Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 3, 2026

A STRUCTURED LITERATURE REVIEW OF CLOUD-NATIVE AI-BASED CYBER PROTECTION AND DIGITAL FORENSICS FOR MILITARY RADAR INFRASTRUCTURE

Sikandar Hayat[*1], Abdul Moiz[2], Abdul Rehman Chishti[3]

[*1,2,3]*Department of Information & Communication Engineering, The Islamia University of Bahawalpur Bahawalpur, Pakistan*

[*1]sh363525@gmail.com, [2]moiz13494@gmail.com, [3]rehman.chishti@iub.edu.pk

DOI: https://doi.org/10.5281/zenodo.23664598

Keywords
Cloud-native security, artificial intelligence, cyber protection, digital forensics, military radar systems, electronic warfare, Zero Trust architecture

Article History
Received: 19 January 2026
Accepted: 04 March 2026
Published: 18 March 2026

Copyright @Author
Corresponding Author: *
Sikandar Hayat

Abstract
Cloud-native technologies, distributed communication systems, and artificial intelligence (AI) are increasingly considered for military radar infrastructure, but they introduce cybersecurity and forensic risks in the defense missions where they would be deployed. This paper presents a structured narrative review of recent work on AI-based cyber protection and digital forensics for military radar systems in a cloud-computing context. It examines cloud-native security architectures, including DevSecOps and Zero Trust; AI-driven cyber defense; digital forensics in cloud environments; and electronic warfare (EW) threats to radar. The reviewed studies explore anomaly detection, predictive threat analysis, automated response, and cyber situational awareness in distributed systems, but their performance in operational military radar environments is unverified. Most address cloud security, threat intelligence, or forensics in isolation, and few address integrated solutions. We organize the threats discussed in the literature by the layer they target, compare representative studies and approach classes against explicit qualitative criteria, map relevant civilian standards, identify five research gaps, and outline an illustrative conceptual architecture with evaluation considerations. No experimental evaluation was performed, and findings are extrapolated from enterprise, maritime, and civilian sources rather than validated for military radar.

I. INTRODUCTION
Military radar systems underpin surveillance, target tracking, missile guidance, threat identification, and electronic warfare (EW) operations [1], [2]. Their sensing and processing chains were traditionally closed, purpose-built, and physically isolated. Defense organizations are now considering cloud-based applications, decentralized communication networks, and artificial intelligence (AI) for operational capability [3], [4]. In enterprise settings these technologies provide scalability, operational flexibility, adaptive resource management, and real-time analytics [5], [6]; whether corresponding benefits carry over to military radar ecosystems still requires evaluation. Cloud-native infrastructures also introduce additional cyber risks to military systems [7], [8].

Potential threats to radar infrastructure include advanced persistent threats (APTs), radar spoofing, ransomware, false data injection attacks (FDIA), communication interception, and EW attacks. The radar studies cited here address signal manipulation and false data injection [2], [9]. Perimeter-based security models are poorly matched to the

interdependent, dispersed digital architectures of present-day defense environments [7], [10]. Containers simplify deployment [11], orchestration platforms descended from large-scale cluster managers automate it [12], and microservices and DevSecOps pipelines improve adaptability and scalability [13]–[15]. Intelligent cybersecurity systems support anomaly detection, predictive threat analysis, malware identification, and automated response [16], [17]. Digital forensics contributes to cyber resilience through evidence preservation, incident reconstruction, malware analysis, and attack attribution [18]–[20].

Adaptive cybersecurity frameworks are therefore of growing interest for military environments. Distributed defense systems risk operational disruption and information manipulation through cyber operations and EW [2], and wartime forensic practice additionally involves legal and institutional coordination [21]. AI is widely investigated for threat detection, anomaly classification, behavioral analysis, and predictive cyber intelligence [16], [17], [22], although its use in security settings raises concerns about adversarial manipulation and explainability [23], [24].

An important caveat shapes the whole review. The radar evidence examined here includes maritime and civilian systems [1], [25], and the cyber-protection and forensic evidence is largely enterprise-oriented. Application to military radar is therefore an extrapolation rather than direct operational validation. Section VIII-A and Fig. 2 outline a conceptual integrated architecture, and Section VIII-B and Fig. 3 give an illustrative working flow.

The contributions of this review are: (i) a structured qualitative synthesis across four interrelated domains (cloud-native security, AI-driven cyber defense, cloud digital forensics, and EW protection); (ii) a layered organization of the threats discussed in the literature (Fig. 1); (iii) qualitative comparisons of representative studies and approach classes against explicit criteria (Tables III and IV); (iv) a mapping of relevant civilian and defense-adjacent standards and guidance (Table I); (v) identification of five research gaps; and (vi) an illustrative architecture and working flow with design principles and evaluation considerations for future work (Table V).

The remainder of the paper is organized as follows. Section II gives background and a layered view of threats, Section III describes the scope and approach of the review, Section IV reviews the literature, Section V compares the reviewed approaches, Section VI discusses forensics and EW together, Section VII states the research gaps, Section VIII outlines future directions, Section IX states the limitations of this review, and Section X concludes.

II. Background

A. Cloud-Native Architectures in Defense Contexts

Distributed cloud-native architectures are being considered for mission-critical operations in modern military ecosystems [3], [4]. The standard definition of cloud computing emphasizes on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service, delivered through infrastructure, platform, or software service models [6]. Edge computing, Kubernetes orchestration, virtualized workloads, and serverless systems may support adaptive resource management and distributed intelligence processing within radar environments [5], [15], [26]. Moving computation toward the edge is particularly relevant to radar, where latency and bandwidth constraints make it impractical to ship all raw returns to a central facility [26].

These architectures may bring flexible deployment, quick resource provisioning, and interoperable communication to the military sector [7], [14]. Their adoption nonetheless raises concerns about orchestration vulnerabilities, insecure APIs, supply-chain attacks, and identity-management weaknesses [8], [27]. Container-specific risks span images, registries, orchestrators, container runtimes, and host operating systems [28], and microservice architectures enlarge the attack surface through numerous service-to-service interfaces [14], [29].

B. AI for Cyber Defense

AI has been investigated for next-generation cybersecurity tasks such as anomaly detection, predictive threat analysis, malware classification, and orchestration of automated responses [16], [30]. Machine learning techniques such as Random Forest and Support Vector Machines

are used for intrusion detection and behavioral analysis in cloud-based infrastructures [17], [31], and broader surveys catalog data-mining and machine-learning methods for intrusion detection [22] and for anomaly detection in general [32]. Deep models have been applied to system logs [33] and to online network traffic analysis [34]. AI-powered Security Information and Event Management (SIEM) solutions can support visibility and real-time cyber situational awareness (CSA) in distributed infrastructures [35].

Caution is warranted when moving from laboratory results to operations. Sommer and Paxson argue that intrusion detection differs from many machine-learning applications because the cost of errors is high, the semantic gap between an anomaly and an actual attack is wide, and traffic is highly diverse [36]. These observations remain relevant to any proposal to deploy learned detectors in a radar network.

C. Digital Forensics Fundamentals

Digital forensics supports resilience by preserving evidence, reconstructing incidents, investigating malware, and attributing attacks [18], [19]. Forensic practice is commonly described as a sequence of collection, examination, analysis, and reporting, and is closely tied to incident handling, whose lifecycle covers preparation, detection and analysis, containment, eradication, recovery, and post-incident activity [20], [37]. Cloud forensics extends this practice to settings in which evidence is distributed, shared with a provider, and subject to organizational, technical, and legal constraints [38]. Acquiring evidence from infrastructure-as-a-service environments, for instance, depends on trust in the provider and on the available acquisition techniques [39].

Cloud-native infrastructures create further forensic challenges because evidence can reside in short-lived containers, virtualized infrastructure, and multi-cloud deployments [18]. Automated telemetry monitoring, centralized logging, and AI-aided forensic tools are therefore important for investigations in distributed cloud systems [17], [18].

D. Radar and Electronic Warfare Threat Landscape

Radar systems transmit and receive electromagnetic energy to detect and track targets, and their performance depends on signal processing chains whose assumptions an adversary can attack [40], [41]. EW is conventionally divided into electronic attack, electronic protection, and electronic support, and covers deceptive and noise jamming as well as signal exploitation [42]. EW can manipulate radar signals, disrupt communication links, and degrade target-tracking accuracy [1], [2]. Research examines AI-based adaptive detection and signal analysis for radar spoofing, jamming, and electromagnetic interference [2]; this does not establish the performance of an integrated cloud-native military-radar system. Analogous signal-spoofing research in satellite navigation shows that attack feasibility depends on specific signal and receiver properties [43], which cautions against assuming that findings for one signal-layer system transfer directly to another.

Networked radar adds a cyber dimension to these signal-level concerns. Simulation-based analysis of radar networks identifies cyber risks to the data and communication layer [9], and studies of maritime radar demonstrate attacks and defenses on a deployed civilian radar system [1], [25].

E. A Layered View of Threats

For the purposes of this review, the threats discussed in the literature can be organized by the layer they target (Fig. 1). At the signal layer, spoofing, jamming, and electromagnetic interference act on the sensing function of the radar [1], [2], [9]. At the data and communication layer, false data injection and interception can corrupt or expose radar tracks and command traffic [2], [9]. At the cloud and platform layer, orchestration weaknesses, insecure APIs, container escape, privilege escalation, and supply-chain compromise affect the infrastructure that hosts analytics and control functions [8], [27]. APTs and ransomware can span several layers.

Layer	Representative threats	Principal defenses	Evidence
Signal	Spoofing, jamming, electromagnetic interference	Signal analysis, adaptive EW countermeasures	RF/IQ captures, spectrum logs
Data and comm.	False data injection, interception, track tampering	Encryption, mutual authentication, anomaly detection	Network and track-data logs
Cloud and platform	Insecure APIs, container escape, supply-chain attack	DevSecOps, container hardening, Zero Trust access	Container, API, orchestrator logs
Cross-layer	Advanced persistent threats, ransomware	Zero Trust, SIEM/ SOAR, response playbooks	Correlated multi-source timeline

Fig. 1. Layered organization of threats, principal defenses, and forensic evidence sources used in this review. The layering is an organizing device of the authors, not a taxonomy validated in the cited works, and it implies no ranking, prevalence, or study counts.

This layered view helps explain why defenses designed for a single layer can leave the others exposed. A signal-processing countermeasure does not protect a container registry, and a Zero Trust access policy does not detect a spoofed return. It also shows that the evidence needed to investigate an incident differs by layer: radio-frequency captures at the signal layer, network and track logs at the data layer, and container, API, and orchestrator logs at the platform layer. Reconstructing a cross-layer incident requires correlating all three.

III. Scope and Approach of the Review

This article is a structured narrative review rather than a systematic review. The literature was drawn from IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, and Google Scholar. Studies were selected for relevance to at least one of five themes (cloud-native security, AI-driven cybersecurity, digital forensics, EW resilience, and Zero Trust defense) and are discussed under those themes. Foundational works and official standards documents were added where they define concepts that the recent studies rely on. Because the search was not exhaustive and screening counts were not retained, the synthesis supports qualitative research directions and does not support claims of comprehensive coverage or of how common any topic is in the literature.

Three features of the evidence base affect how it should be read. First, the reviewed sources vary in venue visibility, and several are recent publications whose influence is not yet established; findings from them are reported as claims of those works rather than as settled results. Second, most cyber-protection and

forensic sources concern enterprise or general cloud settings. Third, the radar sources include maritime and civilian systems. Statements about military radar are therefore framed as extrapolations throughout.

IV. Literature Review

A. Cloud-Native Security Architectures

The literature indicates that cloud-native infrastructures improve scalability, operational flexibility, distributed intelligence processing, and adaptive resource management [5], [7]. Kubernetes orchestration, Docker containers, microservices, and serverless computing may support dynamic mission environments [14], [15], [44]. Surveys of cloud-native security catalog threats and countermeasures across these layers [7], [45].

Orchestration vulnerabilities, insecure APIs, container escape, privilege escalation, and supply-chain attacks are major concerns [8], [27]. An empirical study of open-source Kubernetes manifests found security misconfigurations to be a recurring problem [27], and container-focused surveys classify exploits, attacks, and defenses across the container lifecycle [8]. Official guidance recommends hardening images, registries, orchestrators, and runtimes [28], and microservice-specific guidance addresses authentication, authorization, and service communication [29]. Current research also highlights the limitations of perimeter-based defense in distributed settings, with implications for radar systems that rely on interconnected communication networks and cloud services [7], [46].

DevSecOps and Infrastructure as Code (IaC) security research examines automation of vulnerability assessment, runtime monitoring, and continuous compliance to improve resilience in distributed infrastructures [13], [47]. Controls catalogs such as NIST SP 800-53 provide a common vocabulary for access control, audit, and system integrity requirements that such automation must evidence [48]. However, most of the solutions reviewed are enterprise-centric and are not validated in operational radar environments.

B. AI-Driven Cybersecurity

AI is a significant research field in cybersecurity because of its potential to improve automated threat detection, predictive analysis, malware classification, and adaptive response [17]. Studies explore Random Forest, Support Vector Machines (SVM), Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) models for intrusion detection and anomaly analysis [17], [30]. In Kubernetes and cloud settings, AI-assisted threat intelligence and vulnerability management are described as ways to prioritize and automate remediation [16], [49]. Reported detection performance depends on the model, dataset, and evaluation setting [17]; these findings do not establish consistent superiority over rule-based intrusion detection systems (IDSs) or validated performance in military radar environments.

AI-powered SIEM systems and Security Orchestration, Automation, and Response (SOAR) platforms can support automated threat-intelligence correlation and adaptive response orchestration [35]. Challenges remain, including adversarial AI attacks, explainability, model bias, and computational complexity [50]. Adversarial examples (small, deliberately crafted input perturbations that cause confident misclassification) were first described for neural networks [51] and are explained in part by the near-linear behavior of models in high-dimensional spaces [52]. Subsequent work proposed stronger attacks and defenses [53], [54], and surveys of the cyber-security domain show that detectors for malware, intrusions, and similar tasks face analogous attacks [23]. Official taxonomies now organize attacks on machine-learning systems by lifecycle stage and attacker objective [55]. Explainable AI (XAI) is a crucial research area where decisions are mission critical [24], [56]; post-hoc methods such as LIME and SHAP attribute a prediction to input features [57], [58], although whether such attributions meet operator needs in radar settings has not been established.

C. Digital Forensics in Cloud Environments

Digital forensics supports cyberattack investigation, evidence preservation, malware analysis, and operational restoration in distributed systems [18]. Existing research concentrates on cloud forensics, telemetry analysis, automatic evidence collection, RF fingerprinting, and forensic-readiness

mechanisms [18], [19], [59]. AI has been investigated for supporting attack investigation through traffic classification, malware analysis, and anomaly detection [17].

Cloud-native infrastructures pose further challenges because of their distributed nature, dynamic workloads, virtualized resources, and multi-cloud platforms [18]. Early cloud-forensics work already identified evidence acquisition, provider dependence, and jurisdictional questions as central difficulties [38], [39]. Centralized logging, secure data synchronization, and automated telemetry monitoring can support forensic readiness in distributed infrastructure [18]. Cloud-native evidence is also ephemeral: a container that is rescheduled may take its filesystem state with it, so collection must be designed into the platform rather than added after an incident [20], [28]. However, integrated forensic tools geared to military radar domains were not identified in the reviewed literature.

D. Electronic Warfare and Radar Protection

EW is one of the most critical challenges for military radar infrastructure [2]. Studies examine radar spoofing, jamming, signal manipulation, electromagnetic interference, and false data injection [9], [25]. A review of EW against radar systems surveys attack and protection techniques at the signal level [2], while work on maritime radar shows that attacks on a deployed civilian system are practical and that defenses can be designed and evaluated [1], [25]. Deep learning has also been applied to RF-based drone identification [19], and drone-security research addresses related signal-analysis and forensic challenges [59]. These signal-level and drone-forensic findings do not establish the performance of an integrated cloud-native military-radar protection system. Integrating EW protection with cloud cybersecurity and digital forensics remains a research gap.

E. Zero Trust and Autonomous Defense

Zero Trust architecture is a leading security approach for distributed cloud-native applications. Its core premise is that no implicit trust is granted to a user, device, or network location, and that access decisions are made per request by a policy decision point and enforced at a policy enforcement point [10]. An early industrial realization eliminated the privileged internal network in favor of device- and user-based access decisions [60]. Previous research discusses identity-based authentication, least-privilege access control, continuous authentication, and micro-segmentation to restrict unauthorized access and lateral movement [7], [61]. MilTAP addresses authentication and policy enforcement in military VPN networks [62]; its scope does not establish radar EW protection.

Researchers have also investigated autonomous cyber defense for automated threat response, recovery, and adaptive response orchestration [35], [50]. Autonomous SOC platforms and intelligent defense pipelines are intended to improve situational awareness and incident response in distributed infrastructures. Fully autonomous defense remains a challenge in mission-critical military infrastructures, where explainability, adversarial AI threats, and operational trust are additional concerns.

F. Standards and Guidance

A growing body of civilian standards and guidance addresses the building blocks discussed above. Table I lists those referenced in this review and what each covers. None is specific to military radar, and none should be read as certifying that a radar deployment is secure. They are included because they define terminology and controls on which radar-specific work can build, and because the reviewed academic studies rarely map their proposals onto them.

TABLE I
STANDARDS AND GUIDANCE REFERENCED IN THIS REVIEW

Document	Scope	Relevance to military radar (authors' reading)
Zero trust architecture [10]	Tenets, logical components, and deployment models for zero trust	Basis for identity-centric access to radar analytics, control, and data services; not radar-specific
Application container security [28]	Risks and countermeasures for images, registries, orchestrators, runtimes, hosts	Relevant to containerized signal-processing and analytics workloads
Microservices security [29]	Security strategies for microservice-based systems	Relevant to service-to-service authentication and API protection
Security and privacy controls [48]	Control catalog including access control and audit	Common vocabulary for evidencing access, audit, and integrity requirements
Forensic techniques in incident response [20]	Collection, examination, analysis, and reporting	Basis for evidence handling procedures across signal, data, and platform layers
Incident handling [37]	Incident response lifecycle and coordination	Frames how automated response and forensics interact
AI risk management framework [63]	Governance of AI risks across the lifecycle	Relevant to trust, transparency, and oversight of AI-based detectors
Adversarial machine learning taxonomy [55]	Attacks on ML systems and mitigations	Vocabulary for threat-modeling the detection models themselves
Module-lattice key encapsulation [64]	Post-quantum key-establishment standard	Relevant to long-lived radar data and command channels

These documents are civilian or enterprise-oriented. The relevance column is the authors' interpretation and does not indicate that any document has been applied to radar systems.

V. COMPARATIVE ANALYSIS

A survey of the reviewed studies suggests a trend: cybersecurity research in cloud environments has gradually shifted toward more intelligent and autonomous defense architectures. Current approaches address operational visibility, anomaly detection, adaptive response automation, and distributed infrastructure management [16], [50]. However, most solutions were developed for enterprise cloud environments, with military radar ecosystems underserved [7], [13]. AI-based intrusion detection can identify anomalous behavior, but comparisons with signature-based methods depend on the evaluation setting [17], [30], [36]. Research on SIEM, SOAR, and Zero Trust architectures addresses operational visibility and identity-based access control in distributed environments [35], [61]. Partial integrations exist: Farzaan et al. combine AI incident detection, cloud deployment, and forensic support [17]. Nevertheless, integrated operational architectures combining cloud resilience, AI-based cyber defense, forensic readiness, and radar-specific EW protection remain a research gap, which motivates operational cybersecurity models designed specifically for military radar infrastructures.

A common constraint across the literature is limited explainability: intelligent analytical models can enhance threat detection, but many machine-learning systems act as black boxes without revealing how they reach their decisions [50], [56]. Fig. 1 summarizes the threat layers and Table II the criteria and rating scales; Table III compares the coverage of representative works,

and Table IV contrasts approach classes with the capabilities sought in an envisioned integrated framework.

TABLE II
RATING SCALES AND CRITERIA USED IN TABLES III AND IV

Column	Criterion (what a mark denotes)	Used in
AI defense	Degree to which AI is central (High), supporting (Medium), or minimal/absent (Low) in the work	Table III
Cloud-native	Container, microservice, or orchestrated deployment is addressed	Tables III, IV
Real-time detection	Online (streaming) detection or response is addressed	Tables III, IV
Digital forensics	Evidence collection or investigation is addressed	Tables III, IV
Radar/EW protection	Radar or EW threats are addressed	Tables III, IV
Zero Trust	Identity-based, least-privilege access control is addressed	Tables III, IV
Explainability	Explanation or audit of automated decisions is addressed	Table III

Marks: ✓ = explicit substantive coverage; Partial = limited, enabling, or prospective coverage; No = no established coverage in the assessed source. Ratings are the authors' qualitative judgments and are not performance scores.

TABLE III
QUALITATIVE COMPARISON OF REPRESENTATIVE STUDIES

Work	Year	AI defense	Cloud-native	Real-time detection	Digital forensics	Radar/EW protection	Zero Trust	Explain-ability
Aggarwal [16]	2025	High	✓	✓	No	No	Partial	No
Kamadi [49]	2024	High	✓	✓	No	No	No	Partial
Morikawa [47]	2025	High	✓	✓	No	No	Partial	Partial
Longo et al. [1]	2023	Low	No	Partial	No	✓	No	No
Reddy and Sinha [2]	2025	Medium	No	✓	No	✓	No	No
Kampa [15]	2024	Low	✓	Partial	Partial	No	Partial	No
Sihag et al. [59]	2023	Medium	No	Partial	✓	Partial	No	No
Li et al. [19]	2022	High	No	✓	✓	Partial	No	No
Ogundipe [65]	2025	Medium	✓	Partial	No	No	✓	No
Shonubi and Adelere [50]	2025	High	✓	✓	Partial	No	✓	Partial
Balaji [61]	2026	Low	✓	Partial	Partial	No	✓	Partial

Ratings are the authors' qualitative assessments of the topics covered, using the scales in Table II; they are not comparative performance scores. Coverage can be conceptual and does not imply implementation or military-radar validation.

TABLE IV
QUALITATIVE COMPARISON OF CYBERSECURITY APPROACHES

Framework/tool	AI defense	Cloud-native	Digital forensics	Real-time response	Radar/EW protection	Zero Trust
Traditional IDS/IPS	No	No	No	Partial	No	No
SIEM/SOAR platforms	✓	Partial	Partial	✓	No	Partial
Kubernetes security	Partial	✓	No	Partial	No	Partial
DevSecOps pipelines	Partial	✓	No	Partial	No	Partial
AI threat intelligence	✓	Partial	Partial	✓	No	Partial
Digital forensic systems	Partial	Partial	✓	No	No	No
EW defense systems	Partial	No	No	✓	✓	No
Zero Trust architectures	Partial	Partial	No	✓	No	✓
Autonomous SOC platforms	✓	Partial	Partial	✓	No	Partial
Envisioned integrated framework (research gap)	✓	✓	✓	✓	✓	✓

Ratings are the authors' qualitative judgments of illustrative approach classes, not measured performance. ✓ = defining or explicitly addressed capability; Partial = conditional or optional support; No = no capability assumed in this comparison. Capabilities depend on configuration and implementation. The final row is an envisioned research target; its marks indicate desired capabilities, not an implemented or evaluated system.

Reading the tables together, several patterns appear within the authors' qualitative ratings. In Table III, the works rated as having high AI-defense coverage together with explicit cloud-native and real-time detection coverage [16], [47], [49], [50] are not rated as addressing radar/EW protection, whereas the works with explicit radar/EW coverage [1], [2] are not rated as cloud-native. Only two works [19], [59] receive an explicit check mark for digital forensics; both are rated as only partially addressing radar/EW protection, and neither is rated as cloud-native. In Table IV, the approach classes with AI-based capability (SIEM/SOAR platforms, AI threat intelligence, and autonomous SOC platforms) are rated as not covering radar/EW protection, and EW defense systems are rated as not covering cloud-native deployment or digital forensics. Only the envisioned integrated framework is marked across all six capabilities, and it is a research target rather than an existing system. These patterns reflect the ratings and criteria stated in the table notes and should not be read as performance rankings.

VI. DIGITAL FORENSICS AND ELECTRONIC WARFARE

Sections IV-C and IV-D treat cloud forensics and EW separately; this section considers how the two relate. Forensic capabilities support incident response by collecting evidence, analyzing malware, reconstructing events, and supporting recovery [18], [37]. In cloud-native systems, the evidence discussed in the forensic literature consists mainly of logs, telemetry, containers, and virtualized or multi-cloud workloads [18]. In contrast, the EW studies reviewed concentrate on signal-level threats to radar and communication systems, such as spoofing, jamming, false data injection, and electromagnetic interference [2], [9], [25].

RF-based forensic identification has been demonstrated for drones [19], and drone-security research addresses related signal-analysis and forensic challenges [59], but these works do not establish performance in operational military radar environments. In the reviewed literature, therefore, signal-layer evidence and cloud-layer evidence are treated in separate bodies of work. Practical consequences follow. An incident that begins with a spoofed return and ends with tampered tracks in a cloud

database would leave traces in RF captures, network logs, and orchestrator records, yet no reviewed work describes how those traces would be preserved with consistent time references and chain of custody, or correlated into a single timeline. A significant research gap remains in integrating EW protection with cloud-native cybersecurity and digital forensics.

VII. Research Gaps

The existing literature indicates that military radar protection and cloud-based security face several key challenges that have yet to be addressed.

1) Lack of integrated frameworks. Most existing studies focus on a single aspect, such as cloud security, intrusion detection, or AI-based anomaly detection, and do not treat these as parts of an integrated ecosystem [5], [35]. Approaches combining cloud-native resilience, AI-powered cyber defense, forensic readiness, and EW protection for military radar remain scarce in the reviewed literature [61], [66].

2) Limited explainability and operational transparency. AI-driven systems can improve detection accuracy, but they often lack transparency about how decisions are reached [24], [50]. This could reduce operator confidence in mission-critical environments, where analytical decisions must be interrogated and validated.

3) Vulnerability to adversarial AI. The susceptibility of AI-powered cybersecurity systems to adversarial attack is insufficiently addressed in relation to military radar. Adversarially constructed inputs can cause models to produce false outcomes, reduce detection accuracy, and affect automated response mechanisms [23], [50], [52]. The general attack literature concerns mostly image and traffic classifiers [53], [54]; how it transfers to radar-signal and radar-network detectors is an open question.

4) Immature forensic readiness for distributed military environments. Forensic readiness is still emerging, owing to the dynamic orchestration of distributed environments and the difficulty of preserving evidence and reconstructing attacks [18], [39].

5) Disconnection between EW and cloud cybersecurity architectures. A major gap remains in incorporating EW resilience into cloud-based cybersecurity architectures for military radar. Radar-signal protection research does not by itself establish integration with cloud architectures and digital forensic systems [2]. This should be a focus of future research to develop integrated cybersecurity models that support adaptive defense across the entire distributed radar system.

VIII. Future Directions

Future military radar systems will require cybersecurity architectures that do more than detect and react to known threats. They will have to detect emerging threats, adapt rapidly, collect forensic information continuously, and defend against advanced EW [2], [50]. Developing intelligent defense systems that operate across distributed cloud-native environments with appropriate human oversight remains a research priority. Directions include explainable AI, federated defense intelligence, AI-assisted forensic automation, Zero Trust radar ecosystems, autonomous SOC platforms, quantum-resistant security mechanisms, and intelligent edge-based defense architectures [7], [50].

Among these, explainable AI is particularly relevant to mission-critical decisions [24]. Federated learning may support distributed cyber defense without centralizing raw training data [67], although its privacy and security guarantees require evaluation in military settings [50], [68]. Edge-based security systems may support real-time threat assessment and resilience under the low-latency requirements of military operations [26]. Quantum-resistant mechanisms are relevant because radar data and command channels can have long confidentiality lifetimes, and standardized post-quantum key establishment now exists [64]. Governance frameworks for AI risk offer a structure for documenting these trade-offs [63]. Future research should investigate integrating cloud-native security, cyber defense, digital forensics, and EW protection into a single operational framework capable of meeting the resilience requirements of next-generation radar systems.

A. Illustrative Conceptual Architecture

Fig. 2 presents an illustrative conceptual architecture for such an integrated system. It is

not an implemented or evaluated framework and does not demonstrate performance, security, or suitability for military deployment. Its purpose is to show where cyber protection and forensic functions could sit alongside detection in a single workflow.

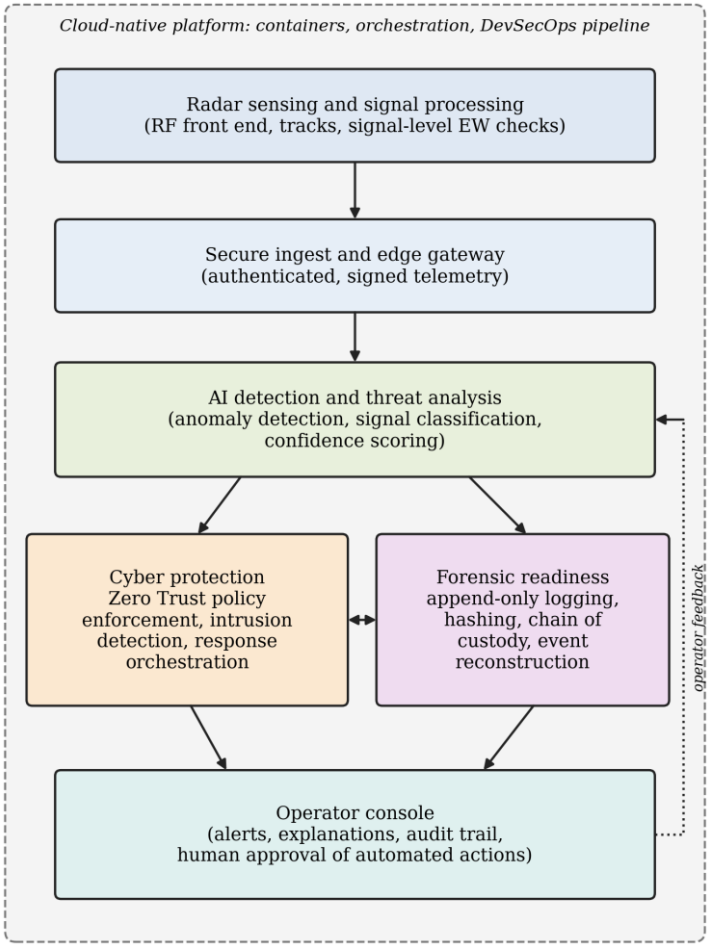


Fig. 2. Illustrative conceptual architecture for an integrated military-radar protection system.

Radar returns and tracks enter from the sensing and signal-processing stage, where signal-level EW checks run close to the sensor. Data then pass through a secure ingest and edge gateway that authenticates sources and signs telemetry, consistent with Zero Trust principles [10]. An AI detection and threat-analysis stage classifies signals and objects and attributes confidence scores; single-pass real-time detectors such as YOLO [69] illustrate the class of model that could be used for object-level detection, though the literature reviewed here does not validate any specific model for military radar. Downstream, a cyber-protection stage enforces access policy, runs intrusion detection, and orchestrates responses, while a forensic-readiness stage keeps append-only logs, hashes evidence, and maintains chain of custody [20]. Both feed an operator console that presents alerts with explanations and requires human approval of consequential automated actions; operator feedback returns to the detection stage. The whole workflow runs on a cloud-native platform with a DevSecOps pipeline [13], [29].

B. Illustrative Working Flow

Fig. 3 gives a complementary, application-level view of the same idea as a ten-stage working flow. It is an illustrative workflow sketch produced by the authors; YOLOv8, Node.js, Express, and MongoDB appear only as example component choices, and the flow has not been implemented, evaluated, or validated for military radar. Where Fig. 2 organizes functions by security role, Fig. 3 follows a request through a concrete web-based system.

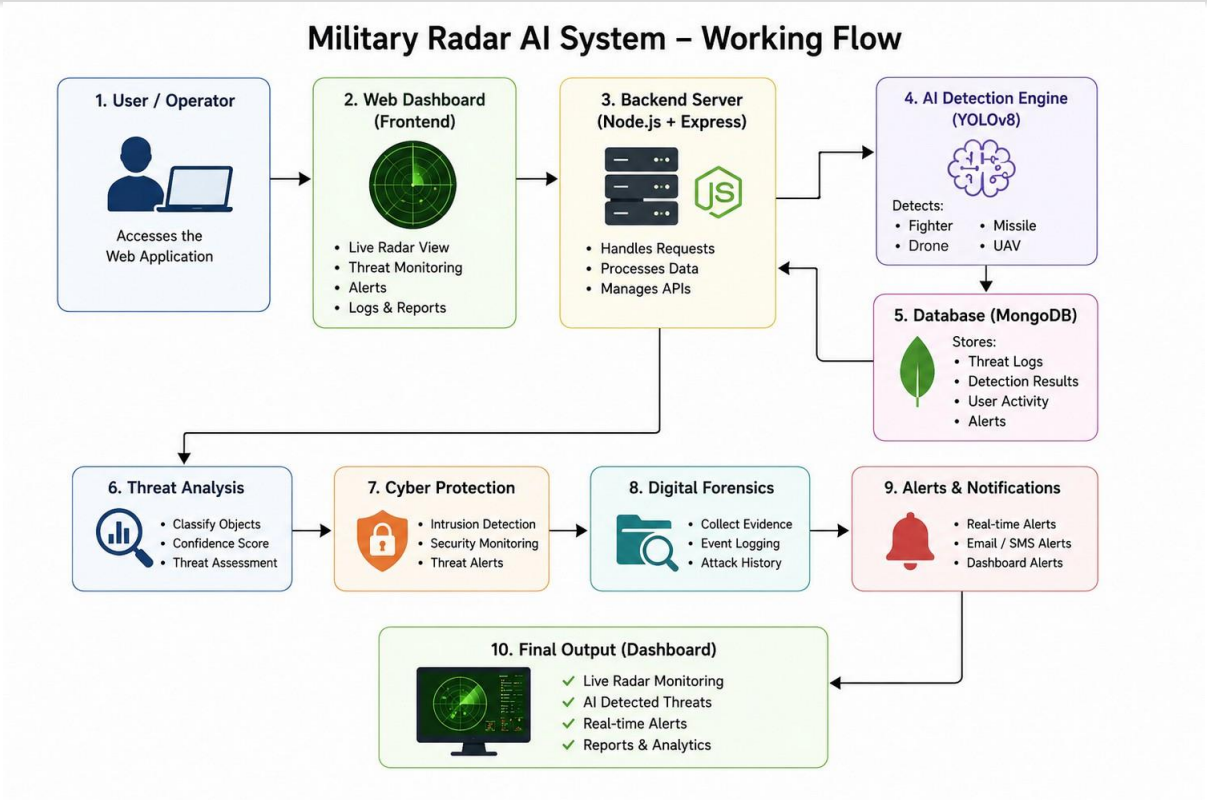


Fig. 3. Illustrative working flow of a military-radar AI system, from operator access to dashboard output. YOLOv8, Node.js, Express, and MongoDB are example component choices only.

The flow proceeds as follows. (1) An operator accesses the web application. (2) A web dashboard provides live radar view, threat monitoring, alerts, and logs and reports. (3) A backend server handles requests, processes data, and manages application programming interfaces. (4) An AI detection engine classifies objects of interest such as fighters, missiles, drones, and unmanned aerial vehicles; real-time single-pass detectors such as YOLO [69] are an example of this model class. (5) A database stores threat logs, detection results, user activity, and alerts. (6) Threat analysis performs object classification, confidence scoring, and threat assessment. (7) Cyber protection performs intrusion detection, security monitoring, and threat alerting. (8) Digital forensics collects evidence, logs events, and keeps attack history. (9) Alerts and notifications are delivered in real time and through email, SMS, and the dashboard. (10) The final output presents live radar monitoring, AI-detected threats, real-time alerts, and reports and analytics.

Read against the gaps identified in this review, the flow shows where integration could occur and also where it is incomplete. Cyber protection and forensics sit downstream of detection, which is the arrangement the reviewed enterprise literature most often assumes [17], [35]. The flow does not by itself address signal-layer threats such as spoofing or jamming [2], protection of the detection model against adversarial inputs [23], [55], explanation of detections to operators [24], or tamper-evident preservation of evidence with chain of custody [20]. Several choices that are reasonable for an enterprise web application, such as a single backend server and a general-purpose database, would need to be revisited for contested military networks, where availability, access control, and auditability are central [10], [48]. These omissions are the reason Section VII frames integration as an open problem rather than a solved engineering task.

Two practical observations follow. First, an object-level detector trained on one sensing modality does not establish performance on radar returns, which differ from optical imagery in structure and noise [40], [41]; any such model would need radar-specific data and evaluation [1], [9]. Second, because logs, alerts, and user activity are concentrated in one database, that store becomes both a forensic asset and a high-value target, which argues for append-only,

integrity-protected logging and strict access control around it [20], [28].

C. Design Principles

The gaps identified above suggest design principles for future integrated systems. These are derived from the literature reviewed rather than validated in deployment.

- Assume no implicit trust: authenticate and authorize every request between sensors, services, and operators [10].
- Design forensic readiness in from the start: centralized, tamper-evident logging and secure time synchronization across signal, data, and platform layers [18], [20].
- Treat the detection models as attack targets: include adversarial testing and monitoring of model inputs in the threat model [23], [55].
- Keep humans in the loop: automated actions with significant operational consequences should require operator approval, supported by explanations and an audit trail [24], [63].
- Harden the platform: apply container and microservice security guidance and secure the build pipeline [13], [28], [29].
- Place computation deliberately: use edge processing where latency or bandwidth demands it, and account for the larger attack surface this creates [26].

D. Evaluation Considerations

Evaluating integrated frameworks of this kind will require more than detection accuracy. Based on the gaps identified, the following considerations appear necessary for future studies. First, evaluation should use realistic radar-relevant data or testbeds, since the reviewed cyber studies are mostly enterprise-centric and the radar studies mostly signal-level [1], [9]. Second, metrics should cover detection and false-alarm behavior, response latency under real-time constraints, completeness and integrity of preserved forensic evidence, and the quality of explanations given to operators (Table V). Third, adversarial robustness should be tested explicitly, including attacks on the detection models themselves [50], [54]. Fourth, evaluation should respect the base-rate and cost-of-error issues that make intrusion detection hard to assess [36]. Finally, human oversight and auditability should be treated as requirements rather than optional features, because operational trust depends on operators being able to validate automated decisions [50].

IEER
Institute for Excellence in Education & Research

TABLE V EVALUATION DIMENSIONS FOR FUTURE INTEGRATED FRAMEWORKS

Dimension	Example measures	Rationale
Detection quality	Detection rate, false-alarm rate, precision and recall per threat class	Costs of missed and false detections differ sharply in operations
Timeliness	Detection latency, time to contain, end-to-end response latency	Real-time constraints at the radar and network edge
Forensic quality	Evidence completeness, integrity verification (e.g., hash checks), timeline consistency across layers	Cross-layer incidents need correlated, trustworthy evidence
Explanation quality	Fidelity of explanations to model behavior; operator-judged usefulness	Operators must be able to validate automated decisions
Adversarial robustness	Performance under defined perturbation budgets and attacker knowledge assumptions	Detection models are themselves attack targets
Resilience	Service availability and degraded-mode behavior under combined cyber and EW stress	Integrated attacks may span layers
Governance	Auditability of automated actions; documentation of model limits	Supports operational trust and accountability

The dimensions are proposed by the authors from the gaps identified in this review. They are suggestions for future work, not an established benchmark, and no values are reported.

IX. Limitations

This review has several limitations. The search was not exhaustive and screening counts were not retained, so the synthesis cannot support claims about the prevalence of topics in the literature or the completeness of coverage. The reviewed sources come from journals and venues of varying visibility, and several are recent publications whose impact is not yet established. Most cyber-protection and forensic sources concern enterprise or general cloud settings, and the radar sources include maritime and civilian systems [1], [25]; findings are therefore extrapolated to military radar infrastructure rather than validated for it. The comparative ratings in Tables III and IV are qualitative judgments by the authors against stated criteria, and a different set of criteria or raters could yield different ratings. Finally, no experimental evaluation was performed, and the conceptual architecture in Fig. 2 is illustrative only. The conclusions are therefore best read as a map of research directions and open problems.

X. Conclusion

This review examined the current state of AI-based cyber protection and digital forensics for military radar infrastructure. It mapped four interrelated security domains: cloud-based architectures, AI-based security systems, digital forensic systems, and EW [2], [7]. The literature examines intelligent cybersecurity solutions for anomaly detection, threat prediction, automated response, and situational awareness in distributed systems [16], [17], [50]; their performance in operational military radar environments remains unverified. Kubernetes orchestration, DevSecOps pipelines, SIEM, SOAR, and Zero Trust architectures are discussed in the reviewed literature as components of cyber defense postures [13], [15], [35], [61]. Establishing true integration of cloud-based resilience, AI-based cyber defense, forensic readiness, and EW protection in military radar systems remains an open problem [66].

Other areas requiring further research include explainability, adversarial robustness, forensic readiness, and operational trust. Future work should focus on explainable and auditable analytical systems, autonomous cyber defense architectures, federated defense intelligence networks, and AI-assisted forensic automation, evaluated on radar-relevant testbeds against the dimensions proposed here. The objective is to develop systems that military operators can understand, trust, and rely on during critical operations.

References

[1] G. Longo, E. Russo, A. Armando, and A. Merlo, "Attacking (and defending) the maritime radar system," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 3575–3589, 2023, doi: 10.1109/TIFS.2023.3282132.

[2] R. Reddy and S. Sinha, "State-of-the-art review: Electronic warfare against radar systems," *IEEE Access*, vol. 13, pp. 57530–57567, 2025, doi: 10.1109/ACCESS.2025.3555493.

[3] I. Kolawole, "Advancing U.S. national security with cloud computing: Strengthening intelligence, cyber resilience, and homeland defense strategies," *Int. J. Eng. Technol. Res. Manage.*, vol. 9, no. 2, pp. 316–334, 2025, doi: 10.5281/zenodo.14937982.

[4] M. A. Rangel, "Military breaking boundaries: Implementing third-party cloud computing practices for data storage," Ph.D. dissertation, Walden Univ., Minneapolis, MN, USA, 2021. [Online]. Available: https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=12392&context=dissertations

[5] A. Mamun and M. J. I. Saidur, "Cloud-native frameworks for real-time threat detection and data security in enterprise networks," *Int. J. Sci. Interdiscip. Res.*, vol. 2, no. 2, pp. 34–62, 2021, doi: 10.63125/0t27av85.

[6] P. Mell and T. Grance, "The NIST definition of cloud computing," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST Spec. Publ. 800-145, Sep. 2011, doi: 10.6028/NIST.SP.800-145.

[7] T. Theodoropoulos et al., "Security in cloud-native services: A survey," *J. Cybersecur. Privacy*, vol. 3, no. 4, pp. 758–793, 2023, doi: 10.3390/jcp3040034.

[8] O. Jarkas, R. Ko, N. Dong, and R. Mahmud, "A container security survey: Exploits, attacks, and defenses," *ACM Comput. Surv.*, vol. 57, no. 7, pp. 1–36, 2025, Art. no. 170, doi: 10.1145/3715001.

[9] R. Chen, Y. Zhang, X. Li, and J. Ran, "An analysis and simulation of security risks in radar networks from the perspective of cybersecurity," *Sensors*, vol. 25, no. 17, 2025, Art. no. 5239, doi: 10.3390/s25175239.

[10] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST Spec. Publ. 800-207, Aug. 2020, doi: 10.6028/NIST.SP.800-207.

[11] D. Merkel, "Docker: Lightweight Linux containers for consistent development and deployment," *Linux J.*, vol. 2014, no. 239, Art. no. 2, Mar. 2014.

[12] B. Burns, B. Grant, D. Oppenheimer, E. Brewer, and J. Wilkes, "Borg, Omega, and Kubernetes," *ACM Queue*, vol. 14, no. 1, pp. 70–93, 2016, doi: 10.1145/2890784.

[13] R. Manchana, "DevSecOps in cloud native cybersecurity: Shifting left for early security, securing right with continuous protection," *Int. J. Sci. Res.*, vol. 13, no. 8, pp. 1374–1382, 2024, doi: 10.21275/SR24822104530.

[14] D. Berardi, S. Giallorenzo, J. Mauro, A. Melis, F. Montesi, and M. Prandini, "Microservice security: A systematic literature review," *PeerJ Comput. Sci.*, vol. 8, 2022, Art. no. e779, doi: 10.7717/peerj-cs.779.

[15] S. Kampa, "Navigating the landscape of Kubernetes security threats and challenges," *J. Knowl. Learn. Sci. Technol.*, vol. 3, no. 4, pp. 274–281, 2024, doi: 10.60087/jklst.v3.n4.p274.

[16] A. Aggarwal, "Adoption of AI-powered threat intelligence in cloud infrastructures for real-time risk mitigation and automated anomaly detection through predictive security analytics," *J. Digit. Secur. Forensics*, vol. 2, no. 1, pp. 139–150, 2025, doi: 10.29121/digisecforensics.v2.i1.2025.87.

[17] M. A. M. Farzaan, M. C. Ghanem, A. El-Hajjar, and D. N. Ratnayake, "AI-powered system for an efficient and effective cyber incidents detection and response in cloud environments," *IEEE Trans. Mach. Learn. Commun. Netw.*, vol. 3, pp. 623–643, 2025, doi: 10.1109/TMLCN.2025.3564912.

[18] A. W. Malik, D. S. Bhatti, T.-J. Park, H. U. Ishtiaq, J.-C. Ryou, and K.-I. Kim, "Cloud digital forensics: Beyond tools, techniques, and challenges," *Sensors*, vol. 24, no. 2, 2024, Art. no. 433, doi: 10.3390/s24020433.

[19] Z. Li et al., "Reliable digital forensics in the air: Exploring an RF-based drone identification system," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 6, no. 2, pp. 1–25, 2022, Art. no. 63, doi: 10.1145/3534598.

[20] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST Spec. Publ. 800-86, Aug. 2006, doi: 10.6028/NIST.SP.800-86.

[21] V. Yatskiv, M. Kasianchuk, L. Babala, and S. Kulyna, "Digital forensics and cyber threat management during wartime: Analysis of new legislative initiatives," in *Proc. Cyber Security and Data Protection (CSDP)*, CEUR Workshop Proc., vol. 4042, 2025, pp. 216–225. [Online]. Available: https://ceur-ws.org/Vol-4042/paper17.pdf

[22] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1153–1176, 2nd Quart. 2016, doi: 10.1109/COMST.2015.2494502.

[23] I. Rosenberg, A. Shabtai, Y. Elovici, and L. Rokach, "Adversarial machine learning attacks and defense methods in the cyber security domain," *ACM Comput. Surv.*, vol. 54, no. 5, Art. no. 108, 2021, doi: 10.1145/3453158.

[24] A. B. Arrieta et al., "Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI," *Inf. Fusion*, vol. 58, pp. 82–115, 2020, doi: 10.1016/j.inffus.2019.12.012.

[25] F. Basels, K. Wolsing, E. Padilla, and J. Bauer, "Demo: Maritime radar systems under attack. Help is on the way!" in *Proc. IEEE 49th Conf. Local Comput. Netw. (LCN)*, 2024, pp. 1–4.

[26] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, Oct. 2016, doi: 10.1109/JIOT.2016.2579198.

[27] A. Rahman, S. I. Shamim, D. B. Bose, and R. Pandita, "Security misconfigurations in open source Kubernetes manifests: An empirical study," *ACM Trans. Softw. Eng. Methodol.*, vol. 32, no. 4, pp. 1–36, 2023, doi: 10.1145/3579639.

[28] M. Souppaya, J. Morello, and K. Scarfone, "Application container security guide," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST Spec. Publ. 800-190, Sep. 2017, doi: 10.6028/NIST.SP.800-190.

[29] R. Chandramouli, "Security strategies for microservices-based application systems," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST Spec. Publ. 800-204, Aug. 2019, doi: 10.6028/NIST.SP.800-204.

[30] A. K. Bhardwaj, P. K. Dutta, and P. Chintale, "AI-powered anomaly detection for Kubernetes security: A systematic approach to identifying threats," *Babylonian J. Mach. Learn.*, vol. 2024, pp. 142–148, 2024, doi: 10.58496/BJML/2024/014.

[31] H. A. Salman, A. Kalakech, and A. Steiti, "Random forest algorithm overview," *Babylonian J. Mach. Learn.*, vol. 2024, pp. 69–79, 2024, doi: 10.58496/BJML/2024/007.

[32] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, no. 3, Art. no. 15, 2009, doi: 10.1145/1541880.1541882.

[33] M. Du, F. Li, G. Zheng, and V. Srikumar, "DeepLog: Anomaly detection and diagnosis from system logs through deep learning," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2017, pp. 1285–1298, doi: 10.1145/3133956.3134015.

[34] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An ensemble of autoencoders for online network intrusion detection," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, 2018, doi: 10.14722/ndss.2018.23204.

[35] T. O. Oshoba, K. S. Ahmed, and O. D. Odejobi, "Proactive threat intelligence and detection model using cloud-native security tools," *Int. J. Adv. Multidiscip. Res. Stud.*, vol. 3, no. 1, pp. 1481–1490, 2023, doi: 10.62225/2583049X.2023.3.1.5140.

[36] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proc. IEEE Symp. Secur. Privacy (SP)*, 2010, pp. 305–316, doi: 10.1109/SP.2010.25.

[37] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST Spec. Publ. 800-61 Rev. 2, Aug. 2012, doi: 10.6028/NIST.SP.800-61r2.

[38] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics," in *Advances in Digital Forensics VII*, IFIP Adv. Inf. Commun. Technol., vol. 361. Berlin, Germany: Springer, 2011, pp. 35–46, doi: 10.1007/978-3-642-24212-0_3.

[39] J. Dykstra and A. T. Sherman, "Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques," *Digit. Investig.*, vol. 9, pp. S90–S98, 2012, doi: 10.1016/j.diin.2012.05.001.

[40] M. I. Skolnik, *Introduction to Radar Systems*, 3rd ed. New York, NY, USA: McGraw-Hill, 2001.

[41] M. A. Richards, *Fundamentals of Radar Signal Processing*, 2nd ed. New York, NY, USA: McGraw-Hill, 2014.

[42] D. L. Adamy, *EW 101: A First Course in Electronic Warfare*. Norwood, MA, USA: Artech House, 2001.

[43] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," in *Proc. 18th ACM Conf. Comput. Commun. Secur. (CCS)*, 2011, pp. 75–86, doi: 10.1145/2046707.2046719.

[44] T. Alyas et al., "Container performance and vulnerability management for container security using Docker engine," *Secur. Commun. Netw.*, vol. 2022, 2022, Art. no. 6819002, doi: 10.1155/2022/6819002.

[45] T. Arif, B. Jo, and J. H. Park, "A comprehensive survey of privacy-enhancing and trust-centric cloud-native security techniques against cyber threats," *Sensors*, vol. 25, no. 8, 2025, Art. no. 2350, doi: 10.3390/s25082350.

[46] S. A. Oladosu et al., "Next-generation network security: Conceptualizing a unified, AI-powered security architecture for cloud-native and on-premise environments," *Int. J. Sci. Technol. Res. Archive*, vol. 3, no. 2, pp. 270–280, 2022, doi: 10.53771/ijstra.2022.3.2.0143.

[47] K. T. Morikawa, "Automated vulnerability governance: Integrating AI-driven risk mitigation and DevSecOps in high-scale cloud infrastructures," *Int. Multidiscip. J. Res. Develop.*, vol. 12, no. 11, pp. 579–587, 2025. [Online]. Available: https://ijmrd.org/index.php/mrdj/article/view/3

[48] Joint Task Force, "Security and privacy controls for information systems and organizations," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST Spec. Publ. 800-53 Rev. 5, Sep. 2020, doi: 10.6028/NIST.SP.800-53r5.

[49] S. Kamadi, "AI-augmented threat intelligence for autonomous vulnerability management in cloud-native clusters," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 10, no. 1, pp. 378–387, 2024, doi: 10.32628/CSEIT2425451.

[50] J. A. Shonubi and M. A. Adelere, "AI-augmented cyber resilience frameworks for predictive threat modeling across software-defined network layers and cloud-native infrastructures," *Int. J. Comput. Appl. Technol. Res.*, vol. 14, no. 7, pp. 45–60, 2025, doi: 10.7753/IJCATR1407.1005.

[51] C. Szegedy et al., "Intriguing properties of neural networks," in *Proc. Int. Conf. Learn. Represent. (ICLR)*, 2014, arXiv:1312.6199.

[52] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," in *Proc. Int. Conf. Learn. Represent. (ICLR)*, 2015, arXiv:1412.6572.

[53] N. Carlini and D. Wagner, "Towards evaluating the robustness of neural networks," in *Proc. IEEE Symp. Secur. Privacy (SP)*, 2017, pp. 39–57, doi: 10.1109/SP.2017.49.

[54] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, "Towards deep learning models resistant to adversarial attacks," in *Proc. Int. Conf. Learn. Represent. (ICLR)*, 2018, arXiv:1706.06083.

[55] A. Vassilev, A. Oprea, A. Fordyce, and H. Anderson, "Adversarial machine learning: A taxonomy and terminology of attacks and mitigations," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST AI 100-2 E2023, Jan. 2024, doi: 10.6028/NIST.AI.100-2e2023.

[56] A. Adadi and M. Berrada, "Peeking inside the black-box: A survey on explainable artificial intelligence (XAI)," *IEEE Access*, vol. 6, pp. 52138–52160, 2018, doi: 10.1109/ACCESS.2018.2870052.

[57] M. T. Ribeiro, S. Singh, and C. Guestrin, "'Why should I trust you?' Explaining the predictions of any classifier," in *Proc. 22nd ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2016, pp. 1135–1144, doi: 10.1145/2939672.2939778.

[58] S. M. Lundberg and S.-I. Lee, "A unified approach to interpreting model predictions," in *Proc. Adv. Neural Inf. Process. Syst. (NeurIPS)*, vol. 30, 2017, pp. 4765–4774.

[59] V. Sihag, G. Choudhary, P. Choudhary, and N. Dragoni, "Cyber4Drone: A systematic review of cyber security and forensics in next-generation drones," *Drones*, vol. 7, no. 7, 2023, Art. no. 430, doi: 10.3390/drones7070430.

[60] R. Ward and B. Beyer, "BeyondCorp: A new approach to enterprise security," *;login:*, vol. 39, no. 6, pp. 6–11, Dec. 2014.

[61] R. Balaji, "Design and evaluation of cloud-native zero-trust networking models for contemporary cybersecurity risks," *J. Emerg. Trends Novel Res.*, vol. 4, no. 1, pp. a52–a65, 2026.

[62] G. Sunkara, K. M. N. Shaik, and C. R. Yeddula, "MilTAP: A tunnel-aware authentication and AI-driven policy enforcement protocol for military VPN networks," *IEEE Access*, vol. 13, pp. 216842–216855, 2025, doi: 10.1109/ACCESS.2025.3643316.

[63] "Artificial intelligence risk management framework (AI RMF 1.0)," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST AI 100-1, Jan. 2023, doi: 10.6028/NIST.AI.100-1.

[64] "Module-lattice-based key-encapsulation mechanism standard," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Fed. Inf. Process. Stand. (FIPS) 203, Aug. 2024, doi: 10.6028/NIST.FIPS.203.

[65] A. O. Ogundipe, "Advancing U.S. leadership in cloud-based infrastructure and serverless architecture for real-time data analytics," *Int. J. Sci. Archit. Technol. Environ.*, vol. 2, no. 7, pp. 309–330, 2025, doi: 10.63680/ijsate0625043.

[66] M. Maqbool et al., "Integrated cyber defense strategies for the modern digital ecosystem: Evaluating zero trust models, AI-driven threat intelligence, and secure cloud architecture for resilient infrastructure protection," *J. Manage. Sci. Res. Rev.*, vol. 5, no. 1, pp. 28–43, 2026, doi: 10.5281/zenodo.18207381.

[67] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. 20th Int. Conf. Artif. Intell. Statist. (AISTATS)*, PMLR vol. 54, 2017, pp. 1273–1282.

[68] P. Kairouz et al., "Advances and open problems in federated learning," *Found. Trends Mach. Learn.*, vol. 14, no. 1–2, pp. 1–210, 2021, doi: 10.1561/2200000083.

[69] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You only look once: Unified, real-time object detection," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, 2016, pp. 779–788, doi: 10.1109/CVPR.2016.91.

IEER
Institute for Excellence in Education & Research