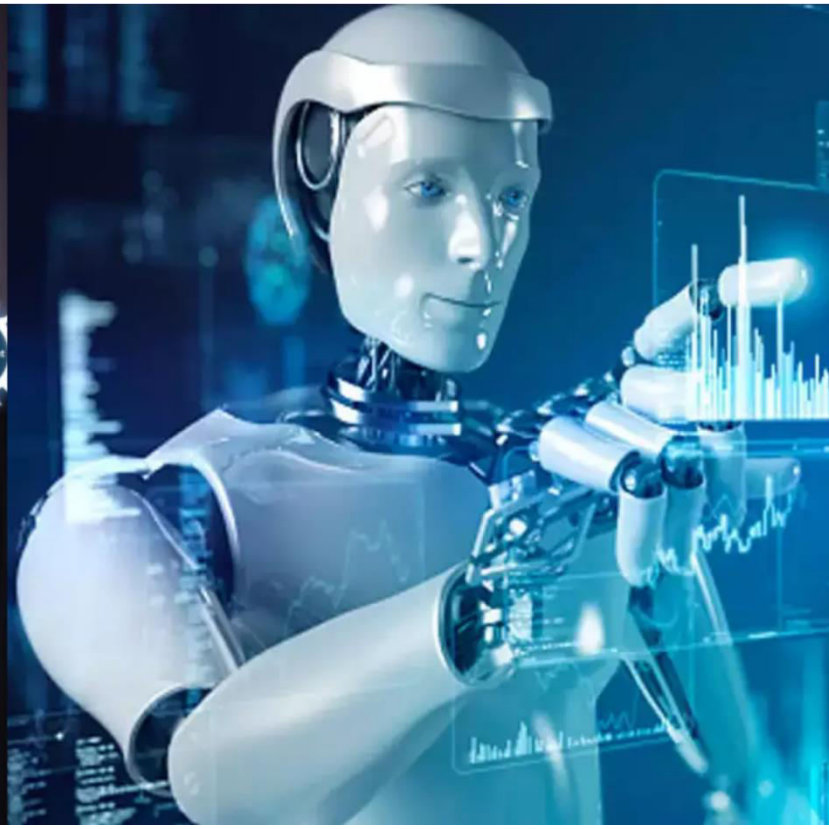
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503331|

AI-Driven Banking Security System (Attack vs Defense Simulation)

Govindarajulu Venkateswaran [1], K.Lokesh[2]

PG Scholar, Department of Computer Science Engineering, Kuppam Engineering College (Autonomous), Kuppam, Andhra Pradesh, India[1]

HOD, Department of CSE, Kuppam Engineering College (Autonomous), Kuppam, Andhra Pradesh, India[2]

ABSTRACT: The AI-Driven Banking Security System (Attack vs Defense Simulation) is an intelligent cybersecurity platform designed to simulate real-world banking application attacks and evaluate advanced defense mechanisms in real time. The system focuses on detecting and mitigating brute-force login attempts using a combination of traditional security techniques and AI-based anomaly detection. The platform integrates a multi-threaded automated attack engine that generates large-scale login requests to test system resilience. On the defense side, it implements layered security mechanisms including smart rate limiting, failed login tracking, rule-based, and machine learning-driven behavioral analysis. These techniques work together to identify abnormal patterns, detect suspicious activity, and automatically block malicious IP addresses. A real-time interactive dashboard provides continuous monitoring of key security metrics such as total login attempts, allowed requests, blocked requests, active threats, and dynamic threat level indicators. The system also includes automated with countdown timers and manual unblock functionality for enhanced control.

I. INTRODUCTION

In the digital era, banking systems have rapidly evolved from traditional branch-based services to fully digital platforms. Online banking applications now handle millions of transactions daily, making them prime targets for cyberattacks. Among various threats, brute-force login attacks, credential stuffing, and automated bot-based intrusions pose significant risks to user accounts and financial data. As cyber threats grow in complexity and scale, traditional security mechanisms alone are no longer sufficient to protect sensitive financial systems. Conventional banking security measures such as static password verification, simple lockout policies, and firewall-based filtering provide a basic level of protection. However, attackers increasingly use automated tools capable of generating thousands of login attempts within seconds, making it essential to adopt intelligent and adaptive defense mechanisms. This is where Artificial Intelligence (AI) and machine learning techniques play a transformative role.

OBJECTIVES

- To simulate real-time brute-force login attacks in order to evaluate the robustness of banking application security mechanisms.
- To design and implement a multi-threaded attack engine capable of generating large-scale automated login attempts.
- To develop rule-based security mechanisms such as failed login tracking and threshold-based IP blocking.
- To implement smart rate limiting algorithms to restrict excessive login attempts within a specific time window.
- To integrate machine learning-based anomaly detection for identifying abnormal login behaviors and suspicious activity patterns.
- To automatically block malicious IP addresses with a timer-based unblocking mechanism

II. LITERATURE SURVEY

1. **Sommer, R., and Paxson, V. (2010) in their paper "Outside the Closed World:** On Using Machine Learning for Network Intrusion Detection" discussed the challenges of applying machine learning techniques to real-world intrusion detection systems. The authors highlighted the limitations of traditional signature-based detection methods and emphasized the importance of anomaly detection models that can identify previously unseen attacks. Their work

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503331|

demonstrated that machine learning can significantly enhance detection accuracy by analyzing traffic patterns and behavioral deviations, making it highly relevant for AI-driven banking security systems.

2. Goodfellow, I., Bengio, Y., and Courville, A. (2016) in their book "Deep Learning" provided foundational knowledge on neural networks and deep learning architectures used for anomaly detection and cybersecurity applications. The authors explained how deep learning models can automatically extract complex patterns from large datasets and detect irregular behaviors. Their research supports the integration of AI-based behavioral analysis in security systems to identify suspicious login attempts and abnormal user activity..

3. G., and Vazquez, E. (2009) in their paper "Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges" presented a comprehensive review of anomaly detection methods used in cybersecurity. They discussed statistical approaches, machine learning algorithms, and hybrid detection systems that combine rule-based and intelligent methods. Their findings emphasized that combining multiple defense strategies significantly improves detection efficiency and reduces false positives, which aligns with the layered defense approach used in AI-driven banking security systems.

4. Buczak, A. L., and Guven, E. (2016) in their paper "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection" examined various data mining and machine learning techniques applied in intrusion detection systems. The study compared supervised and unsupervised learning models, highlighting their strengths in identifying malicious patterns in login behavior and network traffic. The authors concluded that machine learning models provide adaptive security solutions capable of responding to evolving cyber threats.

V. EXISTING & PROPOSED SYSTEM

5.1 EXISTING SYSTEM

In traditional banking applications, security mechanisms primarily rely on basic authentication methods such as username-password verification, CAPTCHA validation, and simple account lockout policies. These systems are generally protected by firewalls and standard intrusion detection systems (IDS) that operate using predefined rules or signature-based detection. While such approaches provide a foundational level of security, they are often reactive rather than proactive in handling advanced cyber threats. Most existing systems implement fixed threshold-based account locking mechanisms, where a user account is temporarily blocked after a certain number of failed login attempts. Although this method reduces brute-force attacks to some extent, attackers can bypass it by distributing login attempts across multiple IP addresses. Additionally, traditional systems often lack real-time behavioral analysis, making it difficult to detect abnormal access patterns or automated bot-driven attacks. Conventional intrusion detection systems depend heavily on known attack signatures and predefined rules. As a result, they struggle to identify zero-day attacks or previously unseen attack patterns. These systems also generate high false-positive rates, leading to unnecessary blocking of legitimate users and reduced user experience. Furthermore, static rate limiting without adaptive intelligence may either be too strict or too lenient under varying traffic conditions.

5.2 PROPOSED SYSTEM

The proposed AI-Driven Banking Security System is designed to provide a comprehensive and intelligent defense mechanism against brute-force and abnormal login attacks in banking applications. Unlike traditional security models that rely solely on static rules, the proposed system integrates rule-based protection with AI-driven anomaly detection to create a layered and adaptive security framework. The system consists of two primary modules the Attack Simulation Module and the Defense Mechanism Module. The attack module generates automated brute-force login attempts using a multi-threaded engine to simulate real-world cyberattacks. This allows the system to test its resilience under high-volume malicious traffic conditions. The defense module continuously monitors login activities and applies multiple security checks in real time. The defense mechanism incorporates smart rate limiting to control excessive login attempts within a specific time interval. If the number of failed attempts exceeds a predefined threshold, the system automatically blocks the suspicious IP address. Additionally, the system maintains a database of login attempts, failed login counts, blocked IP addresses, and security logs to ensure traceability and monitoring.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503331|

VI. BLOCK DIAGRAM

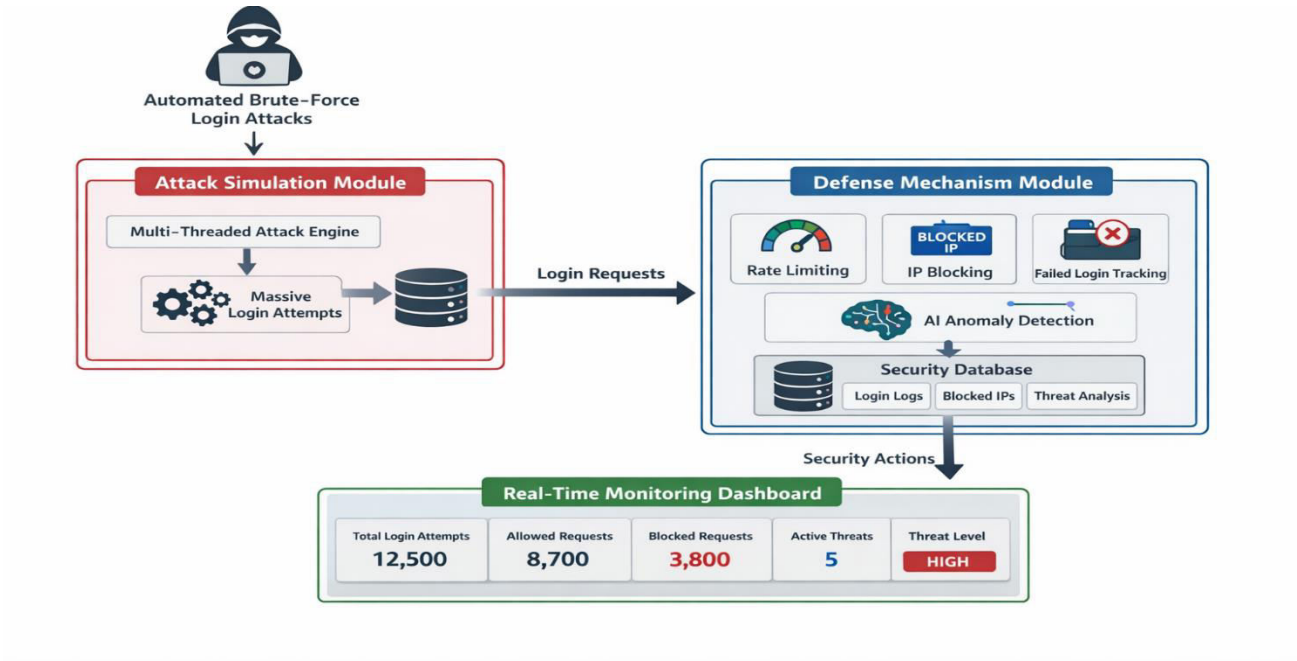


Fig No: 1 Software block diagram

VII. SOFTWARE REQUIREMENTS

1. **Operating System**

The project can be implemented on Windows 10 or 11, Linux (such as Ubuntu 20.04 or later), or macOS. A 64-bit operating system is recommended to ensure compatibility with deep learning libraries and efficient memory utilization. Linux is often preferred for large-scale training due to better GPU and driver support.

Fig No: 2 Operating System

2. **Programming Language**

Python 3.8 or above is used as the primary programming language for this project. Python is widely used in Natural Language Processing and Machine Learning because of its simplicity, readability, and vast ecosystem of libraries. It provides strong support for implementing transformer-based models efficiently.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503331|

Fig No: 3 Programming Language

3. **Development Environment / IDE**

The project can be developed using Integrated Development Environments (IDEs) such as Jupyter Notebook, Visual Studio Code (VS Code), or PyCharm. Jupyter Notebook is especially useful for experimentation and visualization, while VS Code and PyCharm provide structured project development features. Anaconda can also be used for managing virtual environments and dependencies.

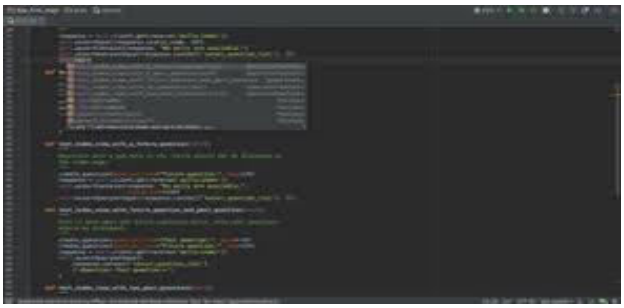


Fig No: 4 Development Environment / IDE

4. **Backend Framework**

Flask is a lightweight and flexible web framework used as the backend foundation of the AI-Driven Banking Security System. It is written in Python and is designed to be simple, modular, and easy to integrate with various libraries and tools. Flask follows a minimalistic approach, providing essential components for web development while allowing developers to customize additional features as required. In this project, Flask is used to handle routing, API creation, request processing, and communication between the frontend dashboard and backend security logic.

Fig No: 5 Backend Framework

5. **Frontend Technologies**

The frontend of the AI-Driven Banking Security System is developed using HTML5, CSS3, and Vanilla JavaScript to create an interactive and responsive user interface. HTML5 is used to structure the login page and real-time monitoring dashboard, ensuring clear organization of components such as login forms, attack control buttons, statistics panels, and

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

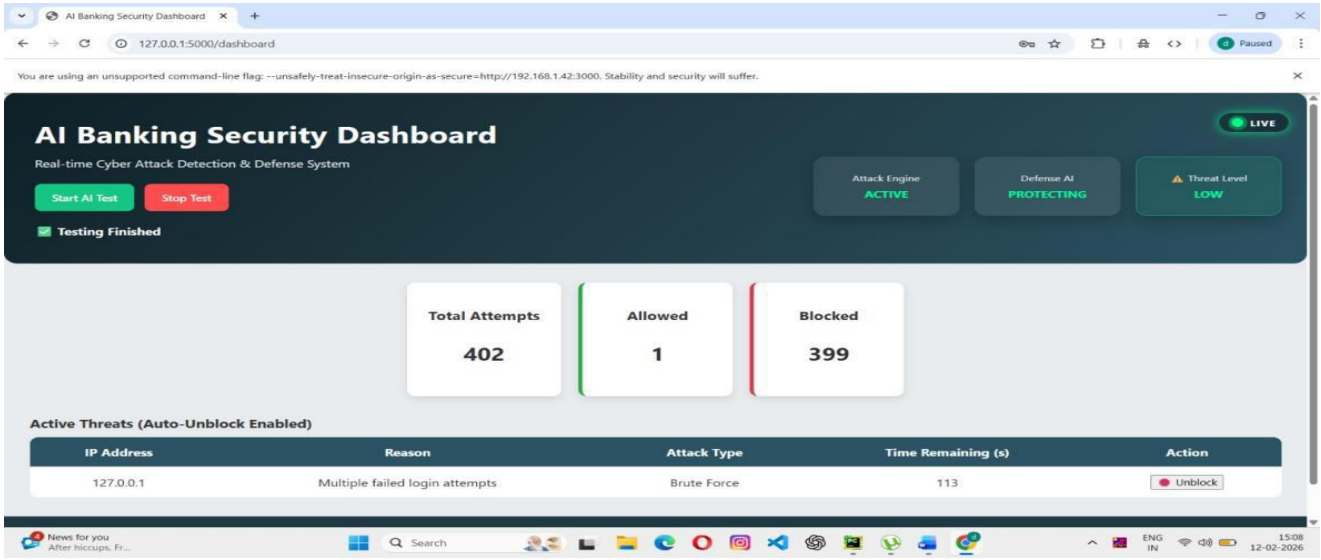
|DOI: 10.15680/IJIRSET.2026.1503331|

threat level indicators. It provides semantic elements that improve readability and maintainability of the application interface.

Fig No: 6 Frontend Technologies

VIII. RESULT

The AI-Driven Banking Security System was successfully implemented and tested under simulated brute-force attack conditions. The multi-threaded attack engine generated large volumes of login attempts to evaluate the robustness of the defense mechanisms. During testing, the system effectively monitored all incoming login requests and recorded them in the security database for analysis. The rate limiting mechanism successfully restricted excessive login attempts within a defined time window. When the number of failed login attempts exceeded the predefined threshold, the system automatically blocked the suspicious IP addresses. The auto IP blocking feature with timer-based unblocking ensured that malicious activity was controlled without permanently restricting legitimate users. The AI-based anomaly detection module demonstrated the ability to identify abnormal login behavior patterns such as rapid request bursts, repeated failed attempts, and unusual access frequency. Upon detecting suspicious activity, the system dynamically increased the threat level indicator (Low, Medium, High) and triggered defensive actions. This adaptive behavior improved overall security effectiveness compared to static rule-based systems.



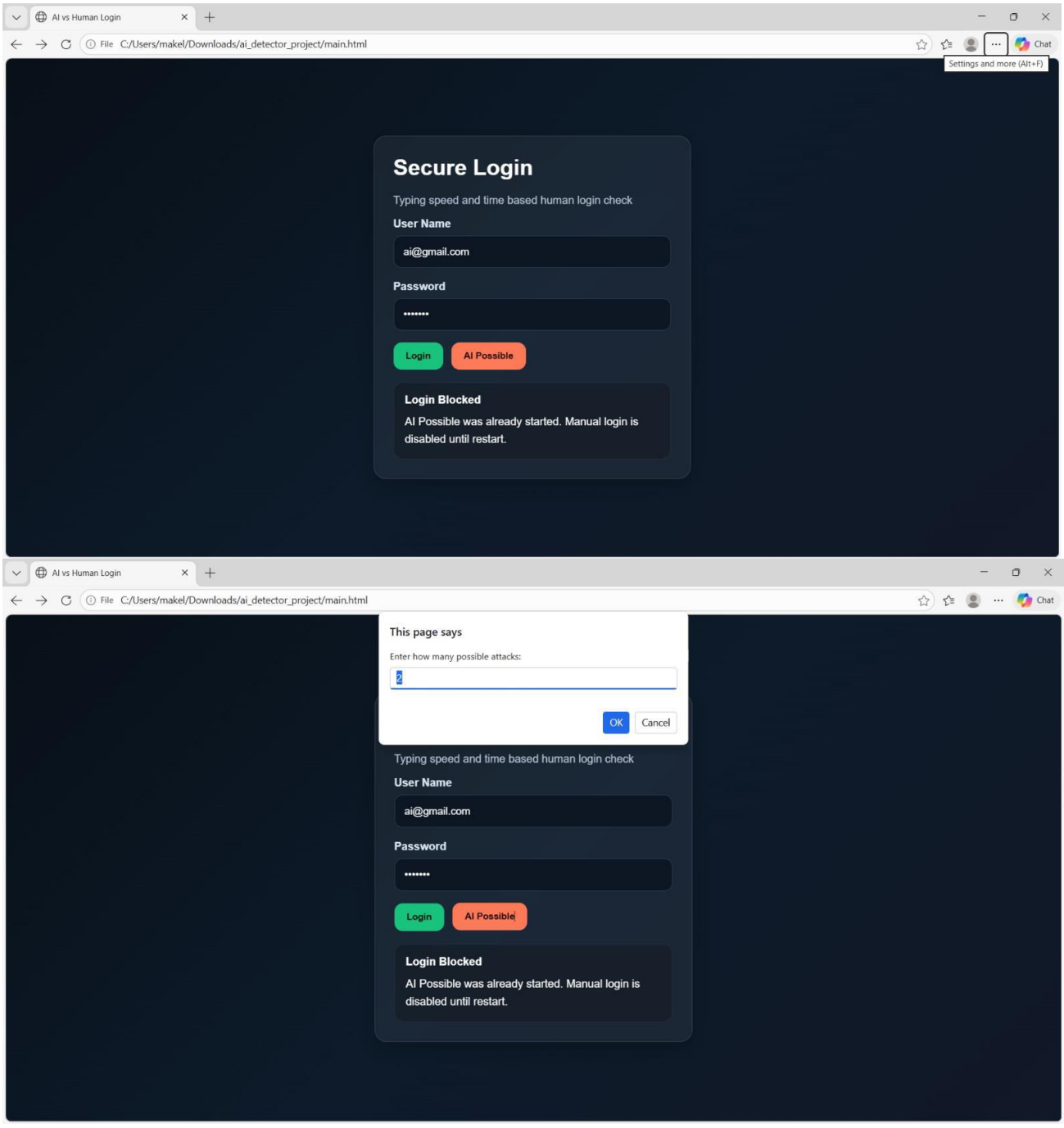
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503331|



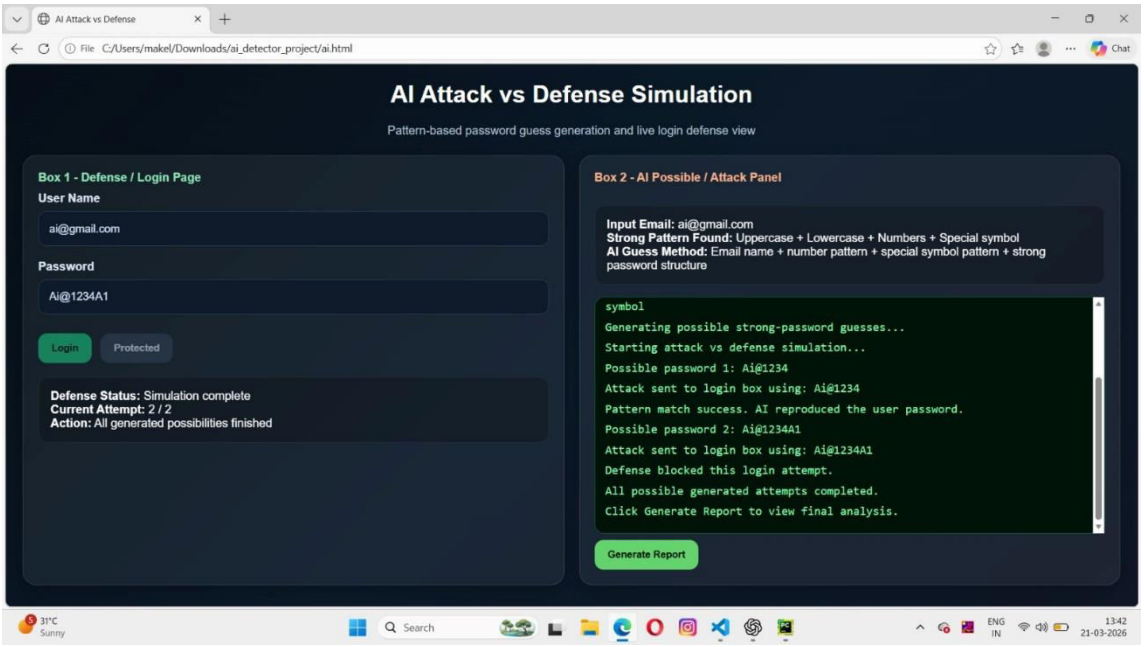
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503331|



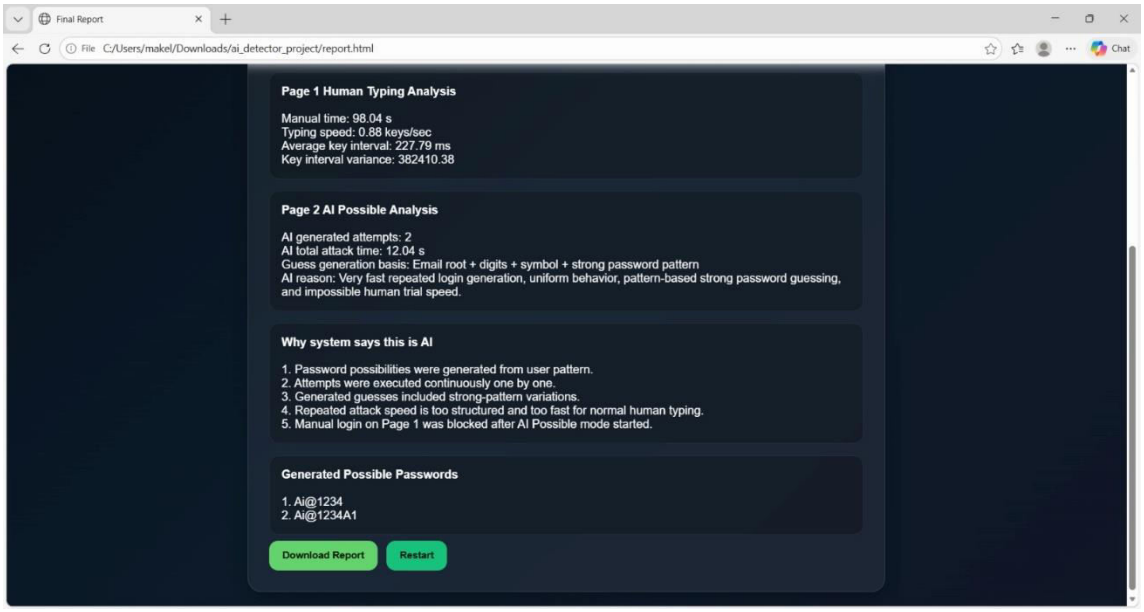


Fig no:7 Output screen

REFERENCES

1. Sommer, R., and Paxson, V. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy, pp. 305–316.
2. Garcia-Teodoro, P., Diaz-Verdejo, J., Macia-Fernandez, G., and Vazquez, E. (2009). Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges. Computers & Security, 28(1–2), pp. 18–28.
3. Buczak, A. L., and Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials, 18(2), pp. 1153–1176.
4. Goodfellow, I., Bengio, Y., and Courville, A. (2016). Deep Learning. MIT Press, Cambridge, MA.
5. Scikit-learn Developers. (2023). Scikit-learn: Machine Learning in Python. Available at: https://scikit-learn.org

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503331|

6. Flask Documentation. (2023). Flask Web Development Framework Documentation. Available at: https://flask.palletsprojects.com
7. OWASP Foundation. (2021). OWASP Top 10: The Ten Most Critical Web Application Security Risks. Available at: https://owasp.org
8. Stallings, W., and Brown, L. (2018). Computer Security: Principles and Practice. Pearson Education.
9. Behl, A., and Behl, K. (2020). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.
10. Chandola, V., Banerjee, A., and Kumar, V. (2009). Anomaly Detection: A Survey. ACM Computing Surveys, 41(3), Article 15.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details