Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Guerrero: An Advanced Anti-Hack Firewall-Enabled Defence Mechanism

Dr. M. Balamurugan[1], Khalandar Basha A[2], Kathiravan R[3], Sanjay S[4], Naveen N C[5]

[1,2,3,4,5] Department of Computer Science and Engineering, The Kavery Engineering College, Salem, Tamil Nadu, India

Abstract
Guerrero was developed to address the limited adaptability of static firewalls in environments exposed to evolving attacks. The framework integrates continuous traffic monitoring, cryptography-based authentication, hybrid attack detection, dynamic firewall enforcement, and service replication. A prototype was implemented using Python, Flask, Scapy, SQL logging, and host-level firewall integration. Evaluation in a controlled testbed showed 96.4% detection accuracy, 97.2% recall, and 99.2% availability during attack simulations, while maintaining low response latency.

Keywords: cybersecurity, intrusion detection, dynamic firewall, anomaly detection, service replication

1. Introduction

The expansion of cloud services, mobile access, and interconnected enterprise platforms has significantly increased the attack surface of modern organisations. Traditional firewalls remain useful for filtering recognised traffic patterns, yet they are often insufficient against polymorphic malware, distributed denial-of-service attacks, zero-day exploits, and lateral movement. For this reason, current environments require defence mechanisms that can observe traffic continuously and react without delay.

A persistent limitation in deployed security stacks is their fragmentation. Traffic analysis, authentication, firewall control, and recovery are frequently managed by separate tools. This separation slows incident response and increases downtime. In addition, rule-based systems may not reliably distinguish malicious anomalies from legitimate traffic surges, while weak authentication can expose management channels and logs to interception. Consequently, secure and adaptive coordination is needed [1], [3], [5].

To address this gap, Guerrero was designed as a unified anti-hack firewall-enabled defence mechanism. It combines real-time monitoring, cryptography-based authentication, hybrid attack detection, dynamic firewall enforcement, and service replication. The framework was implemented as a prototype and assessed in a controlled testbed. This paper presents the architecture, methodology, and performance outcomes, and demonstrates how coordinated control can improve both security and availability.

2. Literature Review

Foundational research established the key principles behind intrusion detection and prevention. Denning introduced behavioural monitoring through audit data, while Lee and Stolfo demonstrated that structured

feature construction can strengthen intrusion-detection modelling. NIST guidance clarified deployment considerations for intrusion detection and prevention systems, and Snort showed the effectiveness of lightweight signature-based inspection in operational networks [1], [2], [3], [4]. These studies remain influential, but they depend heavily on fixed rules, manual tuning, and separated control layers.

More recent work has focused on adaptive firewalls, deep learning, layered defence, and integrated threat analysis. Reinforcement learning-based policy updates, LSTM-CNN orchestration, and firewall-IDS integration have reported strong results in specialised settings. However, these approaches are often limited by computational overhead, narrow deployment scope, or interoperability issues. A practical gap still exists for a framework that unifies monitoring, secure authentication, dynamic containment, and service continuity within one operational loop.

No.	Author(s) and Year	Technique Used	Focus / Strength	Limitation / Research Gap
1	Denning (1987)	Audit-data intrusion detection	Established behavioural monitoring	Limited automation and adaptation
2	Ahmadi (2025)	Reinforcement learning and continual learning	Adaptive firewall retraining	High computational overhead
3	Saeidlou et al. (2025)	LSTM-CNN parallel orchestration	High-accuracy intrusion detection	Requires GPU-class resources
4	Diningrat (2025)	Firewall and IDS integration review	Better prevention through synergy	Needs careful deployment and tuning

Table 1: Literature Comparison

3. Methodology

Guerrero was developed as a modular cybersecurity platform that continuously monitors traffic, secures communication, identifies suspicious behaviour, applies automated containment, and preserves service availability. Its architecture consists of six connected functional layers: traffic monitoring, cryptography and authentication, attack detection, dynamic firewall control, clone/replication management, and an interactive dashboard supported by centralised logging. The prototype was implemented using Python for packet analysis and logic processing, Flask for service APIs, HTML/CSS and JavaScript for the interface, SQL for event storage, and operating-system firewall integration through iptables. This design supports both on-premises and cloud-assisted deployment.

The monitoring layer captures inbound and outbound packets and extracts the source address, destination address, port, protocol, packet size, request frequency, and timestamp. A recent traffic baseline is maintained to estimate normal behaviour. Let x_t denote the current traffic rate, μ_t the moving average, and σ_t the standard deviation. The anomaly score is defined as $A_t = |x_t - \mu_t| / \sigma_t$. A higher value indicates a stronger deviation from expected traffic. Events that exceed the threshold are forwarded to the detection engine for deeper analysis. The engine then combines signature matching with behavioural scoring to identify repeated login failures, multi-port probing, protocol misuse, and traffic surges.

The risk score is computed as $R = \alpha S + \beta A_t + \gamma F$, where S is the signature score, F is the recurrence factor, and α, β, and γ are tunable weights. Low-risk events are logged for later review. Moderate-risk events trigger alerts and temporary restrictions. High-risk events activate immediate firewall containment through IP blocking, port restriction, or traffic throttling. Authentication is protected through salted hashing, JSON Web Token (JWT) validation, Transport Layer Security (TLS), and role-based access control. When service availability is threatened, the replication layer activates a clone and redirects traffic until the threat subsides.

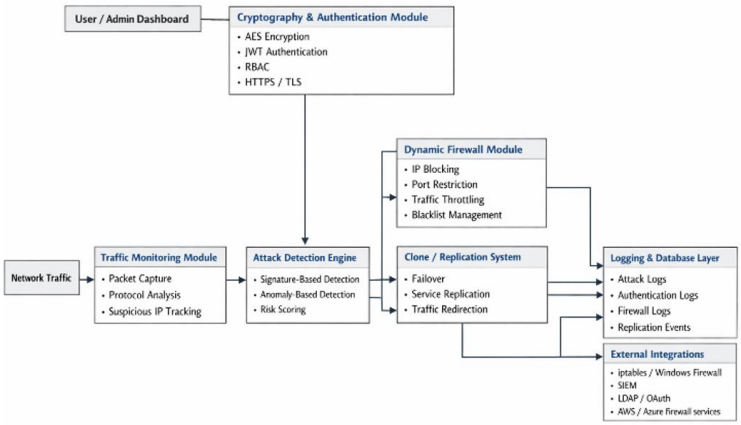

Fig 1: System Architecture Diagram

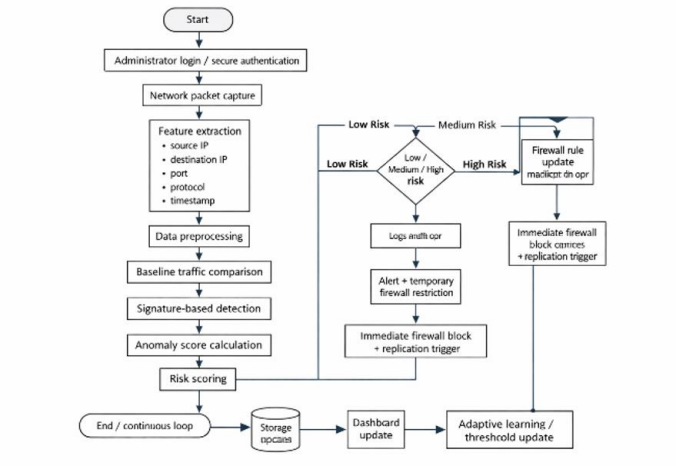

Fig 2: Workflow Diagram

4. Results and Discussion

A functional prototype of Guerrero was evaluated in a controlled Linux-based testbed. Python services, SQL-backed logging, HTTPS-secured APIs, and iptables-based firewall enforcement were deployed on the host. Client nodes generated legitimate HTTP, HTTPS, DNS, and SSH traffic, while scripted attack traffic represented brute-force login attempts, port scans, flooding, and repeated suspicious requests. Approximately 15,000 sessions were generated, including 12,000 benign sessions and 3,000 malicious events. The system was evaluated using detection quality, latency, firewall response time, authentication overhead, and service availability.

The prototype demonstrated stable real-time behaviour across the primary attack scenarios. Signature-based rules were effective for brute-force and port-scanning detection, while anomaly scoring improved

recognition of traffic bursts that were not easily captured by rules alone. The firewall control path responded quickly after high-risk classification, and the replication mechanism preserved service continuity during attacks aimed at availability. Additional observations showed an average firewall rule deployment time of 1.3 s, authentication overhead of 41 ms, failover activation time of 3.6 s, and a false-positive rate of 3.4%.

Metric	Observed Value	Interpretation
Overall detection accuracy	96.4%	Hybrid detection identified most malicious events
Precision	95.1%	Low volume of irrelevant alerts
Recall	97.2%	Strong capture of true attack activity
Mean packet/flow analysis latency	68 ms	Suitable for near real-time monitoring
Availability during attack simulation	99.2%	High uptime maintained under stress

Table 2: System Performance

The findings indicate that Guerrero benefits from combining multiple defensive layers within one coordinated workflow. The hybrid detection model reduced the blind spots associated with static rule-based systems, and dynamic firewall automation shortened the response window after threat confirmation. The replication mechanism further improved resilience by preserving service availability during active attacks. The primary limitation was the appearance of false positives during abrupt but legitimate traffic spikes, which indicates that threshold calibration remains important in highly variable environments.

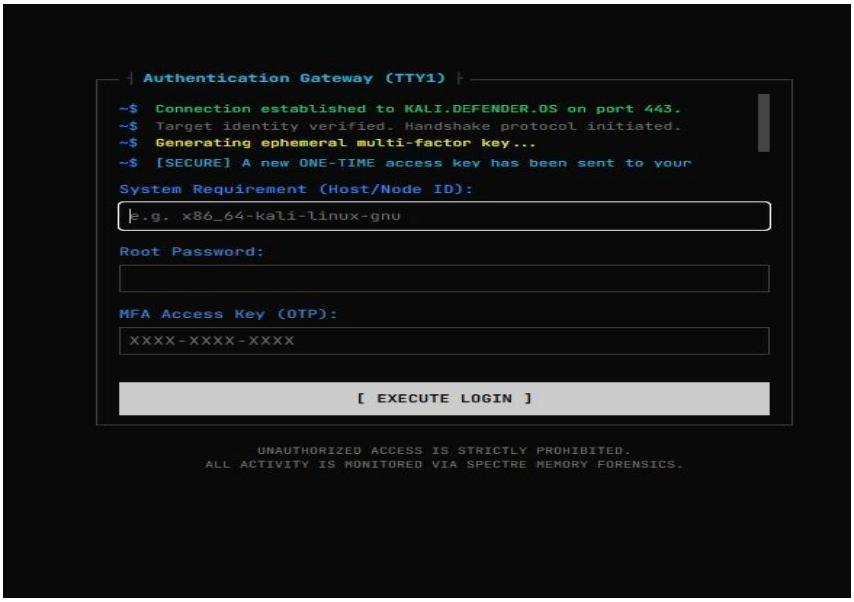

Fig 3: Application Screenshot – Home Page

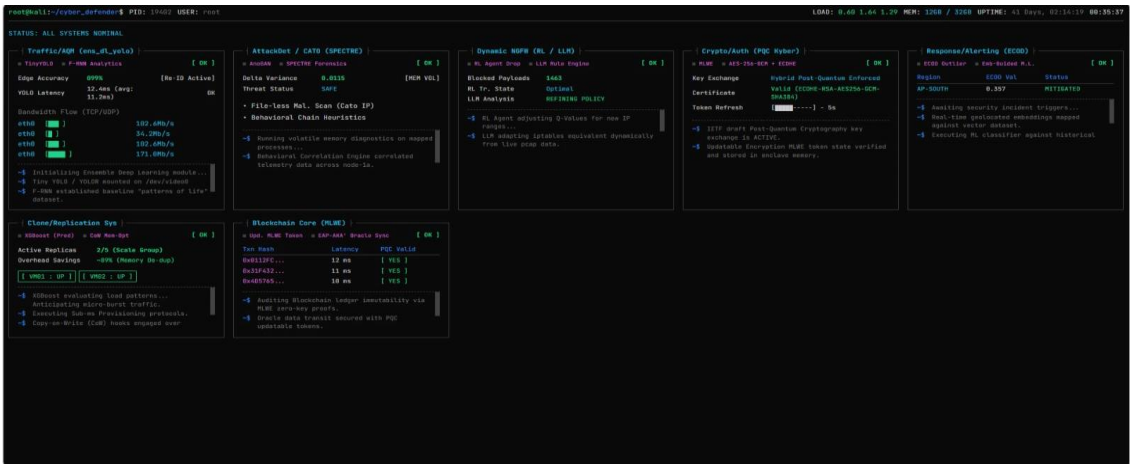

Fig 4: Application Screenshot – Results Page

5. Conclusion

Guerrero was presented as an advanced anti-hack firewall-enabled defence mechanism that unifies traffic monitoring, secure authentication, hybrid attack detection, dynamic firewall control, and service replication within a single framework. The prototype achieved high detection accuracy, low response latency, and strong service continuity under attack conditions. The results suggest that coordinated multi-layer defence can offer more practical protection than static standalone firewalls in dynamic network environments.

6. Acknowledgement

The authors sincerely thank the institution, the Department of Computer Science and Engineering, and the project guide for their support and guidance throughout this work. The authors also acknowledge the laboratory staff and administrative team for providing the facilities required for the study.

References

1. D. E. Denning, “An intrusion-detection model,” IEEE Transactions on Software Engineering, vol. SE-13, no. 2, pp. 222–232, Feb. 1987.
2. W. Lee and S. J. Stolfo, “A framework for constructing features and models for intrusion detection systems,” ACM Transactions on Information and System Security, vol. 3, no. 4, pp. 227–261, Nov. 2000.
3. K. Scarfone and P. Mell, Guide to Intrusion Detection and Prevention Systems (IDPS), NIST Special Publication 800-94, 2007
4. M. Roesch, “Snort: Lightweight intrusion detection for networks,” in Proc. 13th USENIX Conf. System Administration, 1999, pp. 229–238.
5. E. Rescorla, “The Transport Layer Security (TLS) protocol version 1.3,” IETF RFC 8446, Aug. 2018.
6. Cisco Systems, “Next-generation firewall overview,” Technical Whitepaper, 2023.