IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940



International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026

DOI: 10.17148/IJARCCE.2026.151062

A Review of AI-Driven Cyber Emergency Response Systems: Edge Intelligence, Digital Cyber First Aid, and Human-Centric Cybersecurity

Devendra Singh Kushwaha[1], Uday Payghon[2], Manjushree Dighe[3], Riya Pagar[4], Anushka Shinde[5]

Department of Computer Engineering, Sandip Institute of Technology and Research Centre (SITRC), Nashik, Maharashtra, India[1,2,3,4,5]

Abstract: In the area of cyber security research, many advances have been made in the areas of automated threat detection, malware analysis, phishing identification, anomaly detection, and cyber threat intelligence. However, detection capability alone does not ensure effective assistance to the victims during active cyber incidents. This review explores the intersection of Artificial Intelligence (AI), Edge Intelligence, digital incident response, Digital Cyber First Aid, multilingual natural language processing and human-centric cyber security. The literature is organized around the cyber-incident life cycle and in particular in terms of latency, privacy, explainability, accessibility, evidence preservation, incident reporting, and oversight by humans. The review reveals a persistent fragmentation problem, i.e., many existing approaches are optimizing an individual task, while relatively few approaches connect detection, triage, immediate user guidance, structured reporting, stakeholder coordination, recovery, and post-incident learning. Based on this synthesis, an integrated reference architecture is proposed that places privacy-preserving edge triage at the user boundary and connects it to AI-assisted threat intelligence, Digital Cyber First Aid, multilingual interaction, secure case management, and authority-aware coordination. A risk-oriented evaluation framework is also defined to assess response time, triage quality, privacy, usability, accessibility, evidence integrity, and resilience. The proposed architecture is presented as a research framework rather than as an experimentally validated product; consequently, quantitative performance claims are not made. The review concludes that future cyber emergency systems should move from detection-centric automation toward trustworthy, human-in-the-loop, lifecycle-aware response ecosystems.

Keywords: Artificial intelligence, cyber emergency response, edge intelligence, digital cyber first aid, human-centric cyber security, multilingual NLP, incident response, cyber resilience, threat intelligence.

I. INTRODUCTION

The fast paced digitization of financial services, e-governance, healthcare, education, social networking, cloud computing, online commerce and mobile applications has changed the way individuals and organizations interact with digital systems. While these technologies offer significant benefits in terms of accessibility, efficiency and connectivity, they have at the same time increased the cyber-attack surface and the possibility of security incidents. Today's users routinely use web applications, mobile platforms, digital payment systems, cloud services, social media and connected devices across multiple identities and accounts. Thus, a single compromised credential, malicious application, fraudulent transaction, or phishing interaction can potentially spread across multiple interconnected services. Thus, cyber assaults like phishing, ransomware, identity theft, credential compromise, online financial fraud, malicious mobile applications, social engineering, and account takeover are not only a technical security problem but also an immediate operational and human-safety problem [1]–[4], [11]–[14].

The difference between cyber emergencies and traditional cybersecurity events is the urgency of these incidents. In many cases, the time available for an appropriate decision may be minutes rather than hours or days. For example, a victim who receives a fraudulent banking message may need to determine whether the message is legitimate, avoid clicking on the malicious link, secure the associated account, contact the financial institution, preserve relevant evidence, and potentially initiate a transaction-dispute or fraud-reporting process. Similarly, a ransomware incident might involve rapidly isolating an affected device or network segment before more systems are affected. In an account takeover scenario, the attacker may not be able to exploit the compromised identity further until passwords are changed, active sessions are revoked, stronger authentication is enabled, and recovery mechanisms are verified. But average users often do not have the technical knowledge, situational awareness and coordinated support needed to properly execute these

 This work is licensed under a Creative Commons Attribution 4.0 International License



International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026
DOI: 10.17148/IJARCCE.2026.151062

actions under time pressure. Thus, the success of a cyber-emergency response is not only dependent on detection of malicious activity but also on timely, understandable, trustworthy and context-aware guidance to the affected individual.

Recent advances in Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL), Natural Language Processing (NLP), transformer-based language models, multimodal learning and Edge Intelligence have significantly improved the capability of the cybersecurity systems to process huge amounts of heterogeneous data and detect potentially malicious behavior [5]–[10], [17], [18]. AI-based techniques have been applied to phishing detection, malware classification, intrusion detection, anomaly detection, fraud detection, malicious URL detection, user-behavior analysis, threat intelligence, and automatic security monitoring . Deep neural networks can detect complicated patterns in network traffic and system telemetry; transformer-based models can evaluate textual and semantic information in emails, messages, websites, incident reports, and security logs. Edge intelligence allows certain AI capabilities to be placed closer to users and data sources, potentially reducing latency, bandwidth requirements and reliance on centralized cloud infrastructure.

Still, a good share of existing research is still largely detection-oriented. Many studies related to cybersecurity AI focus on whether a system can successfully identify if a URL, application, message, network flow, transaction, file or user behavior is malicious or not. Detection is certainly a critical part of cybersecurity, but identifying a threat is just the first part of the response. When a suspicious activity is identified, the affected user or organization needs to decide what to do next. This is a critical transition from “detecting the problem” to “helping the user respond to the problem.” For example, a detection system that reports a URL as malicious may not provide guidance on whether a user should close the browser, change credentials, revoke sessions, contact a service provider, monitor financial accounts, preserve evidence, or report the incident. Hence, the detection accuracy itself is not a good measure for the practical effectiveness of a cyber-emergency response system. [25]-[27]

This distinction motivates the idea of Digital Cyber First Aid, in which AI-enabled systems deliver instant, structured and risk-aware assistance after a cyber-incident. Physical first aid is about what can be done to limit damage until a full investigation or professional intervention can take place. So too, digital cyber first aid is about taking immediate action. Depending on the incident, this assistance may include disconnecting an affected device from a network, blocking a malicious application, changing compromised credentials, enabling multi-factor authentication, terminating suspicious sessions, contacting a financial institution, preserving screenshots and transaction records, reporting fraudulent activity, or escalating the case to an appropriate cybersecurity authority. However, such recommendations need to be sensitive to context, as inappropriate action can sometimes destroy evidence, increase financial loss, or cause further disruption. Therefore, an AI-enabled cyber emergency assistant should not only provide generic security advice but also provide prioritized recommendations based on the severity, confidence, context, and potential consequences of the detected incident.[26], [27]

Another big problem is that cyber emergencies are human in nature. Existing security tools are often designed for security professionals and assume knowledge of terms such as indicators of compromise, attack vectors, malware families, authentication tokens, endpoint telemetry and network-level containment. But these concepts may not be familiar to common users. An emergency that is overloaded with technical information increases confusion and cognitive load and can lead to delayed or incorrect decisions. Therefore, artificial intelligence systems must be able to reduce complex security assessments into short, actionable and understandable instructions. This is especially true in multilingual and heterogeneous user environments where language skills, digital literacy levels, accessibility needs and cultural context can impact the understanding and following of cybersecurity instructions.

The growing availability of large language models (LLMs) opens up new opportunities for this human-facing layer of cyber emergency response. LLM-based systems can interpret natural-language descriptions of incidents, summarize technical findings, generate step-by-step instructions, explain security warnings, assist with reporting, and support conversational interaction. Multimodal AI could also give systems the ability to analyze screenshots, suspicious messages, documents, URLs, application interfaces and other types of evidence. However, these capabilities also bring significant challenges such as hallucination, overconfident recommendations, prompt injection, adversarial manipulation, privacy leakage, model bias, insufficient explainability and the potential to generate unsafe or inappropriate security instructions. Thus, the cyber emergency guidance driven by AI must be restricted through security policies, confidence estimation, verification mechanisms, human supervision, and well-defined escalation paths.

Another key consideration is where the AI processing is architecturally located. Cloud-centric cybersecurity platforms can offer significant computational resources and centralized threat intelligence; however, sending sensitive user data to remote infrastructure can raise privacy, latency, connectivity, and data-sovereignty concerns. Edge



International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026
DOI: 10.17148/IJARCCE.2026.151062

Intelligence provides an alternative that allows some detection, classification and decision support functions to be performed locally on smartphones, personal computers, routers, gateways and other edge devices. Local processing can also cut response latency, and cut the transmission of sensitive information. However, edge devices are usually resource-limited, energy-constrained, and may have weaker security controls than centralized infrastructure. Thus, an effective cyber emergency architecture needs to strike a proper balance between the local intelligence and the cloud-based analysis, rather than blindly considering edge or cloud processing to be superior in all cases.

Cyber incident response is also changing from a narrowly defined incident handling activity to a broader, risk-informed and lifecycle-oriented cybersecurity capability. The NIST Cybersecurity Framework (CSF) 2.0 provides a high-level framework for managing cybersecurity risk across organizational contexts, while NIST SP 800-61 Rev. 3, published in 2025, supersedes Rev. 2 and aligns incident response more closely with CSF 2.0. Therefore, contemporary research on AI-enabled cyber emergency response should not treat the 2012 incident-handling guidance as the primary baseline. Instead, AI capabilities should be considered in relation to the broader lifecycle of cybersecurity risk management, including preparation, detection, response, recovery, continuous improvement, and organizational governance [1], [4].

In this context, this paper reviews AI-driven cyber security capabilities from a cyber-emergency perspective and synthesizes them into an integrated human-centric reference architecture. The paper contributes three things: (1) a lifecycle-oriented taxonomy of relevant technologies, (2) a comparative analysis of capability gaps in detection, edge processing, first aid, reporting, multilingual assistance and coordination, and (3) a conceptual architecture and evaluation framework for future cyber emergency response systems.

II. REVIEW SCOPE AND ANALYTICAL METHODOLOGY

The method used in this paper is a structured narrative review. The analysis is organized by capability, not by individual algorithm: threat detection, edge intelligence, incident response, digital forensics/evidence handling, multilingual NLP, human-centric security, cyber resilience, and integrated response. Sources of the review include standards, peer-reviewed journal papers, and conference papers and related scholarly works. The synthesis emphasizes whether a study supports detection, triage, user assistance, evidence preservation, reporting, coordination, privacy, explainability, or lifecycle continuity.

One limitation of this review is that the present manuscript does not report on a reproducible database query, screening count, duplicate removal process or PRISMA-style flow. This paper therefore makes no claim to be a systematic literature review or meta-analysis. This terminology should be used in a conference submission unless the authors do a formal systematic search and document it afterward.

III. LITERATURE REVIEW

A. AI-powered threat detection

ML and DL have been well established as approaches for phishing detection, malware classification, intrusion detection and anomaly analysis [5]–[8], [11]–[14]. Transformer models are also capable of semantic analysis of messages and multilingual communication [8], [17], [18]. Their main strength is scalable pattern recognition. Their limitation for emergency response is that a high-confidence detection does not automatically determine the safest action for a non-expert user.

B. Edge Intelligence & Privacy

Edge Intelligence reduces communication latency and minimizes the sensitive content transferred to the centralized infrastructure by moving the computation closer to the source of the data [9], [10]. For cyber emergency applications, preliminary triage of URL, QR-code, application or message can be done using local analysis. Edge models, however, are challenged by resource constraints, model-update difficulties, adversarial manipulation, heterogeneous hardware, and the fact that decisions made locally alone may lack the larger context that can be provided by centralized threat intelligence.

C. Incident Response and Cyber Forensics

Detection is not the full story of incident response. This includes analysis, containment, recovery and documentation and lessons learned. The incident-response reference used today is NIST SP 800-61 Rev. 3 , which supersedes Rev. 2 [4]. Digital forensic research has focused on standardization of the acquisition, preservation, examination, and reporting



International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026
DOI: 10.17148/IJARCCE.2026.151062

processes [16]. These requirements mean that an AI emergency assistant needs to maintain provenance and integrity, not just deliver conversational advice.

D. Multilingual and Human-Centered Assistance

Multilingual NLP can improve accessibility for users who are not comfortable interacting with cyber security services in English [17, 18]. Human-centric cyber security also requires human-understandable explanations, calibrated confidence, usable interfaces, human escalation, and protections against overreliance on automated recommendations. Such requirements are especially important where advice may affect financial accounts, identity credentials or evidence that may be used in an investigation later.

E. RESEARCH GAP

The central gap is architectural rather than purely algorithmic. Existing studies frequently optimize a single task such as phishing classification, malware detection, fraud detection, threat intelligence, or incident reporting while fewer approaches connect these capabilities into a continuous user-centered workflow. A recent 2026 review of AI-based reactive cybersecurity systems further demonstrates the importance of comparing AI-driven reaction mechanisms, countermeasure selection, and lifecycle integration [26]. The present paper therefore focuses on the underexplored intersection of AI response automation with citizen-facing cyber first aid, privacy-preserving edge triage, multilingual assistance, and coordinated reporting.

TABLE I
COMPARATIVE ANALYSIS OF REPRESENTATIVE LITERATURE

Ref.	Research focus	Major contribution	Key limitation
[5]-[8]	AI / phishing / ML security	Automated classification and pattern recognition	Often task-specific; limited user-facing response
[9], [10]	Edge Intelligence	Low-latency, localized processing	Resource constraints; limited incident-workflow integration
[11]-[14]	Malware, phishing, intrusion, cognitive security	Threat identification and analysis	Detection-centric evaluation
[16]	Digital forensics	Evidence-oriented investigation workflow	Limited AI-assisted citizen triage
[17], [18]	NLP / multilingual language models	Semantic and cross-lingual representation	Standalone language capability; safety and governance remain open
[22]	Cyber resilience	Lifecycle and resilience perspective	Broad framework; not a citizen cyber-first-aid architecture
[26]	AI-driven reactive systems	Comparative view of AI reaction/countermeasures	Primarily security reaction; less emphasis on citizen-facing first aid

IV. PROPOSED INTEGRATED REFERENCE ARCHITECTURE

The proposed architecture is a conceptual synthesis of the literature reviewed. It is not described as an implementation validated by experiment. The design separates latency sensitive, privacy-sensitive edge processing from centralized correlation and coordination while preserving a human-in-the-loop control path.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026

DOI: 10.17148/IJARCCE.2026.151062

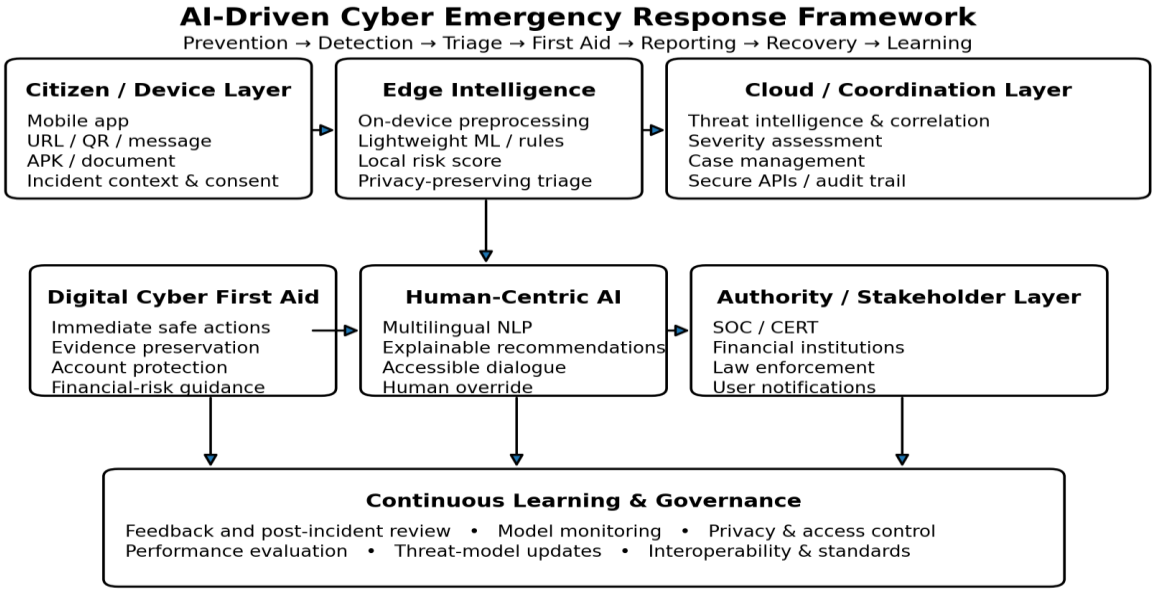


Fig. 1. Proposed AI-driven cyber emergency response architecture.

A. Workflow life cycle

- Input and consent: the user submits suspicious content or incident context and explicitly consents to the relevant processing.
- Edge triage: lightweight local models and deterministic checks perform preliminary analysis and provide a local risk estimate.
- Correlation with threat intelligence: selected indicators are correlated with centralized threat intelligence and contextual information, when permitted.
- Severity and decision support: the system predicts incident severity and provides explainable recommended actions instead of silently taking high impact actions.

- Digital Cyber First Aid: the user receives prioritized containment, account-protection, and evidence-preservation and recovery advice.
- Structured reporting: Incident facts, indicators, timestamps and provenance metadata are transformed into a structured case record.
- Human/authority escalation: cases that meet predefined criteria are routed to appropriate human analysts, service providers, financial institutions, CERT/SOC functions or law-enforcement channels.
- Recovery & learning: Outcomes are logged, user feedback is collected, models are tracked, and lessons learned are used to update policies and threat knowledge.

B. Risk and Severity Formulation

A useful response system would disentangle model confidence from incident severity. A conceptual severity score can combine estimated likelihood, potential impact, exposure and confidence:

$S = w_LL + w_II + w_EE + w_CC,\ \Sigma w_k = 1,\ 0 <= L,I,E,C <= 1$

Where S is the normalized severity score; L is the estimated likelihood; I is the potential effect; E is the exposure or scope; C is the model confidence; and w_L, w_I, w_E, and w_C are application-specific weights. The expression is purposely conceptual: weights should be calibrated from domain evidence and not as validated clinical- or financial-risk thresholds.

C. Trust, Safety, and Privacy Controls

Because emergency recommendations can affect financial or identity decisions, the architecture must support least privilege, explicit consent, secure storage, provenance tracking, audit logging, encryption, model-update integrity, human escalation, and conservative defaults. High-impact operations such as account closure, fund transfer, credential reset or



International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026
DOI: 10.17148/IJARCCE.2026.151062

deletion of evidence should require clear user confirmation or human approval. Explainability should convey what has been detected, why an action is being recommended, and what uncertainty is still present.

V. IMPLEMENTATION AND EVALUATION FRAMEWORK

A prototype can include a cross-platform mobile client, RESTful services, a relational case database, secure authentication, and lightweight edge models. However, the specific technology stack should be considered as a matter of implementation rather than a contribution of the review. An evaluation of a publication quality should compare the integrated workflow to suitable baselines and provide quantitative evidence instead of only qualitative claims.

Dimension	Metric	Evaluation objective	Suggested evidence
Response efficiency	Median time-to-guidance; time-to-escalation	Measure emergency responsiveness	Controlled scenarios / logs
Triage quality	Precision, recall, F1, calibration	Measure threat classification and confidence	Labeled benchmark set
Edge performance	Latency, memory, energy, bandwidth	Quantify local inference cost	Device-level benchmark
Privacy	Data transferred; sensitive fields exposed	Measure data minimization	Privacy audit / traffic analysis
Usability	Task completion; SUS or equivalent	Measure non-expert usability	User study
Accessibility	Language coverage; comprehension	Measure multilingual accessibility	Multilingual user evaluation
Evidence integrity	Provenance completeness; hash consistency	Preserve forensic value	Controlled evidence tests
Safety	Unsafe recommendation rate; human override rate	Assess AI failure consequences	Red-team / safety evaluation
Resilience	Availability; recovery time; degraded-mode success	Assess continuity under disruption	Fault-injection scenarios

VI. CRITICAL LIMITATIONS AND OPEN RESEARCH QUESTIONS

The current manuscript is a conceptual review and architecture synthesis and does not report an experimental implementation, benchmark dataset, user study or statistically validated performance. Do not add such claims unless there is evidence to back them up.

Second, cyber emergency response is multi-agency and multi-jurisdictional. Automation routing must consider legal requirements, consent, data retention, rules of evidence, and organizational boundaries.

Third, the artificial intelligence systems also create the attack surfaces, including prompt injection, adversarial inputs, model poisoning, data leakage, hallucinated recommendations, and unsafe automation. Future work should thus evaluate the response assistant as an attackable security component.

Fourth, translation accuracy cannot solve multilingual assistance alone. Each task requires evaluation of terminology, cultural context, literacy, accessibility and the consequences of mistranslation.

Last but not least, interoperability is a big challenge. Future systems should map incident records and indicators to established standards and machine-readable formats, enabling citizen-facing tools to interoperate with SOC, CERT, financial and law enforcement workflows.

VII. CONCLUSION

This review shows the significant augmentation of cyber threat detection with AI, but additionally emphasizes the need for a broader lifecycle approach for an effective cyber emergency response. Detection, edge triage, Digital Cyber First Aid, evidence preservation, structured reporting, multilingual interaction, human escalation, recovery, and continuous learning are to be seen as connected capabilities, not as stand-alone functions.

The proposed reference architecture provides a research-oriented approach to interconnect these capabilities while maintaining privacy-sensitive edge processing and oversight by humans. The architecture should be evaluated empirically by using response-time, detection/triage, privacy, usability, accessibility, evidence-integrity, safety and resilience metrics. The main research challenge is therefore not only to develop more granular classifiers but also to

DOI: 10.17148/IJARCCE.2026.151062

develop trustworthy systems that translate cyber intelligence into secure, understandable and usable support for the entire lifecycle of an incident.

REFERENCES

[1] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," NIST CSWP 29, Gaithersburg, MD, USA, Feb. 2024, doi: 10.6028/NIST.CSWP.29.

[2] B. Al-Sada, A. Sadighian, and G. Oligeri, "Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database," IEEE Access, vol. 12, pp. 1217-1234, 2024, doi: 10.1109/ACCESS.2023.3344680.

[3] L. Ferrari, F. Pagano, L. Verderame, and A. Merlo, "The OWApp Benchmark: An OWASP-Compliant Vulnerable Android App Dataset," in Proc. 2025 IEEE Eur. Symp. Security Privacy Workshops (EuroS&PW), Venice, Italy, 2025, pp. 569-580, doi: 10.1109/EuroSPW67616.2025.00072.

[4] A. Nelson, S. Rekhi, M. Souppaya, and K. Scarfone, "Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile," NIST SP 800-61 Rev. 3, Gaithersburg, MD, USA, Apr. 2025, doi: 10.6028/NIST.SP.800-61r3.

[5] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436-444, 2015, doi: 10.1038/nature14539.

[6] S. Mahdavifar and A. A. Ghorbani, "Application of Deep Learning to Cybersecurity: A Survey," Neurocomputing, vol. 347, pp. 149-176, 2019, doi: 10.1016/j.neucom.2019.02.056.

[7] G. S. Chhabra et al., "Modelling Deep Learning and Machine Learning Methods in IoT Based Cybersecurity," in Proc. 2024 Int. Conf. Intelligent Innovative Practices Engineering Management (IIPEM), Singapore, 2024, pp. 1-6, doi: 10.1109/IIPEM62726.2024.10925822.

[8] A. A. Kumar, T. P. Imthias Ahamed, and N. A. Shukoor, "Detecting Human-Written and AI-Generated Phishing Emails with DistilBERT and Explainable AI," in Proc. 2025 IEEE 2nd Int. Conf. Women Computing (InCoWoCo), India, 2025, pp. 1-5, doi: 10.1109/InCoWoCo68239.2025.11407086.

[9] Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo, and J. Zhang, "Edge Intelligence: Paving the Last Mile of Artificial Intelligence With Edge Computing," Proc. IEEE, vol. 107, no. 8, pp. 1738-1762, Aug. 2019, doi: 10.1109/JPROC.2019.2918951.

[10] 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.

[11] D. Arp, M. Spreitzenbarth, M. Hübner, H. Gascon, and K. Rieck, "DREBIN: Effective and Explainable Detection of Android Malware in Your Pocket," in Proc. Network and Distributed System Security Symp. (NDSS), San Diego, CA, USA, 2014.

[12] S. Priya, D. Gutema, and S. Singh, "A Comprehensive Survey of Recent Phishing Attacks Detection Techniques," in Proc. 2024 5th Int. Conf. Innovative Trends Information Technology (ICITIIT), Kottayam, India, 2024, pp. 1-6, doi: 10.1109/ICITIIT61487.2024.10580446.

[13] W. Khan et al., "A Comprehensive Survey on Cognitive Cyber Security Analysis Using Machine Learning Approaches," IEEE Access, vol. 13, pp. 169314-169326, 2025, doi: 10.1109/ACCESS.2025.3614388.

[14] S. Çimen, "AI-Driven Network Intrusion Detection Systems: A Survey of Techniques, Datasets and Deployment Challenges," in Proc. 2025 IEEE Int. Conf. Artificial Intelligence Engineering Technology (IICAIET), Kota Kinabalu, Malaysia, 2025, pp. 274-279, doi: 10.1109/IICAIET67254.2025.11265502.

[15] F. Al-Doghman et al., "AI-Enabled Secure Microservices in Edge Computing: Opportunities and Challenges," IEEE Trans. Services Comput., vol. 16, no. 2, pp. 1485-1504, Mar.-Apr. 2023, doi: 10.1109/TSC.2022.3155447.

[16] A. Valjarevic, H. S. Venter, and M. Ingles, "Towards a Prototype for Guidance and Implementation of a Standardized Digital Forensic Investigation Process," in Proc. 2014 Information Security for South Africa (ISSA), Johannesburg, South Africa, 2014, pp. 1-8, doi: 10.1109/ISSA.2014.6950488.

[17] J. Devlin, M. W. Chang, K. Lee, and K. Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," in Proc. NAACL-HLT, Minneapolis, MN, USA, 2019, pp. 4171-4186, doi: 10.18653/v1/N19-1423.

[18] A. Conneau et al., "Unsupervised Cross-lingual Representation Learning at Scale," in Proc. 58th Annu. Meeting Assoc. Computational Linguistics (ACL), 2020, pp. 8440-8451, doi: 10.18653/v1/2020.acl-main.747.

[19] S. M. Alhidaifi, M. R. Asghar, and I. S. Ansari, "A Survey on Cyber Resilience: Key Strategies, Research Challenges, and Future Directions," ACM Comput. Surv., vol. 56, no. 8, Art. no. 196, pp. 1-48, 2024, doi: 10.1145/3649218.

[20] I. Yadav et al., "Artificial Intelligence for Cybersecurity: Emerging Techniques, Challenges, and Future Trends," in Proc. 2025 3rd Int. Conf. Sustainable Computing Data Communication Systems (ICSCDS), Erode, India, 2025, pp. 1176-1180, doi: 10.1109/ICSCDS65426.2025.11167191.



International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026

DOI: 10.17148/IJARCCE.2026.151062

[21] M. Kamruzzaman et al., "Exploring the Landscape: A Systematic Review of Artificial Intelligence Techniques in Cybersecurity," in Proc. 2024 Int. Conf. Communications, Computing, Cybersecurity, and Informatics (CCCI), Beijing, China, 2024, pp. 1-6, doi: 10.1109/CCCI61916.2024.10736474.

[22] S. Raicevic, C. Sriratanaban, and T. Tantiathimongkhon, "AI as Human Amplification in Cybersecurity: An Intelligence-Centered Design Framework for Risk Management," in Proc. 2026 IEEE Int. Conf. Cybernetics Innovations (ICCI), Chonburi, Thailand, 2026, pp. 1-6, doi: 10.1109/ICCI68752.2026.11506452.

[23] J. Mwangi, J. Wall, U. Ismail, and A. Al-Nemrat, "Building a Human-Centric SOC: A New Framework for Success," in Cybersecurity and Human Capabilities Through Symbiotic Artificial Intelligence, Springer, 2025, pp. 537-558, doi: 10.1007/978-3-031-82031-1_27.

[24] S. Ang et al., "AI-Driven Optimization of the Cybersecurity Incident Response Lifecycle: A Review and Framework Based on NIST SP 800-61," in Proc. 2026 2nd Int. Conf. Computational Intelligence Approaches Applications (ICCIAA), Amman, Jordan, 2026, pp. 1-6, doi: 10.1109/ICCIAA68481.2026.11544038.

[25] P. K. Mannepalli, D. Singh Kushwaha, S. Kalamdhar, V. Nagrale and V. Rajpoot, "Face Recognition Based on Cascade Classifier Using Deep Learning," 2023 1st International Conference on Innovations in High Speed Communication and Signal Processing (IHCSP), BHOPAL, India, 2023, pp. 63-68, doi: 10.1109/IHCSP56702.2023.10127172.

[26] P. Nespoli, S. Bernardez Molina, P. Beltrán-López, and F. Gómez Mármol, "Tackling Cyberattacks Through AI-Based Reactive Systems: A Holistic Review and Future Vision," IEEE Commun. Surv. Tutorials, vol. 28, pp. 1557-1596, 2026, doi: 10.1109/COMST.2025.358388.

[27] Ganesh R. Kadam, Narendra U. Jadhav, Md Abdul Wassay, Yash R. Mohabe, Kaushal B. Loharkar, Devendra Singh Kushwaha" Facial Recognition-Based Classroom Attendance System with Real-Time Group Photo Processing Using Machine Learning Approach" Proceedings of International Conference on Computer Science and Communication Engineering (ICCSCE 2025),Atlantis Press, p:1166-1177, doi:10. 2991/978-94-64 63-8 58-5_97