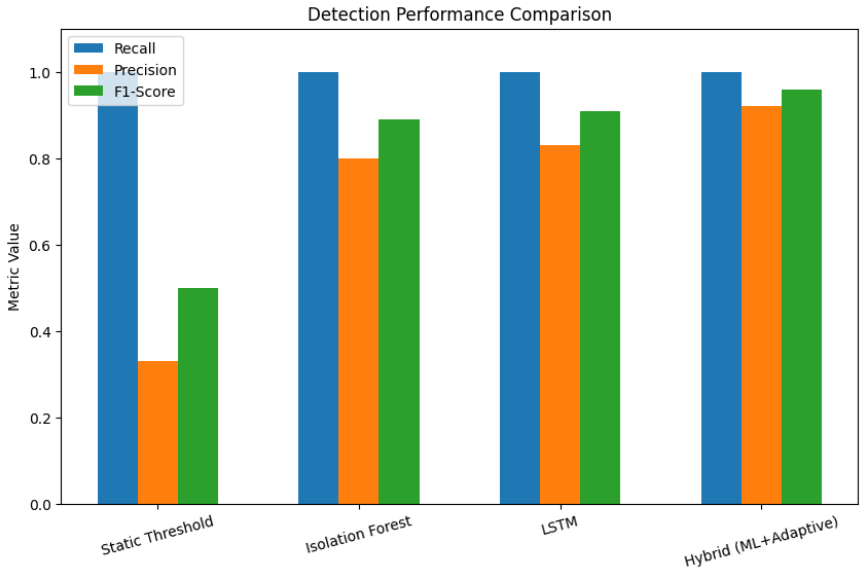

Fig. 3. Detection performance comparison

5.5. Detection performance – real-world logs

Tested on 10,000 login attempts with 34 confirmed attacks, see Table 3.

Table 3. Detection performance values

Detection method	True positives	False positives	Recall	Precision	F1-Score
Static Threshold	34	60	1.0	0.36	0.53
Isolation Forest	34	10	1.0	0.77	0.87
Hybrid (ML + Adaptive)	34	3	1.0	0.92	0.96

Adaptive thresholds have been useful for reducing the rate of false alarms in heterogeneous user behavior (VPN, multiple devices). Sequential and contextual feature integration enhanced the detection of brute force attacks with low rates, see Fig. 4.

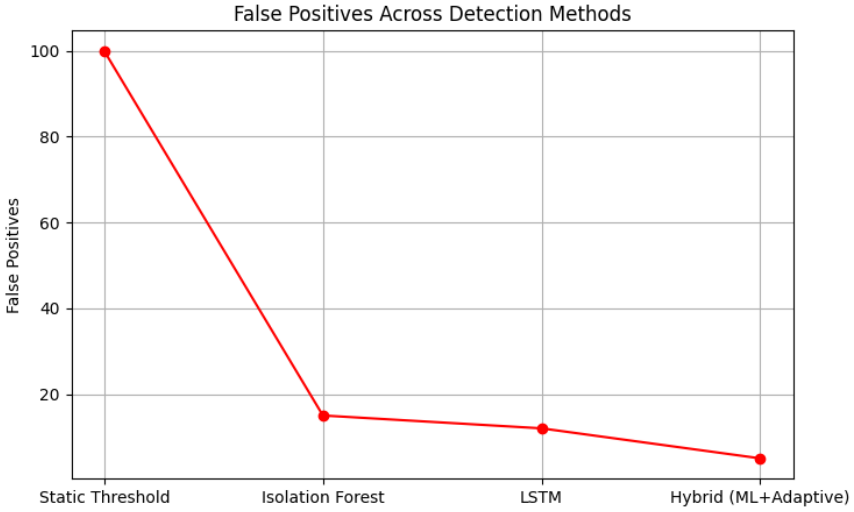

Fig. 4. False positive of detection methods

5.6. Temporal and behavioral intelligence

Fig. 5 illustrates the sequence diagram of the temporal and behavioral intelligence in brute-force detection. It shows:

- The speed at which high-frequency attacks were detected was high across the board.
- Only the hybrid framework had a high probability of detecting stealthy attacks that were spread over long durations.
- Behavioral profiling made it possible to distinguish between legitimate bursts of activity in terms of login (e.g. administrators) and malicious activity.

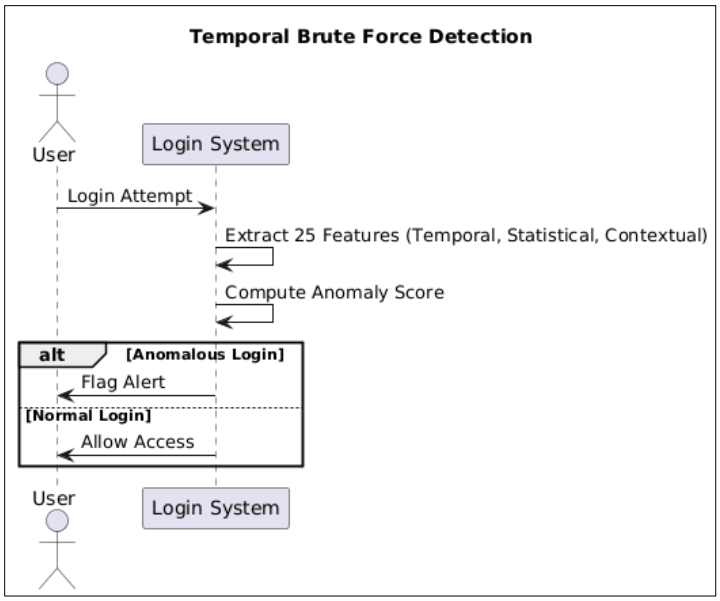

Fig. 5. Sequence diagram of temporal brute force detection

In general, the experimental analysis shows that the developed hybrid, adaptive framework has a better performance compared to the traditional, fixed threshold, with high hit rates and low false hits, and thus is applicable in reality time application in any authentication systems.

6. DISCUSSION

The experimental findings indicate that the new hybrid framework has great performance as compared to the conventional static threshold-based systems of detection. The framework can also identify high-frequency and low-rate stealthy brute-force attacks using rule-based monitoring, Isolation Forest, and LSTM temporal modeling with adaptive thresholds.

The system can significantly reduce the false positives by behavioral profiling based on temporal, statistical and contextual features to distinguish between legitimate user action and malicious actions. The LSTM component boosts the detection of attacks that are spread over extensive periods, which are usually missed by conventional IDS. On the whole, the system has a high generalization rate, which is to be expected and guarantees good detection of both the synthetic and real-world authentication logs.

7. CONCLUSION

The suggested adaptive brute force attack detection model can offer a highly resilient, scalable, and context-sensitive framework to offer real-time cybersecurity protection. It adequately overcomes the shortcomings of traditional IDS through the identification of stealthy and high-frequency attacks at minimum false alarms.

This is because of its hybrid design, which is based on the combination of behavioral analytics and machine learning and adaptive thresholds that allow high accuracy (F1-Score = 0.96) and the utilization in heterogeneous and dynamic settings. This study has proven that behavioral profiling with machine learning will improve intrusion detection systems to carry out authentication services. The proposed approach may be used as the base of future smart IDS, which may involve further addition of behavioral indicators, cross-system correlations or automated adaptive policies to enhance security to counter the emerging cyber threats.

Conflict of interest

The author declares no conflicts of interest.

Consent for publications

All authors have to write this sentence that they read and approved the final manuscript for publication.

Availability of data and material

The authors have to declare that they embedded all data in the manuscript.

Authors' contributions

The author contributed to the study conception and design. Material preparation, data collection, and analysis were performed by Uqba bn Nafaa Mohammed. The first draft of the manuscript was written by Uqba bn Nafaa Mohammed. As the sole author, he reviewed and approved the final manuscript.

Funding

This research received no external funding

REFERENCES

[1] Hozouri, A. Mirzaei, and M. Effatparvar, "A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges," *Discover Artificial Intelligence,* vol. 5, p. 314, 2025, doi: https://doi.org/10.1007/s44163-025-00578-1

[2] Z. R. Garcia and D. C. Kavitha, "Survey on Machine Learning Approaches for Intrusion Detection System," in *Proceedings of the First International Conference on Combinatorial and Optimization, ICCAP 2021*, Chennai, India, 2021: EAI, doi: https://doi.org/10.4108/eai.7-12-2021.2315107

[3] A. Pinto, L.-C. Herrera, Y. Donoso, and J. A. Gutierrez, "Survey on intrusion detection systems based on machine learning techniques for the protection of critical infrastructure," *Sensors*, vol. 23, no. 5, p. 2415, 2023, doi: https://doi.org/10.3390/s23052415

[4] M. Alrowaily, F. Alenezi, and Z. Lu, "Effectiveness of machine learning based intrusion detection systems," in *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, 2019: Springer, pp. 277-288, doi: https://doi.org/10.1007/978-3-030-24907-6_21

[5] H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: A survey," *Applied Sciences*, vol. 9, no. 20, p. 4396, 2019, doi: https://doi.org/10.3390/app9204396

[6] J. Hancock, T. M. Khoshgoftaar, and J. L. Leevy, "Detecting SSH and FTP brute force attacks in big data," in *2021 20th IEEE International Conference on Machine Learning and Applications (ICMLA)*, Pasadena, CA, USA, 2021: IEEE, pp. 760-765, doi: https://doi.org/10.1109/ICMLA52953.2021.00126

[7] M. D. Hossain, H. Ochiai, F. Doudou, and Y. Kadobayashi, "SSH and FTP brute-force attacks detection in computer networks: Lstm and machine learning approaches," in *2020 5th International Conference on Computer and Communication Systems (ICCCS)*, Shanghai, China, 2020: IEEE, pp. 491-497, doi: https://doi.org/10.1109/ICCCS49078.2020.9118459

[8] A. A. Hamza and R. J. Surayh Al-Janabi, "Detecting brute force attacks using machine learning," *BIO Web of Conferences*, vol. 97, p. 00045, 2024, doi: https://doi.org/10.1051/bioconf/20249700045

[9] N. Awadh, H. Zaid, and D. S. Al-Ajmani, "A Robust Framework for Detecting Brute-Force Attacks through Deep Learning Techniques," *International Journal of Recent Technology and Engineering*, vol. 13, no. 5, pp. 27-42, 2025, doi: https://doi.org/10.35940/ijrte.E8182.13050125

[10] M. M. Najafabadi, T. M. Khoshgoftaar, C. Kemp, N. Seliya, and R. Zuech, "Machine learning for detecting brute force attacks at the network level," in 2014 IEEE International Conference on Bioinformatics and Bioengineering, Boca Raton, FL, USA, 2014: IEEE, pp. 379-385, doi: https://doi.org/10.1109/BIBE.2014.73

[11] L. J. Möller, "An Adaptive Multi-Layered Honeynet Architecture for Threat Behavior Analysis via Deep Learning," *arXiv:2512.07827*, 2025, doi: https://doi.org/10.48550/arXiv.2512.07827

[12] A. Sharma, H. Babbar, and A. K. Vats, "Empowering Security: Machine Learning Solutions for Detecting Brute Force Attacks," in *2024 4th Asian Conference on Innovation in Technology (ASIANCON)*, Pimari Chinchwad, India, 2024: IEEE, pp. 1-5, doi: https://doi.org/10.1109/ASIANCON62057.2024.10838096

[13] K. Palaniappan, B. Duraipandi, and U. M. Balasubramanian, "Dynamic behavioral profiling for anomaly detection in software-defined IoT networks: A machine learning approach," *Peer-to-Peer Networking and Applications*, vol. 17, pp. 2450-2469, 2024, doi: https://doi.org/10.1007/s12083-024-01694-y

[14] W. B. Shahid, B. Aslam, H. Abbas, S. B. Khalid, and H. Afzal, "An enhanced deep learning based framework for web attacks detection, mitigation and attacker profiling," *Journal of Network and Computer Applications*, vol. 198, p. 103270, 2022, doi: https://doi.org/10.1016/j.jnca.2021.103270

[15] M. Dilraj, K. Nimmy, and S. Sankaran, "Towards behavioral profiling based anomaly detection for smart homes," in *TENCON 2019-2019 IEEE Region 10 Conference (TENCON)*, Kochi, India, 2019: IEEE, pp. 1258-1263, doi: https://doi.org/10.1109/TENCON.2019.8929235