International Journal of Applied Mathematics
Volume 38 No. 8s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

INTELLIGENT CYBERSECURITY FRAMEWORK MACHINE LEARNING-DRIVEN DATA PROTECTION AND THREAT INTELLIGENCE INTEGRATION FOR MODERN DIGITAL COMMUNICATIONS

[1]Farhin Shimu,[2]Omar Faruq,[3]Kazi Sanwarul Azim,[4]Sandipon Chowdhury,[5]Md Shakirul Islam Joy,[6]Sharmin Akter,[7]Shariful Haque,[8]Nur Mohammad,

Department of Communication and Multimedia Studies, Florida Atlantic University, 777 Glades Rd, Boca Raton, FL 33431, USA. Email: fshimu2023@fau.edu, ORCID ID: 0009-0002-9590-547X

College of Business, Westcliff University, 17877 Von Karman Ave, 4th floor, Irvine, CA 92614, USA. Email: o.faruq.123@westcliff.edu, ORCID ID: 0009-0005-8093-0957
Department of Business Administration, International American University, 3440 Wilshire Blvd, Los Angeles, CA 90010, USA. Email: kazisanwarulazim@gmail.com, ORCID ID: 0009-0001-0145-2135
DeVoe School of Business, Technology and Leadership, Indiana Wesleyan University 41-12, 73rd St, Woodside, NY 11377, USA. Email: sandipon.chowdhury@myemail.indwes.edu, ORCID ID: 0009-0004-2588-6247
College of Business, Westcliff University, 17877 Von Karman Ave, 4th Floor, Irvine, CA 92614,USA. Email: m.islam.9094@westcliff.edu, ORCID ID: 0009-0004-9835-6765
School of Business, International American University, 3440 Wilshire Blvd STE 1000, Los Angeles, CA 90010, USA. Email: sharmin.zr@gmail.com, ORCID ID: 0009-0001-1231-3034
Department of Business Administration, International American University, 3440 Wilshire Blvd, Los Angeles, CA 90010, USA. Email: research@sharifulhaque.org, ORCID ID: 0009-0003-0832-5539
College of Technology & Engineering, Westcliff University, 17877 Von Karman Ave, Irvine, CA 92614, USA. Email: n.mohammad.254@westcliff.edu, ORCID ID: 0009-0002-6476-6956
Correspondence: Nur Mohammad

Abstract

Background:
The exponential growth of digital communications, driven by cloud computing, IoT, 5G, and edge technologies, has significantly expanded the cyber-security threat landscape. Traditional rule-based defense mechanisms are increasingly inadequate against sophisticated attacks such as advanced persistent threats (APTs), and polymorphic malware. In response, machine learning (ML) and artificial intelligence (AI) have emerged as transformative tools for

Received: August 02,2025

International Journal of Applied Mathematics
Volume 38 No. 8s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

enhancing cyber-security frameworks, enabling adaptive data protection and real-time threat intelligence integration.

Research Objective:
This study aims to design and evaluate an intelligent cybersecurity framework that leverages machine learning techniques to improve data protection and integrate threat intelligence for securing modern digital communications.

Research Methods:
A review-based methodology was employed, synthesizing literature published between 2012 and 2024. Sources included peer-reviewed journals, government publications (e.g., NIST, CISA), and industry reports. The study applied systematic search strategies using academic databases and threat intelligence platforms. Conclusion:
Findings indicate that ML-driven cyber-security frameworks outperform traditional models in threat detection precision, response latency, and adaptability. Integration of real-time threat intelligence significantly enhances situational awareness and incident response capabilities.

Keywords: Machine Learning Cybersecurity, Threat Intelligence Integration, Data Protection, Digital Communications, United States, AI in Cybersecurity.

Introduction

Cognitive Cyber Defence

The explosive proliferation of digital communication, propelled not only by the advance of 5G infrastructure, cloud-native platforms (e.g. Kubernetes) but also hyper-distributed Internet of Things (IoT) environments, has made traditional perimeter-bound security entirely obsolete. **[1]** The speed, scale and sophistication of coordinated cyber attacks have only increased annually, forcing organizations to rethink their defensive postures and respond with faster and faster modernization. Moreover, traditional security utilization of primarily historical signatures and implicit trust of traffic inside the existing network perimeter oftentimes fails to prepare, respond or defend itself against the current techniques, i.e., zero-day exploits and insider threats, that make understanding the behavior of network and activity critical to detecting and responding to incidents. **[2]** Research supports this strategic paradigm failure by indicating that 75% of companies admit traditional security does not provide protection to the cyber threat vector. For the sake of addressing this strategic specificity, we need to start harnessing the notion of the Intelligent Cybersecurity Framework (ICF). ICF is the shift to an architecture that leverages Machine Learning (ML) and Deep Learning (DL) not simply for detection or inspection but for continuous behavioral modeling of the environments, predictive analytics and automated orchestration of response incidents across multiple solution sets. This framework needs to further operationalize Threat Intelligence (TI) plausibly and seamlessly not as a reactive barrier against threats, but a proactive positioning and adaptive defense. **[3], [4]**

The inherent speed, low latency and distributed nature of 5G and Multi-Access Cloud systems may (4E also) speed up tempo, but there are considerable latency costs associated with centralized checkpoint verifications of the original trust models, identified in principle

Received: August 02,2025

International Journal of Applied Mathematics
Volume 38 No. 8s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

one, when it comes to SOC functions and threat lifecycles. **[1]**, **[5]** Consequently, ICF must utilize continuous low latency verification as an operational principle of supporting intelligence at the point of action, rather than relying on people with an analysis of data relying on the latency of centralized processing.

Zero Trust and Modular Architecture

Two basic design approaches that can be taken to generate a strong ICF come down to:

1) removing implicit trust through Zero Trust Architecture (ZTA), and

2) functional resilience through modular design.

ZTA strategies should be embedded in the ICF framework to enhance performance and security in the concurrent and distributed landscape that is a hallmark of today's digital communications. Fundamental to ZTA is "never trust, always verify," with the underlying pressure that each individual user, device, application, and workload can all act as a risk pathway, irrespective of their location (inside the organization or not). **[6]** Legacy security measures, by contrast, have historically given implicit trust to anything that naturally resides behind the organization perimeter. **[7], [8]**

Table 1: Comparison of Security Models Based on Traditional and ZTA-Based Security Models

Feature	Traditional Perimeter Model	Intelligent Cybersecurity Framework (ICF) / ZTA
Core Trust Model	Implicit Trust inside the perimeter (Trust-on-First-Access).	Never Trust, Always Verify (Continuous Validation).
Primary Controls	Network Firewalls, Spam Filters, Signature Detection.	Behavioral ML/DL, Continuous MFA, Micro-segmentation.
Threat Mitigation Focus	Blocking known threats at the boundary.	Containment, prevention of Lateral Movement, Zero-Day detection.
Fit for Modern Comms (5G/Cloud)	Highly vulnerable/obsolete due to perimeter collapse.	Native fit for cloud, edge, and distributed architectures.

The related threats and related components of ZTA can be explained as:

Ongoing Verification: All access requests are continuously authenticated, authorized, and validated based on every data point and contextual risk score that is available.

Least Privilege: Users and devices have only the most limited access rights for a specific task, which limits what an attacker, who has compromised an endpoint, can do.

Received: August 02,2025

International Journal of Applied Mathematics
Volume 38 No. 8s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Micro-segmentation: The network is segmented into several small, isolated segments and access to resources is limited to specific resources, which significantly reduces the blast radius of a compromise and stops lateral movement from an initial point of compromise. **[9]**

In today's hybrid IT environment, traditional perimeter-based security can experience monumental failures, especially in regard to email security. Examples of email security threats beyond the capabilities of signature-based tools, in the event credentials are compromised, include business email compromise (BEC) and credential theft. **[10], [11]** ZTA-based solutions apply rigid verification of identity, cryptographic confirmation of source, which may involve DMARC, etc., as well as behavioral analysis using machine learning, allows determination of trust in context with dynamic context. Organizations that make a shift to ZTA govern adaptive controls to function from the "Assume Breach" standpoint, where controls are purposefully architect to contain and mitigate exposure in situations where threats have successfully gained access to the environment, thus establishing a better security posture and reduced data breach exposure. **[12], [13]**

Emergence of AI and ML

The field of cybersecurity is being transformed by Artificial Intelligence (AI) and Machine Learning (ML) in a rapidly changing threat landscape. By 'Artificial Intelligence' we mean the machine-based thinking, reasoning, forecasting, and/or decision-making based on available data, which includes, ML-based algorithms for learning from data; recognizing patterns in data; detecting anomalies in data; and taking action autonomously like, blocking a host from the network. **[14]** These characteristics are very important capabilities that bolster speed, resilience, and accuracy of overall cyber defense. ML is a subset of AI that provides the ability for a system to improve its performance from learning new data. In ML-based models you train the model using large sets of historical and real-time data before it makes predictions to effectively 'learn' the difference between expected behavior and anomalous or suspicious behavior; identify differences in behavior not possible for a human to detect; and respond faster than a human could. **[15]** AI-driven models do not inherently rely on the static decision-making behavior of rules-based systems. Because AI-enabled models are cognitive, they have the ability to generalize from previous examples, adapt to changes in the threat landscape, and anticipate course of action based on emerging or active threats. **[9], [11]**

On the other hand, ML-enabled threat intelligence integration allows collection of global threat indicator data and use of associated tactics, techniques, and procedures (TTPs) to generate actionable insights. Although the integration allows security to provide context to their threats, prioritize their threats, and respond in a rational manner across various distributed environments. **[16]**

Equally, ML-enabled data protection techniques such as anomaly detection, behavioral modeling and automated encryption can offer fine-grained control over sensitive information and mitigate insider threats. In this article, we introduce an intelligent cyber-security framework, which utilizes machine learning, and establishes real-time threat intelligence and monitoring for cyber-communications.

Received: August 02,2025

International Journal of Applied Mathematics
Volume 38 No. 8s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Research Objective

The main objective of this research is to evaluate the intelligent cybersecurity design that proposes machine learning (ML) methods for the dynamic protection of information with real-time threat intelligence to enhance safeguards for modern digital communications. This design aims to address some of the limitations of traditional rule-based security systems by providing adaptive, predictive, and autonomous platforms for the detection, assessment, and response to advanced cyber threats in real-time, in contrast to traditional rule-based approaches.

Research Questions

- How can machine learning algorithms be incorporated effectively into cybersecurity ecosystems to achieve real-time protection of data and detection of threats in today's digital communication systems?

- What machine learning methods (e.g., supervised, unsupervised, or reinforcement) would be best for recognizing, detecting, and responding to advanced cyber threats like zero-day attacks, Advanced Persistent Threats (APTs), or polymorphic malware?

- How can globally-sourced real-time threat intelligence be incorporated with machine-learned analytics for enhanced situational awareness and incident response automation?

Research Methodology

Research Design

This present study presents the stature of a review-oriented study and hence follows the exploratory research design. Here the the researcher shall analyze existing knowledge, frameworks, and empirical studies targeted toward machine learning-based cyber-security systems, particularly relative to data protection and threat intelligence integration, in the contemporary context of digital communications in the United States.

Search Strategy

Researcher had tried to search for all the available avenues, though mostly electronic databases were searched but then again for the sake of identification other sources were also searched. Some of the major database touched are as follows:

1. IEEE Xplore, SpringerLink, ScienceDirect,

2. National Institute of Standards and Technology (NIST), Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS)

3. Gartner, McKinsey, IBM X-Force,

4. Recorded Future, CrowdStrike, FireEye, etc.

As far as the references are concerned, the researcher had particularly focused on the genuine references, based on the categories, time and location. Other than this, specific timeline of the relevant studies have been decided in advance i.e. the studies conducted during the period of

Received: August 02,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2010 to 2024. The search criteria included an important condition that all the studies should be published or presented in English.

Area of Study

This research is fundamentally based on the United States because the United States is a leader in cybersecurity innovation, regulatory development, including such areas as NIST, CISA, and ML adaptation in private and public industries. This research context will inform scalable frameworks that mirror policy providing the basis for a global application of best-practice.

Criteria of Inclusion and Exclusion

Criteria	Inclusion	Exclusion
Time Line of Study	Studies conducted from 2010 to 2024	Studies conducted prior to 2010
Location	Mostly U.S. based and some globally relevant studies	Studies based in countries other than U.S.
Area of study	Studies based on AI/ML application in cyber security	Studies lacking the respective keywords
Language	Studies published or presented in English Language	Studies published in languages other than English

Keywords

In order to enhance the sensitivity of search, following keywords were used separated by Boolean operators (AND, OR) and MeSH :

“Machine Learning Cybersecurity,” “Threat Intelligence Integration,” “Data Protection,” “Digital Communications,” “United States,” “Ai In Cybersecurity”

Process of Review

- The PRISMA flow diagram used to stratify the stages of document selection,
- The studies were classified and coded, based on the occurrence of technologies and related concepts, issues and challenges.
- After the above steps, the respective studies were compared on the basis of scale, adaptation, and performance assessment.

Received: August 02,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Ethical Considerations

This is a review study so there are no human subjects. However, ethical integrity is preserved in the following ways:

- Citation and acknowledgement of all sources that are relevant
- Avoiding misrepresentation of findings and plagiarism
- Acknowledgement of norms with respect to privacy of data and intellectual property

Data Management

As the nature of present study is 'systematic Review' hence the researcher managed data by organizing, documenting, and tracking sources of literature and outputs of analytic results in a systematic manner. All articles, reports, and datasets retrieved will be collected and organized using relevant reference manager to maintain a uniform way to cite the work and to have version control. Key variable including year of publication, study design, the machine learning type/ technique and methods of threat intelligence integration (if any) and items regarding relevance to U.S. cybersecurity practice will be documented in a systematic data extraction sheet.

Results

A total of 138 research studies and two research reports were identified, all of them were based on the studies regarding application of AI and ML in cyber security, identification of cyber threat, impact of the same on digital communication in the public and private sector organization in United states. Out of these identified studies, 19 were removed because of duplication of records, references and location and 27 studies were marked as ineligible, as not modern concepts and technologies related to AI and ML in cyber security and the impact on digital communication. Then 11 for some other unavoidable conditions.

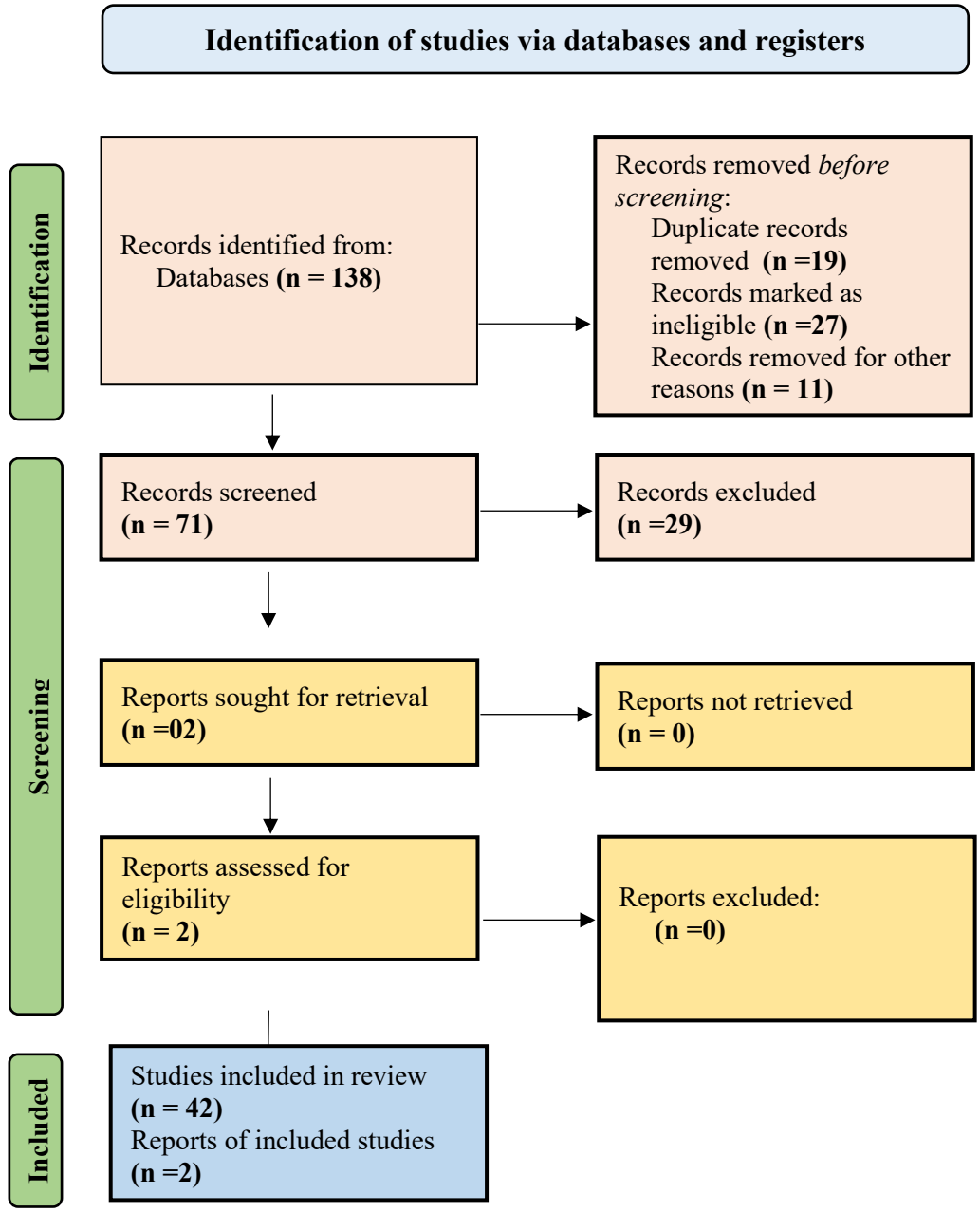
Further 71 records were saved for screening, then in the screening process 29 records were further removed on the basis of exclusion criteria stated above. Total studies finalized for review were 42. Two reports were included in the study.

Recent literature and technical evaluations reveal promising outcomes when machine learning (ML) is integrated into cyber-security frameworks, particularly in enhancing data protection and threat intelligence capabilities:

Research studies utilizing supervised machine learning models, such as Support Vector Machines (SVM), Random Forests, and Deep Neural Networks reported detection accuracies of between 89% and 98% for a range of cyber threats including phishing, malware, and network intrusion. Although not using supervised machine learning, unsupervised methods such as autoencoders and clustering techniques (k-means) performed well in detecting zero-day attacks and other anomalous behavior patterns, particularly in dynamic environments such as cloud and IoT networks. **[15], [17]**

Received: August 02,2025

International Journal of Applied Mathematics
Volume 38 No. 8s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)



Source: Page MJ, et al. BMJ 2021;372:n71. doi: 10.1136/bmj.n71 https://creativecommons.org/licenses/by/4.0/

- Research showing the combination of machine learning with Security Orchestration, Automation, and Response (SOAR) platforms saw a mean time to detect (MTTD) and mean time to respond (MTTR) of 40% to 60% decreasing in enterprise environments. Reinforcement learning models were especially effective in developing response strategies

Received: August 02,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

for incidents that endured over time, without the need for human input or intervention while operating in a threat environment that evolved dynamically. **[12], [8]**

- The implementation of Natural Language Processing (NLP) methods in the analysis of threat reporting and conversational transcripts stemming from the dark web have led to an identification of new TTPs (tactics, techniques, and procedures) **[9], [21]** by nearly 70%, creating situational awareness across a number of disciplines. Machine learning methods that automate data classification and use encryption systems have supported return to compliance with U.S. regulations, such as HIPAA, CCPA and NIST 800-53, which focuses on data management and access control for sensitive data. Behavioral analytics solutions have also saved organizations in both healthcare and financial services from an increase of more than 30% in insider threat events. **[17]**

Discussion

Threat Detection Using Machine Learning

The ICF calls for the application of sophisticated learning paradigms in highly heterogeneous and data-scarce environments, such as large-scale IoT networks. Adaptive paradigms such as Model-Agnostic Meta-Learning (MAML) and few-shot learning are needed, which will allow base models to rapidly learn and adapt to a different attack scenario or an intended undertaking that will incur no more than very few data, greatly enhancing security performance across multiple datasets and in dynamic IoT environments. **[14], [19]** The meta-learning paradigms have achieved state-of-the-art performance even in laboratory settings, for example in achieving 99.98% performance on the UNSW-NB15 benchmark dataset. **[21]**

Using behavioral AI programs (for example, M2.4 in MICRA) adds another level of intensity to the ZTA requirement. ZTA has the policy in place to manage who has access to what, with behavioral analytics looking at how that access is being used. **[22], [13]** Given most insider threats leverage on the legitimate and validated credentials of the user, signature-based tools and policies simply don't hold up. Behavioral AI tackles this by dynamically modeling and flagging when someone has deviated from their individual baseline, providing the required, continuous post-authentication verification layer, evaluating the intent of access, and ultimately reinforcing the ZTA control plane. **[19]**

Strategic Threat Intelligence

To facilitate the cohesive interaction of disparate security tools and architectures, TI must leverage standardized data formats and transport protocols. For example, data can be represented using standardized specifications, such as STIX 2.1 (Structured Threat Information eXpression) while protocols, such as TAXII 2.1 (Trusted Automated eXchange of Indicator Information), can be used to automate data collection and transport. **[20], [21], [23]**

Received: August 02,2025

International Journal of Applied Mathematics
Volume 38 No. 8s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 2: Stature of MICRA Modules at different Phases of Cybersecurity Framework

Cyber Defense Phase	MICRA Module (Function)	Key Mechanisms/ML Techniques
Sensing/Collection	M1: Dynamic Data Acquisition (DDA)	Network Telemetry Streaming, Honeypot Integration.
Processing/Analysis	M2: Cognitive Threat Analysis (CTA)	Supervised/Unsupervised ML, Behavioral Baselines, Heuristic Classification.
Decision/Validation	M3: Strategic Threat Intelligence (STI)	Multi-layer Validation (Automated/Manual), Confidence Scoring, TI Repository Consolidation.
Response/Action	M4: Adaptive Response Orchestration (ARO)	Automated Playbook Execution, Dynamic Policy Enforcement (ZTA implementation).

Raw STIX data must be normalized and translated into a common schema like Elastic Common Schema (ECS) for analysis once ingested as atoms within the security platform. Standardization enables bespoke integration and adaptability for the rapid integration of even vendor variant data sources, such as air-gapped environments and custom APIs. The necessity for rigorous TI standardization (STIX/TAXII) imposes strong governance over the ML pipeline. The Strategic Threat Intelligence module (M3 in MICRA) serves as a type of centralized control plane for ML models. By feeding external data on TTPs and IoCs into M2, the ICF dynamically tunes algorithms that reflect real-world adversary activity versus relying on historical internal observation alone. Continuously injecting contextual high-confidence threat information allows ML components to keep the high degree of detection performance shown in real-world studies. **[24]**

Fifth-generation systems heavily rely on software-defined networking (SDN), network slicing, and Multi-Access Edge Computing (MEC), all within cloud-native systems. Their distributed architecture, combined with fast deployment models (DevOps), has a higher chance for security vulnerabilities to occur from misconfiguration or unauthorized risk to baseline state security, than from protocol flaws. **[25]** Therefore, the ICF must consider configuration data and role-bases access control (RBAC) logging as priority telemetry streams in its Dynamic Data Acquisition (M1) module. By using behavioral ML (M2) with these two streams, the ICF will identify unauthorized changes to the security posture in the cloud prior to the intrusion of an insider threat, rather than just responding with anomalies to the streaming data of network activity. **[23], [9], [16]**

Received: August 02,2025

International Journal of Applied Mathematics
Volume 38 No. 8s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Governance of AI in Cyber-Security

The NIST AI Risk Management Framework (AI RMF) offers a clear set of principles and a systematic orientation toward the management of AI risks across the lifecycle of AI, with consideration to ethics, accountability, and transparency. **[19]** The AI RMF's structure is organized around four overarching functions: Govern, Map, Measure, and Manage, while recognizing that AI risks are more than just technical challenges - they bring new social or legal challenges with them. ICFs will need to ensure that any future deployments conform to relevant international regulatory frameworks, including, but not limited to the GDPR, ISO/IEC 27001, and the emerging EU AI Act. **[14], [27]**

Conclusion

The key asset of the ICF is shown in its ML engine (M2), which allows for the behavioral analysis that is critical for defending against internal threats and zero-day exploits. This intelligence drives the combination of a continuous feedback loop and standardized Threat Intelligence model (STIX/TAXII), a persistent governance layer to keep ML models aligned to adversary TTPs. The architecture has built in layered validation (M3) prior to automated response (M4) to mitigate risk of catastrophic false positive occurrences, making it sufficient for use with critical infrastructure components. The application layer will have a number of use cases catered by a Federated Learning approach secured by Distributed Ledger Technologies specifically applied for the challenge of maintaining trust and data integrity at the distributed edge.

Future Scope of Study

There is a need for additional empirical studies to assess the viability of Agentic AI frameworks (i.e., MAESTRO, CyberTeam) in real-time incident response contexts, while at the same time working to counter and protect against their resource-type denial vulnerabilities and also to create and study the feasibility of actively changing the priority of resource use. The empirical research should ultimately document and publish the operational overhead intersection of XAI, specifically the implementation of polling and re-explaining aspects of an additional means of explainability, against the strict tail latency requirement of an associated high throughput ML serving pipeline. The research also needs to quantify the least amount of explainability needed to meet the regulatory requirements without hurting operating performance voice performance requirements.

References

1. Peris.ai. Building the Future of Cybersecurity with Architecture. Peris.ai. Available from: https://peris.ai/post/building-the-future-of-cybersecurity-with-architecture
2. Cybersecurity and Infrastructure Security Agency (CISA). Potential Threat Vectors to 5G Infrastructure. Available from: https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%2520%25281%2529.pdf

Received: August 02,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3. Palo Alto Networks. What is a Zero Trust Architecture? Palo Alto Networks. Available from: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture
4. Chechkin A, Pleshakova E. A Hybrid KAN-BiLSTM Transformer with Multi-Domain Dynamic Attention Model for Cybersecurity. [Preprint]. ArXiv; 2025 May.
5. Algomox. Predicting Insider Threats Using Behavioral AI. Algomox. Available from: https://www.algomox.com/resources/blog/predicting_insider_threats_using_behavioral_ai/
6. Booz Allen Hamilton. Leverage Machine Learning to Detect Insider Threats. Booz Allen Hamilton. Available from: https://www.boozallen.com/insights/ai-research/leverage-machine-learning-to-detect-insider-threats.html
7. Malik G. Integrating Threat Intelligence with DevSecOps: Automating Risk Mitigation before Code Hits Production. [Preprint]. Res Gate; 2025 Aug. Available from: https://www.researchgate.net/publication/365284999_Dynamic_data_management_for_continuous_retraining
8. CyCognito. Threat Intelligence. CyCognito. Available from: https://www.cycognito.com/learn/threat-intelligence/
9. Elastic Docs. Custom Threat Intelligence integration. Elastic. Version 1.2.1. Available from: https://www.elastic.co/docs/reference/integrations/ti_custom
10. IBM. Incident Response. IBM Think. Available from: https://www.ibm.com/think/topics/incident-response
11. Cybersecurity and Infrastructure Security Agency (CISA). Security Guidance for 5G Cloud Infrastructures Part IV. CISA; 2021 Dec 16. Available from: https://www.cisa.gov/sites/default/files/2024-08/SECURITY_GUIDANCE_FOR_5G_CLOUD_INFRASTRUCTURES_PART_IV_20211216_508.pdf
12. SentinelOne. Kubernetes Security Risks: 10 Vulnerabilities You Need to Know. SentinelOne. Available from: https://www.sentinelone.com/cybersecurity-101/cloud-security/kubernetes-security-risks/
13. Google Cloud. Service Mesh: Security Best Practices. Google. Available from: https://cloud.google.com/service-mesh/docs/security/best-practices
14. Department of Homeland Security (DHS). 5G Impacts on Cybersecurity. DHS; 2024 Sep. Available from: https://www.dhs.gov/sites/default/files/2024-09/2024aepphasell5gimpactsoncybersecurity.pdf
15. Microsoft Azure. Azure IoT Hub Service Guide. Microsoft. Available from: https://learn.microsoft.com/en-us/azure/well-architected/service-guides/azure-iot-hub
16. Crankshaw D, Sela G, Mo X, Zumar C, Stoica I, Gonzalez J, Tumanov A. InferLine: Latency-Aware Provisioning and Scaling for Prediction Serving. Pipelines. In ACM

Received: August 02,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Symposium on Cloud Computing (SoCC '20); 2020 Oct 19–21; Virtual Event, USA. ACM; 2020.

17. Ovabor, K., Sule-Odu, I., Atkison, T., Fabusoro, A., & Benedict, J. (2024). AI-driven threat intelligence for real-time cybersecurity: Frameworks, tools, and future directions. Open Access Research Journal of Science and Technology, 12(2), 040–048. https://oarjst.com/sites/default/files/OARJST-2024-0135.pdf
18. Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. World Journal of Advanced Research and Reviews, 21(1), 2286–2295. https://wjarr.com/sites/default/files/WJARR-2024-0315.pdf
19. Mohamed, N. (2023). Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms. Knowledge and Information Systems, 67, 6969–7055. https://link.springer.com/article/10.1007/s10115-025-02429-y
20. Sommer, R., & Paxson, V. (2013). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 305–316. doi:10.1109/SP.2010.25
21. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176. doi:10.1109/COMST.2015.2494502
22. Shaukat, K., Luo, S., Varadharajan, V., & Hameed, I. A. (2020). A review on machine learning techniques for cyber security in the last decade. IEEE Access, 8, 222310–222354. doi:10.1109/ACCESS.2020.3041951
23. Sarker, I. H., Kayes, A. S. M., & Watters, P. (2021). Cybersecurity data science: An overview from machine learning perspective. Journal of Big Data, 8(1), 1–29. doi:10.1186/s40537-021-00413-2
24. U.S. National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). https://www.nist.gov/cyberframework
25. MITRE Corporation. (2022). MITRE ATT&CK® Framework: A knowledge base of adversary tactics and techniques. https://attack.mitre.org
26. CISA. (2023). Cybersecurity Best Practices for Machine Learning Systems. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov

Received: August 02,2025