Hackathon Round 2 – PPT Submission & Prototype

1. Title and Domain

Title

HK-02 – AI-Based Brute Force Attack Detection System (AI)

Domain

Artificial Intelligence

Team Name

Algorithm Avengers

2. Introduction

Brute force attacks are a major cybersecurity threat. Login-based systems are primary targets. Traditional security mechanisms are rule-based. Advanced attacks bypass fixed rules. There is a need for an intelligent AI-driven solution.

3. Problem Statement

Brute force attacks use repeated login attempts. They widely affect banking, education, and business portals. Existing systems rely on fixed thresholds, which fail against slow and distributed attacks, causing security breaches and data loss.

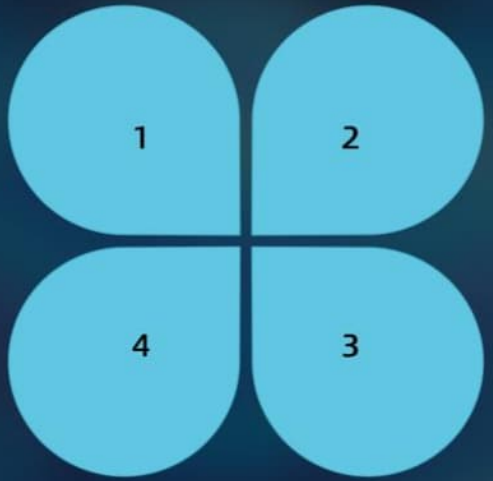
4. Existing System

- Login attempt limits
- CAPTCHA
- IP blocking

Limitations

Easily bypassed

High false positives



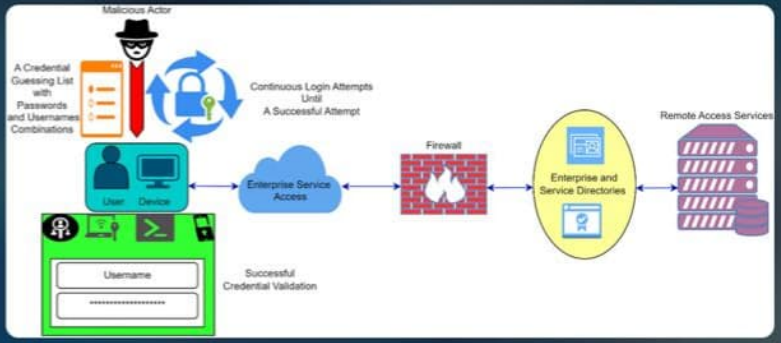
Poor user experience

No learning capability

5. Proposed Solution

AI-Based Brute Force Attack Detection System uses Machine Learning algorithms to continuously analyze login behavior, detect attacks in real-time, and automatically trigger security actions.

6. System Design



7. System Architecture

User login requests are monitored. Login data is collected and analyzed. An AI model classifies behavior, and a security response is activated.

8. Data Parameters

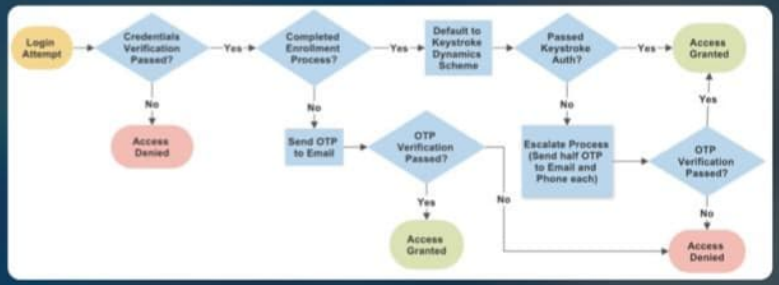
1. Username
2. Login success / failure
3. Number of attempts
4. IP address behavior
5. Login time patterns
6. Multiple account access from the same IP

9. AI / ML Workflow

Steps

1. Login data collection
2. Data preprocessing
3. Feature extraction
4. Machine learning analysis
5. Attack classification
6. Response execution

10. Prototype Workflow



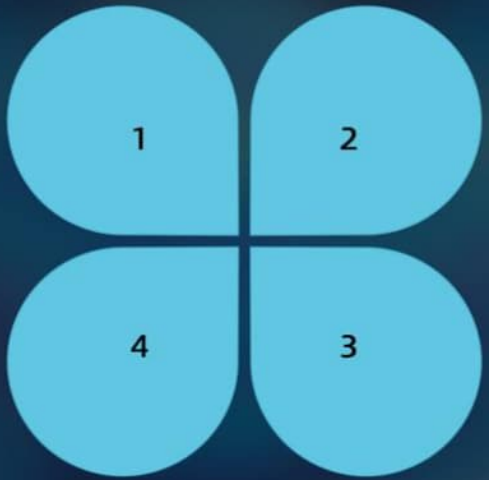
11. Prototype Workflow Explanation

User attempts login. The system records login activity. The AI model evaluates behavior. An attack is detected or rejected, and the action is taken automatically.

12. Automated Security Actions

Temporary IP address blocking

User account locking



Dashboard–based monitoring

Admin alert notification

13. Innovation

1. AI-driven detection (not rule-based)
2. Adaptive learning over time
3. Detects slow & distributed attacks
4. Real-time automated response
5. Scalable across applications

14. Applications

- Educational portals
- Enterprise software
- Banking systems
- Cloud platforms
- Business applications

15. Technology Stack

Backend

Java 17

Framework

Spring Boot

Security

Spring Security

Database

MySQL

ML Logic

Anomaly logic

Build Tool

Maven

Thank You