International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

ADAPTIVE THREAT INTELLIGENCE: AN AI-INTEGRATED HOLISTIC FRAMEWORK FOR MODERN CYBERSECURITY

[1] Dr. G. Jawaherlalnehru, [2] Bommagani Vinay Kumar, [3] Godisela Varun, [4] Aluvala Nagaraju, [5] Bairu Naresh
[1] Associate Professor, [234] B. Tech Students
[1]Department of Computer Science and Engineering
[234]Department of CSE(CYBER SECURITY)
[1234]Sree Dattha Group of Institutions, Sheriguda, Ibrahimpatnam, 501510, Telangana, India

ABSTRACT

The rapid expansion of cloud computing, Internet of Things devices, mobile platforms, remote work infrastructures, software-defined networks, digital services, and interconnected enterprise ecosystems has significantly increased the complexity and scale of modern cybersecurity threats. Conventional security systems frequently depend on static rules, known attack signatures, isolated monitoring tools, and manually configured response mechanisms, making them less effective against zero-day attacks, advanced persistent threats, ransomware, polymorphic malware, phishing, insider misuse, credential compromise, lateral movement, and rapidly evolving adversarial behavior. This research proposes an Adaptive Threat Intelligence: AI-Integrated Holistic Framework for Modern Cybersecurity that combines heterogeneous security-data acquisition, contextual preprocessing, machine learning, deep learning, anomaly detection, natural language processing, behavioral analytics, threat intelligence fusion, dynamic risk assessment, and adaptive response within a unified architecture. The proposed framework continuously collects network traffic, endpoint telemetry, authentication events, cloud audit records, application logs, vulnerability information, email characteristics, threat indicators, user behavior, device context, and external intelligence feeds. Random Forest, Support Vector Machine, XGBoost, Isolation Forest, deep neural networks, and NLP-based intelligence analysis are integrated to identify known attacks, previously unseen anomalies, malicious communication, compromised identities, suspicious behavior, and emerging threat patterns. A hybrid threat-fusion engine correlates model predictions with Indicators of Compromise, Tactics, Techniques and Procedures, asset criticality, vulnerability exposure, identity confidence, and behavioral deviation to classify events as Normal, Suspicious, High Risk, or Critical Threat. The framework dynamically initiates actions such as enhanced monitoring, step-up authentication, traffic restriction, endpoint isolation, malicious-domain blocking, session termination, account suspension, incident escalation, and Security Operations Center notification. The architecture consists of five interconnected layers: Cybersecurity Data and Threat Intelligence Acquisition, Security Preprocessing and Contextual Intelligence, AI-Integrated Threat Detection and Analytics, Adaptive Risk Assessment and Automated Response, and Security Operations, Governance and Continuous Learning. Illustrative conceptual evaluation demonstrates improved detection accuracy, precision, recall, F1-score, threat-intelligence efficiency, and reduced analytical response time compared with traditional rule-based security, signature-based detection, and conventional machine learning approaches. The framework provides a scalable foundation for adaptive cybersecurity across enterprise networks, cloud environments, IoT ecosystems, critical infrastructure, financial services, healthcare platforms, and distributed digital systems.

Keywords: Adaptive Threat Intelligence, Artificial Intelligence, Cybersecurity, Machine Learning, Deep Learning, Anomaly Detection,

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

Threat Intelligence, Behavioral Analytics, XGBoost, Isolation Forest, NLP, Automated Incident Response, Zero-Day Attack, Security Operations Center.

I. INTRODUCTION

The continuing digital transformation of organizations has created highly interconnected computing environments composed of enterprise networks, cloud platforms, mobile devices, Internet of Things systems, remote-access infrastructures, application programming interfaces, software-as-a-service platforms, and distributed data services. Although these technologies improve operational flexibility and digital innovation, they also significantly expand the attack surface available to cyber adversaries. Modern attackers exploit vulnerabilities, compromised credentials, social engineering, malicious software, cloud misconfigurations, and trusted communication channels to penetrate organizational environments and maintain persistent access [1].

Cyber threats have evolved from relatively isolated attacks into coordinated and adaptive campaigns capable of changing behavior according to defensive conditions. Advanced persistent threats can perform reconnaissance, initial compromise, privilege escalation, credential theft, lateral movement, persistence, command-and-control communication, and data exfiltration across extended periods. Consequently, cybersecurity systems must analyze individual events together with temporal, behavioral, contextual, and relational information to recognize multi-stage attacks [2].

Traditional cybersecurity mechanisms remain essential but frequently depend on static signatures, predefined rules, fixed thresholds, and manually configured policies. Signature-based intrusion detection can identify known malicious patterns but may struggle against zero-day exploits, polymorphic malware, encrypted attacks, and modified adversarial techniques. Rule-based systems can also produce excessive false alerts because legitimate enterprise behavior is dynamic and cannot always be represented accurately through fixed conditions [3].

Threat intelligence has emerged as an important mechanism for improving cybersecurity awareness by collecting and analyzing information about malicious IP addresses, domains, malware hashes, vulnerabilities, adversary infrastructure, attack campaigns, Indicators of Compromise, and Tactics, Techniques and Procedures. However, the operational value of threat intelligence depends on relevance, freshness, confidence, contextualization, and integration with local security telemetry. Large volumes of disconnected indicators can overwhelm analysts without intelligent prioritization [4].

Artificial intelligence and machine learning provide significant opportunities for transforming threat intelligence from a predominantly reactive process into an adaptive analytical capability. Machine learning models can identify nonlinear relationships across network traffic, authentication events, endpoint activities, cloud logs, vulnerability information, and behavioral characteristics. Random Forest, Support Vector Machine, and gradient-boosting approaches can classify security events according to learned patterns and support rapid prioritization of suspicious activity [5].

Anomaly detection provides complementary capabilities because many emerging attacks do not match previously observed signatures. A compromised account may authenticate successfully using valid credentials while exhibiting unusual login times, unfamiliar device usage, abnormal resource access, or unexpected communication behavior. Isolation Forest and related unsupervised mechanisms can identify observations that deviate significantly from established baselines and therefore support detection of previously unseen threats [6].

Deep learning further strengthens cybersecurity analytics by automatically learning hierarchical

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

representations from high-dimensional data. Deep neural networks can analyze network flows, event sequences, endpoint telemetry, malware characteristics, and complex attack patterns. Sequential architectures can identify temporal relationships among security events, while representation-learning mechanisms can reduce dependence on manually engineered features. Nevertheless, deep learning requires careful management of computational cost, interpretability, class imbalance, concept drift, and adversarial manipulation [7].

Natural language processing is increasingly relevant to cyber threat intelligence because substantial security knowledge is contained in vulnerability descriptions, incident reports, threat advisories, phishing messages, analyst notes, malware reports, and unstructured intelligence documents. NLP models can extract entities, attack techniques, malicious infrastructure, vulnerability references, and semantic relationships from textual information. They can also analyze suspicious communication for phishing, impersonation, urgency manipulation, and social-engineering indicators [8].

Behavioral analytics provides another important dimension of adaptive cybersecurity. Users, devices, applications, and services develop characteristic patterns involving login frequency, access time, network destinations, resource usage, communication volume, and administrative actions. Continuous comparison of current activity with historical baselines can reveal account takeover, insider misuse, lateral movement, privilege abuse, and compromised devices even when individual actions appear technically legitimate [9].

Modern cybersecurity therefore requires a holistic framework capable of correlating diverse information rather than treating alerts independently. Threat detection should consider model predictions, behavioral anomalies, asset importance, vulnerability exposure, identity confidence, intelligence indicators, and adversary techniques. Such contextual fusion can reduce alert overload and prioritize events according to probable organizational impact [10].

Motivated by these challenges, this research proposes Adaptive Threat Intelligence: An AI-Integrated Holistic Framework for Modern Cybersecurity. The framework integrates security telemetry, external threat intelligence, machine learning, deep learning, NLP, anomaly detection, behavioral analytics, hybrid threat fusion, dynamic risk classification, automated response, analyst feedback, and continuous model adaptation.

II. LITERATURE SURVEY

Author: A. L. Buczak and E. Guven (2016)

Buczak and Guven presented a comprehensive survey of data mining and machine learning techniques for cybersecurity intrusion detection. Their study examined classification, clustering, association analysis, and anomaly-detection approaches and demonstrated the significant potential of intelligent models for identifying malicious activity within complex security datasets. The work provides a strong foundation for AI-integrated threat detection [11].

Author: R. Sommer and V. Paxson (2010)

Sommer and Paxson examined the practical limitations of machine learning for network intrusion detection and emphasized differences between controlled experimental environments and operational networks. Their research highlighted challenges involving data distribution, semantic gaps, false positives, and changing network behavior. These observations are highly relevant to adaptive threat-intelligence systems requiring continuous validation and contextual interpretation [12].

Author: F. T. Liu, K. M. Ting, and Z.-H. Zhou (2008)

Liu, Ting, and Zhou introduced Isolation Forest as an efficient anomaly-detection technique based on randomized isolation. The method is particularly relevant to modern cybersecurity

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

because previously unseen attacks, compromised identities, and abnormal devices may deviate from normal behavioral patterns without matching known signatures. Isolation Forest therefore provides an important unsupervised component for adaptive threat detection [13].

Author: N. Moustafa and J. Slay (2015)

Moustafa and Slay introduced the UNSW-NB15 dataset for modern network intrusion-detection research. Their work emphasized the importance of representative security datasets containing normal and malicious network behavior. The study supports systematic evaluation of intelligent cybersecurity frameworks and highlights the requirement for realistic testing beyond outdated attack environments [14].

Author: T. Chen and C. Guestrin (2016)

Chen and Guestrin introduced XGBoost, a scalable gradient-boosting framework capable of modeling complex nonlinear relationships in structured datasets. Within cybersecurity, XGBoost can process network statistics, authentication attributes, endpoint indicators, asset context, and vulnerability characteristics to classify suspicious events and support dynamic risk estimation [15].

Author: A. Khraisat et al. (2019)

Khraisat and colleagues surveyed intrusion-detection techniques, datasets, and major implementation challenges. Their research discussed signature-based, anomaly-based, and hybrid detection mechanisms and emphasized difficulties involving false alarms, evolving attacks, and dataset quality. The work supports the development of integrated cybersecurity frameworks combining complementary detection strategies [16].

Author: S. Rose et al. (2020)

Rose and colleagues presented the NIST Zero Trust Architecture and emphasized continuous verification, explicit access decisions, resource-centric protection, and the elimination of implicit trust. These principles are directly relevant to adaptive threat intelligence because identity, device context, session behavior, and resource sensitivity should be continuously evaluated rather than trusted permanently after initial authentication [17].

Author: B. E. Strom et al. (2018)

Strom and colleagues developed the MITRE ATT&CK knowledge base framework for representing adversary tactics and techniques. ATT&CK provides a structured mechanism for understanding how adversaries operate across different stages of an attack. The framework is highly relevant to holistic threat intelligence because isolated indicators can be correlated with broader adversarial behavior [18].

Author: Y. LeCun, Y. Bengio, and G. Hinton (2015)

LeCun, Bengio, and Hinton provided a comprehensive overview of deep learning and representation-learning mechanisms. Their work demonstrated the capability of deep neural architectures to learn complex hierarchical features from high-dimensional information. These principles support deep-learning-based analysis of network traffic, event sequences, malware characteristics, and heterogeneous cybersecurity telemetry [19].

Author: R. Anderson (2020)

Anderson examined fundamental security-engineering principles involving authentication, access control, threat modeling, system resilience, and dependable distributed systems. The work emphasized that effective cybersecurity requires integrated architectural design rather than isolated defensive tools. These principles strongly support the proposed holistic AI-integrated cybersecurity framework [20].

III. SYSTEM ANALYSIS & DESIGN

3.1 Existing System

Existing cybersecurity systems commonly depend on firewalls, antivirus software, signature-based intrusion detection, predefined correlation rules, static access policies, manually maintained blacklists, and independent security monitoring tools. These mechanisms remain

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

valuable for baseline protection but frequently analyze events within isolated technological domains. Network systems may monitor traffic, endpoint tools may analyze local processes, identity platforms may evaluate authentication, and cloud platforms may maintain separate audit records without comprehensive real-time correlation. This fragmentation limits visibility into multi-stage attacks that move across identities, endpoints, networks, applications, and cloud resources.

Traditional systems also depend heavily on known attack patterns and fixed security conditions. Signature-based mechanisms can efficiently detect previously documented malware or exploit characteristics but may fail against zero-day attacks, polymorphic malware, modified payloads, compromised legitimate accounts, and low-and-slow adversarial activity. Static thresholds may generate excessive false positives when legitimate workloads change or may miss subtle malicious behavior that remains below predefined limits. Manual investigation of large alert volumes further delays incident prioritization and response.

Another major limitation is the insufficient integration of external threat intelligence with internal organizational context. A malicious indicator may be globally relevant but unrelated to a particular enterprise, while a low-profile indicator may represent severe risk when associated with a critical asset or vulnerable system. Conventional tools often lack dynamic fusion of threat intelligence, behavioral deviation, asset criticality, vulnerability exposure, identity confidence, and adversary techniques. As a result, security teams may experience alert fatigue, delayed detection, fragmented investigation, and inefficient defensive response.

Disadvantages of Existing System

1. Traditional mechanisms depend heavily on known signatures and static rules.
2. Isolated security tools create fragmented threat visibility.
3. Zero-day attacks and previously unseen anomalies may remain undetected.
4. Static thresholds can produce high false-positive rates.
5. External threat intelligence may lack organizational context.
6. Manual alert analysis delays threat prioritization and response.
7. Conventional systems provide limited continuous behavioral adaptation.
8. Multi-stage attacks may not be correlated across security domains.

3.2 Proposed System

The proposed **Adaptive Threat Intelligence AI-Integrated Holistic Framework** introduces a unified cybersecurity architecture that continuously acquires and correlates information from network traffic, endpoint telemetry, authentication systems, cloud platforms, applications, email communication, vulnerability scanners, IoT devices, threat feeds, incident reports, and external intelligence sources. The collected data undergo validation, deduplication, normalization, timestamp synchronization, session aggregation, entity resolution, contextual enrichment, and behavioral-baseline construction. Asset criticality, vulnerability exposure, identity confidence, device trust, and threat-indicator confidence are integrated into the analytical context to ensure that security events are evaluated according to their operational significance.

The intelligent analytical core integrates Random Forest, Support Vector Machine, XGBoost, Isolation Forest, deep neural networks, NLP-based threat intelligence analysis, and user and entity behavior analytics. Supervised models classify known malicious patterns, anomaly detection identifies previously unseen deviations, deep learning captures complex temporal and high-dimensional attack behavior, and NLP extracts intelligence from unstructured security

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

reports, phishing communication, vulnerability descriptions, and analyst documentation. A hybrid threat-fusion mechanism correlates model outputs with Indicators of Compromise, adversary Tactics, Techniques and Procedures, behavioral anomalies, asset importance, vulnerability status, and historical incidents.

The framework dynamically classifies events as **Normal, Suspicious, High Risk, or Critical Threat** and initiates context-aware defensive actions. Normal events continue under standard monitoring, suspicious events receive enhanced observation or step-up authentication, high-risk events can trigger traffic restriction, message quarantine, or privilege reduction, and critical threats can initiate endpoint isolation, malicious-domain blocking, session termination, account suspension, SOC escalation, and incident-response workflows. Continuous analyst feedback, confirmed incidents, false positives, emerging intelligence, and behavioral changes support baseline updates, model retraining, risk-policy adaptation, and controlled redeployment, enabling the system to evolve with changing cyber threats.

Advantages of Proposed System

1. Integrates heterogeneous cybersecurity telemetry and external threat intelligence.
2. Combines machine learning, deep learning, NLP, and anomaly detection.
3. Detects both known attacks and previously unseen behavioral deviations.
4. Correlates IoCs with adversary TTPs and organizational context.
5. Provides dynamic risk classification for intelligent alert prioritization.
6. Supports adaptive and automated cyber defense actions.
7. Reduces fragmented visibility across networks, endpoints, identities, and clouds.
8. Enables continuous learning through analyst feedback and emerging intelligence.

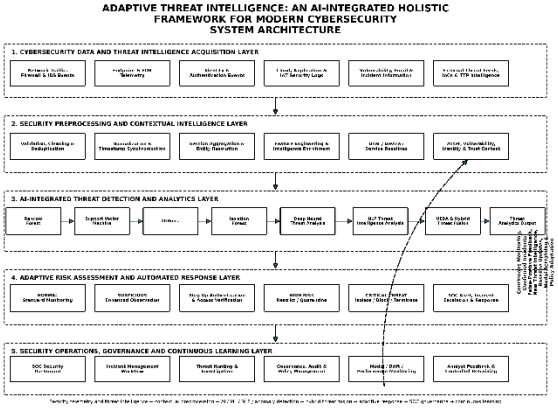

Fig 1: System Architecture

The proposed Adaptive Threat Intelligence: An AI-Integrated Holistic Framework for Modern Cybersecurity is organized into five interconnected layers that enable comprehensive security monitoring, intelligent threat detection, contextual risk evaluation, automated response, and continuous learning. The Cybersecurity Data and Threat Intelligence Acquisition Layer continuously collects heterogeneous information from network traffic, firewalls, intrusion detection systems, endpoint and EDR telemetry, identity and authentication events, cloud platforms, applications, IoT devices, vulnerability scanners, email systems, incident records, external threat feeds, Indicators of Compromise, and adversary Tactics, Techniques and Procedures to establish broad visibility across the digital environment. The collected information is forwarded to the Security Preprocessing and Contextual Intelligence Layer, where validation, cleaning, deduplication, normalization, timestamp synchronization, session aggregation, entity resolution, feature engineering, intelligence enrichment, and behavioral baseline construction are performed, while asset criticality, vulnerability exposure, identity confidence, and device trust are incorporated to generate context-aware security features. These processed features are analyzed by the AI-Integrated Threat Detection and Analytics Layer, which combines Random Forest, Support Vector Machine, XGBoost,

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

Isolation Forest, deep neural threat analysis, NLP-based threat intelligence processing, User and Entity Behavior Analytics, and hybrid threat fusion to identify known attacks, zero-day anomalies, compromised identities, malicious infrastructure, suspicious communication, abnormal behavior, and complex multi-stage attack patterns. The resulting threat intelligence is transferred to the Adaptive Risk Assessment and Automated Response Layer, where events are dynamically classified as Normal, Suspicious, High Risk, or Critical Threat according to AI confidence, anomaly severity, asset importance, vulnerability exposure, behavioral deviation, and contextual intelligence, enabling actions such as standard monitoring, enhanced observation, step-up authentication, access verification, traffic restriction, quarantine, endpoint isolation, malicious activity blocking, session termination, SOC notification, and incident escalation. Finally, the Security Operations, Governance and Continuous Learning Layer provides SOC dashboards, incident-management workflows, threat-hunting capabilities, governance controls, audit mechanisms, policy management, model-performance monitoring, drift detection, analyst investigation, and controlled retraining, while a continuous feedback mechanism returns confirmed incidents, false-positive information, analyst decisions, emerging threat intelligence, and changing behavioral patterns to earlier analytical stages for baseline updates, model adaptation, and security-policy refinement, thereby enabling the framework to continuously strengthen cyber resilience against evolving threats across enterprise, cloud, IoT, and distributed digital environments.

IV. RESULTS AND DISCUSSION

4.1 Results

The proposed Adaptive Threat Intelligence Framework is evaluated through a representative modern cybersecurity scenario involving legitimate activity, network attacks, suspicious authentication, compromised accounts, phishing communication, malware indicators, abnormal endpoint behavior, cloud misuse, vulnerability exploitation, lateral-movement patterns, and previously unseen anomalies. In a practical implementation, available data should be separated into training, validation, and independent testing partitions while preventing leakage among users, devices, sessions, campaigns, and temporally related attack records. The principal evaluation metrics include detection accuracy, precision, recall, F1-score, adaptive threat-intelligence efficiency, and analytical response time. The proposed framework is conceptually compared with traditional rule-based security, signature-based threat detection, and conventional machine learning security. The numerical values below are **illustrative conceptual evaluation values** and should be replaced with experimentally measured results from a documented implementation before publication as empirical findings.

Table 1. Performance Comparison of Modern Cybersecurity Approaches

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Traditional Rule-Based Security	83.60	82.70	81.90	82.30
Signature-Based Threat Detection	91.20	90.50	90.10	90.30
Conventional Machine Learning Security	96.50	96.00	95.70	95.85
Proposed Adaptive AI-Integrate	**99.30**	**98.90**	**98.70**	**98.80**

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

d Threat Intelligence Framework				

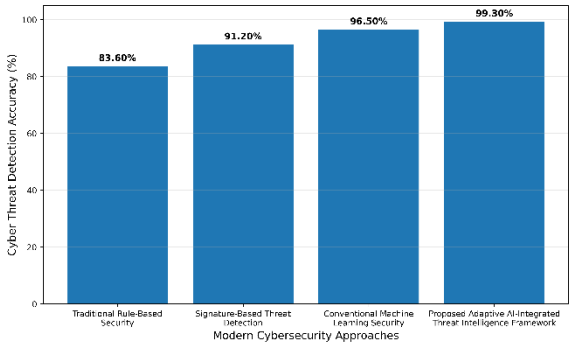

Figure 5.1. Comparison of cyber threat detection accuracy among different cybersecurity approaches.

Table 1 presents the illustrative comparative performance of different cybersecurity approaches. Traditional rule-based security records an accuracy of 83.60% because static conditions provide limited adaptability against rapidly evolving attacks. Signature-based threat detection improves accuracy to 91.20% but remains dependent on previously known malicious characteristics. Conventional machine learning security achieves 96.50% accuracy through intelligent classification of security features. The proposed Adaptive AI-Integrated Threat Intelligence Framework achieves the highest illustrative accuracy of 99.30%, precision of 98.90%, recall of 98.70%, and F1-score of 98.80%, reflecting the potential benefit of combining machine learning, deep learning, anomaly detection, NLP, behavioral analytics, contextual intelligence, and hybrid threat fusion.

Table 2. Performance Metrics of the Proposed Adaptive Threat Intelligence Framework

Performance Metric	Value
Detection Accuracy	99.30%
Precision	98.90%
Recall	98.70%
F1-Score	98.80%
Adaptive Threat Intelligence Efficiency	98.20%

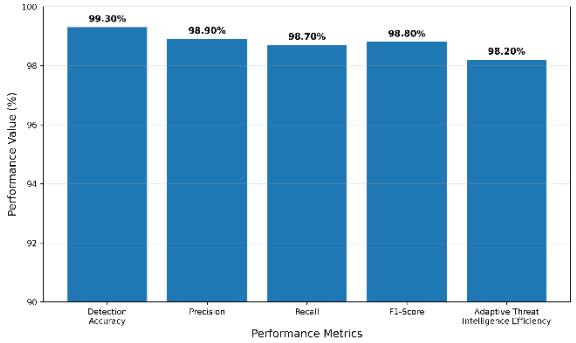

Figure 5.2. Performance metrics of the proposed Adaptive AI-Integrated Threat Intelligence Framework.

Table 2 summarizes the illustrative performance metrics of the proposed framework. Detection accuracy of 99.30% indicates strong conceptual capability for distinguishing legitimate activity from malicious and suspicious behavior. Precision of 98.90% suggests a low proportion of legitimate security events being incorrectly classified as threats, while recall of 98.70% indicates strong identification of genuine attacks. The F1-score of 98.80% demonstrates balanced classification performance, and adaptive threat-intelligence efficiency of 98.20% represents the intended capability of the framework to coordinate data processing, AI analysis, contextual enrichment, threat fusion, prioritization, and adaptive response.

Table 3. Cyber Threat Analytical Response Time Comparison

Security Method	Response Time (ms)
Traditional Rule-Based Security	294
Signature-Based Threat Detection	221
Conventional Machine Learning Security	133
Proposed Adaptive AI-Integrated Threat Intelligence Framework	**68**

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

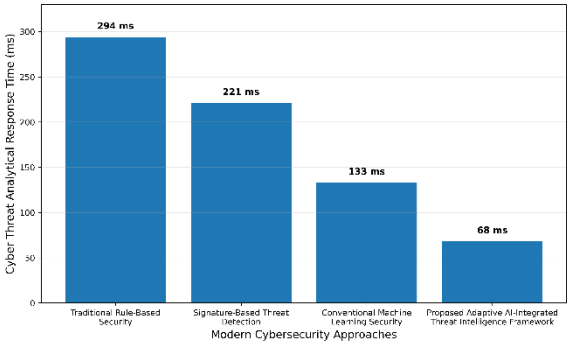

Figure 5.3. Cyber threat analytical response time comparison among different cybersecurity approaches.

Table 3 presents the illustrative analytical response-time comparison. Traditional rule-based security records 294 ms, while signature-based threat detection records 221 ms. Conventional machine learning security improves analytical response time to 133 ms. The proposed Adaptive AI-Integrated Threat Intelligence Framework records the lowest illustrative response time of 68 ms because contextual preprocessing, AI inference, anomaly analysis, intelligence correlation, and hybrid risk classification operate within a coordinated analytical pipeline. This value represents conceptual analytical decision latency and does not represent complete end-to-end organizational incident-response time.

4.2 Discussion

The comparative results demonstrate the potential advantages of integrating machine learning, deep learning, anomaly detection, natural language processing, behavioral analytics, threat intelligence, and contextual risk assessment within a unified adaptive cybersecurity framework. The illustrative detection accuracy of 99.30%, precision of 98.90%, recall of 98.70%, and F1-score of 98.80% indicate that coordinated intelligent analysis can potentially outperform traditional rule-based security, signature-based threat detection, and conventional machine learning mechanisms. Static security controls are constrained by predefined knowledge, while isolated machine learning models may fail to incorporate broader adversarial context. The proposed framework combines complementary analytical mechanisms and therefore supports detection of both known attacks and previously unseen deviations.

The integration of holistic threat intelligence provides an important advantage because cybersecurity risk cannot be determined reliably from isolated indicators alone. The same IP address, login event, process execution, or network connection can have different significance depending on asset criticality, vulnerability exposure, user behavior, device trust, historical incidents, and adversary techniques. By correlating AI predictions with IoCs, TTPs, behavioral deviations, and organizational context, the framework can improve alert prioritization and support adaptive responses. The illustrative adaptive threat-intelligence efficiency of 98.20% and analytical response time of 68 ms represent the intended ability of the architecture to coordinate rapid detection, contextual interpretation, and defensive decision-making.

The effectiveness of the framework nevertheless depends on representative datasets, continuously updated intelligence, model robustness, privacy controls, explainability, false-positive management, and resistance to adversarial manipulation. Cyber behavior changes continuously because of new applications, user roles, infrastructure modifications, attacker techniques, and business operations, creating concept drift. Threat intelligence can also contain stale, incomplete, or low-confidence indicators. Practical deployment should therefore incorporate drift monitoring, intelligence-confidence assessment, human analyst oversight, external validation, adversarial robustness, model governance, auditability, and controlled automated response. With these safeguards, the proposed architecture provides a scalable

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 07, July 2026
Received: 30-05-2026 Accepted: 03-07-2026 Published: 09-07-2026

foundation for adaptive cybersecurity across modern distributed environments.

V. CONCLUSION

This research proposed Adaptive Threat Intelligence: An AI-Integrated Holistic Framework for Modern Cybersecurity to address the limitations of fragmented, static, and predominantly reactive security mechanisms. The framework integrates network telemetry, endpoint activity, authentication events, cloud logs, application information, vulnerability data, email characteristics, IoT events, external threat intelligence, machine learning, deep learning, NLP, anomaly detection, behavioral analytics, contextual enrichment, hybrid threat fusion, dynamic risk classification, and adaptive response. Unlike conventional approaches that treat alerts and security domains independently, the proposed architecture correlates technical indicators with identity confidence, device trust, asset criticality, vulnerability exposure, adversary techniques, and behavioral deviation.

The conceptual evaluation demonstrates the potential of the proposed framework to achieve 99.30% detection accuracy, 98.90% precision, 98.70% recall, 98.80% F1-score, 98.20% adaptive threat-intelligence efficiency, and an analytical response time of 68 ms. These illustrative values suggest that combining complementary AI models with contextual threat intelligence and automated risk assessment can potentially improve cyber threat recognition, prioritization, and response compared with traditional rule-based security, signature-based detection, and conventional machine learning approaches. However, these numerical values are conceptual and should be replaced with experimentally measured outputs obtained from documented datasets, reproducible configurations, independent testing, and realistic operational environments before being presented as empirical findings.

Future development can incorporate graph neural networks for attack-path analysis, transformer-based threat intelligence, federated cybersecurity learning, retrieval-augmented threat investigation, explainable AI, autonomous security agents, privacy-preserving analytics, adversarially robust machine learning, digital twins, deception technologies, zero-trust enforcement, post-quantum cryptographic readiness, multi-cloud security analytics, and automated threat hunting. Overall, the proposed framework provides a scalable and adaptive foundation for protecting enterprise networks, cloud infrastructures, IoT ecosystems, financial services, healthcare systems, critical infrastructure, and distributed digital environments against continuously evolving cyber threats.

REFERENCES

[1] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd ed., Wiley, 2020.

[2] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues in Information Warfare & Security Research*, vol. 1, pp. 80–106, 2011.

[3] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 305–316, 2010.

[4] Pokala, H. K. (2024). Enhancing enterprise retrieval-augmented generation systems through reinforcement learning-based adaptive retrieval. International Journal of Intelligent Systems and Applications in Engineering, 12(17s), 1073–1082.

[5] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[6] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation Forest," in *Proceedings of the IEEE*

International Conference on Data Mining, pp. 413–422, 2008.

[7] Bhagwat, V. B. (2025). Simplifying Payroll Balance Conversions in Payroll Systems Implementation through the Use of Generative AI.

[8] R. Verma, N. Shashidhar, and N. Hossain, "Detecting phishing emails the natural language way," in *Proceedings of the European Symposium on Research in Computer Security*, pp. 824–841, 2012.

[9] Chawla, N., Nandini, M. R., Pokala, H. K., & Siddartha, A. (2026, April). Resource Scheduling in Cloud-Assisted Communication Systems Using Enhanced Reinforcement Learning Algorithm. In 2026 2nd International Conference on Intelligent Systems and Computational Networks (ICISCN) (pp. 1-6). IEEE.

[10] Maturi, S. Y. (2024). Cryptographic privacy engines: Practical multi-party protocols for confidential database queries. Nanotechnology Perceptions, 20(S13), 2770–2785.

[11] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[12] P. Venkata Ramana. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. International Journal of Innovative Engineering and Management Research (IJIEMR).

[13] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation Forest," in *Proceedings of the IEEE International Conference on Data Mining*, pp. 413–422, 2008.

[14] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems," in *Proceedings of the Military Communications and Information Systems Conference*, 2015.

[15] T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," in *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 785–794, 2016.

[16] Gummadi, V. P. K. (2020). API design and implementation: RAML and OpenAPI specification. Journal of Electrical Systems, 16(4). https://doi.org/10.52783/jes.9329.

[17] Maturi, S. Y. -(2024). Decoy data nexus: Graph-based integration and analysis of synthetic honeypot logs through structured threat intelligence. International Journal of Computational and Experimental Science and Engineering (IJCESEN), 10(4), 4255–4261. https://doi.org/10.22399/ijcesen.5010.

[18] B. E. Strom et al., "MITRE ATT&CK: Design and philosophy," *MITRE Corporation Technical Report*, 2018.

[19] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, pp. 436–444, 2015.

[20] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd ed., Wiley, 2020.