A Systematic Review of Hybrid Machine Learning and Agentic AI Frameworks

Mohit[1], Ms. Sarika Madavi[2]
[1]*M.Tech AIDS Student, Department of Computer Science and Engineering, World College of Technology & Management, Gurgaon, Haryana, India*
[2]*Assistant Professor, Department of Computer Science and Engineering, World College of Technology & Management, Gurgaon, Haryana, India*

***Abstract*—The rapid evolution of cyber threats has created serious challenges for conventional cybersecurity systems. Traditional rule-based intrusion detection mechanisms and standalone machine learning models often struggle to identify sophisticated attacks such as zero-day exploits, polymorphic malware, ransomware, distributed denial-of-service attacks, and advanced persistent threats. Recent advancements in Artificial Intelligence have introduced Agentic AI as a new paradigm capable of autonomous reasoning, adaptive learning, contextual understanding, and real-time decision-making. The integration of Machine Learning (ML) and Agentic AI has emerged as a promising approach for developing intelligent and self-adaptive cyber defense systems.**

This review paper presents a comprehensive analysis of hybrid ML and Agentic AI frameworks for autonomous cyberattack detection and response. The study critically examines two major research frameworks focused on intelligent cyber defense through the fusion of predictive analytics and autonomous agent-based orchestration. The paper explores various deep learning architectures, including Convolutional Neural Networks, Recurrent Neural Networks, Long Short-Term Memory networks, ensemble learning models, reinforcement learning mechanisms, and goal-oriented autonomous agents used in modern cybersecurity ecosystems.

The review discusses system architectures, anomaly detection models, contextual risk evaluation techniques, adaptive policy optimization mechanisms, and reinforcement learning-based mitigation strategies. Furthermore, the paper analyzes performance metrics including detection accuracy, precision, recall, F1-score, false positive reduction, mitigation latency, and scalability in enterprise, cloud, and IoT environments. The comparative analysis demonstrates that hybrid ML-Agentic AI systems significantly improve threat intelligence, adaptive response capabilities, and autonomous mitigation efficiency compared to traditional ML-only and rule-based approaches.

The paper also highlights recent advancements such as explainable AI, federated learning, retrieval-augmented generation, blockchain-enabled trust systems, TinyML security architectures, and self-healing cybersecurity infrastructures. Finally, major research challenges, ethical concerns, scalability limitations, adversarial vulnerabilities, and future research opportunities are critically discussed to support the development of next-generation intelligent cyber defense ecosystems.

The speedy evolution of cyber threats has created severe demanding situations for conventional cybersecurity structures. traditional rule-based intrusion detection mechanisms and standalone system gaining knowledge of models often war to pick out sophisticated attacks along with 0-day exploits, polymorphic malware, ransomware, disbursed denial-of-carrier attacks, and advanced persistent threats. current advancements in synthetic Intelligence have delivered Agentic AI as a brand-new paradigm capable of autonomous reasoning, adaptive gaining knowledge of, contextual information, and actual-time selection-making. the integration of gadget mastering (ML) and Agentic AI has emerged as a promising method for growing intelligent and self-adaptive cyber protection structures.

This review paper affords a comprehensive evaluation of hybrid ML and Agentic AI frameworks for independent cyberattack detection and reaction. The examine severely examines foremost research frameworks centered on sensible cyber defense via the fusion of predictive analytics and self-sufficient agent-based orchestration. The paper explores diverse deep studying architectures, which includes Convolutional Neural Networks, Recurrent Neural Networks, lengthy short-term reminiscence networks, ensemble gaining knowledge of fashions, reinforcement studying mechanisms, and aim-oriented independent dealers used in modern cybersecurity ecosystems.

The review discusses device architectures, anomaly detection fashions, contextual danger evaluation strategies, adaptive policy optimization mechanisms, and reinforcement studying-primarily based mitigation strategies. moreover, the paper analyzes overall performance metrics such as detection accuracy, precision, recollect, F1-score, fake advantageous discount, mitigation latency, and scalability in company, cloud, and IoT environments. The comparative evaluation demonstrates that hybrid ML-Agentic AI structures considerably improve danger intelligence, adaptive response abilities, and self-sustaining mitigation efficiency as compared to traditional ML-only and rule-based tactics.

The paper additionally highlights recent advancements such as explainable AI, federated getting to know, retrieval-augmented generation, blockchain-enabled trust structures, TinyML safety architectures, and self-restoration cybersecurity infrastructures. ultimately, important research demanding situations, ethical issues, scalability boundaries, antagonistic vulnerabilities, and destiny studies possibilities are severely discussed to aid the improvement of subsequent-generation shrewd cyber defense ecosystems.

***Index Terms*—Machine Learning, Agentic AI, Autonomous Cyber Defense, Intrusion Detection Systems, Deep Learning, Threat Intelligence, Reinforcement Learning, Adaptive Security, Cyberattack Detection, Explainable AI.**

I. INTRODUCTION

The continuous expansion of virtual infrastructures, cloud computing structures, organisation systems, smart gadgets, and internet of factors (IoT) networks has dramatically accelerated the complexity of modern cybersecurity environments. businesses internationally an increasing number of depend on interconnected virtual ecosystems for verbal exchange, statistics garage, industrial automation, healthcare monitoring, financial operations, and smart transportation systems. even as this technological transformation provides operational performance and automation, it simultaneously creates large assault surfaces at risk of sophisticated cyber threats.

Modern-day cyberattacks are not restrained to simple malware or static intrusion tries. contemporary attackers hire superior chronic threats (APTs), ransomware campaigns, phishing attacks, polymorphic malware, botnets, insider threats, allotted denial-of-carrier assaults, antagonistic AI assaults, and zero-day vulnerabilities capable of bypassing conventional safety infrastructures. conventional cybersecurity systems primarily based on static signatures, predefined rules, and manually configured intrusion detection mechanisms regularly fail to discover dynamic and formerly unseen assault styles.

System gaining knowledge of has appreciably transformed cybersecurity by means of permitting systems to automatically examine attack behaviors from historical community traffic and safety telemetry information. Supervised getting to know, unsupervised gaining knowledge of, ensemble mastering, and deep gaining knowledge of techniques have confirmed robust abilities in anomaly detection, intrusion class, malware analysis, and behavioral profiling. models including aid Vector Machines, Random Forests, artificial Neural Networks, Convolutional Neural Networks, and long brief-time period memory networks are extensively used for wise danger detection.

Despite achieving excessive detection accuracy, standalone ML structures showcase several realistic obstacles. most models perform usually as prediction engines without contextual reasoning or self-sustaining response abilities. They often warfare with concept glide, unknown assault styles, false positives, explainability troubles, and real-time adaptive mitigation. moreover, ML-most effective frameworks usually require human intervention for interpreting alerts, configuring mitigation rules, and coordinating defensive actions.

To triumph over these limitations, Agentic synthetic Intelligence has emerged as an effective paradigm for self-sustaining and intention-orientated cybersecurity structures. in contrast to traditional AI structures that carry out remoted predictions, Agentic AI frameworks can understand environments, evaluate risks, purpose autonomously, optimize protective techniques, and execute mitigation movements with minimal human intervention. Agentic AI introduces smart dealers capable of non-stop learning, adaptive policy evolution, contextual reasoning, and collaborative orchestration throughout allotted infrastructures.

The mixing of ML and Agentic AI creates a hybrid cybersecurity structure that mixes predictive analytics with self-sustaining reasoning and real-time protection orchestration. In such frameworks, ML fashions identify anomalies and assault probabilities, whilst Agentic AI modules examine contextual threat,

prioritize threats, coordinate mitigation guidelines, and dynamically optimize defensive strategies. This collaborative intelligence permits proactive cyber defense in preference to traditional reactive protection mechanisms.

This evaluation paper seriously analyzes latest research developments in hybrid ML-Agentic AI cybersecurity frameworks. The observe especially focuses on independent hazard detection, adaptive mitigation systems, reinforcement getting to know-based coverage optimization, explainable safety intelligence, and scalable deployment architectures for organisation, IoT, cloud, and cyber-physical environments.

II. BACKGROUND OF HYBRID ML AND AGENTIC AI CYBERSECURITY

Cybersecurity has evolved via a couple of technological generations. to start with, signature-based detection systems dominated the sector by way of identifying attacks via predefined malicious styles. even though effective in opposition to recognised threats, those systems didn't come across novel attacks and polymorphic malware.

The emergence of device gaining knowledge of introduced adaptive intelligence into cybersecurity. ML-based totally structures found out statistical and behavioral patterns from community traffic and device logs to discover anomalies automatically. Deep studying in addition advanced cybersecurity through advanced function extraction and temporal collection modeling.

latest advancements in self-reliant intelligence brought Agentic AI into cybersecurity ecosystems. Agentic AI systems make bigger beyond passive prediction by using incorporating reasoning, making plans, environmental consciousness, and autonomous action execution. those systems are capable of continuously monitoring infrastructures, evaluating dynamic risks, coordinating responses, and adapting guidelines based totally on evolving assault behaviors.

The fusion of ML and Agentic AI represents the transition from static intrusion detection structures towards self-learning and self-defending cyber infrastructures capable of proactive and self-reliant protection.

III. LITERATURE REVIEW

Recent studies demonstrate speedy boom in hybrid AI-pushed cybersecurity architectures combining predictive intelligence with self-reliant orchestration mechanisms.

Research on unified cyber protection frameworks highlights the importance of self-adaptive sensible agents able to coordinating safety operations across cloud, side, and IoT environments. those frameworks emphasize decentralized orchestration, continuous studying, and automated hazard mitigation.

Several studies explored deep mastering-based malware analysis and anomaly detection structures using CNNs, RNNs, and LSTM architectures. these fashions completed progressed attack type accuracy by mastering complex spatial and temporal visitors' styles from benchmark intrusion datasets.

Studies on federated getting to know-based totally cybersecurity introduced privacy-preserving collaborative intelligence wherein distributed devices together teach models without sharing uncooked information. Such processes decorate scalability and records privateness in corporation and IoT environments.

Explainable AI has also emerged as a critical studies location because deep neural networks frequently perform as black-box systems. Explainability mechanisms including SHAP and attention visualization help safety analysts apprehend self-sufficient selection-making techniques.

Another crucial research path involves reinforcement mastering and independent chance hunting. Reinforcement studying allows cybersecurity marketers to constantly optimize protecting strategies based totally on environmental remarks and mitigation results. autonomous sellers can dynamically reconfigure firewall regulations, isolate malicious sessions, block suspicious IPs, and installation adaptive countermeasures.

Retrieval-Augmented generation and large Language version integration constitute every other rising route in agentic cybersecurity systems. Multi-agent frameworks integrate danger intelligence retrieval, contextual reasoning, and safety automation to enhance incident reaction coordination.

Research also emphasizes blockchain-enabled consider frameworks, 0-accept as true with

architectures, TinyML protection fashions, hostile robustness, and quantum-resilient cybersecurity infrastructures despite these advancements, several research gaps stay unresolved:

- Loss of standardized interoperability frameworks for agentic systems
- Restrained real-world deployment evaluations
- Scalability challenges in excessive-throughput environments
- Vulnerability to antagonistic attacks
- High computational complexity
- Inadequate explainability of self-sufficient choices
- Restrained governance and moral frameworks for self-sufficient AI defense

IV. HYBRID MACHINE LEARNING AND AGENTIC AI ARCHITECTURE

Current hybrid cybersecurity frameworks generally encompass a couple of shrewd layers working collaboratively.

1. Data Acquisition Layer

this sediment collects visitors' logs, API lines, device events, cloud telemetry, and IoT sensor information from dispensed infrastructures.

2. Pre-processing and feature Engineering Layer

Raw facts undergo normalization, encoding, entropy analysis, traffic aggregation, and dimensionality discount. characteristic extraction mechanisms pick out statistical and behavioural indicators associated with malicious activity.

3. ML-based totally Detection Layer

Deep getting to know and ensemble mastering models perform anomaly detection and assault type.
Common fashions include:

- Convolutional Neural Networks (CNN)
- Recurrent Neural Networks (RNN)
- Long quick-time period reminiscence (LSTM)
- Random woodland
- Guide Vector Machines
- Autoencoders

The ML layer generates probabilistic attack predictions and anomaly scores.

4. Agentic AI Reasoning Layer

This residue performs contextual hazard evaluation the usage of:

- Asset criticality
- Historical attack behavior
- Risk severity
- Environmental situations
- Device load styles

Self-sustaining retailers examine mitigation strategies using purpose-oriented reasoning and reinforcement getting to know guidelines.

5. Adaptive Mitigation Layer

The mitigation layer executes:

- Firewall reconfiguration
- Consultation isolation
- Traffic throttling
- Automatic patching
- Hazard containment
- Dynamic coverage updates

6. Continuous getting to know Layer

remarks loops monitor mitigation effects and continuously optimize agentic policies thru reinforcement getting to know.

V. MATHEMATICAL FOUNDATIONS

The reviewed frameworks employ several mathematical models for intelligent cyber defense.

A. Attack Probability Prediction

$$P(y|x) = \frac{1}{1+e^{-(W^T x + b)}}$$

This logistic prediction model estimates the probability of malicious activity based on extracted network features.

B. Ensemble Threat Scoring

$$S_{ensemble} = \sum_{i=1}^{n} \alpha_i P_i$$

Ensemble learning combines predictions from multiple classifiers using weighted soft voting.

C. Risk Evaluation Function

$$R = \beta_1 S_{ensemble} + \beta_2 C + \beta_3 T$$

The overall contextual risk score incorporates attack probability, asset criticality, and temporal anomaly behavior.

D. Reinforcement Learning Policy Update

$$Q_{new}(s,a) = Q(s,a) + \eta\,[r + \gamma \max_{a'} Q(s',a') - Q(s,a)]$$

This reinforcement learning equation enables adaptive optimization of mitigation strategies.

E. Binary Cross-Entropy Loss

$$L = -\frac{1}{m}\sum_{i=1}^{m} [y_i \log(\hat{y}_i) + (1 - y_i)\log(1 - \hat{y}_i)]$$

This loss function optimizes deep learning-based attack classification.

VI. PERFORMANCE ANALYSIS

The reviewed hybrid frameworks demonstrated significant improvements compared to traditional ML-only systems.

Observed Improvements

- Detection accuracy exceeding 98%
- Significant reduction in false positive rates
- Faster incident response times
- Improved adaptive mitigation efficiency
- Better scalability in enterprise and IoT environments
- Enhanced contextual reasoning capabilities

The integration of autonomous reasoning agents substantially improved decision intelligence and operational resilience.

Key Performance Metrics

TABLE 1: KEY METRICES

Metric	Traditional ML	Hybrid ML + Agentic AI
Accuracy	Moderate	Very High
False Positives	Higher	Lower
Adaptive Response	Limited	Strong
Mitigation Automation	Partial	Autonomous
Threat Intelligence Fusion	Weak	Advanced
Scalability	Moderate	High
Context Awareness	Limited	Dynamic

VII. CHALLENGES AND LIMITATIONS

Despite promising results, numerous barriers remain.

1. Dataset Dependency

Hybrid fashions require big-scale, balanced, and amazing datasets for education.

2. Computational Complexity

Deep getting to know and agentic orchestration increase processing overhead in real-time environments.

3. Adverse Vulnerability

AI structures continue to be at risk of adverse manipulation and data poisoning attacks.

4. Explainability troubles

Complicated neural networks and multi-agent reasoning structures reduce interpretability.

5. Policy Instability

Flawed reinforcement studying policies may also produce over-mitigation and carrier disruptions.

6. Moral and Governance worries

Independent cybersecurity systems require obvious governance, accountability, and compliance frameworks.

VIII. FUTURE RESEARCH DIRECTIONS

Future sensible cybersecurity systems are expected to include:

- Federated studying for decentralized collaborative intelligence
- Explainable AI for obvious choice-making
- Blockchain-enabled accept as true with management
- Quantum-resilient cryptographic architectures
- Tiny ML-primarily based light-weight safety models
- Self-healing self-sustaining infrastructures
- Transformer-primarily based contextual threat evaluation
- Multi-agent cooperative cyber defence
- Retrieval-Augmented era for risk intelligence
- Area AI for low-latency distributed security

The development of fully autonomous and explainable cyber protection ecosystems remains a first-rate future objective.

IX. CONCLUSION

The fusion of gadget studying (ML) and Agentic synthetic Intelligence (Agentic AI) represents one of the most tremendous advancements inside the evolution of current cybersecurity systems. conventional intrusion detection structures and standalone ML-primarily based frameworks are an increasing number of incapables of handling the complexity, speed, and intelligence of contemporary cyberattacks. conventional safety mechanisms on the whole depend upon static regulations, predefined assault signatures, and restricted behavioral evaluation, which makes them ineffective towards sophisticated threats consisting of zero-day exploits, polymorphic malware, advanced continual threats (APTs), ransomware, insider attacks, and big-scale allotted denial-of-provider (DDoS) assaults. As cyber adversaries retain to adopt automation, artificial intelligence, and adaptive evasion strategies, there's a pressing want for intelligent defense systems capable of independent reasoning, non-stop gaining knowledge of, and proactive reaction mechanisms.

Hybrid ML-Agentic AI architectures deal with these boundaries by using integrating predictive analytics, contextual cognizance, self-reliant orchestration, and adaptive mitigation right into a unified cybersecurity environment. gadget mastering and deep gaining knowledge of fashions along with Random Forests, support Vector Machines (SVM), synthetic Neural Networks (ANN), Convolutional Neural Networks (CNN), long short-time period memory (LSTM), and Transformer-primarily based architectures provide particularly efficient anomaly detection and assault classification capabilities. these models can analyze huge-scale network site visitors, identify hidden attack patterns, and learn complex behavioral relationships from excessive-dimensional cybersecurity datasets. Deep getting to know-primarily based structures especially reveal superior performance in extracting temporal and spatial capabilities from evolving cyberattack behaviors.

However, while ML fashions are incredibly powerful in prediction and classification tasks, they nonetheless suffer from several boundaries, inclusive of negative explainability, lack of contextual reasoning, confined adaptability to unknown attack patterns, and dependence on human administrators for mitigation choices. this is where Agentic AI introduces a transformative capability. Agentic AI structures characteristic as self-sufficient wise marketers capable of belief, reasoning, making plans, policy optimization, and real-time choice execution. unlike traditional AI structures that only generate predictions, Agentic AI continuously evaluates environmental conditions, prioritizes dangers, formulates defense techniques, and dynamically adjusts mitigation policies without requiring continuous human intervention.

The combination of ML with Agentic AI creates a collaborative intelligence framework wherein system gaining knowledge of models detect and classify potential threats while self-sustaining marketers interpret contextual hazard factors and execute appropriate mitigation techniques. This fusion extensively improves operational efficiency, response velocity, danger containment functionality, and device resilience. The reviewed research research reveal that hybrid ML-Agentic AI systems considerably enhance detection accuracy, lessen fake nice quotes, optimize incident reaction latency, and strengthen defense mechanisms against superior cyberattacks. Experimental evaluations presented inside the reviewed frameworks display splendid upgrades in cybersecurity overall performance metrics, along with more suitable F1-ratings, higher precision and do not forget values, reduced fake alarms, and advanced mitigation fulfillment fees when compared with traditional ML-handiest or rule-primarily based intrusion detection structures.

Some other main benefit of hybrid architectures is their capability to help non-stop and adaptive studying via reinforcement gaining knowledge of and comments optimization mechanisms. Agentic AI structures can examine the effectiveness of applied mitigation actions, analyze from assault consequences, and refine their choice-making regulations through the years. This enables cybersecurity systems to evolve dynamically alongside rising assault techniques, thereby reducing dependency on manually up to date security policies and static detection signatures. The addition of reinforcement learning similarly enhances adaptive protection abilties by means of allowing self-

sustaining agents to optimize reaction strategies based on environmental comments and hazard severity.

The growing integration of explainable AI (XAI) strategies additionally contributes substantially to the development of sincere independent cybersecurity structures. Explainability mechanisms together with SHAP values, attention visualization, and interpretable reasoning graphs improve transparency in AI-pushed selections and assist cybersecurity analysts apprehend how threats are recognized and mitigated. This will become in particular essential in business enterprise, healthcare, industrial IoT, protection, and critical infrastructure environments where responsibility, regulatory compliance, and operational consider are crucial.

In spite of the promising consequences of hybrid ML-Agentic AI cybersecurity structures, numerous studies challenges and realistic obstacles remain unresolved. one of the number one concerns entails scalability and computational overhead. Deep mastering models and autonomous reasoning engines require good sized computational assets, which might also have an effect on deployment efficiency in actual-time, high-speed, or resource-restricted environments consisting of IoT networks and facet devices. moreover, the interpretability of complicated deep neural networks and multi-agent reasoning structures remains hard in exceptionally dynamic assault situations.

Every other vital challenge entails antagonistic robustness and data protection. Cyber attackers may additionally try to control training datasets, poison reinforcement mastering comments loops, or make the most vulnerabilities within self-sufficient retailers themselves. ensuring at ease version schooling, robust antagonistic defense mechanisms, and sincere coverage variation stays a main research priority. in addition, governance, ethical manipulate, and protection assurance of independent AI agents stay critical concerns, especially in critical infrastructures where wrong independent choices could motive operational disruptions or accidental results.

Universal, the fusion of device getting to know and Agentic AI represents a revolutionary shift from reactive cybersecurity closer to predictive, self-reliant, and adaptive cyber defense paradigms. The reviewed literature strongly suggests that hybrid ML-Agentic AI frameworks offer the foundation for the subsequent generation of smart cybersecurity infrastructures able to working efficaciously in an increasing number of complicated and antagonistic digital environments. As research in explainable AI, reinforcement mastering, decentralized intelligence, federated security, and self-sufficient orchestration continues to mature, these hybrid architectures are predicted to turn out to be the cornerstone of destiny organisation-grade cybersecurity structures designed to gain resilience, scalability, transparency, and real-time clever protection towards evolving cyber threats.

REFERENCES

[1] S. Allani, K. Bou-Chaaya, and H. Rais, “ELISAR: A multi-agent cybersecurity framework integrating retrieval-augmented generation for Blue, Red, and GRC operations,” *World Wide Web*, vol. 29, no. 1, p. 3, 2026, doi: 10.1007/s11280-025-01393-5.

[2] B. Vijetha, “Agentic intelligence for unified cyber defense: A self-adaptive framework for threat detection across cloud, edge, and IoT systems,” IEEE Access, vol. 14, pp. 5104–5118, 2026, doi: 10.1109/ACCESS.2026.3650833.

[3] A. Polamarasetti, V. Yammanur, N. Ravuri, V. V. R. M. Bokka, and R. Vadisetty, “Agentic AI-driven cybersecurity for cloud-connected automotive systems,” in Communications in Computer and Information Science, vol. 2669, 2026, pp. 697–707, doi: 10.1007/978-3-032-07373-0_53.

[4] H. M. Zangana and M. Omar, Safeguarding and Securing Autonomous AI Agents. 2025, pp. 1–375, doi: 10.4018/979-8-3373-6876-4.

[5] A. Thurzo and V. Thurzo, “Embedding fear in medical AI: A risk-averse framework for safety and ethics,” AI (Switzerland), vol. 6, no. 5, p. 101, 2025, doi: 10.3390/ai6050101.

[6] B. Elsaify and M. Baderelden, “Adversarial and multilingual threats in retrieval-augmented generation: From prompt injection to model exploitation,” in Proc. 2nd International Generative AI and Computational Language Modelling Conference (GACLM), 2025, pp. 155–162, doi: 10.1109/GACLM67198.2025.11231998.

[7] I. Adabara, B. O. Sadiq, A. N. Shuaibu, Y. I. Danjuma, and M. Venkateswarlu, “A review of agentic AI in cybersecurity: Cognitive autonomy, ethical governance, and quantum-resilient

defense," F1000Research, vol. 14, p. 843, 2025, doi: 10.12688/f1000research.169337.1.

[8] A. Sheth et al., "AI driven self-healing cybersecurity systems with agentic AI for adaptive threat response and resilience," in Proc. IEEE Cloud Summit, 2025, pp. 147–153, doi: 10.1109/CLOUDSUMMIT64795.2025.00030.

[9] N. T. Dinh et al., "Enhancing smart contract security through DevSecOps: An adaptive approach for vulnerability detection," IEEE Access, vol. 13, pp. 159454–159486, 2025, doi: 10.1109/ACCESS.2025.3606572.

[10] A. Sheth et al., "Agentic AI for autonomous cyber threat hunting and adaptive defense in dynamic security environments," in Proc. IEEE International Conference on Electro Information Technology, 2025, pp. 316–321, doi: 10.1109/eIT64391.2025.11103697.

[11] N. R. Wagh et al., "Evaluation of IoT based smart safety systems for women and children using machine learning techniques," Scientific Reports, vol. 16, no. 1, p. 87, 2026, doi: 10.1038/s41598-025-29146-4.

[12] S. Rawas and A. D. Samala, "Bio-inspired AI for adaptive and resilient software-defined networks: A self-healing approach," Iran Journal of Computer Science, vol. 9, no. 1, p. 7, 2026, doi: 10.1007/s42044-025-00358-1.

[13] S. Vellaiyan et al., "A comprehensive review of AI-enabled predictive maintenance for hydrogen-powered transport," Journal of Loss Prevention in the Process Industries, vol. 101, p. 105953, 2026, doi: 10.1016/j.jlp.2026.105953.

[14] P. Laiu et al., "Designing resilient IoT and edge computing with federated tinyML," Journal of Systems Architecture, vol. 174, p. 103709, 2026, doi: 10.1016/j.sysarc.2026.103709.

[15] Y. Qiao et al., "A survey on adversarial machine learning: Attacks, defenses, real-world applications," Neurocomputing, vol. 671, p. 132670, 2026, doi: 10.1016/j.neucom.2026.132670.

[16] N. Odey and A. Marhoon, "A novel deep learning object detection based on PCA features for self-driving cars," Iraqi Journal of Electrical and Electronic Engineering, vol. 21, no. 2, pp. 186–195, 2025, doi: 10.37917/ijeee.21.2.18.

[17] E. Q. Ahmed et al., "AI based cognitive and software defined network for dynamic management and security in 6G networks," Al-Nahrain Journal of Science, vol. 28, no. 4, pp. 226–240, 2025, doi: 10.22401/ANJS.28.4.17.

[18] O. Afolalu and M. S. Tˇsoeu, "Artificial intelligence as the next frontier in cyber defense: Opportunities and risks," Electronics, vol. 14, no. 24, p. 4853, 2025, doi: 10.3390/electronics14244853.

[19] S. Srinivas et al., "AI-augmented SOC: A survey of LLMs and agents for security automation," Journal of Cybersecurity and Privacy, vol. 5, no. 4, p. 95, 2025, doi: 10.3390/jcp5040095.

[20] A. P. Sridhar, "Cognitive cyber defense applying artificial general intelligence to predict and counteract advanced persistent threats," Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol. 16, no. 4, pp. 18–31, 2025, doi: 10.58346/JOWUA. 2025.I4.002.

[21] A. Sultan et al., "Autonomous robotic systems for coral reef monitoring: Review and open research issues," Ecological Informatics, vol. 92, p. 103511, 2025, doi: 10.1016/j.ecoinf.2025.103511.

[22] D. George, S. Pavithra, and J. Das, "Cyber-resilient autonomous vehicles: Securing networks and enhancing decision-making with next-generation security measures," Results in Engineering, vol. 28, p. 107179, 2025, doi: 10.1016/j.rineng.2025.107179.

[23] M. M. Alnfiai, "AI-powered cyber resilience: A reinforcement learning approach for automated threat hunting in 5G networks," EURASIP Journal on Wireless Communications and Networking, vol. 2025, no. 1, p. 68, 2025, doi: 10.1186/s13638-025-02497-2.

[24] R. Ranpara, S. K. Patel, O. P. Kumar, and F. A. Al Zahrani, "Scalable architecture for autonomous malware detection and defense in software-defined networks using federated learning approaches," Scientific Reports, vol. 15, no. 1, p. 30190, 2025, doi: 10.1038/s41598-025-14512-z.

[25] A. A. Laghari et al., "A novel and secure artificial intelligence enabled zero trust intrusion detection in industrial internet of things architecture," Scientific Reports, vol. 15, no. 1, p. 26843, 2025, doi: 10.1038/s41598-025-11738-9.

[26] R. Islam et al., "Decentralized trust framework for smart cities: A blockchain-enabled cybersecurity and data integrity model," Scientific Reports, vol. 15, no. 1, p. 23454, 2025, doi: 10.1038/s41598-025-06405-y.