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

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

Adaptive Zero-Trust and AI-Driven Defense Framework for Modern Network Cybersecurity

Ms. Rutuja Phadtare
Dr. D. Y. Patil Arts, Commerce and Science College,
Pimpri, Maharashtra, India

Ms. Dnyanda Salunkhe
Dr. D. Y.Patil Arts, Commerce and Science College,
Pimpri, Pune, Maharashtra, India

Abstract - The rapid growth of modern network environments driven by IoT adoption, 5G infrastructure, cloud computing, and remote work models has significantly expanded the cybersecurity attack surface. Organizations are increasingly exposed to advanced persistent threats, ransomware campaigns, zero-day exploits, supply chain attacks such as SolarWinds and Log4j, and large-scale distributed denial-of-service attacks. Traditional perimeter-based security mechanisms, including firewalls and signature-based intrusion detection systems, are no longer sufficient against adaptive and stealthy adversaries that use automation and AI-assisted evasion techniques. This study examines current cyber threat patterns and evaluates weaknesses in legacy security architectures through comparative analysis and enterprise security scenarios. To address these gaps, the paper proposes a layered defense framework based on zero-trust principles, continuous identity verification, behavioral monitoring, and automated response coordination. The proposed model integrates AI-driven anomaly detection, machine-learning-enhanced endpoint detection and response, and centralized SIEM orchestration to improve visibility, detection speed, and response accuracy across network layers. The framework is evaluated using controlled attack simulations and practical deployment scenarios, with performance measured through detection latency, breach dwell time, and containment efficiency.The results demonstrate improved early threat detection and up to a 40% reduction in breach dwell time compared to conventional security approaches, along with more consistent incident response performance. Implementation challenges such as skill shortages and system integration complexity are also identified. The study supports adoption of adaptive, intelligence-driven cybersecurity architectures to strengthen resilience in evolving digital network environments.

Keywords:

- **Zero Trust Security AI-Driven Cyber Defense,**
- **Network Threat Detection,**
- **SIEM and EDR**
- **Cybersecurity Framework**

I. INTRODUCTION

Enterprise computing has shifted from centralized, perimeter-protected networks to distributed and service-oriented environments built on cloud platforms, remote endpoints, and connected devices. This transformation improves flexibility but increases exposure to cyber threats. Industry breach investigations consistently show that attackers increasingly exploit identity, misconfiguration, and lateral movement paths rather than only perimeter weaknesses .

Modern adversaries use multi-stage intrusion chains, credential abuse, and stealth persistence techniques. Many attacks are designed to blend with legitimate administrative behavior, making signature-only detection unreliable [8]. As defined in zero-trust security models, implicit trust based on network location is no longer acceptable

This paper proposes a layered, adaptive defense framework combining zero-trust access control, AI-assisted anomaly detection, endpoint intelligence, and centralized orchestration, and evaluates its effectiveness using controlled scenarios.

II. BACKGROUND AND THREAT LANDSCAPE

Recent threat reports show that ransomware and advanced intrusion campaigns increasingly involve staged execution, privilege escalation, and data exfiltration before impact delivery , Supply-chain compromises demonstrate that even trusted software distribution channels can be abused. Zero-day vulnerabilities remain especially dangerous because they bypass signature-based controls .

Behavioral mapping frameworks such as the ATT&CK knowledge base document how attackers reuse legitimate tools and processes to avoid detection . Large botnets composed of poorly secured devices continue to enable high-volume denial-of-service attacks.

These patterns indicate that detection strategies must move beyond known indicators toward behavioral and anomaly-based methods.

III. LIMITATIONS OF LEGACY SECURITY MODELS

Traditional perimeter-centric architectures rely on firewalls, static rules, and signature-based intrusion detection systems . While still necessary, these controls show several weaknesses:

- Limited internal traffic visibility
- Failure against unknown or modified threats

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

- Disconnected security tool alerts
- Manual response delays
- Static trust zones that allow lateral spread

Empirical studies of intrusion detection have shown that purely signature-driven approaches struggle in dynamic environments . As a result, attackers may remain undetected for extended periods, increasing operational damage.

IV. RELATED WORK

Zero-trust architecture formally defines continuous verification of identity, device, and context for every access request . Micro-segmentation and least-privilege access reduce lateral movement risk.

Machine learning has been widely studied for anomaly and intrusion detection. Research demonstrates that ML models can detect deviations from baseline behavior without prior signatures, though model tuning is critical .

Cloud and distributed system security guidance emphasizes centralized telemetry and cross-layer visibility. Integrated monitoring and correlation platforms improve response coordination but introduce integration complexity.

Most prior work examines these approaches separately. This study evaluates their combined layered application.

V. PROPOSED MULTI-LAYERED DEFENSE FRAMEWORK

The framework applies coordinated defense-in-depth with continuous verification.

- **A. Zero-Trust Access Layer**
  Access is evaluated continuously using identity, device posture, and context signals, aligned with zero-trust architecture guidance . Multi-factor authentication and least-privilege enforcement are applied.
- **B. Behavioral Monitoring Layer**
  User and system behavior baselines are established. Deviations such as unusual login timing or abnormal transfer patterns are flagged .
- **C. AI-Based Anomaly Detection**
  Unsupervised ML models analyze traffic and activity features to detect irregular patterns beyond known signatures .
- **D. Endpoint Detection and Response**
  Endpoint telemetry captures process chains and memory behavior, supporting rapid host isolation and containment.
- **E. Centralized Event Orchestration**
  Cross-layer telemetry is aggregated and correlated in a central platform, enabling automated response playbooks consistent with modern SIEM practice .

VI. FRAMEWORK ARCHITECTURE OVERVIEW

Figure 1 — Proposed Framework Architecture (to be drawn):

Draw five stacked layers:

1. Identity & Zero-Trust Access
2. Behavioral Analytics Engine
3. AI Anomaly Detection
4. Endpoint Detection & Response
5. Central SIEM & Orchestration

Show arrows upward labeled “Telemetry & Logs” and arrows downward labeled “Automated Response Actions.”

(One clean block diagram is sufficient for IEEE UG submission.)

VII. METHODOLOGY

A comparative experimental design was used with two environments:

- Baseline legacy layered security
- Proposed adaptive layered framework

  A hybrid testbed included endpoints, cloud workloads, identity services, and centralized logging.
- **Attack Scenarios**
- Credential compromise and lateral movement
- Ransomware execution chain
- Covert command-and-control traffic
- Insider-style data exfiltration

  These scenarios reflect commonly documented attack behaviors .
- **Metrics**
- Detection latency
- Attacker dwell time
- Containment start time
- Alert precision
- False positives
- **Method Justification**

Scenario simulation allows repeatable measurement across architectures and is commonly used in intrusion detection research evaluation . Selected metrics align with breach impact measurements used in industry reports .

VIII. RESULTS

The adaptive framework detected abnormal behavior earlier across most scenarios. Behavioral and ML-based analytics identified suspicious access sequences without prior signatures.

Correlation across layers reduced investigation delay. Automated endpoint isolation and credential revocation shortened response time.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 02, NCRTCS - 2026

- **Results Summary**

Metric	Legacy Model	Proposed Framework
Average Detection Time	18 min	7 min
Mean Dwell Time	5.2 days	3.1 days
Containment Start	Manual	Automated
Alert Precision	Moderate	High
False Positives	Low	Medium (before tuning)

Observed dwell time reduction was approximately **40%**, consistent with faster cross-layer correlation and automated response [10].

IX. DISCUSSION

Results support the effectiveness of layered verification and behavioral analytics. AI-assisted detection improves visibility into subtle deviations missed by rule-based systems . Central orchestration improves coordination across controls.

However, ML systems require careful tuning and retraining . Telemetry volume increases processing load. Automation must be governed to avoid operational disruption.

X. IMPLEMENTATION CHALLENGES

Deployment challenges include:

- Skill gaps in advanced security analytics
- Tool integration complexity
- Data normalization needs
- Compute overhead
- Regulatory monitoring limits

Industry cloud security guidance also notes interoperability and governance challenges in integrated monitoring environments .

XI. LIMITATIONS

This study is limited to simulated scenarios and short-duration observation. Real attacker behavior may vary. ML models may experience drift and require retraining . Enterprise-scale performance overhead was not fully measured. Longer-term field studies are needed.

XII. FUTURE WORK

Future work should explore adversarial-resistant ML detection, privacy-preserving analytics, and autonomous response coordination. Integration with emerging cryptographic and identity standards is another direction .

XIII. CONCLUSION

Modern distributed networks require security architectures that assume compromise and verify continuously. This paper presented a multi-layered framework integrating zero-trust access control, AI-driven anomaly detection, endpoint intelligence, and centralized orchestration. Comparative evaluation showed faster detection and reduced attacker dwell time compared to legacy models. Despite integration and skill challenges, adaptive layered security provides a practical path forward for modern cyber defense.

REFERENCES

[1] S. Rose et al., *Zero Trust Architecture*, NIST SP 800-207, 2020.
[2] Guide to Intrusion Detection and Prevention Systems, NIST SP 800-94, 2012.
[3] Data Breach Investigations Report, 2023, Verizon.
[4] Security Guidance for Critical Areas of Focus in Cloud Computing, Cloud Security Alliance, 2022.
[5] J. Kindervag, “Zero Trust Network Architecture,” Forrester, 2010.