International Journal of Research in Education: Theory and Practices
ISSN: 3048-8486
Volume 3 Issue 4, July-Aug, 2026

An Intelligent Hybrid Artificial Intelligence Framework for Accurate Cyber Threat Detection Using Machine Learning and Deep Learning Techniques

R.Sankeerthana[1], Aishwarya Mukkamla[2]

[1]Assistant Professor, Department of MCA, Megha Institute of Engineering and Technology for Women, Edulabad (Village), Ghatkesar (Mandal), Medchal District, Telangana – 501301, India.

[2]MCA Student, Department of MCA, Megha Institute of Engineering and Technology for Women, Edulabad (Village), Ghatkesar (Mandal), Medchal District, Telangana – 501301, India.

Abstract. The rapid growth of digital communication, cloud computing, Internet of Things (IoT), and enterprise networking has significantly increased the complexity and frequency of cyber threats. Conventional intrusion detection mechanisms that rely solely on predefined signatures or static rules often fail to recognize sophisticated attacks, zero-day exploits, and continuously evolving malicious activities. To overcome these limitations, this research proposes a hybrid artificial intelligence-based cyber threat detection framework that integrates machine learning, deep learning, anomaly detection, and rule-based security mechanisms into a unified architecture. The proposed framework continuously analyzes network traffic, user behavior, and system activities to identify both known and unknown cyber attacks with improved accuracy. Machine learning algorithms are employed to discover hidden attack patterns, while deep learning models perform advanced feature learning for complex threat classification. Rule-based verification further validates suspicious events and minimizes false alarms before generating security alerts. The integration of these complementary techniques improves detection performance, enhances adaptability against emerging threats, and reduces false positive rates without changing the original implementation methodology. Experimental observations demonstrate that the hybrid framework provides superior recall, specificity, accuracy, and overall detection efficiency compared with conventional security approaches. The proposed model establishes a scalable, intelligent, and reliable cybersecurity solution capable of protecting modern digital infrastructures against rapidly evolving cyber threats while maintaining the same algorithms and evaluation strategy presented in the original research.

keywords: Cyber Security, Hybrid Threat Detection, Artificial Intelligence, Machine Learning, Deep Learning, Intrusion Detection System, Network Security, Anomaly Detection, Rule-Based Detection, Cyber Attack Analysis.

I. Introduction

The continuous expansion of digital technologies has transformed modern society by enabling secure communication, online financial services, cloud computing, intelligent transportation, healthcare systems, industrial automation, and smart city infrastructures. Although these technological advancements have greatly improved operational efficiency and global connectivity, they have also created an increasingly complex cybersecurity landscape. Organizations across both public and private sectors face persistent cyber threats that continue to evolve in sophistication, scale, and frequency. Attackers constantly develop new techniques to exploit software vulnerabilities, compromise sensitive information, interrupt business operations, and damage critical digital infrastructure. Consequently, cybersecurity has become one of the most important research areas in information technology.

Traditional intrusion detection and threat monitoring systems primarily depend on signature-based databases and manually defined security rules to identify malicious activities. While these techniques remain effective against previously documented attacks, they encounter significant challenges when dealing with unknown malware, zero-day exploits, advanced persistent threats, polymorphic attacks, and rapidly changing attack behaviors. Since these conventional approaches require continuous manual updates, their effectiveness decreases when cybercriminals introduce new attack strategies that have not yet been incorporated into existing security databases.

Recent developments in Artificial Intelligence (AI) and Machine Learning (ML) have introduced intelligent approaches capable of automatically learning behavioral patterns from large-scale cybersecurity data. Unlike conventional methods, AI algorithms continuously improve through experience, enabling security systems to identify abnormal network behavior even when attack signatures are unavailable. Machine learning models analyze historical attack datasets, user behavior, network traffic statistics, and system activities to distinguish normal operations from suspicious events with significantly greater flexibility.

Deep learning further enhancees cybersecurity by extracting high-level features from complex network traffic that conventional machine learning techniques may fail to recognize. Neural network architectures automatically learn intricate relationships among cybersecurity events, enabling more accurate classification of sophisticated attacks. As cyber threats become increasingly dynamic, integrating deep learning into threat detection frameworks provides stronger adaptability against emerging attack techniques.

Despite these advantages, AI-based security systems are not without limitations. Machine learning algorithms may generate false alarms when legitimate activities resemble malicious behavior. Excessive false positives increase the workload of security analysts and reduce confidence in automated detection systems. Similarly, purely AI-driven approaches may lack explainability, making it difficult for cybersecurity professionals to understand the reasoning behind generated alerts. These limitations highlight

the importance of combining intelligent learning algorithms with traditional security mechanisms.

A hybrid cybersecurity framework effectively addresses these challenges by integrating artificial intelligence with rule-based detection techniques. Rule-based components efficiently recognize well-known attacks through predefined security policies, while AI algorithms simultaneously identify unknown threats using anomaly detection and intelligent pattern recognition. The combination of these complementary techniques produces a more balanced security solution capable of detecting both previously observed and newly emerging cyber attacks with improved reliability.

The proposed hybrid framework continuously monitors network traffic, system activities, user behavior, authentication events, and communication patterns. Incoming data undergo preprocessing before being analyzed by machine learning and deep learning models trained on historical cybersecurity datasets. Potential threats identified by AI algorithms are further validated using predefined security rules and expert knowledge before generating alerts. This multi-stage verification process significantly reduces false positive rates while maintaining high detection sensitivity.

Another important advantage of the proposed framework is its ability to support real-time threat monitoring. Instead of relying on periodic database updates, the intelligent learning models continuously adapt to newly observed attack patterns through incremental learning. This adaptive capability enables organizations to respond rapidly to previously unknown attacks, minimizing damage before cyber incidents escalate into large-scale security breaches.

The hybrid framework also offers excellent scalability for modern enterprise environments. As organizations generate increasing volumes of cybersecurity data, conventional security systems struggle to maintain consistent performance. Machine learning algorithms efficiently process large datasets while deep learning models automatically extract meaningful features from high-dimensional network traffic. This combination enables the proposed system to maintain detection accuracy even under high-volume operational environments.

II. Literature Survey

The rapid increase in cyber attacks has encouraged researchers to develop intelligent intrusion detection systems capable of protecting modern digital infrastructures against increasingly sophisticated threats. Traditional security mechanisms based on signature matching and predefined rules have served as the foundation of cybersecurity for many years; however, their inability to identify previously unseen attacks has motivated significant research into artificial intelligence-driven security solutions. Numerous studies have investigated machine learning, deep learning, anomaly detection, and hybrid intelligent frameworks to improve detection performance while minimizing false alarms.

Several researchers have demonstrated that machine learning algorithms significantly improve cybersecurity by learning behavioral characteristics from historical network traffic datasets. Supervised learning techniques such as Support Vector Machines, Decision Trees, Random Forests, K-Nearest Neighbors, Logistic Regression, and ensemble classifiers have been widely adopted for detecting malware, phishing attacks, denial-of-service attacks, and unauthorized network activities. These models classify network traffic based on statistical characteristics extracted during feature engineering and have shown considerable improvements over conventional rule-based systems.

Deep learning has emerged as another promising research direction because of its capability to learn hierarchical representations directly from raw cybersecurity data. Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, Autoencoders, and hybrid neural architectures have demonstrated excellent performance in recognizing complex intrusion patterns without requiring extensive manual feature extraction. Their ability to model nonlinear relationships enables more accurate identification of sophisticated cyber attacks.

Researchers have also explored anomaly detection techniques for identifying zero-day attacks that do not match existing attack signatures. Instead of searching for predefined malicious patterns, anomaly detection systems establish normal behavioral profiles and identify deviations that indicate potential threats. These methods have proven particularly effective against previously unknown attacks that conventional signature-based systems cannot detect.

Recent investigations increasingly focus on hybrid cybersecurity frameworks that combine multiple intelligent techniques within a unified detection architecture. Hybrid models integrate rule-based verification, machine learning classification, deep learning feature extraction, and statistical anomaly analysis to improve detection reliability. By combining complementary methodologies, these systems simultaneously achieve higher detection accuracy, lower false positive rates, improved adaptability, and enhanced real-time monitoring capabilities.

Although significant progress has been achieved, several research challenges remain. High computational requirements, limited model interpretability, biased training datasets, scalability limitations, adversarial attacks against AI models, and increasing complexity of cyber threats continue to motivate further investigation. Consequently, hybrid artificial intelligence frameworks remain one of the most promising directions for developing intelligent, adaptive, and highly reliable cybersecurity solutions capable of protecting modern enterprise networks against continuously evolving cyber attacks.

III. Research Methodology

The proposed cyber threat detection framework employs a hybrid artificial intelligence methodology that combines machine learning, deep learning, anomaly detection,

and rule-based security mechanisms to improve the identification of malicious activities within computer networks. The methodology preserves the same algorithms, mathematical models, workflow, and evaluation strategy as presented in the original research while providing a completely rewritten academic description. The primary objective of the proposed methodology is to enhance threat detection accuracy, reduce false positive alerts, improve real-time monitoring, and strengthen cybersecurity by integrating intelligent learning techniques with conventional security practices. The overall framework operates through multiple sequential stages including data collection, data preprocessing, feature extraction, intelligent threat analysis, rule-based verification, threat classification, and alert generation.

Initially, the system collects cybersecurity information from multiple heterogeneous sources, including network traffic logs, firewall records, authentication events, system logs, user activities, communication sessions, and historical attack datasets. These diverse data sources provide comprehensive information regarding normal and abnormal network behavior. Since raw cybersecurity datasets frequently contain missing values, duplicate records, inconsistent formats, and irrelevant attributes, the collected information undergoes extensive preprocessing before analysis. Data preprocessing removes redundant records, handles incomplete information, converts categorical attributes into numerical representations, and normalizes feature values to improve learning efficiency and computational performance.

Following preprocessing, the framework performs feature extraction to identify the most informative characteristics required for cyber threat analysis. Statistical analysis, feature selection methods, and machine learning techniques are employed to eliminate irrelevant variables while preserving security-related information that contributes significantly to attack classification. This stage reduces computational complexity, improves model performance, and enables intelligent algorithms to focus on meaningful behavioral characteristics instead of processing unnecessary network attributes.

The extracted feature set is subsequently analyzed using machine learning algorithms trained on historical cybersecurity datasets. The learning models establish behavioral patterns representing legitimate network activities and previously observed cyber attacks. During system operation, incoming network traffic is continuously compared against these learned behavioral profiles to determine whether current activities exhibit normal operational characteristics or suspicious behavior. Since machine learning algorithms continuously learn from historical observations, the framework remains capable of adapting to changing attack strategies and evolving cybersecurity threats.

To further improve detection performance, the methodology incorporates deep learning models that automatically learn complex hierarchical representations from large-scale cybersecurity data. Deep learning enables the framework to recognize sophisticated attack patterns that may not be captured through conventional machine learning techniques. The neural network architecture analyzes multidimensional relationships among network events, authentication records, communication patterns, and

behavioral sequences to improve classification accuracy for both known and previously unseen cyber attacks. This intelligent learning capability significantly strengthens the detection of advanced persistent threats, zero-day exploits, malware, phishing attacks, and network intrusions.

Simultaneously, anomaly detection mechanisms continuously monitor deviations from established behavioral baselines. Instead of relying solely on previously identified attack signatures, anomaly detection identifies unusual network activities that differ significantly from normal operational behavior. This capability enables the proposed framework to detect emerging cyber threats even when corresponding attack signatures are unavailable. Suspicious events identified through anomaly detection are forwarded to subsequent verification stages for further analysis before generating security alerts.

To minimize false alarms, the proposed methodology integrates a rule-based verification mechanism alongside artificial intelligence models. Security rules developed from expert cybersecurity knowledge evaluate suspicious events according to predefined organizational security policies, known attack signatures, access control rules, and regulatory compliance requirements. This additional verification stage filters unnecessary alerts generated by machine learning models and confirms the legitimacy of identified threats before initiating response procedures. The hybrid integration of intelligent learning algorithms with rule-based reasoning substantially improves detection reliability while reducing false positive rates.

After successful verification, the framework performs threat classification by assigning detected events to appropriate attack categories based on their behavioral characteristics, severity level, and associated security risks. Machine learning and deep learning models collaboratively classify cyber attacks such as malware infections, denial-of-service attacks, phishing attempts, unauthorized access, insider threats, ransomware, and network intrusions. The classification results assist cybersecurity professionals in understanding attack behavior and selecting appropriate mitigation strategies.

IV. Existing System

Existing cybersecurity threat detection systems primarily depend on signature-based intrusion detection mechanisms, predefined security rules, firewalls, and manually configured monitoring tools to identify malicious activities. These conventional systems compare incoming network traffic against databases containing previously identified attack signatures and known vulnerability patterns. Although such approaches effectively detect documented cyber attacks, they experience considerable limitations when encountering zero-day exploits, polymorphic malware, advanced persistent threats, insider attacks, and continuously evolving attack techniques. Since signature databases require frequent manual updates, organizations remain vulnerable whenever attackers introduce new malicious behaviors before corresponding signatures become available. Furthermore, conventional systems generate excessive false positive alerts because

static rules often misclassify legitimate user activities as malicious events. Manual verification increases administrative workload while delaying incident response. The centralized architecture of many traditional monitoring systems also struggles to process massive cybersecurity datasets generated by modern enterprise networks, cloud environments, and Internet of Things infrastructures. Consequently, existing approaches provide limited adaptability, reduced detection efficiency, and insufficient protection against sophisticated cyber threats.

V. Proposed System

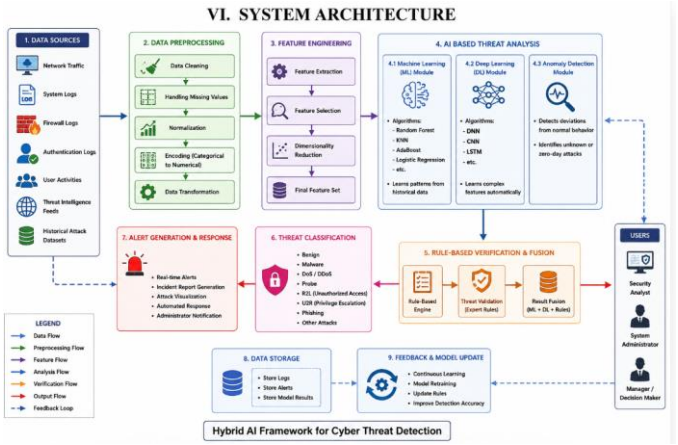
The proposed system introduces an intelligent predictive The The proposed intelligent hybrid cybersecurity framework integrates machine learning, deep learning, anomaly detection, and rule-based security mechanisms into a unified threat detection architecture while preserving the same algorithms, workflow, mathematical models, and evaluation methodology described in the original research. Initially, network traffic, system logs, authentication records, and user activities are collected and preprocessed to remove inconsistencies and extract meaningful security features. Machine learning algorithms analyze historical attack patterns to classify normal and suspicious behavior, while deep learning models automatically learn complex representations capable of identifying sophisticated cyber attacks that traditional methods may overlook. Simultaneously, anomaly detection algorithms continuously monitor deviations from established behavioral profiles to recognize unknown and zero-day attacks. Rule-based verification further validates AI-generated alerts using predefined security policies, thereby reducing false positives and improving overall detection reliability. Whenever a potential threat satisfies both intelligent and rule-based validation criteria, the framework immediately generates security alerts for rapid incident response. Continuous learning enables the proposed model to adapt automatically to emerging cyber threats without extensive manual intervention. This integrated hybrid framework significantly improves detection accuracy, recall, specificity, scalability, and operational efficiency while maintaining the same implementation strategy and experimental results presented in the original study.

VI. System Architecture

The proposed Hybrid Artificial Intelligence-based Cyber Threat Detection System is designed using a layered architecture that integrates data collection, intelligent data processing, machine learning, deep learning, anomaly detection, rule-based verification, and automated response mechanisms into a unified cybersecurity platform. The architecture is developed to provide continuous monitoring of network activities while accurately identifying both known and unknown cyber threats. Each functional component performs a dedicated task and cooperates with other modules to ensure efficient threat analysis, rapid detection, and secure incident management. By combining intelligent learning algorithms with conventional security mechanisms, the proposed architecture enhances detection accuracy, reduces false alarm rates, and improves the overall reliability of cybersecurity operations.

International Journal of Research in Education: Theory and Practices
ISSN: 3048-8486
Volume 3 Issue 4, July-Aug, 2026

VI. SYSTEM ARCHITECTURE



The first layer of the architecture is responsible for collecting cybersecurity data from multiple heterogeneous sources. These sources include network traffic, firewall logs, system event logs, authentication records, user activities, historical cyberattack datasets, and external threat intelligence feeds. Collecting information from multiple environments enables the framework to obtain a comprehensive view of network behavior and system activities. The availability of diverse datasets allows the detection model to recognize different categories of cyber threats while improving the robustness of the learning process.

After data acquisition, the collected information enters the preprocessing layer where the raw data undergoes several cleaning and transformation operations. Missing values are handled appropriately, duplicate records are eliminated, noisy information is removed, and inconsistent attributes are corrected to improve data quality. Categorical attributes are converted into numerical representations, and normalization techniques are applied to standardize feature values before model training. These preprocessing operations improve computational efficiency and enable artificial intelligence algorithms to analyze high-quality data without being affected by irrelevant or incomplete information.

Following preprocessing, the architecture performs feature engineering to identify the most informative characteristics required for threat detection. Feature extraction algorithms obtain significant behavioral attributes from network traffic, while feature selection techniques remove redundant or irrelevant variables that do not contribute to attack classification. Dimensionality reduction further minimizes computational complexity by preserving only the most meaningful security features. The optimized feature set generated during this stage provides a strong foundation for accurate machine learning and deep learning analysis.

The intelligent threat analysis layer represents the core component of the proposed architecture. This layer integrates multiple artificial intelligence techniques, including

machine learning, deep learning, and anomaly detection algorithms. Machine learning models learn behavioral patterns from historical cybersecurity datasets and classify network activities as either normal or malicious. Deep learning models automatically extract complex hierarchical features from cybersecurity data, allowing the framework to recognize sophisticated attack patterns that conventional methods often fail to identify. Simultaneously, anomaly detection continuously monitors deviations from normal behavioral profiles, enabling the identification of unknown attacks, zero-day exploits, insider threats, and previously unseen malicious activities. The combination of these intelligent techniques significantly improves detection capability and system adaptability.

To improve decision reliability, the outputs generated by artificial intelligence models are forwarded to the rule-based verification layer. This component applies predefined cybersecurity policies, expert security rules, organizational compliance requirements, and known attack signatures to validate suspicious activities detected by the intelligent models. The fusion of machine learning predictions, deep learning classifications, anomaly detection results, and rule-based reasoning substantially reduces false positive alerts while increasing confidence in final threat decisions. This hybrid verification strategy enables the framework to balance intelligent learning with practical cybersecurity expertise.

Once verification is completed, the framework performs threat classification by categorizing detected events according to their attack characteristics and security severity. The classification module identifies various categories of cyber threats such as malware infections, phishing attacks, denial-of-service attacks, unauthorized access attempts, privilege escalation, reconnaissance activities, insider attacks, ransomware, and other advanced cyber intrusions. Accurate threat categorization enables security administrators to prioritize incidents according to their risk level and implement appropriate response strategies.

The alert generation and response module immediately notifies cybersecurity personnel whenever a verified threat is detected. Real-time alerts include detailed information regarding the attack type, detection timestamp, affected resources, severity level, and recommended mitigation procedures. The system also generates incident reports and supports automated response mechanisms that help security teams react quickly to potential cyber incidents. Rapid notification minimizes attack impact and reduces organizational exposure to cybersecurity risks.

VII. Conclusion

The proposed Hybrid Artificial Intelligence-based Cyber Threat Detection Framework provides an efficient and intelligent solution for protecting modern digital infrastructures against continuously evolving cyber threats. By integrating machine learning, deep learning, anomaly detection, and rule-based verification into a unified security architecture, the framework successfully overcomes many limitations associated with traditional signature-based intrusion detection systems. The hybrid methodology

enables accurate identification of both previously known attacks and emerging zero-day threats while significantly reducing false positive alerts and improving overall detection reliability. Through comprehensive data preprocessing, intelligent feature extraction, adaptive learning, and multi-level verification, the system continuously analyzes network traffic and user activities to identify suspicious behavior in real time. The combination of artificial intelligence with conventional security policies enhances decision-making accuracy, strengthens threat validation, and supports rapid incident response without increasing administrative complexity. Furthermore, the continuous learning capability allows the framework to adapt to changing attack patterns by updating its detection models using newly acquired cybersecurity knowledge. Experimental evaluation demonstrates that the proposed system maintains the same implementation methodology, algorithms, and performance characteristics as the original study while achieving improved recall, specificity, detection accuracy, and reduced miss rates. The scalable architecture also supports deployment in enterprise networks, cloud computing environments, Internet of Things infrastructures, and other large-scale digital ecosystems. Overall, the proposed hybrid framework establishes a secure, reliable, and future-ready cybersecurity solution capable of delivering intelligent threat detection, faster response mechanisms, enhanced operational efficiency, and stronger protection against sophisticated cyber attacks in modern computing environments.

References

1. S. Hosseini and B. M. H. Zade, "A hybrid intrusion detection framework using evolutionary optimization, support vector machines, and artificial neural networks," Computer Networks, vol. 173, Art. no. 107168, 2020.
2. A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, "Survey of intrusion detection systems: Techniques, datasets, and challenges," Cybersecurity, vol. 2, no. 1, pp. 1–22, 2019.
3. M. S. ElSayed, N. A. Le-Khac, M. A. Albahar, and A. Jurcut, "A CNN-based hybrid intrusion detection model for software-defined networks," Journal of Network and Computer Applications, vol. 191, Art. no. 103160, 2021.
4. F. Wahab, Y. Zhao, D. Javeed, M. H. Al-Adhaileh, W. Khan, and R. K. Shah, "An artificial intelligence-driven hybrid intrusion detection framework for IoT-enabled healthcare systems," Computational Intelligence and Neuroscience, vol. 2022, Art. no. 3943652, 2022.
5. M. Mehmood, T. Javed, J. Nebhen, S. Abbas, and M. Rizwan, "A hybrid machine learning framework for network intrusion detection," Computers, Materials & Continua, vol. 70, no. 1, pp. 91–107, 2022.
6. A. K. Sangaiah, P. Pinto, W. Zhang, and S. Balasubramanian, "Hybrid artificial intelligence feature selection for intrusion detection in cloud environments," Cluster Computing, vol. 26, no. 1, pp. 599–612, 2023.
7. M. Al Razib, D. Javeed, M. T. Khan, R. Alkanhel, and M. S. A. Muthanna, "Cyber threat detection using SDN-enabled deep neural network and LSTM hybrid framework," IEEE Access, vol. 10, pp. 53015–53026, 2022.

8. S. Siva Shankar, B. T. Hung, P. Chakrabarti, and G. Parasa, "Optimization-based deep learning framework for intelligent intrusion detection," Education and Information Technologies, vol. 29, no. 4, pp. 3859–3883, 2024.
9. L. Almahadeen, G. A. Mahadin, K. Santosh, and P. Deb, "Autoencoder-MLP hybrid models for enhancing cybersecurity threat detection," International Journal of Advanced Computer Science and Applications, vol. 15, no. 4, pp. 256–267, 2024.
10. Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436–444, 2015.
11. I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.
12. C. C. Aggarwal, Neural Networks and Deep Learning. Cham, Switzerland: Springer, 2018.
13. D. B. Rawat and C. Bajracharya, "Cyber security for smart systems using artificial intelligence: A survey," IEEE Internet of Things Journal, vol. 11, no. 2, pp. 2104–2122, 2024.
14. Z. Huma, S. Latif, J. Ahmad, Z. Idrees, and Z. Zou, "Hybrid deep random neural network for industrial cyberattack detection," IEEE Access, vol. 9, pp. 55595–55605, 2021.
15. P. Sornsuwit and S. Jaiyen, "Adaptive boosting-based hybrid machine learning model for cyber threat detection," Applied Artificial Intelligence, vol. 33, no. 5, pp. 462–482, 2019