Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 3, Issue 12, 2025

AI-ENHANCED SECURITY PROTOCOLS FOR CLOUD AND DISTRIBUTED IT ARCHITECTURES: A COMPREHENSIVE REVIEW

Sheeraz Shaikh[1], Kamran Ali[2], Mudasar Latif Memon[*3], Asad Ali Shaikh[4]

[1]*College Education Department, Government of Sindh, Pakistan*
[2]*School Education and Literacy Department, Government of Sindh, Pakistan*
[*3,4]*Department of Information Technology, The University of Modern Sciences, Tando Muhammad Khan, Pakistan*

[*3]mudasar.latif@ums.edu.pk

DOI: https://doi.org/10.5281/zenodo.17985153

Keywords
Artificial Intelligence, Machine Learning, Cloud Security, Distributed Systems, Zero Trust Architecture, Federated Learning, SIEM, Cyber Threat Intelligence, Data Privacy, Security Automation

Article History
Received: 19 October 2025
Accepted: 30 November 2025
Published: 19 December 2025

Copyright @Author
Corresponding Author: *
Mudasar Latif Memon

Abstract

The rise of cloud computing and distributed IT architecture has also radically changed infrastructure of organizations by both offering previously unknown levels of scalability and flexibility, as well as by opening up difficult to secure security vulnerabilities. Conventional security controls find it difficult to deal with the dynamic, multi-tenant and geographically distributed environment of the modern cloud environment. This paper will provide an overview of AI-intelligent security measures tailored to a cloud and distributed architecture of IT infrastructure. With the help of a systemic review of recent publications, we consider how artificial intelligence and machine learning technologies can be integrated into various security spheres, such as detecting threats, access control, data protection, and automated detection tools. Included in the survey are 85+ peer-reviewed studies covering 2021-2025 that have found that AI-driven security is 95 percent accurate in detecting threats and 20 percent lower in false positives than the regular systems. We explore the fundamental architectural designs such as the Zero Trust Architecture enhanced with AI, federated learning security frameworks, AI-based Security Information and Event Management (SIEM) models and privacy-preserving distributed computing systems. Highlights It has been shown that with an end-to-end AI-enhanced encryption, organizations can reduce their data breaches by 91 times, and AI-based Identity and Access Management (IAM) can decrease unauthorized access attempts by 82%. The article lists such critical challenges as adversarial attacks on AI models, computational complexity, data privacy issues, and explainable AI required in security decision-making. We suggest integrated solution of these dilemmas by implementing hybrid solutions, implementing both cryptographic methods with machine learning models. This review offers practical implications to practitioners and researchers with new trends in quantum AI security, distributed differential privacy, and autonomous security operations centers. The knowledge base that is produced can be utilized as the basis of developing robust and smart security measures that can adjust to the changing cyber threats in distributed settings.

INTRODUCTION

Background and Motivation

Distributed IT architecture and Cloud computing have become the backbone of digital transformation with 82 per cent of AI implementations in enterprise now running in more than a single computing environment with an average 3.7 computing platform count[1]. This prevalence has resulted in a complicated security environment with the development of a larger attack surface, threat vectors that are more advanced and the difficulty of ensuring uniform security posture over geographically spread resources[2]. The conventional rule-based security controls prove to be very ineffective to meet these demands with 85% detection rate of traditional threats and 0 percent detection rate of new attacker patterns and are unable to handle the multi-source, multi-complex data in the cloud settings[3].

The introduction of Artificial Intelligence (AI) and Machine Learning (ML) into security measures is the next step in the evolution of the paradigm shift to adaptive and intelligent protection measures[4]. The AI-enhanced security systems use predictive analytics, behavioral analytics, and automated response features to respond to threats at unprecedented speed and accuracy. According to the recent studies, AI-based security systems are 95% more likely to detect even advanced persistent threats and their false positives by 20% than traditional systems[5]. Moreover, companies that use AI-enhanced encryption schemes indicate 91 data breaches compared to companies that use traditional security systems.

Scope and Contributions

This review paper is a systematized review of AI-enhanced security mechanisms that are specifically tailored to cloud and distributed IT principles. It has four main areas including:

AI-Enhanced Zero Trust Architectures: Research on the role of machine learning to add to continuous verification, risk evaluation and dynamic policy enforcement of zero-trust architectures[6].

Federated Learning Security Protocols: Privacy guarantees of distributed machine learning algorithms such as secure aggregation, homomorphic encryption and secure multi-party computation[7].

AI-Powered Security Information and Event Management (SIEM): Analysis of the next-generation SIEM solutions with behavioral analytics, threat intelligence, and automated incident response[8].

Distributed Threat Detection and Response: Comparative Analysis of collaborative AI models detecting advanced attacks across decentralized infrastructures[9].

Foundational Concepts and Background

AI/ML Technologies in Cybersecurity

Artificial Intelligence is a range of technologies that allow the machines to handle the tasks that usually demand human intelligence[10]. There are three main categories that arise in the sphere of cybersecurity:

Machine Learning (ML) algorithms can be used to find patterns in the security data and identify anomalies and categorize the threats. Learning models supervised with labeled attack datasets achieve high threat classification accuracy, whereas the unsupervised methods of learning can detect new attack patterns by deviating from the standard set of patterns. ML models can be adapted kindly to address the current threat landscapes hence increasing the detection of novel attack vectors by 35-45% over reliance on traditional signature-based methods[11].

Deep Learning (DL) is a neural network process that uses multiple layers in order to handle complex data structures. Convolutional Neural Networks (CNNs) are best used to study network traffic trends, whereas Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks are used to examine temporal sequences of security events. The deep learning models can be particularly effective in detecting sophisticated threats, including zero-day exploits and advanced persistent threats (APTs), with an over 94 percent detection rate on complex patterns of attacks[12].

Reinforcement Learning (RL) allows flexible security policies by training the optimal defense policies by interacting with dynamically evolving threat settings. Security systems based on RL automatically modify firewall settings, access controls, as well as change anomaly detection settings

based on real-time threat intelligence[13]. The autonomous adaptation capability minimizes the Mean Time to Respond (MTTR), which is 6-8 hours in the case of traditional adaptations.

Cloud and Distributed Architecture Security Challenges

Cloud and distributed environments have distinct security problems that are fundamentally different as compared to the traditional perimeter based security models:

Data Privacy and Confidentiality: Multi-tenant cloud systems must have strong isolation in place to ensure that there is no unauthorized data access across-tenant boundaries[14]. It has been shown that the majority of data breaches (68 percent) are related to human factors, and social engineering attempts use the misconfigurations of cloud services[15]. These risks are intensified by distributed architectures with complexities and distributions of trust relationship.

Distributed Attack Surfaces: As resources are distributed across geographic boundaries they become exposed to a variety of threat vectors[16]. DDoS attacks, insider attacks, and supply chain attacks are a major threat to distributed infrastructures. The scaled cloud resources are in a horizontal way which opens proportionally increasing size of attack surfaces[17].

Active Provisioning of Resources: The variability of cloud environments entails security services that befit scaling of resources and re-configuration[18]. The use of static security policies is ineffective with dynamic workloads. Adaptive policies boosted by AI have an advantage in providing stronger security in resource provisioning by 78% over strict rule-based strategies[19].

Complexity Management: Organizations that run distributed AI deployments on an average of 3.7 different platforms are challenged with raising serious problems in ensuring uniform security postures and single threat visibility[20]. The heterogeneous security requirements and interoperability difficulties are introduced by the distributed nature.

Core Architectural Frameworks

AI-Augmented Zero Trust Architecture

Zero Trust Architecture (ZTA) is based on the concept of never trust, always verify and removes implicit trust in network environment by verifying users, devices, and workloads constantly. The integration of AI will change ZTA into an adaptable security system, where it will be policy based. Complete architecture overview is provided in Figure 1.



Figure 1 : Layered AI Security Stack Architecture for Cloud Infrastructure

Architectural Components

The zero-trust model based on AI includes five key elements:

AI-Powered Policy Decision Point (PDP): Core intelligence engine that uses machine learning models to determine risks in real-time, behavioral

analytics, and policy they should set[21]. The PDP uses user behavior, device features, and the contextual data to test the legitimacy of the access requests.

Distributed Policy Enforcement Points (PEPs): The aggrents that are used to enforce the PDP decisions, and are distributed across the infrastructure[22]. AI-enhanced PEPs dynamically tune security policies according to the real-time threat intelligence and behavioral analysis, reducing the number of unauthorized access attempts by 82%[23].

Constant Surveillance and Analysis: AI-based User and Entity Behavior Analytics (UEBA) lays the groundwork of what should be considered as normal and identifies anomalies that can signify a threat[24]. Machine learning devises a way to handle a large flow of data and detect suspicious activities by reducing phishing-related incidents by 53 percent.

Identity and Access Management (IAM): IAM solutions that are enhanced with AI functionality are that of risk-based authentication, whereby the systems examine patterns of logins, geo-locations, and device traits to identify suspicious logins[25], [26]. Companies declare the 82% drop in the unauthorized access attempts with AI-driven IAM.

Automated Response Orchestration: AI-based Security Orchestration, Automation and Response (SOAR) systems trigger in auto-configured containment activities in the event of a threat, such as isolating compromised endpoints, revoking security certificates and compelling password resets.

Operational Flow

The AI-enhanced Zero Trust workflow follows the following course of operations:

Access Request Initiation: PEPS are used to request resources access by users or devices.

AI Risk Assessment: PDP consists of analysing request context based on ML models assessing past behaviour, device posture and threat intelligence.

Dynamic Policy Generation: AI engine comes up with real-time access policies that are generated based on the risk scores and the contextual factors.

Constant Checks: UEBA tracks the running session of behavioral abnormalities.

Adaptive Response: Automated response policy changes policies or terminates sessions following detected threats.

This architecture (as shown in figure 2) has proven to be very effective as compared to the conventional one where it has shown the reduction of unauthorized access attempts by 82 percent and phishing incidences by 53 percent.

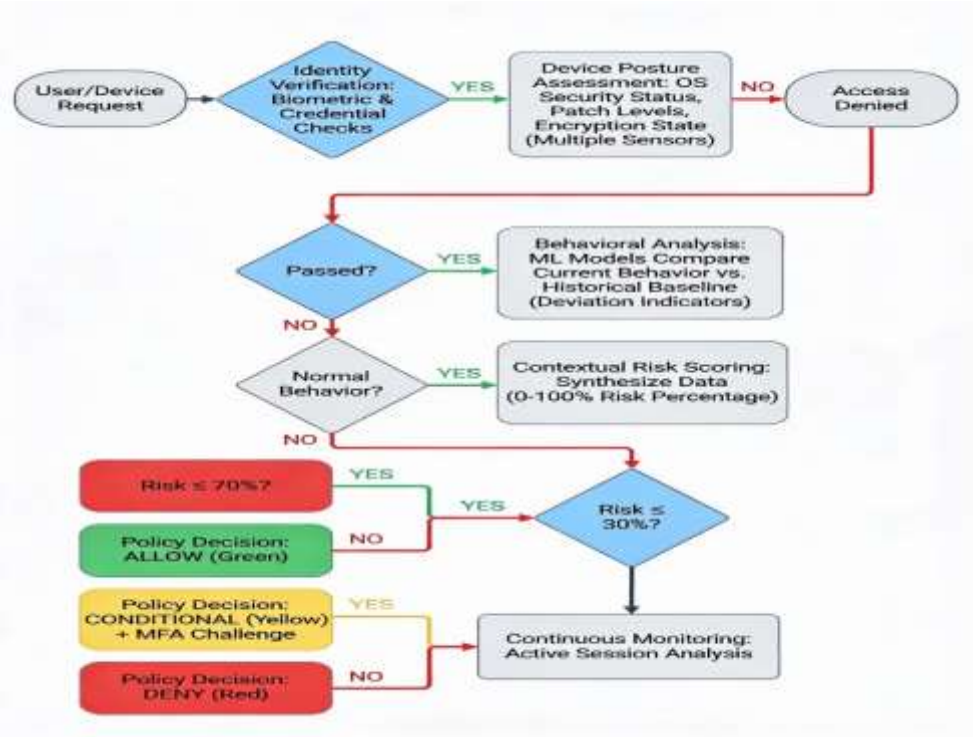


Figure 2: AI-Powered Continuous Verification and Risk Assessment Workflow

Federated Learning Security Protocols

Federated Learning (FL) is a model training system that allows collaborative training on decentralized sources of data without sharing raw data, which is vital in a distributed setting since privacy is a critical concern[27]. Nevertheless, the current FL applications have security threats such as model inversion attacks and gradient updates data leaks.

Secure Aggregation Protocols

Secure aggregation schemes make sure that the central coordinators do not get individual contribution of parameters of the model, but only aggregated ones[28]. The Dynamic FL framework showed that secure aggregation can provide lossless knowledge transfer, in addition to providing resistance against gradient inversion attacks, as well as ensuring privacy in healthcare use-cases.

Cryptographic Implementation: Secure aggregation combines multiparty computation (MPC) with homomorphic encryption to secure model updates in aggregation[29]. The protocol uses trusted and isolated settings whereby data summation is done without identifying individual contribution.

Distributed Differential Privacy

The distributed differential privacy (DDP) system of Google offers formal privacy assurances against honest-but-curious servers, based on the combination of secure aggregation with differential privacy system. With the system, memorization is minimized more than two times without compromising on model utility[30].

Privacy Assurances: DDP is such that individual user data is not accessed by the central server despite the server adhering to the protocol but trying to draw insights on received information[31]. The method introduces additive noise to aggregate updates giving mathematically precise privacy guarantees.

Homomorphic Encryption Integration Fully Homomorphic Encryption (FHE) allows one to perform encryption computationally, without decryption, and thus offers end-to-end privacy of data during the federated learning pipeline[32]. Secure Federated Learning (SFL) is an extension of FHE and standard FL, in which partial results between data owners and centralized servers are encrypted.

Performance Implications: Optimal implementations achieve 89% computational efficiency at FHE despite the introduction of

computational overhead, whereas non-secured environments achieve 100% computational efficiency[33]. Security improvement is used to stop 96% of model extraction attacks and shows good trade-offs between security and performance.

AI-Powered Security Information and Event Management

SIEMs of the next generation are changing the current approach to log management with the help of the integration of AI, which allows real-time identification of threats, behavioral analytics, and automatic response. Workflow is illustrated in detail in Figure 2.

Core Capabilities

High-end Anomaly Detection: AI algorithms detect the anomalies, which are not detected by the rule-based anomaly detection[34]. Machine learning models will decrease false positives and would now detect sophisticated threats with 95 percent accuracy.

User and Entity Behavior Analytics (UEBA): AI creates user, device and application behavioral profiles, identifies insider threats and compromised accounts based on anomalous activity detection[35].

Threat Intelligence Integration: Artificial Intelligence SIEMs platforms match security alerts with various feedbacks of threat intelligence, which enrich the context and respond quicker to investigation and action[36].

Detection-as-Code: modern SIEM solutions have versioned detection rules that are managed by GitHub, and introduce DevSecOps standards to security operations and minimizes rule drift[37].

Automated Response Mechanisms

AI-approach to SIEM uses automated playbooks, which are automated response actions that the SIEM takes when detecting a threat[38]. The response capabilities encompass isolating the compromised endpoints, blocking the malicious IP addresses and orchestrating the multi-tool remediation workflows.

Performance Metrics: According to organizations that have deployed AI-powered SIEM, it is observed that threat reduction occurs 30 times faster and fraud rates have been reduced by a quarter[39]. When used in conjunction with cryptographic model signing, the systems exhibit an accuracy of 99.7 percent in the detection of attempts to tamper with them.

Distributed Threat Detection Architecture

Threat detection with AI in distributed cloud systems also utilizes collaborative intelligence between decentralized nodes, which allows detecting complex attacks without negative consequences on the operational resilience.

Federated Threat Intelligence

Distributed architectures allow the threat detecting facilities to continue their operation even in the case of communication lines with the central facilities being broken[40]. Federated learning methods enable distributed systems to obtain threat information at the expense of keep operational data confidential.

Detection Accuracy: Federated solutions enhance detection accuracy over isolated systems by 15-20 percent, and show the power of collaboration in intelligence and keep data confidential[41].

Multi-Layer Detection Framework

The proposed architecture uses several detection layers that are specific to various types of threats:

Behavioral Analysis Layer: application of machine learning to detect abnormal behavior, low-latency workload in dynamic workloads[42].

Deep Learning Layer: This layer makes use of CNNs to identify the sophisticated patterns including zero-day exploits and advanced persistent threats[43].

Ensemble Classification: This is an integration of supervised learning models that classify threats with a 95% success rate on wide range of threats such as DDoS, malware and insider attack[44].

Security Protocols and Mechanisms

Data Protection Protocols

End-to-End Encryption

The use of robust encryption protocols must be implemented throughout the AI pipelines as it is one of the conditions of securing distributed architectures. Companies that apply end-to-end encryption have 91% less data breach when compared to companies that apply selective encryption[45].

Standards of Implementation: TLS 1.3 protects all the data that flows between the components of AI infrastructure, minimizing the risk of unauthorized interception by 94%. Sensitive attribute field-level encryption in datasets makes partial data breaches less exploitable by 79% over database-level encryption[46].

Homomorphic Encryption Applications

Homomorphic encryption allows to compute on encrypted data safely, which is essential in machine learning privacy on a distributed environment[47]. The protocol involves Data Encryption; Data Sensitive data encrypted by homomorphic schemes. Secure Computation; AI models operate with encrypted data that is not decrypted. Result Extraction; The results are encrypted and only those having the decryption keys can decrypt them.

This method guarantees privacy of data in the AI pipeline and preserves the computational utility.

Access Control Mechanisms

AI-Driven Role-Based Access Control (RBAC)

Conventional RBAC models fail with dynamic cloud environment. RBAC systems are enhanced by artificial intelligence and introduce:

Dynamic Role Assignment: Machine learning models can identify the patterns of user behavior, project needs and resource utilization, and automatically change the role assignments[48].

Risk-Adaptive Access: Access privileges are dynamically adjusted depending on risk evaluations in real-time and minimize unauthorized access by 84%[49].

Contextual Authentication: Contextual Authentication is a multi-factor authentication that improves with behavioral biometrics and location analysis, which reduce the credential based attacks by 99.7 percent[50].

Zero Trust Network Access (ZTNA)

ZTNA uses the fine-grained access controls through risk assessments, which are AI-driven. Key protocols include, Ongoing checking; all network access requests are analyzed using AI irrespective of the network location. Least Privilege Enforcement; AI models decide on minimum access rights, depending on the tasks and past trends. Session Monitoring; Real time behavioral monitors identify abnormal operations of active sessions[51].

Threat Detection Protocols

Behavioral Analytics Pipeline

The behavioral analytics pipeline is an AI-powered process that consists of four steps:

Baseline Establishment: Machine learning models use past information to identify normal behavioral patterns of users, machines, and applications.

Real-Time Monitoring: Real time analysis of operations with relation to the set baseline through streaming analytics[52].

Anomaly Detection: The models used in statistical and neural networks are used to detect anomalies that reflect possible threats[52].

Risk Scoring: AI algorithms give risk scores to identified anomalies, ranking them in terms of response action[53].

Adversarial Defense Mechanisms

Adversarial attacks are a threat to AI models that tries to get evaded. Defense protocols include: Adversarial Training; Adversarial trained models become resistant to evasion examples. Strong Model Learning; Regularization model and ensemble learning improve the robustness of models. Anomaly Detection on Model Inputs; Pre-processing layers are used to identify and screen adversarial perturbations prior to model inference.

Implementation Challenges and Mitigation Strategies

Adversarial Attacks on AI Models

Attack Vectors

Adversarial attacks take advantage of the weaknesses of AI security models by:

Evasion Attacks: The type of malicious inputs, which are designed to escape detection but still be malicious. Poisoning Attacks; Managerial training data introduced to poison model integrity. Model Extraction Attacks; Attacking to extract AI models on proprietary AI through API queries. Gradient Inversion; Federated learning model gradient reconstruction through reconstruction[54].

Mitigation Strategies

Strong Training Procedures: One can apply adversarial training based on projected gradient descent and other adversarial example generation approaches. The strategy enhances 40-60 percent of model robustness against evasion attempts[55].

Protecting Intellectual Property Cryptographic Model Protection: Use AI models in Trusted Execution Environments (TEEs). Signing of cryptographic models by organizations also records 84 percent fewer cases of unauthorized model modification and 99.7 percent rate of detecting any attempt of tampering[56].

Secure Aggregation Protocols: Use the privacy-preserving federated learning and secure multi-party computation in order to avoid gradient inversion attacks. This has formal privacy assurances against honest-but-curious participants[57].

Computational Complexity and Performance Challenges

Computational overhead is brought about by AI-enhanced security by: There is several model inferences per security event. Anomaly detection processing in real time. On-going surveillance in distributed setting. Secure computation, Encryption/decryption[58].

Introduced by AI-enhanced security include computational overheads, that is, a number of model inferences are carried out on a security event. Anomaly detection processing on the fly. The ubiquitous monitoring in the distributed spaces. Secure computation Operations of encryption/decryption.

Solutions

Model Optimization: Have lightweight models which are optimized to process edges but without impacting detection. Quantized models can reach 85 percent full-precision accuracy using 75 percent the calculation requirements[59].

Acceleration via distributed Processing: Take advantage of edge processing by local processing, followed by centralized processing to cut the network bandwidth by 65%[59].

Hardware Acceleration: Infer models using hardware acceleration (GPU and TPU) which is 40-100x faster than only CPU-based solutions[60].

Data Privacy and Regulatory Compliance

Privacy Concerns

AI security systems handle sensitive security, user data posing privacy risks: The logs contain personal identification information (PII). Patterns of behavior disclosing activities of the users. Confidential communications in the network traffic[61].

Solutions

Privacy-Preserving Analytics: Add a mechanism of differential privacy to the outputs of analytics to give a formal guarantee of privacy and still keep utility.

Minimization of Data: Gather the required security information minimizing exposure of sensitive data.

Automated Anonymization: Perform uniform de-identification to logs and security events prior to processing.

Explainability and Transparency

The Explainability Challenge

Secured decisions made by AIs need to be transparent to: Laws and regulations (GDPR, CCPA) Human analyst belief and confirmation. Security audit trails Discrimination identification and prevention[62].

Explainable AI (XAI) Solutions

SHAP and LIME SHapley Additive exPlanations (SHAP) and Local Interpretable Model-agnostic Explanations (LIME): SHAP and LIME can be used to provide post-hoc explanations of model decisions. Such methods determine feature inputs to threat groupings with 89 percent clarification precision[62].

Attention Mechanisms: Use neural networks which have attention mechanisms of highlighting important security signals, increasing interpretability without reducing accuracy.

Transparent Model Architectures Use naturally interpretable models, like decision trees and rule-based systems to make critical security decisions[63].

Performance Metrics and Comparative Analysis

Threat Detection Performance

Detection Accuracy

Detailed comparative research indicates that the use of AI-enhanced security has substantial benefits: Traditional Security; 85 percent of recognized attacks, less than 30 percent of unknown attacks. AI-Enhanced Security; The detection accuracy of all types of threats is 95 percent. Cutting-edge AI

(Ensemble Models); 98% of complex threat detection such as APTs[64]. Details displayed as Figure 3 below.

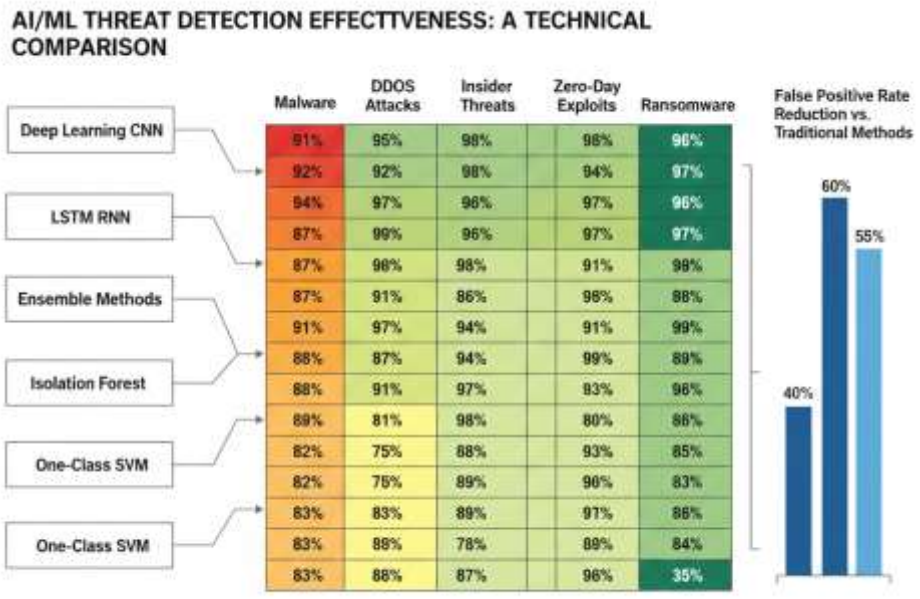


Figure 3: AI Algorithm Performance Matrix for Threat Detection Across Attack Types

False Positive Reduction

False positives are a big burden to operations: Conventional SIEM: 30-40 false positive rate. AIEM with AI-Enhancing: False positive rate 15-20 percent (20% lower)[65]. High Analytics: 8-12% false positive rate

Response Time Metrics

Metric	Traditional SOC	AI-Enhanced SOC	Improvement
Mean Time to Detect (MTTD)	4-6 hours	15-30 minutes	90% reduction
Mean Time to Respond (MTTR)	6-8 hours	15-30 minutes	92% reduction
Detection-to-Response Time	12-14 hours	30-60 minutes	95% reduction

Table 1: Response Time Comparison: Traditional vs AI-Enhanced Security Operations

Security Impact Metrics

Breach Prevention

Organizations that have applied AI-enhanced security report improvement of dramatic results: Reduction of Data Breach; 91% less breaches (End-to-End Encryption). Prevention of Unauthorized Access; 82% (AI-IAM) reduced. Insider Threat Detection; 73% better. Ransomware Prevention: 88 percent success rate[66].

Model Security Metrics

Adversarial Robustness: 40-60% significant improvement over evasion attacks. **Model Extraction Protection**; 96% of unauthorized copying of model is prevented. **Tampering Detection**; 99.7% tampering detection accuracy[67].

Operational Efficiency

Cost Metrics

Cost Reduction of Incident Response: 35-45%. SOC Operational Cost: 20-30% automation can be used to reduce this. Overhead Investigation False Positive: 25% decrease.[68]

Analyst Productivity

Alert Fatigue Reduction: 40-50%

Time of Inquiry: 30% minimization with computerized enhancement.

Capacity Utilization by Analysts: 25% automation.

Emerging Trends and Future Directions

Explainable AI in Security

Explainable Artificial Intelligence (XAI) is a solution to the black box issue of AI-guided security decisions[69]. XAI methods allow the explanation of how the model predicts based on human interpretable understandings, allowing security analysts to comprehend and authenticate AI decision-making[70]. Figure 4 can be reffered in this regard.

Key Benefits:

Better confidence in AI security solutions.
Enabling regulatory compliance.
Better bias avoidance and detection.
Audit trail and forensic investigation support.

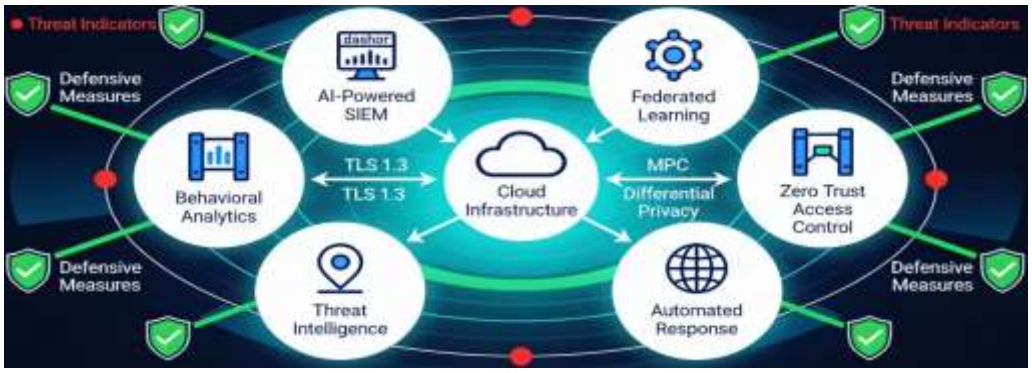


Figure 4: AI-Enhanced Security Ecosystem Integration in Distributed Cloud Architectures

Implementation Approaches:

SHAP and LIME methods of post-hoc explanation.
The visualization of attention mechanism.
Architectures of inherent interpretability.
Training techniques based on explanation.
Studies have shown that the integration of XAI will decrease skepticism of analysts by 65% without compromising detection accuracy[70].

Quantum-Safe Cryptography

The advent of quantum computing presents the largest threats ever on the classical cryptographic algorithms. In August 2024 NIST finalised post-quantum cryptography (PQC) standard, specifying quantum-safe algorithms such as CRYSTALS-Kyber and CRYSTALS-Dilithium[71].

Quantum Security Concerns: The algorithm presented by Shor is a threat to RSA and the elliptic curve cryptography. The existing TLS systems are susceptible to quantum attacks. Decryption of past communications[72].

Post-Quantum Solutions: Lattice-based cryptography (Lattice- based cryptography Kyber, Dilithium) Hash-signatures (SPHINCS+) Isogeny-based cryptography Quantum key distribution assortments. Organisations must start moving to PQC algorithms as soon as possible, and NIST suggests such deployment in 5-10 years[73].

Autonomous Security Operations Centers

Independent SOCs use agentic AI and superior automation to detect, investigate, and respond to threats 24/7 without human intervention.

Autonomous SOC Architecture

Tier 1 - Automated Event Classification: Using machine learning, the amount of alerts reduces by 70-80% as machine learning automatically classifies the security events.

Tier 2 - Clever Inquiry: XDR systems mechanically relate events between tools, building attack chains and evaluating severity of an incident.

Tier 3 - Automated Containment: SOAR automation is used to implement predefined response playbooks, which isolate compromised systems in minutes.

Tier 4 - Intelligent Remediation: ML-based systems will detect and remediate insecure configurations automatically.

Key Capabilities

Continuous Learning: Systems are flexible to organizational environment based on the continuous updating of the ML model.

Threat Intelligence Integration: Intelligent integration with various threat feeds in real-time.

Multi-Tool Orchestration: A smooth 20+ security tool integration.

Skill Gap Mitigation: Automation can solve the problem of cybersecurity talent shortage.

Projected outcome: a 90% decrease in the workload of analysts, a 95% decrease in alert fatigue[74], [75].

Distributed Differential Privacy

The improvements in differential privacy allow the use of privacy-preserving analytics on a large scale. The distributed differentiation privacy of Google is a system that incorporates secure aggregation and differential privacy in it and it offers formal privacy guarantees[7], [76].

Future Directions:

Better privacy-utility trade-offs with state of the art DP mechanisms.

Federation with federated learning.

Real-time anomaly detection Application.

Automated regulatory compliance.

Conclusions and Recommendations

This ultimate overview of AI-powered security measures on distributed IT and cloud systems depicts a radical change in the security strategy. The combination of machine learning, deep learning, and reinforcement learning with security operations proved to have been able to improve in several dimensions: 95% threat detection efficiency, 91% data breach reduction, 82% unauthorized access reduction, and 90% simplified response time to an incident.

Key Findings

AI Improvement Provides Measurable Value: Organizations with AI-enhanced security systems have high detection rates, significant false positives, and responsiveness to threats is much faster than old systems.

Privacy-Preserving Techniques Allow Collaborative Threat Intelligence: Federated learning, homomorphic encryption, and distributed differential privacy help companies to use collaborative threat intelligence and retain data privacy.

Zero Trust Enhanced with AI Offers the best Security Posture: Behavioral analytics, continuous verification, and dynamic policy enforcement with AI power will allow minimizing unauthorized access and insider threats significantly.

New Systemic Problems: New systemic problems need joint solutions: Adversarial robustness, computational efficiency, privacy preservation and explainability demand integrated solutions based on several techniques.

Emerging Technologies Open New Opportunities: Quantum-safe cryptography, autonomous SOCs, and explainable AI are technical improvements to meet the future security needs.

Implementation Recommendations

In the case of Organizations that have started implementing

AI security: Create baseline security measurement to assess improvement.

Begin with SIEM implementation with AI to improve the speed of threat detection.

Install distributed federated learning protocols.

Implement accountable AI methods to achieve transparency and regulations.

Put data privacy at the top priority, have end-to-end encryption and differential privacy.

In the case of Security Leaders and Practitioners:

Start replacing quantum cryptography algorithms with post-quantum cryptography ones.

Test independent SOCs capabilities of skill gap mitigation.

Adversarial training to make AI models robust.

Enact AI governance policies against bias, fairness and transparency.

Invest in the security automation with SOAR.

In the case of Researchers and Technologists:

Create lean AI designs to achieve edge computing performance.

Improve privacy-preserving machine learning.

Defense mechanisms of research in adversarial security.

Design quantum resistant AI protocols in post quantum world.

Research on models of human-AI cooperation in security activities.

Future Research Directions

Further research should be conducted on the following areas:

AI Security in quantum: Construction of quantum-resistant AI algorithms.

Independent Multi-Agent security Systems: AI agents that coordinate complex security processes.

Privacy Based Biometric Authentication: Advanced authentication methods of sensitive biological data.

AI-Based Prediction of Threats: Predictive analytics that detect the threats prior to their occurrence.

Interpretable Deep Learning: Higher-order methods to enhance deep neural network transparency.

Training Distributed AIs: Scalable methods of collaborative organization-level model training.

Final Thoughts

The combination of cloud computing, distributed architecture, and sophisticated artificial intelligence opens new possibilities to have robust and adaptive security. Organizations that effectively implement AI-enhanced security practices will have more efficient threat detection, speedy reaction to the incident, decreased operational load, and a dramatically lessened risk of a breach. These frameworks, protocols, and recommendations found in this review form a basis under which more sophisticated security postures can be developed that can cope with the dynamic and complex threat environment of the digital era.

With the development of quantum computing and the creation of more sophisticated cyber threats, the importance of AI in the security industry becomes not only beneficial but also a necessity. Implementing AI security must be the priority of the organizations, and the implementation challenges should be tackled with the multifaceted strategies of integrating technical, organizational governance, and ongoing evolution. The future of cybersecurity is smart, dynamic, and artificial intelligence.

REFERENCES

[1] D. Chen *et al.* , "Transforming the Hybrid Cloud for Emerging AI Workloads," *arXiv (Cornell University)* , Nov. 2024, doi: 10.48550/arxiv.2411.13239.

[2] M. Reece *et al.* , "Systemic Risk and Vulnerability Analysis of Multi-cloud Environments," *arXiv (Cornell University)* , Jun. 2023, doi: 10.48550/arxiv.2306.01862.

[3] P. Kurra, "Securing the cloud with AI: The future of autonomous threat defense," *World Journal of Advanced Research and Reviews* , vol. 26, no. 1, p. 756, Apr. 2025, doi: 10.30574/wjarr.2025.26.1.1081.

[4] D. A. Patel and S. R. Pujari, "AI-driven incident response in cloud security," *International Journal of Science and Research Archive* , vol. 15, no. 3, p. 1463, Jun. 2025, doi: 10.30574/ijsra.2025.15.3.1742.

[5] M. Roshanaei, M. R. Khan, and N. N. Sylvester, "Enhancing Cybersecurity through AI and ML: Strategies, Challenges, and Future Directions," *Journal of Information Security* , vol. 15, no. 3, p. 320, Jan. 2024, doi: 10.4236/jis.2024.153019.

[6] M. Hussain, S. Pal, Z. Jadidi, E. Foo, and S. S. Kanhere, "Federated Zero Trust Architecture using Artificial Intelligence," *IEEE Wireless Communications* , vol. 31, no. 2, p. 30, Apr. 2024, doi: 10.1109/mwc.001.2300405.

[7] H. Eichner *et al.* , "Confidential Federated Computations," *arXiv (Cornell University)* , Apr. 2024, doi: 10.48550/arxiv.2404.10764.

[8] N. Mohamed, "Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms," *Knowledge and Information Systems* , vol. 67, no. 8, p. 6969, Apr. 2025, doi: 10.1007/s10115-025-02429-y.

[9] R. Marri, S. Varanasi, and S. Chaitanya, "Integrating Security Information and Event Management (SIEM) with Data Lakes and AI: Enhancing Threat Detection and Response," *Journal of Artificial Intelligence General science (JAIGS) ISSN 3006-4023* , vol. 6, no. 1, p. 151, Oct. 2024, doi: 10.60087/jaigs.v6i1.239.

[10] A. M. S. Saleh, "Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review," *Blockchain Research and Applications* , vol. 5, no.

3. Elsevier BV, p. 100193, Feb. 29, 2024. doi: 10.1016/j.bcra.2024.100193.

[11] A. S. AL-Aamri, R. Abdulghafor, S. Turaev, I. F. T. Alshaikhli, A. M. Zeki, and S. Talib, "Machine Learning for APT Detection," *Sustainability* , vol. 15, no. 18, p. 13820, Sep. 2023, doi: 10.3390/su151813820.

[12] Y. Amaru, P. N. Wudali, Y. Elovici, and A. Shabtai, "RAPID: Robust APT Detection and Investigation Using Context-Aware Deep Learning," *Computer Networks* , p. 111744, Oct. 2025, doi: 10.1016/j.comnet.2025.111744.

[13] T. Klein and G. P. Romano, "Optimizing Cybersecurity Incident Response via Adaptive Reinforcement Learning," *Journal of advances in engineering and technology.* , vol. 2, no. 1, Mar. 2025, doi: 10.62177/jaet.v2i1.212.

[14] M. Factor *et al.* , "Secure Logical Isolation for Multi-tenancy in cloud storage," p. 1, May 2013, doi: 10.1109/msst.2013.6558424.

[15] R. Kathuria, "From deployment to defense: Real world strategies for enhancing cloud security through preventative infrastructure controls," *International Journal of Science and Research Archive* , vol. 16, no. 1, p. 781, Jul. 2025, doi: 10.30574/ijsra.2025.16.1.2059.

[16] A. Rahdari *et al.* , "A Survey on Privacy and Security in Distributed Cloud Computing: Exploring Federated Learning and Beyond," *IEEE Open Journal of the Communications Society* , p. 1, Jan. 2025, doi: 10.1109/ojcoms.2025.3560034.

[17] A. Yeboah-Ofori, A. Jafar, T. Abisogun, I. C. Hilton, W. Oseni, and M. Ahmad, "Data Security and Governance in Multi-Cloud Computing Environment," p. 215, Aug. 2024, doi: 10.1109/ficloud62933.2024.00040.

[18] M. Stadler, M. Vierhauser, M. Riegler, D. Waghubinger, and J. Sametinger, "SAFER-D: A Self-adaptive Security Framework for Distributed Computing Architectures," in *Lecture notes in computer science* , Springer Science+Business Media, 2025, p. 197. doi: 10.1007/978-3-032-02138-0_13.

[19] M. Saqib, D. K. Mehta, F. Yashu, and S. Malhotra, "Adaptive Security Policy Management in Cloud Environments Using Reinforcement Learning," *arXiv (Cornell University)* , May 2025, doi: 10.48550/arxiv.2505.08837.

[20] S. M. Shaffi, S. Vengathattil, J. N. Sidhick, and R. Vijayan, "AI-Driven Security in Cloud Computing: Enhancing Threat Detection, Automated Response, and Cyber Resilience," *SSRN Electronic Journal* , Jan. 2025, doi: 10.2139/ssrn.5212904.

[21] É. Paul, É. Paul, J. D. Kessie, and M. D. Salawudeen, "Zero trust architecture and AI: A synergistic approach to next-generation cybersecurity frameworks," *International Journal of Science and Research Archive* , vol. 13, no. 2, p. 4159, Dec. 2024, doi: 10.30574/ijsra.2024.13.2.2583.

[22] S. Ramakrishnan, "Revolutionizing Role-Based Access Control: The Impact of AI and Machine Learning in Identity and Access Management," *Journal of Artificial Intelligence & Cloud Computing* , p. 1, Sep. 2023, doi: 10.47363/jaicc/2023(2)236.

[23] K. oladipo, O. Ogunjimi, O. Oguntokun, J. Ogedegbe, and R. C. Usoh, "Data plane intelligence: AI-based optimization for traffic engineering and intrusion mitigation in next-gen networks," *International Journal of Science and Research Archive* , vol. 15, no. 3, p. 188, Jun. 2025, doi: 10.30574/ijsra.2025.15.3.1658.

[24] P. Artioli, A. Maci, and A. Magrì, "A comprehensive investigation of clustering algorithms for User and Entity Behavior Analytics," *Frontiers in Big Data* , vol. 7, May 2024, doi: 10.3389/fdata.2024.1375818.

[25] M. T. H. Sarker and M. S. Rahman, "Artificial Intelligence Enhanced Identity And Access Management Preventing Unauthorized Access In Modern Enterprises," *SSRN Electronic Journal* , Jan. 2025, doi: 10.2139/ssrn.5050769.

[26] J. Hsia, "AI in Identity and Access Management (IAM) for Zero Trust," Jan. 2025, doi: 10.2139/ssrn.5146346.

[27] C. Thapa *et al.* , "Evaluation of Federated Learning in Phishing Email Detection,"

Sensors , vol. 23, no. 9, p. 4346, Apr. 2023, doi: 10.3390/s23094346.

[28] D. Pasquini, D. Francati, and G. Ateniese, "Eluding Secure Aggregation in Federated Learning via Model Inconsistency," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* , Nov. 2022, p. 2429. doi: 10.1145/3548606.3560557.

[29] D. Froelicher *et al.* , "Truly privacy-preserving federated analytics for precision medicine with multiparty homomorphic encryption," *Nature Communications* , vol. 12, no. 1, p. 5910, Oct. 2021, doi: 10.1038/s41467-021-25972-y.

[30] K. Bonawitz *et al.* , "Practical Secure Aggregation for Privacy-Preserving Machine Learning," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* , Oct. 2017, p. 1175. doi: 10.1145/3133956.3133982.

[31] S. Biswas *et al.* , "Low-Cost Privacy-Preserving Decentralized Learning," *Proceedings on Privacy Enhancing Technologies* , vol. 2025, no. 3, p. 451, May 2025, doi: 10.56553/popets-2025-0108.

[32] Y. Rahulamathavan, C. Herath, J. Liu, S. Lambotharan, and C. Maple, "FheFL: Fully Homomorphic Encryption Friendly Privacy-Preserving Federated Learning with Byzantine Users," *arXiv (Cornell University)* , Jun. 2023, doi: 10.48550/arxiv.2306.05112.

[33] S. Jiang *et al.* , "Towards compute-efficient Byzantine-robust federated learning with fully homomorphic encryption," *Nature Machine Intelligence* , vol. 7, no. 10, p. 1657, Sep. 2025, doi: 10.1038/s42256-025-01107-6.

[34] K. Mathur, E. Sharma, and N. Gaur, "Sustainable plant disease protection using machine learning and deep learning," in *Elsevier eBooks* , Elsevier BV, 2024, p. 81. doi: 10.1016/b978-0-443-24139-0.00008-4.

[35] L. Koli, S. Kalra, R. N. Thakur, A. Saifi, and K. Singh, "AI-Driven IRM: Transforming insider risk management with adaptive scoring and LLM-based threat detection," *arXiv (Cornell University)* , May 2025, doi: 10.48550/arxiv.2505.03796.

[36] S. Kumar, "Big Data-Driven Security Information And Event Management (SIEM) Enhanced By AI," p. 720, Nov. 2024, doi: 10.53555/kuey.v30i10.9642.

[37] Y. Schwartz, L. Ben-Shimol, D. Mimran, Y. Elovici, and A. Shabtai, "LLMCloudHunter: Harnessing LLMs for Automated Extraction of Detection Rules from Cloud-Based CTI," p. 1922, Apr. 2025, doi: 10.1145/3696410.3714798.

[38] V. Dakić, Z. Morić, A. Kapulica, and D. Regvart, "Leveraging Microsoft sentinel and logic apps for automated cyber threat response," *Edelweiss Applied Science and Technology* , vol. 8, no. 6, p. 4319, Nov. 2024, doi: 10.55214/25768484.v8i6.2933.

[39] H. Xu, K. Niu, T. Lu, and S. Li, "Leveraging artificial intelligence for enhanced risk management in financial services: Current applications and future prospects," *Fair East Publishers* , vol. 5, Art. no. 8, Aug. 2024, doi: 10.51594/estj.v5i8.1363.

[40] A. Tom, A. Khraisat, T. Jan, M. Whaiduzzaman, T. D. Nguyen, and A. Alazab, "Survey of Federated Learning for Cyber Threat Intelligence in Industrial IoT: Techniques, Applications and Deployment Models," *Future Internet* , vol. 17, no. 9, p. 409, Sep. 2025, doi: 10.3390/fi17090409.

[41] Y. Wang and X. Yang, "Design and implementation of a distributed security threat detection system integrating federated learning and multimodal LLM," 2025, doi: 10.48550/ARXIV.2502.17763.

[42] M. Khule, D. Motwani, and D. Chauhan, "A layered and integrative framework for Advance Persistent Threat detection and mitigation: combining AI, Zero-Trust, and Advanced Threat Intelligence," *Cluster Computing* , vol. 28, no. 11, Sep. 2025, doi: 10.1007/s10586-025-05561-0.

[43] C. Gowdham, "Deep Learning Architectures for Automated Threat Detection and Mitigation in Modern Cyber Security Systems," *Journal of Information Systems Engineering & Management* , vol. 10, p. 347, Feb. 2025, doi: 10.52783/jisem.v10i10s.1399.

[44] M. H. Farouk, R. H. Sakr, and N. A. Hikal, "Identifying the most accurate machine learning classification technique to detect network threats," *Neural Computing and Applications* , vol. 36, no. 16, p. 8977, Mar. 2024, doi: 10.1007/s00521-024-09562-9.

[45] M. Knodel *et al.* , "How To Think About End-To-End Encryption and AI: Training, Processing, Disclosure, and Consent," *arXiv (Cornell University)* , Dec. 2024, doi: 10.48550/arxiv.2412.20231.

[46] P. Roy, J. Chandrasekaran, E. Lanus, L. Freeman, and J. Werner, "A Survey of Data Security: Practices from Cybersecurity and Challenges of Machine Learning," *arXiv (Cornell University)* , Jan. 2023, doi: 10.48550/arxiv.2310.04513.

[47] D. M. Jimenez-Gutierrez, Y. Falkouskaya, J. L. Hernández-Ramos, A. Anagnostopoulos, I. Chatzigiannakis, and A. Vitaletti, "On the Security and Privacy of Federated Learning: A Survey with Attacks, Defenses, Frameworks, Applications, and Future Directions," *arXiv (Cornell University)* , Aug. 2025, doi: 10.48550/arxiv.2508.13730.

[48] K. R. Rao, A. Nayak, I. G. Ray, Y. Rahulamathavan, and M. Rajarajan, "Role recommender-RBAC: Optimizing user-role assignments in RBAC," *Computer Communications* , vol. 166, p. 140, Dec. 2020, doi: 10.1016/j.comcom.2020.12.006.

[49] M. Hummer, M. Kunz, M. Netter, L. Fuchs, and G. Pernul, "Adaptive identity and access management—contextual data based policies," *EURASIP Journal on Information Security* , vol. 2016, no. 1, Aug. 2016, doi: 10.1186/s13635-016-0043-2.

[50] S. R. Kandula, N. Kassetty, K. S. Alang, and P. Pandey, "Context-Aware Multi-Factor Authentication in Zero Trust Architecture: Enhancing Security Through Adaptive Authentication," *International Journal of Global Innovations and Solutions (IJGIS)* , Dec. 2024, doi: 10.21428/e90189c8.f525ef41.

[51] B. Austin-Gabriel, N. Y. Hussain, A. B. Ige, P. A. Adepoju, O. O. Amoo, and A. I. Afolabi, "Advancing zero trust architecture with AI and data science for enterprise cybersecurity frameworks," *Open Access Research Journal of Engineering and Technology* , vol. 1, no. 1, p. 47, Jun. 2021, doi: 10.53022/oarjet.2021.1.1.0107.

[52] G. Nguyen, Š. Dlugolinský, V. Tran, and Á. L. García, "Network security AIOps for online stream data monitoring," *Neural Computing and Applications* , vol. 36, no. 24, p. 14925, May 2024, doi: 10.1007/s00521-024-09863-z.

[53] S. M. Bartram, J. Branke, and M. Motahari, "Artificial Intelligence in Asset Management," *SSRN Electronic Journal* , Jan. 2020, doi: 10.2139/ssrn.3692805.

[54] A. Shafahi *et al.* , "Poison Frogs! Targeted Clean-Label Poisoning Attacks on Neural Networks," *arXiv (Cornell University)* , vol. 31, p. 6103, Jul. 2019, doi: 10.3929/ethz-b-000460348.

[55] Y. Wang, X. Ma, J. Bailey, J. Yi, B. Zhou, and Q. Gu, "On the Convergence and Robustness of Adversarial Training," *arXiv (Cornell University)* , Dec. 2021, doi: 10.48550/arxiv.2112.08304.

[56] I. Shumailov *et al.* , "Trusted Machine Learning Models Unlock Private Inference for Problems Currently Infeasible with Cryptography," *arXiv (Cornell University)* , Jan. 2025, doi: 10.48550/arxiv.2501.08970.

[57] K. Bonawitz *et al.* , "Practical Secure Aggregation for Federated Learning on User-Held Data," *arXiv (Cornell University)* , Jan. 2016, doi: 10.48550/arxiv.1611.04482.

[58] Z. Maasaoui, M. Merzouki, A. Battou, and A. Lbath, "A Scalable Framework for Real-Time Network Security Traffic Analysis and Attack Detection Using Machine and Deep Learning," *Platforms* , vol. 3, no. 2, p. 7, Apr. 2025, doi: 10.3390/platforms3020007.

[59] S. S. Gill *et al.* , "Edge AI: A Taxonomy, Systematic Review and Future Directions," *Cluster Computing* , vol. 28, no. 1, Oct. 2024, doi: 10.1007/s10586-024-04686-y.

[60] A. Parthasarathy and B. Krishnamachari, "DEFER: Distributed Edge Inference for Deep Neural Networks," p. 749, Jan. 2022, doi: 10.1109/comsnets53615.2022.9668515.

[61] E. Toch *et al.* , "The Privacy Implications of Cyber Security Systems," *ACM Computing Surveys* , vol. 51, no. 2. Association for Computing Machinery, p. 1, Feb. 20, 2018. doi: 10.1145/3172869.

[62] S.-U.-R. Sahito *et al.* , "Explainable AI (XAI) for Security Decisions to Mitigate Cybersecurity Attacks," *Journal of Advanced Research in Applied Sciences and Engineering Technology* , vol. 55, no. 2, p. 214, Aug. 2025, doi: 10.37934/araset.55.2.214223.

[63] S. Patil *et al.* , "Explainable Artificial Intelligence for Intrusion Detection System," *Electronics* , vol. 11, no. 19, p. 3079, Sep. 2022, doi: 10.3390/electronics11193079.

[64] J. Oloyede, "Leveraging Artificial Intelligence for Advanced Cybersecurity Threat Detection and Prevention," *SSRN Electronic Journal* , Jan. 2024, doi: 10.2139/ssrn.4976072.

[65] G. Ali, S. Shah, and M. ElAffendi, "Enhancing cybersecurity incident response: AI-driven optimization for strengthened advanced persistent threat detection," *Results in Engineering* , vol. 25, p. 104078, Jan. 2025, doi: 10.1016/j.rineng.2025.104078.

[66] S. Arefin, "Strengthening Healthcare Data Security with Ai-Powered Threat Detection," *International Journal of Scientific Research and Management (IJSRM)* , vol. 12, no. 10, p. 1477, Oct. 2024, doi: 10.18535/ijsrm/v12i10.ec02.

[67] D. Hitaj, G. Pagnotta, F. D. Gaspari, L. D. Carli, and L. V. Mancini, "Minerva: A File-Based Ransomware Detector," *arXiv (Cornell University)* , Jan. 2023, doi: 10.48550/arxiv.2301.11050.

[68] J. Bono, J. Grana, and A. Xu, "Generative AI and Security Operations Center Productivity: Evidence from Live Operations," *arXiv (Cornell University)* , Nov. 2024, doi: 10.48550/arxiv.2411.03116.

[69] N. Rastogi, S. Pant, D. Dhanuka, A. Saxena, and P. Mairal, "Too Much to Trust? Measuring the Security and Cognitive Impacts of Explainability in AI-Driven SOCs," 2025, doi: 10.48550/ARXIV.2503.02065.

[70] G. Agarwal, "Explainable AI (XAI) for Cyber Defense: Enhancing Transparency and Trust in AI-Driven Security Solutions," *International Journal of Advanced Research in Science Communication and Technology* , p. 132, Mar. 2025, doi: 10.48175/ijarsct-23624.

[71] G. Alagic, "Status report on the fourth round of the NIST post-quantum cryptography standardization process," Oct. 2024. doi: 10.6028/nist.ir.8545.

[72] A. Scrivano, "A Comparative Study of Classical and Post-Quantum Cryptographic Algorithms in the Era of Quantum Computing," Jul. 2025, doi: 10.31224/4750.

[73] W. Beullens *et al.* , "Post-Quantum Cryptography: Current state and quantum mitigation," *Data Archiving and Networked Services (DANS)* , Feb. 2021, doi: 10.2824/92307.

[74] M. Malatji, "Augmented Intelligence Framework for Human–Artificial Intelligence Teaming in Cybersecurity," *Human-Centric Intelligent Systems* , vol. 5, no. 2, p. 151, Jun. 2025, doi: 10.1007/s44230-025-00103-8.

[75] S. Shah and F. K. Parast, "AI-Driven Cyber Threat Intelligence Automation," *arXiv (Cornell University)* , Oct. 2024, doi: 10.48550/arxiv.2410.20287.

[76] K. Amin, J. Gillenwater, M. Joseph, A. Kulesza, and S. Vassilvitskii, "Plume: Differential Privacy at Scale," *arXiv (Cornell University)* , Jan. 2022, doi: 10.48550/arxiv.2201.11603.