Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Weblock: AI-Powered Adaptive Intrusion Detection And Digital Forensic System

D.Supriya
Computer Science & Engineering-Cybersecurity & IoT,
Malla Reddy University, Hyderabad, India

Geethika Vasanth
Computer Science & Engineering-Cyber Security
Malla Reddy University, Hyderabad, India

Hitesh Ksheersagar
Computer Science & Engineering-Cyber Security
Malla Reddy University, Hyderabad, India

Y. Aashrita
Computer Science & Engineering-Cyber Security
Malla Reddy University, Hyderabad, India

Abstract - WebLock is an AI-driven cybersecurity and digital forensics system designed to detect and analyze unauthorized access attempts in real time. Unlike traditional security solutions that simply block suspicious users, WebLock redirects potential intruders into a secure honeypot environment where their activities can be monitored without affecting the actual system. The platform supports deployment across web, desktop, and mobile environments, adapting its security mechanisms accordingly.

By analyzing login behavior, IP activity, and user interaction patterns, the system identifies anomalies using machine learning techniques. WebLock also includes a self-learning mechanism that improves detection accuracy over time by studying system logs and past attack data. All captured information is securely stored and presented through an administrative dashboard, enabling structured reporting and detailed investigation. This integrated approach provides proactive protection while supporting forensic analysis and continuous improvement.

Keywords: Artificial Intelligence (AI), Adaptive Intrusion Detection System (IDS), Honeypot Technology, Digital Forensics, Anomaly Detection, Behavioral Analysis, Cybersecurity Framework.

I. INTRODUCTION

In rapid growth, digital applications have increased the risk of cyber threats such as unauthorized access, credential misuse, and session-based attacks. Traditional security systems mainly focus on blocking suspicious users, but they often fail to analyze behavior or adapt to evolving threat patterns.

To overcome these limitations, intelligent and adaptive security mechanisms are necessary. Artificial Intelligence enables systems to detect abnormal activities by analyzing login behavior, IP addresses, and user interaction patterns in real time. AI-based anomaly detection improves accuracy compared to static rule-based security models.

Weblock is an AI-powered cybersecurity and digital forensics framework that integrates intrusion detection with honeypot-based monitoring. Instead of immediately blocking suspicious users, the system redirects them to a controlled honeypot environment where their actions can be safely observed without affecting the real system. It also included self-learning mechanism that analyze system logs and recoded attack data to improve detection accuracy over time. Additionally, a centralized administrative interface allows secure access to capture logs and supports structured report generation for investigation and documentation.

II.LITERATURE SURVEY

Recent advancements in cybersecurity research emphasize the transition from traditional rule-based systems to intelligent and adaptive intrusion detection mechanisms. Ying et al. [1] analyzed the advantages of AI-based IDS over conventional signature-based approaches. Their study demonstrated that machine learning techniques significantly improve the detection of zero-day and unknown attacks. However, the work lacked real-world implementation analysis and highlighted concerns regarding model explainability. Hybrid intrusion detection models combining rule-based techniques were explored by Raibu et al. [2] and Ahmed et al. [3]. These approaches improve detection performance by integrating signature verification with anomaly filtering.

Combining despite enhanced security accuracy, these systems required manual rule configuration and were primarily evaluated on benchmark datasets, limiting their effectiveness in real-time deployment environments.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Behavioral analysis through User and Entity Behavior Analytics (UEBA) has also gained attention. Research conducted by the Exabeam Research Team [4] and Sharma et al.[5] focused on clustering-based behavioral profiling to detect insider threats and abnormal user activity. While behavioral models improved anomaly detection capability, they suffered from high false positive rates during early training phases and lacked strong forensic evidence integration.

In the domain of mobile and browser security, Arshad et at. [6] proposed permission-based machine learning techniques for android malware detection. Although the model achieved efficient lightweight detection, it relied mainly on static analysis and did not incorporate runtime behavioral monitoring or cross- platform adaptability.

Furthermore, studies on digital forensic integrity, such as blockchain-based evidence preservation techniques, emphasize secure log storage and tamper resistance. However most existing solutions operate independently from detection systems and do not provide automated report generation mechanisms.

From the reviewed literature, it is evident that existing research primarily addresses AI-based detection, behavioral analytics, or forensic integrity as separate components. There remains a need for an integrated framework that real-time anomaly detection, honeypot-based attacker observation, adaptive learning mechanisms, centralized administrative monitoring, and automated forensics reporting. The proposed weblock system aims to bridge this gap by unifying these features into a proactive and investigative cybersecurity solution.

III.SYSTEM ANALYSIS

The Weblock system is developed to overcome the shortcomings of conventional cybersecurity mechanisms by integrating AI-based intrusion detection, honeypot-driven monitoring, and digital forensic support into a unified and adaptive framework. Traditional security systems mainly depend on firewalls, antivirus software, and rule-based Intrusion Detection System (IDS), which are effective against known attack signatures but lack the ability to detect zero-day threats, behavioral anomalies, and sophisticated insider attacks. Moreover, most existing solutions immediately block suspicious users without collecting detailed behavioral evidence, resulting in limited investigative capability and poor adaptability to emerging attack strategies. To address these challenges, Weblock continuously monitors critical parameters such as login attempts, IP addresses, device fingerprints, session attributes, and user interaction patterns to establish a behavioral baseline. Using AI-driven anomaly detection techniques, the system identifies deviations from normal patterns in real time. Instead of simply denying access, potential intruders are redirected to a controlled honeypot environment that simulates system functionality while protecting actual infrastructure and sensitive data.

All activities within the isolated environment are securely recorded and stored for forensic analysis. The system also includes a centralized administrative dashboard that enables authorized personnel to view, filter, and convert security logs into structured reports for documentation and investigation. Additionally, Weblock incorporates a self-learning mechanism that refines detection models over time by analyzing historical logs and newly observed attack behaviors. Through this intelligent, adaptive, and investigation approach, the system ensures real-time monitoring, improved detection accuracy, and secure forensic evidence management across web, desktop, and mobile platforms.

Advantages:

WebLock offers several significant advantages compared to traditional cybersecurity solutions. First, it provides AI-driven anomaly detection, which enables the system to identify unusual login patterns, abnormal user behaviour, potential zero-day threats more effectively that static rule-based systems. Second, instead of immediately blocking suspicious users, Weblock uses a honeypot-based redirection mechanism, allowing attackers to be safely monitored without exposing the real system or sensitive data. Thos approach not only protects infrastructure but also helps in understanding attacker strategies.

Another major advantage is its self-learning capability, where the system continuously analyses daily logs and recorded attack data to refine behavioural baselines and improve detection accuracy over time. This adaptive mechanism ensures that the system evolves alongside emerging cyber threats. Additionally, Weblock supports for web applications, desktop systems, and mobile environments, thereby providing consistent security across multiple platforms.

The project also strengthens digital forensic capabilities by securely storing captured logs and providing a centralized administrative dashboard for monitoring, filtering, and structured report generation. This feature simplifies investigation, documentation, and evidence management. Overall, Weblock delivers a proactive, intelligent, and investigative cybersecurity framework that enhances threat detection, improves response strategies, and supports long-term security improvement.

Weblock provides several additional advantages that strengthen its effectiveness as a modern cybersecurity framework. The system follows a proactive security approach by continuously analyzing behavioral patterns to detect suspicious activity at an early stage, thereby minimizing the risk of large-scale breaches. Its AI-based anomaly detection reduces false positives over time by distinguishing between legitimate unusual behavior and actual malicious actions. The real-time monitoring capability ensures immediate response through intelligent honeypot redirection without interrupting genuine users. By isolating suspicious users in a controlled environment, Weblock safely collects threat and attacker behaviour data without exposing sensitive infrastructure.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

The centralized administrative dashboard simples security management by providing unified access to logs, filtering tools, and automated structured report generation, which is enhances investigation, auditing, and compliance process.

METHODOLOGY

A. Architecture

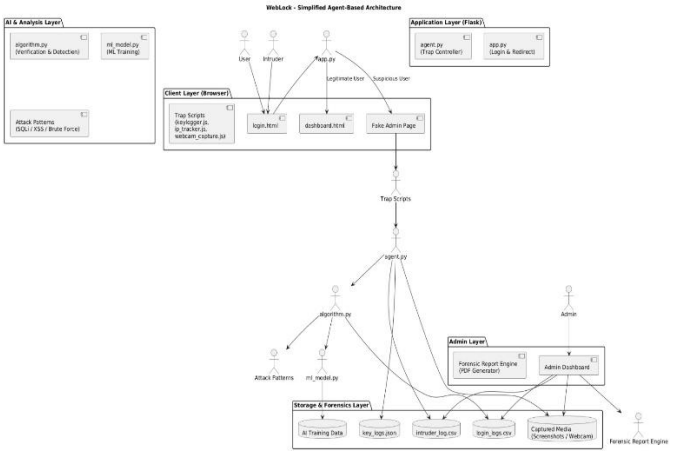

Figure 1: Architecture diagram

The WebLock architecture follows a layered, agent-based designed consisting of Client, Application, AI & Analysis, Storage, and Admin layers. Users access the system through the login interface, where suspicious behavior is detected using AI-based anomaly analysis. Legitimate users are redirected to the dashboard, while the suspicious users are sent to the fake admin page acting as a honeypot. Trap scripts collect behavioural evidence such as keystrokes, IP details, and media captures. All logs are securely stored in the forensic layer. The admin dashboard enables monitoring and automated report generation for investigation.

Frontend

The frontend layer is implemented using HTML, CSS, and JavaScript to provide interactive user interfaces including authentication, dashboard, and honeypot pages. Client-side scripts are responsible for capturing behavioral parameters such as keystrokes dynamics, session timings, and IP metadata. Trap scripts are conditionally activated for suspicious sessions to collect forensic evidence without revealing system defenses. The interface design ensures seamless redirection while maintaining session integrity and minimal latency.

Backend

The backend layer is developed using the flask framework to handle authentication workflows, request routing, and anomaly evaluation processes.

It integrates AI-based detection modules that analyze behavioral deviations using predefined and dynamically learned baselines. The agent controller manages honeypot activation, session isolation, and secure data transmission to storage modules. Role-based access control (RBAC) mechanisms regulate administrative privileges and system operations.

Database

The database layer the storage layer maintains structured and unstructured security logs, including login records, intruder activity logs, key logs, and captured media evidence. It supports AI model training by storing historical behavioral datasets and attack patterns. Data is organized in JSON/CSV formats to facilitate efficient querying, filtering, and forensic report generation. Secure access policies and integrity controls ensure tamper-resistant evidence preservation.

Overall, the architecture demonstrates a well-structured and modular design, promoting scalability, maintainability, and security.

Additional Considerations

While the diagram provides a high-level overview, there are several aspects that could be further explored. These include the deployment environment, caching mechanisms for performance optimization, load balancing strategies for handling increased traffic, and potential integration with other systems.

IV. CONCLUSION

WebLock is a comprehensive and adaptive cybersecurity framework that combines artificial intelligence, honeypot-based monitoring, and digital forensic capabilities into a unified system. Unlike conventional security solutions that primarily focus on blocking unauthorized access, Weblock adopts a proactive and investigative approach. By continuously monitoring login attempts, IP addresses, devices characteristics, and user interaction patterns, the system establishes behavioral baselines and detects anomalies in real-time using AI- driven models. Instead of immediate restricting suspicious users, the framework strategically redirects them to a controlled honeypot environment, where their activities can be safely observed and recorded without compromising the actual infrastructure or sensitive data.

The integration of self-learning mechanism enables Weblock to continuously refine its detection models by analysing historical logs and newly captured attack data. This adaptive capability ensures improved accuracy over time and enhances resilience against emerging and sophisticated cyber threats. Furthermore, the centralized administrative dashboard simplifies monitoring and provides structured log

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

analysis and automated report generation, supporting efficient investigation and documentation of security incidents. By emerging intelligent detection, safe threat observation, and structures forensic reporting, the system moves beyond reactive defences mechanisms and establishes a proactive cybersecurity model focused on continuous improvement behavioral intelligence, and long-term protection.

V. FUTURE SCOPE

The WebLock – AI powered Adaptive Intrusion Detection and Digital Forensic System establish a strong foundation for intelligent threat detection and investigation security; however, significant opportunities exist for further enhancement and expansion. In future developments, advanced deep learning architectures such as Long Short-Term Memory (LSTM) networks, transformer-based behavioral models, or graph-based anomaly detection techniques can be integrated to improve pattern recognition and reduce false positives. These models can enhance the system's ability to detect complex multi-stage attacks and subtle behavioral deviations that traditional algorithms may overlook.

The integration of real-time global threat intelligence feeds can further strengthen detection accuracy by enabling cross-verification of suspicious IP addresses, domains, and attack signatures with external cybersecurity databases. Additionally, incorporating adaptive deception techniques, such as dynamic and context-aware honeypots, can provide deeper attacker engagement and improved threat intelligence collection. Such honeypots could automatically modify system responses based on attacker interaction patterns, allowing more detailed behavioral profiling.

To enhance forensic reliability, blockchain-based log integrity mechanisms can be implemented to ensure tamper proof storage of captured evidence. This would improve the admissibility of digital evidence in legal and compliance investigations. Furthermore, incorporating automated incident response mechanisms such as temporary account isolation, network segmentation, or real time alert escalation can transform Weblock into a semi-autonomous security response system.

From an architectural perspective, the system can be expanded into a cloud-native, microservices-based deployment model to support large-scale enterprise environments. This would enable distributed monitoring, horizontal scalability, and high availability. Integration with Security Information and Event Management (SIEM) platforms and Security Orchestration, Automation, and Response (SOAR) tools can be provided enhanced centralized threat analysis and coordinated response mechanisms.

In future iterations, WebLock can also incorporate predictive analytics and AI -driven risk scoring models to anticipate potential attacks before they occur. Cross-platform behavioral correlation across web, desktop, and mobile environments can improve contextual awareness and strengthen anomaly detection. By evolving toward a fully adaptive intelligent, and predictive cybersecurity ecosystem, Weblock has the potential to become a next-generation defense platform capable of addressing emerging cyber threats with greater precision, automation, and resilience.

REFERENCES

1. L. Ying et al. (2021) presented a study titled "**Advantages of AI-Based IDS over Traditional Methods"**
2. A. Khandelwal et al. (2020) proposed **"Browser-Based IDS and Chrome Extension Attacks**"
3. R. Chinnasamy et al. (2022) conducted a **"Survey on AI-Powered IDS"**
4. M. Rabiu et al. (2019) developed a **"Hybrid Rule-Based and ML IDS"**
5. S. Ahmed et al. (2020) explored **"Hybrid Approaches to IDS"**
6. Exabeam Research Team (2021) published **"UEBA: Concepts and Applications"**
7. P. Sharma et al. (2022) proposed **"UEBA Using Clustering Techniques"**
8. S. Arshad et al. (2018) introduced **"SIGPID: Android Malware Detection"**
9. J. Kim et al. (2019) developed **"Lightweight Malware Detection for Mobile"**
10. N. Peiravian et al. (2018) proposed **"Permission-Based Android Malware Detection"**
11. M. Rabbi et al. (2021) presented **"Mobile Anomaly Detection using Hotelling's T²"**
12. R. Sekar et al. (2019) proposed a **"Browser-Based Intrusion Prevention System"**
13. L. Gómez et al. (2022) studied **"Browser Fingerprinting and Behavioral Analysis"**
14. A. Jain et al. (2020) developed **"ML-Based Behavioral Biometrics"**
15. S. Patil et al. (2023) conducted a study titled **"Survey on Blockchain for Digital Evidence Integrity".**