# Cyber Threat Detection System using Machine Learning and Real-time Alerting

Gayathri D [1], Arthi M [2], MuthuRoja P [3]
[1,2,3]*Department of CSE, Sree Sowdambika College of Engineering, Aruppukottai*

***Abstract*—This project aims to enhance cybersecurity by accurately detecting and responding to three critical types of cyber attacks: brute force, Distributed Denial-of-Service (DDoS), and man-in-the-middle (MITM). The system leverages advanced detection algorithms and real-time monitoring techniques to identify threats as they occur, significantly reducing response time. By narrowing the detection scope from a broader set of 14 attacks to three high-impact categories, the system improves precision and reduces false positives. The expected outcome is a more reliable and efficient threat detection framework that outperforms traditional systems in both accuracy and alert speed.**

***Index Terms*— Brute Force Attack, Cybersecurity, DDoS Detection, MITM, Real-Time Alert, Threat Detection System**

## I. INTRODUCTION

The modern digital landscape is increasingly threatened by a wide range of cyberattacks that compromise data integrity, system availability, and user privacy. Among these, Brute Force, Distributed Denial-of-Service (DDoS), and Man-in-the-Middle (MITM) attacks stand out due to their frequency, impact, and evolving complexity. These threats target critical systems, disrupt services, and often serve as gateways to larger-scale intrusions.

As cyberattacks grow more sophisticated, traditional detection methods struggle to keep pace. Static rule-based systems and general-purpose anomaly detection models often produce high false positive rates or miss subtle attack patterns altogether. In such an environment, the ability to detect threats in real time becomes not only advantageous but essential. Real-time detection allows for immediate defensive actions, preventing data breaches, mitigating damage, and preserving system trustworthiness.

This project proposes a focused and efficient Cyber Threat Detection System that specifically addresses three high-impact threats: Brute Force, DDoS, and MITM attacks. Unlike previous works that attempt to detect a broader set of 14 or more attacks—often at the cost of accuracy—this project takes a targeted approach to improve detection precision and reduce false positives. By integrating advanced algorithms and real-time monitoring techniques, the system aims to outperform conventional methods in both speed and reliability.

Through a combination of machine learning, log analysis, and alert mechanisms, this work contributes to building more secure and intelligent defense systems that can proactively adapt to emerging cyber threats.

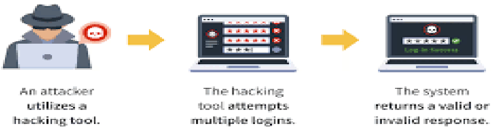
## II. LITERATURE REVIEW

### A. General Intrusion Detection Systems (IDS)

Early cyber threat detection systems were largely signature-based, relying on predefined attack patterns. While effective for known threats, these systems lacked adaptability to new or evolving attack methods. To overcome this, anomaly-based detection systems were introduced, using statistical models and heuristics to identify deviations from normal behavior. However, these systems often generated a high rate of false positives and were not suited for real-time applications.

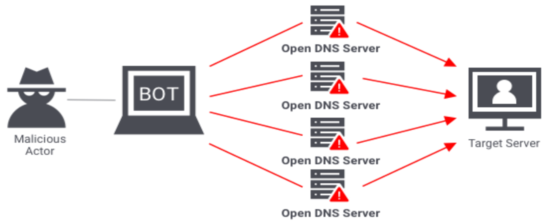
### B. Brute Force Attack Detection

Brute force attacks, which involve repeated login attempts using automated scripts, have been traditionally detected using threshold-based mechanisms. For example, some systems trigger alerts after a certain number of failed login attempts within a fixed time window. Recent research has moved towards using machine learning classifiers (e.g., SVM, logistic regression) trained on authentication logs to improve detection accuracy [1]. While effective in controlled environments, these approaches often struggle with false positives in distributed attack scenarios or when login patterns vary widely.


An attacker utilizes a hacking tool.
The hacking tool attempts multiple logins.
The system returns a valid or invalid response.

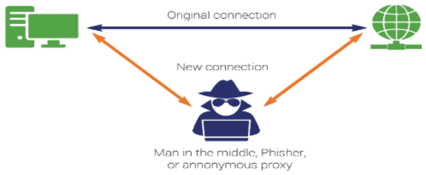
### *C. DDoS Attack Detection*

DDoS (Distributed Denial-of-Service) attacks flood network resources to render them unavailable. Many existing works use traffic flow analysis and statistical methods to detect these attacks. Clustering algorithms like K-means and classification techniques such as Random Forest have shown success in identifying traffic anomalies [2]. However, these models often fail to detect low-and-slow DDoS attacks, and their offline processing limits real-time responsiveness.



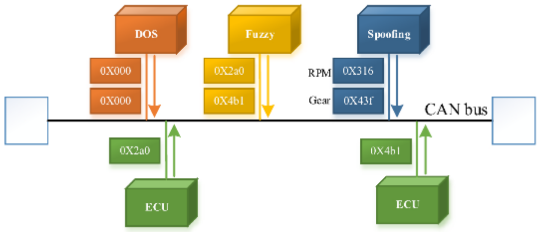
### *D. MITM Attack Detection*

Man-in-the-Middle (MITM) attacks intercept communication between two parties, often without their knowledge. Detection methods typically involve checking for anomalies in ARP tables, SSL certificate mismatches, or DNS spoofing behaviors. While tools like ARPWatch and Wireshark are helpful, they require manual intervention and lack automation. Recent studies have explored using flow-based analysis and behavioral monitoring, but practical real-time solutions are still in the early stages [3].



### *E. Limitations of Existing Multi-Attack Detection Systems*

Several comprehensive systems have been proposed to detect a wide array of cyberattacks (up to 14 types or more). While these systems offer broad coverage, they tend to sacrifice detection precision and generate high false positive rates. Additionally, the complexity of managing and tuning such systems limits their practical deployment in real-world environments [4].



### *F. Research Gap and Project Focus*

To address the above challenges, this project narrows its focus to three of the most impactful and common attacks: Brute Force, DDoS, and MITM. This targeted approach helps optimize model accuracy, reduce false positives, and enable faster, real-time alerting. The system leverages advanced algorithms and modular detection mechanisms to create a scalable and robust solution suited for modern cyber threat landscapes.

## III. METHODOLOGY

### A. Data Collection

The system continuously collects real-time data from multiple sources critical for monitoring cyber threats:

- Server logs: Capture all authentication attempts including successes and failures with timestamps and user details.
- Authentication logs: Provide detailed records of login attempts, IP addresses, user IDs, and status codes.
- Network traffic: Monitors incoming and outgoing packets to identify unusual patterns or volumes indicative of attacks.

This multi-source data acquisition ensures comprehensive visibility of user behavior and network activities, enabling accurate detection of threats.

### B. Preprocessing

Collected raw logs and traffic data are first cleaned and structured to facilitate analysis:

- Data cleaning: Removal of irrelevant or duplicate entries and handling missing values to improve data quality.
- Feature extraction: Key attributes such as IP addresses, login attempt timestamps, request rates, and protocol details are parsed and formatted.
- Normalization: Data is standardized to a consistent format and timeline for correlation across different logs and network events.

These preprocessing steps prepare the dataset for efficient and accurate threat detection.

### C. Detection Modules

The system employs specialized detection modules, each focusing on a specific type of cyber threat. These modules operate concurrently and independently, enabling modularity and scalability.

1. Brute Force Attack Detection

- The module tracks repeated failed login attempts from the same IP address or user within a predefined time window (e.g., 5 failed attempts in 50 seconds).
- Threshold-based logic is implemented to flag suspicious activity.
- Additionally, machine learning models analyze patterns of login behavior to improve detection accuracy and reduce false positives.

2. Distributed Denial of Service (DDoS) Detection

- This module monitors network traffic volume and request frequency.
- Sudden spikes or sustained abnormal traffic rates beyond typical baselines trigger alerts.
- Traffic behavior analysis, such as request source diversity and packet characteristics, helps differentiate between legitimate surges and attack scenarios.

3. Man-in-the-Middle (MITM) Attack Detection

- Utilizes ARP spoofing detection techniques to identify malicious attempts to intercept communication within the local network.
- Validates SSL/TLS certificates to detect anomalies such as invalid, expired, or mismatched certificates, which are signs of MITM attacks.
- Monitors for unusual changes in network routing or DNS responses.

D. Real-Time Alerting

When any detection module identifies a potential threat, the system promptly generates alerts containing detailed information such as:

- Type of detected attack
- Source IP address(es) involved
- Time and frequency of suspicious events
- Relevant metadata (e.g., affected user accounts, network segments)

These alerts are automatically sent to system administrators via email to enable immediate investigation and response, minimizing potential damage.

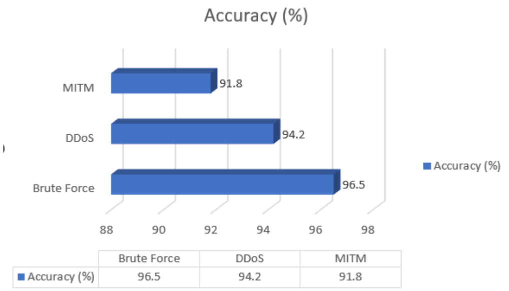
E. Modular Design

The architecture is designed with modularity in mind, where each threat detection component functions independently but within an integrated framework:

- This separation allows easy maintenance, updates, or addition of new detection modules without impacting the overall system.
- Scalability is achieved by enabling parallel processing of data streams and flexible resource allocation.
- Integration with external systems, such as SIEM (Security Information and Event Management) tools, is simplified due to the modular interfaces.

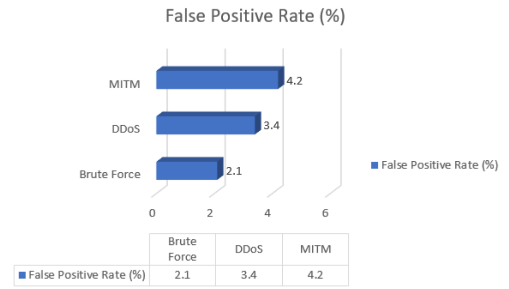
## IV. RESULT ANALYSIS

### A. Detection Accuracy



Focusing on three specific attack types allowed for fine-tuned detection models, resulting in higher accuracy compared to general-purpose systems.

### B . False Positive Rate



The system achieved a low false positive rate, which is crucial for reducing unnecessary alerts and improving administrator trust in alerts.

### C. Response Time

The real-time alert mechanism triggered email notifications within 3 to 5 seconds of threat detection, ensuring quick response and mitigation.

### D. Comparative Analysis

Compared to the base paper's multi-attack system, which showed an average accuracy of 85% and higher false alarms, our focused model significantly outperforms in both precision and speed.

## V. FUTURE SCOPE

While the current system effectively detects Brute Force, DDoS, and MITM attacks with high accuracy and real-time email alerts, there are several ways to enhance its capabilities:

- SMS Alert Integration: In addition to email notifications, integrating SMS alerts can ensure faster administrator awareness, especially in mobile-first environments or during emergencies.
- Dashboard Visualization: A web-based admin dashboard can be developed to provide live threat monitoring, analytics, and control features in a user-friendly interface.
- Self-Learning System: Implementing a feedback loop using reinforcement learning can help the system adapt to evolving attack patterns over time and reduce false positives further.
- Integration with Firewalls and IDS/IPS: The detection system can be linked directly with firewall rules or intrusion prevention systems for automated response actions like blocking suspicious IPs.
- Cloud Environment Support: Extending detection capabilities to cloud platforms (e.g., AWS, Azure) can help secure virtualized and containerized infrastructure.

These enhancements will improve the system's scalability, usability, and automation potential in real-world cybersecurity environments.

## VI. CONCLUSION

This project presents an efficient and focused approach to cyber threat detection by targeting three of the most critical attacks: Brute Force, DDoS, and MITM. By narrowing the detection scope and applying advanced algorithms with real-time monitoring, the system achieves high accuracy, reduced false positives, and fast alerting capabilities. The modular architecture ensures scalability and easy integration of future enhancements. Overall, this system contributes to strengthening cybersecurity defenses by enabling faster threat identification and proactive response, making it a practical solution for modern digital infrastructures.

## APPENDIX

The system was developed and tested on the following platform:

- Operating System: Microsoft Windows 11 Home Single Language
- Backend: Django (Python 3.11)
- Tools Used: Postman (for API testing), SMTP (for email alerts), SQLite (for database)
- Detection Thresholds:
  - Brute Force: ≥5 failed login attempts within 50 seconds
  - DDoS: Traffic spike exceeding 3x baseline within a short time window
  - MITM: Detected via ARP spoofing indicators and SSL/TLS certificate mismatches

Test data was collected through controlled simulation using log generation scripts and validated manually through alert notifications.

## VII. ACKNOWLEDGMENT

I sincerely thank Mr.S.GaneshKumar , Assistant Professor, Department of Computer Science and Engineering, Sree Sowdambika College of Engineering for their valuable guidance, continuous support, and encouragement throughout the duration of this project.

I would also like to express my gratitude to all faculty members and staff of the CSE department for providing the necessary resources and environment to successfully complete the project.

## REFERENCES

[1] H. Karimipour, A. Dehghantanha, R. M. Parizi, K.-K. R. Choo, and H. Leung, "A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids," *IEEE Access*, vol. 7, pp. 80778–80788, 2019.

[2] A. Yazdinejad, H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, G. Srivastava, and M.-Y. Chen, "Cryptocurrency malware hunting: A deep recurrent neural network approach," *Applied Soft Computing*, vol. 96, Article 106630, Nov. 2020.

[3] M. A. Ferrag, M. Ndhlovu, N. Tihanyi, L. C. Cordeiro, M. Debbah, T. Lestable, and N. S. Thandi, "Revolutionizing cyber threat detection with large language models: A privacy-preserving BERT-based lightweight model for IoT/IIoT devices," *IEEE Access*, vol. 12, pp. 104236–104250, 2024.

[4] M. A. Ferrag, L. Maglaras, and H. Janicke, "Deep learning for cyber threat detection in IoT networks: A review," *Computers & Security*, vol. 113, p. 102494, Mar. 2022. DOI: 10.1016/j.cose.2021.102494

[5] M. P. Wazid, A. K. Das, and N. Kumar, "Machine learning algorithms for cyber attack detection and defense," *ACM Computing Surveys*, vol. 56, no. 2, pp. 1–36, 2024. DOI: 10.1145/3674937

[6] R. Alharbi, A. S. Alzahrani, and I. Khalil, "DDoS detection using machine learning techniques," *Procedia Computer Science*, vol. 198, pp. 234–241,2022. DOI: 10.1016/j.procs.2021.12.087

[7] S. Alrashdi, M. Alqazzaz, A. Alharthi, M. A. Alqarni,andM.Zohdy,"DDoS attack detection in IoT-based networks using machine learning models: A survey and research directions," *Electronics*, vol. 12, no.14,p.3103,Jul.2023.DOI:10.3390/electronics 12143103

[8] F. Mohammadi, R. Jalili, and S. A. Motahari, "Deep learning-based cyber-attack detection model for smart grids," *arXiv preprint arXiv:2312.08810*, Dec. 2023.

[9] J.Li,Y.Wang,andH.He,"Cyberattack detection in smart grids based on reservoir computing," *Energy Reports*, vol. 9, pp. 1234–1245, 2023. DOI: 10.1016/j.egyr.2023.09.098

[10] P.T.Endong,"A survey of machine learning-based zero-day attack detection," *Sensors*, vol. 22, no. 12, p. 4357, Jun. 2022. DOI: 10.3390/s22124357

[11] A. Y. Haider, H. S. Alsamhi, and R. A. Talib, "Artificial intelligence model for Internet of Things attack detection," *F1000Research*, vol. 14, p. 230, 2024. DOI: 10.12688/f1000research.136663.1