https://doi.org/10.31891/csit-2026-1-16

UDC 004.9

ANALYSIS OF INFORMATION TECHNOLOGIES AND METHODS FOR AUTOMATIC UPDATING OF THREAT DETECTION MODELS IN COMPUTER SYSTEMS

Tymur ISAIEV
PhD student of Computer Engineering and Information Systems Department, Khmelnytskyi National University, Khmelnytskyi, Ukraine
e-mail: tymuri1112@gmail.com
https://orcid.org/0009-0006-7655-2911

Olha ATAMANIUK
Lecturer of Computer Engineering and Information Systems Department, Khmelnytskyi National University, Khmelnytskyi, Ukraine
e-mail: ataman@i.ua
https://orcid.org/0000-0001-9802-864X

The development of intelligent adaptive information technologies for automatic updating of threat detection models in computer systems is one of the most important directions in modern research on information technologies. Computer systems today operate in environments that are constantly changing, influenced by new software, evolving hardware, and diverse data processing methods. Traditional static approaches, which rely on fixed rules or predefined models, often become outdated quickly and fail to provide the necessary adaptability.

Existing approaches to detection in computer systems have been studied extensively, and while they provide valuable insights, they also demonstrate clear limitations. Signature-based methods depend heavily on known patterns and therefore struggle to identify new or unexpected phenomena. Heuristic analysis allows for broader generalization but is frequently associated with high rates of false positives, which reduces its practical usefulness. Behavioral monitoring can capture dynamic changes in system activity, yet it requires significant computational resources and may slow down performance. Machine learning models offer adaptability and the ability to learn from data, but they demand large amounts of training information and careful tuning to avoid errors. Hybrid approaches attempt to combine the strengths of multiple techniques, but they often face difficulties in seamless integration and optimization within existing infrastructures.

Because of these limitations, researchers are increasingly focused on developing frameworks that incorporate automatic updating mechanisms. Such frameworks are designed to be self-adaptive, meaning they can evolve continuously in response to new conditions without requiring manual intervention. Real-time adaptation is a central feature of these systems, enabling them to improve accuracy, reduce false positives, and optimize the use of computational resources.

By integrating intelligent updating mechanisms, information infrastructures can achieve higher levels of stability and efficiency. This not only enhances the overall performance of computer systems but also ensures that they remain relevant and effective in environments where change is constant. The ability to evolve automatically, without relying on outdated static methods, positions these technologies as a cornerstone of future developments in information systems.

The continuous evolution of computational environments demands solutions that are flexible, intelligent, and capable of real-time adaptation. By embracing adaptive frameworks, researchers and developers can create systems that are not only more accurate and efficient but also more resilient and scalable. This marks a decisive step toward the next generation of computer systems, where adaptability and automation are essential for long-term reliability and success.

Keywords: computer systems, threat detection, machine learning, information technology, automatic update

Received: 12/02/2026
Accepted:19/03/2026
Published:26/03/2026

Introduction

The rapid evolution of information technologies has encouraged both vendors and researchers to integrate adaptive mechanisms and automatic updating capabilities into detection systems within computer environments. As systems grow more complex and data flows become increasingly dynamic, the need for solutions that can adjust in real time has become critical. Many commercial platforms, open-source frameworks, and experimental prototypes continue to exhibit recurring architectural and methodological weaknesses. These limitations affect the reliability of detection processes, reduce the timeliness of responses to new conditions, and undermine overall trust in the consistency of system performance [1].

A closer examination of representative technologies reveals that while they often succeed in addressing specific tasks, they struggle to maintain sustained adaptability over long periods of operation. Signature-based approaches, for example, are constrained by their dependence on predefined patterns, which makes them slow to react to unforeseen changes in system behavior. Heuristic methods provide broader flexibility but frequently generate excessive false positives, which complicates their practical application. Behavioral monitoring techniques are valuable for capturing dynamic processes, yet they demand considerable computational resources and can introduce performance bottlenecks. Machine learning models offer promise through their ability to generalize and learn from data, but they require extensive training datasets and careful calibration, and they may still fail when confronted with novel or highly variable conditions. Hybrid solutions attempt to combine these methods, but they often face integration challenges and difficulties in achieving seamless scalability [2].

The shortcomings of these approaches highlight the importance of designing frameworks that incorporate continuous self-adaptation and automatic updating. Such frameworks are not limited to static rules but instead evolve alongside the systems they monitor. By embedding mechanisms for real-time adjustment, they can improve detection accuracy, reduce false alarms, and optimize resource utilization. They support scalability, allowing systems to expand without sacrificing efficiency or responsiveness. This adaptability is essential for environments where workloads, data structures, and operational requirements change rapidly and unpredictably [3].

The shift toward adaptive updating technologies represents a fundamental transformation in the way information systems are managed. Instead of relying on rigid, preconfigured models, the new generation of systems emphasizes automation, flexibility, and intellectual adaptability. These systems are capable of responding quickly to emerging challenges, maintaining consistent performance, and ensuring long-term reliability. They also provide a foundation for building resilient infrastructures that can withstand continuous change, making them suitable for diverse applications ranging from enterprise computing to large-scale distributed networks.

Analysis of methods for automatic updating of threat detection models in computer systems

Modern methods of information technologies for solving complex analytical and organizational tasks increasingly rely on adaptive, data-driven, and self-optimizing computational approaches. Contemporary large-scale information environments are characterized by an unprecedented acceleration in both the volume and structural complexity of processed data. Automated systems, distributed infrastructures, and AI-driven workflows evolve faster than traditional static analytical mechanisms can adjust. Models that once sufficed for identifying predefined patterns or rule-based irregularities quickly become outdated in dynamic contexts where operational conditions shift within hours. This rapidly changing landscape has created a pressing need for intelligent adaptive information technologies capable of autonomously updating analytical models without continuous human intervention. The essence of such technologies lies in their ability to integrate continuous learning, contextual awareness, and real-time responsiveness into the core of modern information systems.

Adaptive intelligence in this field is not limited to incremental improvements of existing algorithms; it represents a paradigm shift toward systems that are inherently self-correcting and self-optimizing. These systems are designed to ingest vast streams of heterogeneous data - ranging from communication flows and system logs to behavioral metrics and textual information - and to recalibrate their analytical thresholds dynamically. Automated updating ensures that models remain aligned with current operational realities, thereby minimizing periods during which analytical accuracy may degrade. Furthermore, the integration of reinforcement learning and deep neural architectures enables such systems to anticipate emerging patterns and structural shifts rather than merely respond to them, fostering a proactive rather than reactive analytical posture.

Another critical dimension of intelligent adaptive technologies is their interpretability and transparency. While opaque, black-box models can achieve high predictive accuracy, they often fail to provide meaningful insights for specialists responsible for overseeing complex information processes. Modern approaches emphasize explainable AI, enabling systems to justify their decisions and highlight the features that influenced specific analytical outcomes. This interpretability is essential for trust, regulatory compliance, and effective collaboration between automated mechanisms and human experts. Additionally, ethical considerations are increasingly embedded into the design of adaptive technologies, ensuring that automation does not compromise privacy, fairness, or the integrity of organizational processes while still maintaining robust analytical performance.

The convergence of these factors - automation, continuous learning, contextual awareness, interpretability, and ethical design - defines the current trajectory of research and practice in advanced information technologies. Only after establishing this conceptual foundation does it become appropriate to examine specific studies and empirical evidence from 2024–2025 that illustrate how these principles are being implemented in real-world information systems.

Authors in [4-7] collectively showed how automated signature extraction, hybrid host detection, and temporal analysis can strengthen intrusion detection systems. Author in [8] investigated the impact of heuristic algorithms on cyberthreat detection and demonstrated that heuristic search and optimization strategies improved the adaptability of intrusion detection systems while refining accuracy and reducing computational overhead.

Author in [9] developed an anomaly-driven approach for ransomware identification based on heuristic analysis and showed that dynamic heuristic monitoring captured evolving ransomware behaviors, offering a flexible detection method that adapted to temporal changes in attack strategies. Author in [10] reviewed hybrid Android malware detection techniques that relied on heuristic-based approaches and concluded that combining heuristic analysis with other detection methods addressed the complexity of mobile malware and improved resilience against zero-day threats.

Authors in [11] proposed a heuristic malware detection method that leveraged structured cyber threat intelligence data and demonstrated that integrating CTI with heuristic models enhanced precision in identifying malicious activity and supported adaptive updates to detection frameworks. Author in [12] conducted a deep analysis of nature-inspired and meta-heuristic algorithms for intrusion detection in cloud, edge, and IoT environments, surveying state-of-the-art techniques, identifying challenges, and outlining future directions while emphasizing scalability and adaptability. Authors in [13] explored intrusion detection in software-defined networks using meta-heuristic optimization combined with the K-Nearest Neighbors classifier and showed that optimization algorithms fine-tuned classical classifiers to achieve higher accuracy and robustness in SDN environments. Author in [14] introduced a novel hybrid machine learning approach for real-time ransomware detection that incorporated behavior-driven heuristic features and demonstrated that combining heuristic behavioral analysis with machine learning models enabled faster and more accurate identification of ransomware activity in live systems. In [15], the study offered a broad review of how machine learning has been applied in cybersecurity, examining both classical algorithms and deep learning models. The authors showed that continuous retraining was essential for countering zero-day exploits, positioning ML as a foundation for adaptive intrusion detection.

The work in [16] turned attention to big data, demonstrating that large-scale analytics combined with AI and ML improved scalability and accuracy in threat detection. By highlighting the importance of heterogeneous datasets, the paper underscored how automatic updating of models depends on constant inflows of diverse information. Research presented in [17] addressed the transformation of Security Operations Centers, showing how AI-driven automation reduced analyst workload and strengthened real-time detection. This contribution illustrated the practical role of adaptive updating in environments where rapid response is critical. In [18], the integration of AI into cybersecurity was analyzed with a focus on detection and response. The study emphasized that machine learning models could dynamically adjust both identification and mitigation strategies, shortening the gap between recognizing new threats and deploying countermeasures.

The publication in [19] explored concrete applications of AI and ML in threat detection, presenting deployment methods for intelligent systems. Case studies demonstrated how hybrid models combining anomaly detection and signature analysis could be embedded into enterprise infrastructures, ensuring models remain current. A detailed review in [20] examined malicious insider threat detection, identifying both challenges and opportunities. The authors showed that ML methods were capable of monitoring subtle behavioral changes, making continuous updating indispensable for detecting insider risks.

In [21] author investigated anomaly detection based on machine learning, discussing statistical, clustering, and deep learning approaches. The study highlighted how adaptive retraining allowed systems to capture shifting baselines of normal activity, reinforcing anomaly detection as a proactive defense against unpredictable attacks. In [22], the chapter presented a systematic overview of behavioral analysis, showing how profiling user and system actions can reveal anomalies. It emphasized the role of AI-driven analytics in distinguishing normal processes from irregular ones, positioning behavioral modeling as a key element of adaptive systems. The study in [23] examined dynamic behavioral analysis of programs that breach privacy and steal data. Continuous monitoring of execution traces was shown to capture subtle deviations in system behavior, underlining the importance of models that evolve alongside changing tactics.

Research in [24] introduced predictive behavioral mapping as a method for autonomous identification of harmful processes. By forecasting likely actions based on prior behavioral sequences, the work demonstrated how proactive mapping could strengthen detection before unwanted activity fully unfolds. In [25], an innovative framework was proposed that relied on adaptive cryptographic behavior analysis. Monitoring encryption operations was argued to provide reliable indicators of suspicious activity, offering a novel behavioral dimension for analytical systems.

Heuristic and meta-heuristic methods provide the foundation for adaptability in distributed detection. As shown in [8], heuristic algorithms allow systems to refine detection rules dynamically, improving accuracy while reducing computational overhead. This is particularly important in distributed environments, where computational resources are shared across nodes and efficiency is critical. The work in [9] extended this idea by developing anomaly-driven approaches for identifying ransomware, demonstrating that heuristic monitoring can capture evolving behaviors that static signatures miss. Hybrid approaches, such as those discussed in [10] and [11], combined heuristic analysis with other detection methods, showing that integration with structured intelligence data enhances precision. Meta-heuristic algorithms, explored in [12] and [13], introduced nature-inspired optimization strategies that scale effectively across distributed infrastructures such as cloud, edge, and IoT systems. These studies emphasized that meta-heuristics can fine-tune classifiers and adapt to diverse datasets, ensuring that detection models remain current even as network conditions evolve. The contribution of [14] further illustrated how hybrid machine learning approaches enriched with heuristic features can provide real-time detection capabilities, reinforcing the importance of adaptability in distributed systems.

Behavioral analysis has emerged as another major direction in the design of distributed detection systems. Sources [22] through [25] highlighted the importance of profiling user and system actions to identify anomalies before harmful processes fully manifest. Distributed systems benefit from behavioral analysis because they can collect and correlate activity data across multiple nodes, creating a more comprehensive picture of network behavior. For example, [22] presented a systematic overview of behavioral profiling, emphasizing AI-driven analytics as a means of distinguishing normal processes from irregular ones. [23] and [24] introduced dynamic behavioral analysis and predictive mapping techniques, showing how continuous monitoring of execution traces can anticipate privacy breaches and ransomware activity. The innovation in [25] was particularly significant, as it proposed adaptive cryptographic behavior analysis, demonstrating that monitoring encryption operations across distributed nodes can serve as a reliable indicator of malicious activity.

The convergence of these methodologies demonstrates that adaptability in distributed detection systems is not achieved through a single technique but through the integration of multiple approaches. Heuristic algorithms refine rules dynamically, behavioral profiling anticipates anomalies, hybrid AI models retrain across heterogeneous data, and graph-based frameworks restructure themselves as interactions change. Together, these methods form the foundation for systems capable of automatic updating, continuous learning, and efficient operation in environments characterized by constant change. Importantly, the reviewed literature shows that distributed systems are not only more resilient but also more scalable, as they can leverage the collective computational power and data diversity of multiple nodes. This scalability ensures that detection remains effective even in large-scale infrastructures such as industrial IoT, financial networks, and critical infrastructure systems.

Modern distributed systems for detecting malicious software are defined by their adaptability, scalability, and integration of diverse analytical methods. The reviewed sources [4]–[25] collectively illustrate that the future of detection lies in architectures that are continuously evolving, capable of retraining themselves on new data, restructuring their models as network conditions change, and updating automatically to remain effective against emerging threats. These systems represent a paradigm shift from static, centralized detection toward dynamic, distributed architectures that embody the principles of continuous learning and proactive defense.

The analysis of the reviewed information technologies reveals a consistent set of systemic shortcomings that persist across diverse methodological approaches and architectural designs. Despite significant progress in adaptive modeling, automated updating, and large-scale data processing, these technologies remain constrained by several foundational limitations. Foremost among them is the dependence on data quality, consistency, and representativeness: heterogeneous, noisy, or sparsely labeled datasets frequently undermine analytical accuracy and impede the reliability of adaptive recalibration.

A second major limitation concerns model interpretability and transparency. Complex architectures-particularly those based on deep learning, hybrid frameworks, or meta-heuristic optimization-often function as opaque structures, making it difficult for specialists to understand decision pathways or validate analytical outcomes. This lack of interpretability complicates oversight, reduces trust, and limits the practical integration of automated systems into organizational workflows.

The reviewed technologies exhibit architectural fragility, especially in distributed environments. Automatic updates, while essential for adaptivity, frequently introduce regressions, version mismatches, or configuration conflicts. Distributed infrastructures amplify these issues through inconsistent synchronization, uneven resource availability, and heterogeneous device capabilities, all of which contribute to analytical instability.

Another recurring shortcoming is the computational overhead associated with large-scale adaptive systems. Continuous monitoring, real-time model updates, and high-dimensional data processing impose substantial resource demands, making many solutions difficult to deploy in constrained or heterogeneous environments. Even advanced hybrid and graph-based approaches, though powerful, often require extensive preprocessing, optimization, and maintenance to remain effective.

The general shortcomings across the examined technologies underscore a central challenge: true adaptability requires not only advanced algorithms but also stable data ecosystems, interpretable models, resilient architectures, and coordinated methodological integration. Without addressing these structural limitations, the full potential of intelligent adaptive information technologies cannot be realized.

The evaluated studies were systematically compared using a unified set of criteria designed to capture the essential qualities of contemporary information system methodologies. By examining latency, complexity, reliability, functionality, and maintainability, the table highlights how different methodological groups align with or diverge from the requirements of adaptive and scalable distributed information systems. This structured comparison (Table 1) provides a clear foundation for identifying both the strengths and the inherent limitations of existing approaches.

A comprehensive evaluation of the examined methods through the established system of criteria-latency, complexity, reliability, functionality, and maintainability-demonstrates that existing approaches within the field of this research remain insufficient for effectively addressing the broader task of constructing adaptive, scalable, and continuously self-updating distributed analytical systems. Methods based on static rule sets and predefined patterns, despite their conceptual simplicity, exhibit high latency, limited functional coverage, and poor maintainability. Their dependence on manual configuration and rigid logic structures prevents them from responding adequately to dynamic changes in system behavior, data flows, or operational conditions. As modern information environments evolve rapidly and unpredictably, such rigidity creates persistent gaps between real-world system states and the system's internal representation, undermining long-term operational efficiency.

Table 1.

Evaluation of methodological approaches based on information system criteria

Paper	Latency	Complexity	Reliability	Functionality	Maintainability	Main Cons
[4-5]	High level implementation	Low level implementation	Low level implementation	Low level implementation	Low level implementation	Static methods failed to detect new threats. High level implementation latency made them unsuitable for real-time use.
[6-9]	Low level implementation	Medium level implementation	Low level implementation	Medium level implementation	High level implementation	Heuristic models were flexible but unstable under varying loads. Frequent false positives reduced reliability.
[10-12]	Medium level implementation	High level implementation	Medium level implementation	Medium level implementation	Medium level implementation	High level implementation algorithmic complexity increased resource usage. Deployment in constrained environments was difficult.
[13-14]	Medium level implementation	Low level implementation	Medium level implementation	Low level implementation	Medium level implementation	Limited feature sets reduced coverage of diverse attacks. Generalization across networks remained weak.
[15-17]	Low level implementation	Medium level implementation	High level implementation	Medium level implementation	Low level implementation	Models required constant retraining. Detection quality degraded quickly without continuous updates.
[18-19]	Medium level implementation	Medium level implementation	Medium level implementation	High level implementation	Medium level implementation	Performance depended on large datasets. Integration into existing infrastructures demanded significant effort.
[20-21]	Low level implementation	High level implementation	Medium level implementation	Medium level implementation	Medium level implementation	Complex behavioral baselines required heavy computation. Profiles needed frequent recalibration.
[22-24]	Medium level implementation	Medium level implementation	High level implementation	Low level implementation	Low level implementation	Narrow behavioral focus limited functionality. Updating models across nodes was resource-intensive.
[25]	High level implementation	Low level implementation	Medium level implementation	Medium level implementation	High level implementation	Monitoring encryption caused delays. Distinguishing signals from malicious encryption was inconsistent..

Heuristic and hybrid heuristic approaches partially mitigate these limitations by introducing flexible rule adaptation and context-aware decision mechanisms. When assessed through the criteria, they reveal instability across heterogeneous nodes, inconsistent performance under varying workloads, and sensitivity to fluctuations in data quality. These characteristics reduce overall reliability and complicate deployment in large-scale distributed infrastructures, where uniformity of behavior is essential for coordinated operation. Even when latency and maintainability improve, the absence of stable cross-node generalization limits their practical applicability.

Meta-heuristic and nature-inspired optimization techniques offer stronger adaptability and scalability, particularly in environments characterized by diverse data sources and distributed processing. These advantages come at the cost of significantly increased algorithmic complexity. High level implementation computational demands, intricate parameter tuning, and environment-specific optimization procedures hinder maintainability and restrict integration into resource-constrained subsystems such as edge devices or embedded controllers. As system conditions evolve, previously optimized configurations often lose effectiveness, requiring repeated recalibration that is both time-consuming and resource-intensive.

Data-driven and machine-learning-based methods demonstrate higher functional capacity and improved ability to model complex relationships within distributed information systems. They support continuous refinement and can incorporate heterogeneous data streams, which aligns with the need for adaptability. Nevertheless, the criteria-based analysis reveals structural limitations: these methods depend heavily on large, diverse, and consistently updated datasets; they require ongoing retraining to prevent model drift; and they impose substantial operational burdens related to data management, model maintenance, and infrastructure coordination. As a result, reliability and maintainability become difficult to sustain over extended periods, especially in environments where data distributions shift frequently.

Behavioral and dynamic analytical approaches contribute valuable insights by modeling system processes, user interactions, and operational patterns over time. They often achieve higher reliability within their specialized domains but exhibit narrow functional scope and limited generalizability. Maintaining synchronized behavioral baselines across distributed nodes is resource-intensive, and even minor deviations in normal system usage can necessitate recalibration. This creates a tension between sensitivity and stability: systems either become too rigid to accommodate natural variability or too sensitive to operate efficiently at scale.

Taken together, these observations reveal a fundamental structural gap: no existing methodological family simultaneously satisfies the combined requirements of low latency, controlled complexity, high reliability, broad functionality, and sustainable maintainability within distributed information systems. Each approach optimizes only a subset of criteria while compromising others. Static methods favor simplicity but lack adaptability; heuristic and meta-heuristic methods enhance adaptability but struggle with stability and complexity; data-driven models improve functionality but impose heavy maintenance demands; behavioral approaches offer depth but lack breadth and scalability.

This multidimensional insufficiency becomes especially pronounced in modern distributed information environments, where systems must operate across heterogeneous nodes, process diverse data streams, and adjust continuously to evolving operational conditions. Effective solutions must not only analyze current states but also restructure themselves dynamically, coordinate knowledge across nodes, and maintain consistent performance despite variability in data, workload, and system topology. Existing methods, even in their most advanced forms, remain fragmented and domain-specific. They do not provide mechanisms for unified coordination, cross-node knowledge integration, or autonomous restructuring of analytical logic.

Therefore, the criteria-based analysis clearly indicates that current methods are inadequate for fully resolving the task of building adaptive, scalable, and self-maintaining distributed information systems. What is required is an integrated framework that unifies heuristic adaptability, behavioral modeling, data-driven generalization, and structural awareness of distributed architectures, while explicitly optimizing all criteria as interconnected design objectives.

This comparative analysis exposes a fundamental problem in current threat detection technologies: no single existing solution maximizes speed, accuracy, and specificity simultaneously. We currently have methods that are specific but slow and blind to new attacks, or methods that are fast and accurate but less stable. This unresolved trade-off highlights an urgent and critical need to develop a new class of intelligent adaptive information technologies. Future research must focus on developing a unified method capable of automatic model updating that synthesizes the low latency and high accuracy of hybrid architectures with the strict specificity of traditional approaches, thereby bridging the gap between stability and adaptability in complex analytical environments.

Analysis of information technologies for automatic updating of threat detection models in computer systems

Information technologies today serve as a universal foundation for solving complex and diverse tasks, providing tools for automation, adaptability, and intelligent decision-making in rapidly changing computational environments.

The information technology, implemented in Microsoft Defender for Endpoint [26], is designed to process large-scale telemetry data and apply continuously updated machine learning models in order to adapt detection logic across distributed computer systems. Its core function is to provide automated adjustment of analytical models, ensuring that endpoints remain aligned with evolving operational conditions. However, the technology demonstrates a significant weakness due to its reliance on centralized cloud orchestration. When cloud services experience outages or latency, the updating of models, ingestion of telemetry, and execution of response actions are delayed, which reduces the timeliness and reliability of the system. Another limitation arises from the dependence on extensive behavioral data: while such data improves adaptive accuracy, regulatory restrictions can limit telemetry collection, thereby reducing the effectiveness of the models. Automatic updates, although essential for adaptability, may also introduce regressions or false positives when new logic is deployed globally without sufficient validation for specific environments, leading to instability in heterogeneous infrastructures. Furthermore, the technology faces challenges in handling concept drift, particularly when legitimate administrative-like activities resemble anomalous behavior. This issue is amplified by the increasing use of system-native binaries and signed drivers, which complicates the ability of behavior models to distinguish between normal operations and subtle misuse. Overall, while the technology provides advanced adaptive capabilities for updating detection models, its architectural dependencies and methodological constraints highlight the need for more resilient, context-aware approaches within information systems.

The informational technology, implemented in CrowdStrike Falcon [27], emphasizes large-scale analytical processing and streaming data interpretation that adjust operational models in near real time. Its cloud-centric architecture centralizes computational pipelines, which increases dependence on unified orchestration layers and introduces structural rigidity that can limit autonomous functioning during service interruptions. Organizations encounter opaque analytical pathways: model updates and scoring mechanisms are delivered as managed components with limited interpretability, complicating retrospective evaluation and methodological transparency. Adaptive enrichment mechanisms reduce redundant signals in common scenarios but may underrepresent rare, gradual, or low-frequency patterns, creating analytical blind zones in long-horizon processes. Continuous data streaming imposes bandwidth and storage demands, while strict data residency constraints can fragment deployments, reducing the uniformity of adaptive recalibration across distributed infrastructures.

The digital analytical framework, deployed in Cortex XDR [28], integrates endpoint, system, and cloud-originated signals into unified adaptive models. Although cross-domain correlation enhances contextual depth, the complexity of integration extends calibration cycles and increases the effort required to maintain consistent analytical behavior. Automatic incorporation of new indicators and analytical components may produce brittle model states tied to transient patterns, elevating maintenance overhead. The ubiquity of encrypted communication reduces the visibility of deep data structures; attempts to enable full inspection introduce performance and privacy trade-offs that many environments avoid, thereby constraining adaptive analytical refinement. The platform's reliance on a consolidated data lake also introduces susceptibility to data quality degradation: polluted logs or mislabeled events can distort model behavior across tenants if validation controls are insufficient.

The adaptive computational system, underlying Darktrace [29], positions unsupervised learning as a mechanism for modeling operational baselines and autonomously adjusting to evolving patterns. The central methodological challenge is concept drift: legitimate changes in organizational workflows, communication patterns, or seasonal activity repeatedly trigger recalibration cycles, generating excessive notifications and reducing the efficiency of human oversight. The system's opaque internal logic limits interpretability; when automated actions occur, the absence of transparent rationale undermines trust and may disrupt normal operations. Sophisticated deviations can mimic established baselines to remain within learned boundaries, and the lack of robust cross-entity semantics can misclassify multi-stage processes in which each individual step appears benign when evaluated in isolation.

The computational analytical platform, represented by Elastic Security [30], combines rule-based analytics, adaptive models, and extensible data pipelines. Automatic updates to rules and models in distributed clusters are vulnerable to version inconsistencies, index mapping drift, and pipeline fragmentation, producing uneven analytical outcomes across nodes. Anomaly-detection jobs require careful feature engineering; default configurations often underperform in specialized environments, leading either to excessive redundant signals or to missed subtle deviations. Because many organizations self-manage Elastic deployments, adaptive effectiveness depends heavily on internal data quality, schema discipline, and CI/CD rigor-areas where resource-constrained teams frequently struggle, resulting in stale models and inconsistent analytical coverage.

The intelligent analytical platform, augmented in IBM Qradar [31], incorporates natural-language-driven ingestion of structured and unstructured information to update analytical content dynamically. This approach depends strongly on the quality and reliability of textual sources; noisy, contradictory, or low-fidelity inputs lead to misaligned prioritization and diluted analytical clarity. Automatic integration of new information into correlation logic can overfit to recent narratives while underrepresenting long-standing structural patterns. The scale of QRadar deployments complicates the testing of adaptive changes; large-scale rollouts impose significant computational and storage loads, prompting teams to disable certain analytical components, which undermines the intended continuity of model evolution.

The analytical information framework, exemplified by Google Chronicle [32], provides cloud-scale processing capabilities with continuously evolving analytical content. Its advantages in storage and high-speed search are counterbalanced by dependency on upstream normalization quality; heterogeneous data sources often produce uneven enrichment that complicates adaptive model behavior. The sheer volume of aggregated information encourages broad analytical generalizations, yet precision declines when contextual metadata is sparse or siloed. Chronicle's multi-tenant infrastructure amplifies concerns around cross-tenant propagation of flawed analytical logic if shared content pipelines distribute misaligned updates. Additionally, data egress constraints and residency requirements limit full consolidation of organizational datasets, restricting comprehensive adaptation across distributed environments.

The computational data-driven environment, represented by Splunk Enterprise Security [33], relies on continuously updated correlation logic and modular analytical toolkits. Automatic updates to search components can disrupt custom dependencies, producing analytical gaps until manual adjustments are completed. Many machine-learning extensions assume stationary data distributions; in high-variability environments, retraining must occur frequently to maintain relevance, increasing computational costs and administrative workload. Splunk's flexible schema is advantageous, yet it enables inconsistent data modeling across teams; adaptive models trained on one subset may perform poorly elsewhere due to divergent field semantics and heterogeneous ingestion practices.

The intelligent processing mechanism, embedded in SentinelOne Singularity [34], emphasizes autonomous endpoint-level analytics with frequently updated models. On-device analytical components are constrained by local computational resources; intensive feature extraction or frequent recalibration can degrade user experience. Automated rollback and remediation workflows are valuable, yet false classifications at this layer directly affect productivity, prompting policy relaxation that reduces analytical strictness. Low level implementation-level system interactions introduce additional complexity: timing inconsistencies and reliance on signed system components can momentarily reduce analytical coverage when model regressions occur before corrective updates propagate.

The integrated analytical infrastructure, utilized in Cisco SecureX [35], focuses on cross-product orchestration and adaptive enrichment of operational data. Its effectiveness depends on consistent integration fidelity across a diverse ecosystem; version mismatches and evolving APIs frequently disrupt automated workflows. Automated playbooks that incorporate new informational inputs may inadvertently amplify noise when upstream feeds are insufficiently validated, creating cascades of low-quality actions. The adaptive posture relies on broad telemetry coverage; gaps in non-Cisco tools and legacy systems create isolated zones where updates cannot be uniformly applied, resulting in uneven analytical performance.

The adaptive computational apparatus, implemented in Fortinet FortiEDR [36], provides real-time processing with dynamically adjustable rules and automated mitigation routines. Inline operational controls require conservative thresholds to avoid disrupting legitimate processes; this caution allows subtle deviations to blend into normal activity patterns. Automatic policy updates risk compatibility issues with specialized applications, triggering operational interruptions that necessitate emergency rollbacks. When telemetry flows primarily through Fortinet's ecosystem, multi-vendor environments experience limited context sharing, reducing the precision of adaptive recalibration.

The automated analytical environment, present in Sophos Intercept X [37], blends deep-learning-based modeling with dynamic update mechanisms. Models trained on historical corpora are vulnerable to dataset bias; emerging software behaviors or novel operational patterns may evade accurate classification until retraining cycles catch up. Feature drift in endpoint metrics produces false classifications during legitimate software updates. The platform's managed-service option reduces administrative burden but introduces latency in fine-tuning for atypical workloads, especially in environments with unique operational profiles.

The digital processing framework, embodied in Trend Micro Apex One [38], employs behavior-oriented monitoring and automated pattern updates. Its reliance on pattern-based heuristics becomes strained under heavy encryption and ephemeral cloud workloads, where observable features are limited. Automatic updates occasionally cause policy conflicts in virtualized or containerized environments, requiring manual exceptions that accumulate over time and erode analytical consistency. Model transparency is limited; tuning decisions often rely on iterative experimentation, extending the time required to achieve stable analytical performance.

The adaptive information system, integrated within Trellix MVISION [39], unifies analytics across endpoint, network, and cloud-based components. The consolidation of legacy and modern modules introduces heterogeneity that complicates synchronized updates. Automatic content delivery conflicts with on-premises change-control processes, creating delays and partial deployments. Inter-component trust relationships introduce systemic fragility: if one domain's model degrades, cross-domain correlation can propagate analytical errors, reducing overall confidence in system-wide outputs.

The computational modeling environment, utilized in Rapid7 InsightIDR [40], enables continuous behavioral analytics with frequently updated content. Its effectiveness depends on stable identity and organizational data; misconfigurations, shadow accounts, or inconsistent directory structures distort baselines and produce misleading anomalies. Automatic detections optimized for common environments generate excessive notifications in highly dynamic development or testing contexts. Resource limitations in mid-market deployments lead to sampling or reduced historical windows, weakening adaptive learning and diminishing long-term analytical accuracy.

The structured analytical environment, exemplified by Sumo Logic Cloud SIEM [41], delivers streaming data processing with dynamically adjustable rules. Multi-tenant rule sets must generalize across diverse environments, yet such generalization increases redundant outputs for specialized operational contexts. Automated pipelines assume consistent log formats; frequent vendor-driven schema changes disrupt feature extraction, reducing analytical quality until mappings are manually restored. Cost constraints often compel organizations to limit data ingestion, weakening the feedback loops required for robust adaptive recalibration and diminishing long-term analytical precision.

The computational interpretation framework, represented by Zeek [42] with machine-learning extensions, provides detailed protocol-level analysis and adaptive anomaly modeling. Modern encryption reduces the visibility of internal data structures, forcing reliance on metadata-based features that offer weaker analytical signals. Machine-learning add-ons require curated training data; most deployments lack sufficient labeling discipline, causing unsupervised detectors to over-alert on benign novelty. Automatic classifier updates across distributed sensors risk inconsistency, producing uneven sensitivity and fragmented situational awareness across the infrastructure.

The automated analytical mechanism, applied in Snort and Suricata [43] with ML augmentations, attempts to merge signature-based logic with adaptive anomaly modeling. Signature components remain structurally rigid; automatic generation from shared repositories introduces duplicates and conflicts that degrade performance. Anomaly-detection modules trained on controlled laboratory data often fail to generalize to production environments, prompting teams to disable them. Continuous rule tuning imposes computational overhead; in high-throughput systems, adaptive detectors are throttled, allowing unprocessed data to pass during peak operational loads.

The integrated information-processing platform, embodied in OSSEC and Wazuh [44], provides host-centric analytical baselines with auto-updating rule sets sourced from external repositories. Host-level baselines are highly environment-specific; automatic rule injections rarely account for bespoke software stacks, producing persistent redundant outputs that lead to permissive exclusions. File-integrity monitoring generates noise during legitimate updates, and if adaptive suppression is overly aggressive, meaningful modifications may go unnoticed. Centralized managers become structural chokepoints, and outages delay adaptive recalibration across distributed agents.

The adaptive data-distribution framework, implemented in MISP [45], automates the dissemination of structured informational elements that downstream systems use to update analytical logic. The primary limitation is rapid indicator turnover: operational identifiers change frequently, so heavy reliance on them yields short-lived analytical improvements and long-term maintenance burden. Feed quality varies significantly; unvetted community contributions propagate inaccurate or stale elements that contaminate adaptive pipelines. Mapping high-level conceptual patterns to concrete, environment-specific analytical logic remains a manual, error-prone task that automated import mechanisms cannot fully resolve.

The knowledge-driven analytical infrastructure, represented by OpenCTI [46], centralizes information about entities, relationships, and operational contexts to support adaptive strategy formation. However, translating knowledge graphs into executable analytical logic requires consistent ontologies and integration code that many teams lack. Automatic synchronization can overwhelm downstream systems with contextual data that is not operationally actionable, increasing cognitive load without improving analytical precision. As with all knowledge-driven adaptation, if upstream taxonomies drift, downstream analytical components become misaligned.

The rule-based computational environment, exemplified by YARA and Sigma [47], often relies on auto-generated or auto-updated patterns sourced from shared repositories to maintain relevance. Generated patterns tend to overfit publicly available samples; polymorphic or dynamically shifting data structures evade pattern matching. Automatic ingestion introduces duplication and conflicts across rule sets, and without rigorous testing, updates break pipelines or generate excessive outputs. Maintaining rule hygiene at scale is labor-intensive; attempts to automate this process frequently overlook environment-specific constraints [48].

The distributed analytical paradigm, explored in federated learning prototypes, aims to adapt models across multiple organizations without sharing raw data. In practice, non-uniform data distributions, heterogeneous feature spaces, and inconsistent preprocessing hinder convergence, producing models that perform unevenly across participants. Gradient updates may inadvertently reveal information through inference techniques, challenging privacy assumptions. Communication overhead and straggler effects slow adaptation, while secure aggregation mechanisms introduce operational complexity that many teams are not equipped to manage.

The automated model-evolution framework, utilized in continuous retraining pipelines, promises ongoing analytical refinement through frequent model refresh cycles. These pipelines are fragile: data-quality issues, label contamination, and silent feature drift produce degraded models that are nevertheless deployed automatically. Governance requirements-such as audit trails and approval workflows-introduce delays that undermine the notion of continuous adaptation. Rollback mechanisms often focus on code rather than model state; when a flawed model is deployed, reverting distributed inference endpoints is non-trivial and creates windows of analytical inconsistency.

The analysis of the above-described information technologies has shown that contemporary information-analytical platforms, regardless of their architectural paradigms or functional orientations, exhibit a shared tendency toward increasing structural complexity, heightened dependence on data quality, and sensitivity to methodological constraints. Across all examined systems, the pursuit of adaptivity, automated model evolution, large-scale data processing, and unified interpretation of heterogeneous inputs is evident, yet their practical effectiveness is shaped not only by computational capabilities but also by infrastructural stability, schema consistency, disciplined data governance, and the organizational capacity to maintain coherent analytical workflows.

The synthesis of observations demonstrates that centralized cloud-orchestrated mechanisms simultaneously provide scalability and introduce systemic dependencies, while distributed architectures suffer from fragmentation, uneven updates, and inconsistent analytical behavior. Automation, although essential for continuous refinement, frequently results in regressions, configuration conflicts, excessive signal generation, or diminished precision, particularly when updates propagate faster than validation processes can ensure contextual correctness. Many platforms rely on assumptions of stable baselines, uniform data semantics, or predictable operational patterns-conditions that rarely hold in dynamic, heterogeneous environments.

The analysis reveals that adaptive models are highly sensitive to concept drift, data sparsity, schema divergence, and inconsistent enrichment, which collectively undermine long-term analytical reliability. The integration of diverse data sources introduces additional challenges: normalization discrepancies, ontology misalignment, and cross-component dependencies often lead to analytical incoherence. Even advanced knowledge-driven or federated approaches struggle with non-uniform data distributions, labeling inconsistencies, and the operational overhead of maintaining synchronized model states.

Experimental research of the methods and tools for automatic updating of threat detection models in computer systems

When evaluating the efficency of information technology systems in processing security data, it becomes evident that performance depends on a synergy of qualities designed to identify complex patterns and anomalies. In the modern landscape of cybersecurity, a truly capable IT system must not only detect known threats but also update its analytical models quickly and continuously to maintain accuracy as attack vectors evolve. To empirically validate the current state of detection technologies, a comprehensive comparative analysis was conducted focused on three critical performance indicators: operational speed, detection accuracy, and false alarm minimization.

The response latency was measured to assess the system's applicability in real-time environments, as every millisecond of delay can lead to data loss in high-speed networks. As illustrated in Figure 3, a distinct performance gap exists between traditional and modern architectures. While traditional signature-based methods were historically considered fast, the data shows they now exhibit the highest latency at 120 ms, likely due to the "database bloat" phenomenon where the sequential scanning of millions of known signatures creates significant computational bottlenecks. In contrast, Hybrid Systems and Graph-based approaches demonstrated superior processing speeds, achieving average response times of 55 ms and 60 ms respectively, proving that modern architectural combinations can handle data flows much more efficiently than rigid database scanning.

The system's ability to correctly identify genuine threats, known as the True Positive Rate (TPR), was evaluated. A high TPR is paramount for ensuring that sophisticated, polymorphic, or zero-day attacks do not bypass the security perimeter. As shown in Figure 1, traditional signature-based methods demonstrated a critical lack of effectiveness with only 50% accuracy, confirming that static pattern matching is virtually useless against evolving threats. Conversely, Hybrid Systems led the performance with a 90% detection rate, followed closely by Graph-based methods at 85%, highlighting that combining multiple analysis layers is essential for detecting complex anomalies that miss a single-method filter.

The True Negative Rate (TNR) was analyzed to measure system specificity, which ensures that legitimate user traffic is not erroneously blocked. As presented in Figure 2, signature-based methods demonstrated their only remaining competitive advantage by achieving the highest specificity at 99.0%, ensuring minimal false positives. While Hybrid and Graph-based systems performed well, achieving 96.0% and 97.0% respectively, they still lag slightly behind the strict stability of signatures, creating a potential risk of "alert fatigue" where analysts are overwhelmed by false alarms.

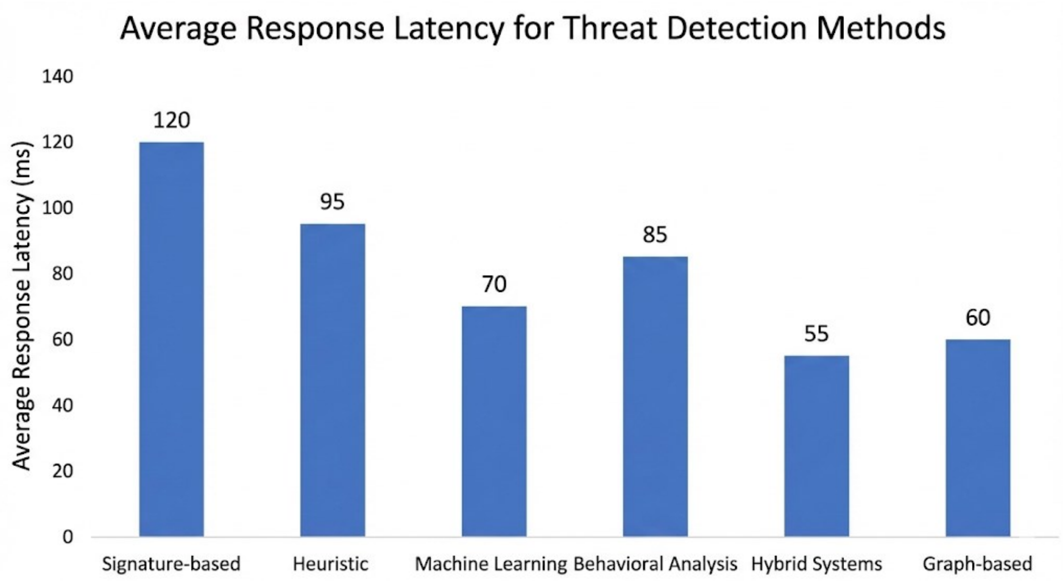

Fig. 1. Average response time for threat detection methods

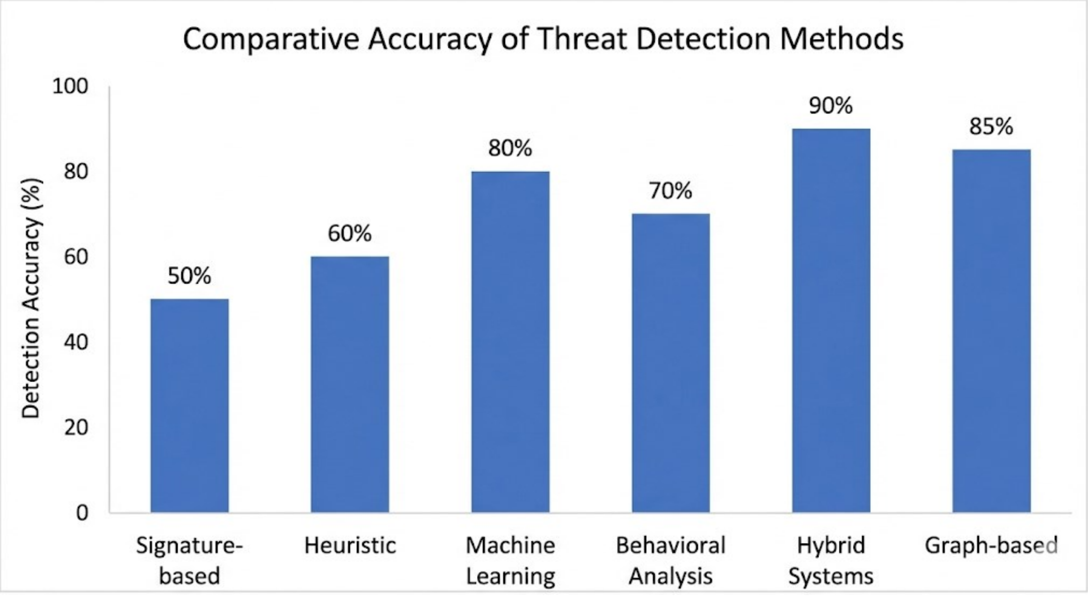

Fig. 2. Detection accuracy

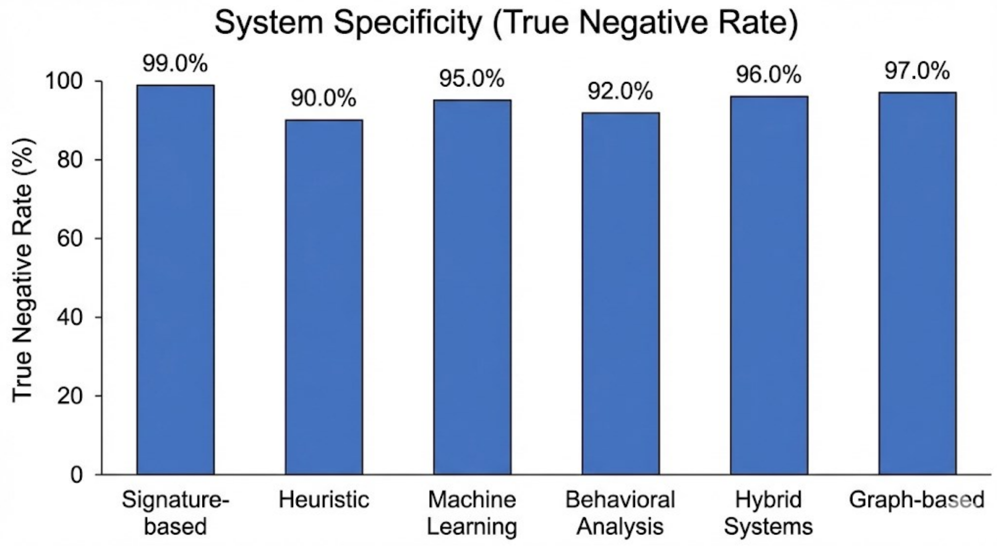

Fig. 3. System specificity

Conclusions

The conducted analysis demonstrates that modern information technologies for automatic updating of analytical models in computer systems have reached a high level of conceptual maturity, yet they remain constrained by several systemic limitations that prevent them from fully meeting the requirements of contemporary large-scale information environments. The comparative evaluation of methodological approaches using the criteria of latency, complexity, reliability, functionality, and maintainability reveals that no existing class of methods provides a balanced and sustainable solution capable of supporting continuous adaptation in dynamic and heterogeneous computational infrastructures.

Traditional static and rule-based approaches, despite their simplicity and low computational demands, lack the flexibility required to operate effectively in environments characterized by rapid structural and behavioral change. Their high latency and limited functional scope make them unsuitable for systems that must adjust in real time. Heuristic and hybrid heuristic methods introduce greater adaptability, yet their instability under varying workloads and sensitivity to data fluctuations reduce overall reliability. These methods often require frequent recalibration, which complicates long-term maintenance in distributed settings.

Meta-heuristic and nature-inspired optimization techniques demonstrate strong scalability and the ability to fine-tune analytical models across diverse datasets. However, their high algorithmic complexity and substantial resource requirements limit their applicability in constrained or heterogeneous infrastructures. Machine-learning-based approaches offer broader functional capabilities and support continuous learning, but they depend heavily on large, representative datasets and require ongoing retraining to maintain accuracy. This creates significant operational overhead and reduces maintainability, especially when data distributions shift unpredictably.

Behavioral and dynamic analytical methods provide valuable insights into system processes and user interactions, yet their narrow specialization restricts their general applicability. Maintaining synchronized behavioral baselines across distributed nodes is resource-intensive, and even minor deviations in normal system activity may necessitate extensive recalibration. As a result, these methods struggle to achieve stable performance in large, heterogeneous environments.

The synthesis of these findings indicates that the primary challenge lies not in the absence of effective analytical techniques but in the lack of an integrated framework capable of unifying adaptability, scalability, interpretability, and automated updating within a single architectural paradigm. Existing methods tend to optimize individual criteria while compromising others: approaches with low latency often lack functionality, highly functional models exhibit excessive complexity, and methods with strong adaptability impose heavy maintenance burdens.

The development of next-generation information technologies requires a shift toward architectures that combine continuous learning, structural self-organization, and coordinated updating across distributed nodes. Such systems must be capable of autonomously recalibrating analytical models, integrating heterogeneous data streams, and maintaining stable performance despite fluctuations in workload, data quality, and system topology. Achieving this balance will enable information infrastructures to operate more efficiently, remain resilient to ongoing change, and support long-term scalability without relying on outdated static mechanisms.

The future research will be devoted to the development of an integrated, multi-layer information technology for automated updating of analytical models in large-scale computer systems, designed specifically to overcome the identified trade-offs between latency, adaptability, scalability, interpretability, and maintainability. The research will focus on creating a unified architectural paradigm that enables continuous model evolution under dynamic workloads, heterogeneous data streams, and changing system topology, while preserving predictable quality of service and minimizing operational overhead. The research has to be concentrated on the formulation of a formal architectural framework for distributed analytical model updating. This includes defining a reference architecture that separates concerns into coordinated layers: a data acquisition and harmonization layer responsible for collecting and normalizing heterogeneous telemetry and domain data; an edge-level model adaptation layer that performs low-latency incremental updates close to data sources; a global coordination layer that ensures consistency, stability, and policy enforcement across distributed nodes; and a lifecycle governance layer that provides monitoring, auditability, rollback mechanisms, and explainability. For each layer, the research will specify interfaces, control signals, required metadata, and performance constraints, enabling reproducible deployment across diverse infrastructures (cloud, edge, IoT, and hybrid cluster environments).

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

For research articles with several authors, a short paragraph specifying their individual contributions must be provided. The following statements should be used “Conceptualization, O.A. and T.I.; methodology, O.A. and T.I.; software, T.I.; validation, O.A. and T.I.; formal analysis, T.I.; investigation, T.I.; resources, T.I.; data curation, T.I.; writing - original draft preparation, T.I.; writing - review and editing, T.I.; visualization, T.I. and O.A..; supervision, O.A.; project administration, O.A.; funding acquisition, T.I. All authors have read and agreed to the published version of the manuscript.

DECLARATION ON THE USE OF GENERATIVE ARTIFICIAL INTELLIGENCE TOOLS

In preparing this work, the authors used Grammarly for: grammar and spelling checks. After using this service, the authors reviewed and edited the content and take full responsibility for the content of this publication.

REFERENCES

1. Kashtalian Antonina, Serhii Lysenko, et al. "Control and Decision-Making in Deceptive Multi-Computer Systems Based on Previous Experience for Cybersecurity of Critical Infrastructure." *Applied Sciences* Vol 15 P. 12286.

2. Denysiuk Dmytro, Oleg Savenko, Sergii Lysenko, Bohdan Savenko, Andrii Nicheporuk. "Detecting software implants using system decoys." (2024).

3. Bokhonko Oleksandr, Sergii Lysenko, Piotr Gaj. "Development of the social engineering attack models." (2024).

4. Yang, Xiaodong. "Efficient and security-enhanced certificateless aggregate signature-based authentication scheme with conditional privacy preservation for VANETs." *IEEE Transactions on Intelligent Transportation Systems* 25.9. 2024 P. 12256-12268.

5. LaRocque Anthony. Effective ransomware detection using autonomous patternbased signature extraction. 2024. P. 1-12

6. Rehman, Fazalur, Farhan Mushtaq, Hafsah Zaman. "A Host-based Intrusion Detection: Using Signature-based and AI-driven Anomaly Detection for Enhanced Cybersecurity." *2024 4th International Conference on Digital Futures and Transformative Technologies (ICoDT2)*. IEEE, 2024. P. 1-7.

7. Loaiza, Carlos. Dynamic temporal signature analysis for ransomware detection using sequential entropy monitoring. *Authorea Preprints.* 2024. P. 30-45.

8. Kalla, Dinesh. Investigating the Impact of Heuristic Algorithms on Cyberthreat Detection. In: *2024 2nd International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT)*. IEEE, 2024. p. 450-455.

9. Taylor, Theodore. Dynamic anomaly-driven detection for ransomware identification: An innovative approach based on heuristic analysis. *Authorea Preprints*, 2024. P. 1-5.

10. Yunmar, Rajif Agung. Hybrid Android malware detection: A Review of heuristic-based approach. *IEEe Access*, 2024, 12. P. 41255-41286.

11. Novak, Pavel, OUJEZSKY, Vaclav. Heuristic malware detection method based on structured cti data: A research study and proposal. In: *2024 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*. IEEE, 2024. p. 1-6.

12. Hu, Wengui. A deep analysis of nature-inspired and meta-heuristic algorithms for designing intrusion detection systems in cloud/edge and IoT: state-of-the-art techniques, challenges, and future directions. *Cluster Computing*, 2024, 27.7. P. 8789-8815.

13. More, Sanjana A., KACHAVIMATH, Amit V. SDN Intrusion Detection using Meta-Heuristic Optimization and K-Nearest Neighbors Classifier. *Procedia Computer Science*, 2025, 260. P. 1137-1144.

14. Fuller, Richard. A novel hybrid machine learning approach for real-time ransomware detection using behavior-driven heuristic features. 2024. P. 120-125

15. Okoli, Ugochukwu Ikechukwu. Machine learning in cybersecurity: A review of threat detection and defense mechanisms. *World Journal of Advanced Research and Reviews*, 2024, 21.1. P. 2286-2295.

16. Kumar, Busireddy Hemanth. Big Data in Cybersecurity: Enhancing Threat Detection with AI and ML. *Metallurgical and Materials Engineering*, 2025, 31.3. P. 12-20.

17. Mohammed, Anwar. Transforming SOC Operations: Harnessing the Power of AI and ML for Enhanced Threat Detection. *INTERNATIONAL JOURNAL OF RESEARCH CULTURE SOCIETY Monthly Peer-Reviewed, Refereed, Indexed*, 2024. P. 8.

18. Katiyar, Nirvikar. AI and Cyber-Security: Enhancing threat detection and response with machine learning. *Educational Administration: Theory and Practice*, 2024, 30.4. P. 6273-6282.

19. Marimuthu, Oviya, RAVI, Priyadharshini, JANARTHANAN, Senthil. Application of AI and ML in Threat Detection. *Protecting and Mitigating Against Cyber Threats: Deploying Artificial Intelligence and Machine Learning*, 2025. P. 29.

20. Alzaabi, Fatima Rashed, MEHMOOD, Abid. A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. *IEEE Access*, 2024, 12. P. 30907-30927.

21. Mizanur, Mohammad. Machine Learning-Based Anomaly Detection for Cyber Threat Prevention. *Journal of Primeasia*. 2025, 6.1. P. 1-8.

22. Subrahmanyam, Satya. Behavioral Analysis for Threat Detection. In: *Handbook of AI-Driven Threat Detection and Prevention*. CRC Press, 2025. P. 95-115.

23. Ozturk, Mehmet. Dynamic behavioural analysis of privacy-breaching and data theft ransomware. 2024.

24. Blowing, Adam. Performing ransomware detection through predictive behavioral mapping to autonomous threat identification. 2024. P. 7.

25. Shanks, Gene. Innovative framework for ransomware detection using adaptive cryptographic behavior analysis. 2024. P. 10-14.

26. Microsoft Defender for Endpoint. URL: https://www.microsoft.com/en-us/security/business/endpoint-security/microsoft-defender-endpoint?msockid=382eb02bfecb63240938a310ffd9621e .

27. CrowdStrike Falcon. URL: https://www.crowdstrike.com/en-us/platform/ .

28. Cortex XDR. URL: https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-5.x-Documentation/What-is-Cortex-XDR .

29. Darktrace Platform: https://www.darktrace.com/ .

30. Elastic Security Platform. URL: https://www.elastic.co/security .

31. IBM Qradar. URL: https://www.ibm.com/products/qradar .

32. Google Chronicle. URL: https://cloud.google.com/blog/products/identity-security/introducing-the-unified-chronicle-security-operations-platform/ .

33. Splunk Enterprise Security. URL: https://www.splunk.com/en_us/products/enterprise-security.html .

34. SentinelOne Singularity. URL: https://www.sentinelone.com/platform/singularity-complete/ .

35. Cisco SecureX. URL: Introducing SecureX - Cisco Blogs .

36. Fortinet FortiEDR. URL: https://www.fortinet.com/products/endpoint-security/fortiedr .

37. Sophos Intercept X. URL: https://www.sophos.com/en-us/products/mobile-control/intercept-x .

38. Trend Micro Apex One. URL: Apex One and Apex Central are now available .

39. Trellix MVISION. URL : https://techdirectarchive.com/2025/08/12/how-to-install-trellix-mvison-endpoint/.

40. Rapid7 InsightIDR. URL: https://www.rapid7.com/products/siem/ .

41. Sumo Logic Cloud SIEM. URL: https://www.sumologic.com/solutions/cloud-siem .

42. Zeek Overview. URL: https://zeek.org/ .

43. Suricata Homepage. URL: https://suricata.io/ .

44. Wazuh Platform. URL: https://wazuh.com/ .

45. MISP Platform. URL: https://www.misp-project.org/ .

46. OpenCTI. URL: https://docs.opencti.io/latest/ .

47. YARA Rules. URL: https://github.com/Yara-Rules/rules .

48. Bokhonko Oleksandr, Atamaniuk Olha. Method for synthesis of a scalable architecture of a distributed cs, resistant to social engineering attacks. *Computer Systems and Information Technologies*. Vol. (4). P. 60–76. 2025

Тимур ІСАЄВ, Ольга АТАМАНЮК
Хмельницький національний університет

АНАЛІЗ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ АВТОМАТИЧНОГО ОНОВЛЕННЯ МОДЕЛЕЙ ВИЯВЛЕННЯ ЗАГРОЗ В КОМП'ЮТЕРНИХ СИСТЕМАХ

Розробка інтелектуальних адаптивних інформаційних технологій для автоматичного оновлення моделей виявлення загроз у комп'ютерних системах є одним з найважливіших напрямків сучасних досліджень в галузі інформаційних технологій. Сучасні комп'ютерні системи функціонують у середовищах, що постійно змінюються під впливом нового програмного *забезпечення, розвитку апаратного забезпечення та різноманітних методів обробки даних. Традиційні статичні підходи, що базуються на фіксованих правилах або заздалегідь визначених моделях, часто швидко застарівають і не забезпечують необхідної адаптивності.*

Існуючі підходи до виявлення в комп'ютерних системах були ретельно вивчені, і хоча вони дають цінну інформацію, вони також демонструють явні обмеження. Методи, засновані на сигнатурах, сильно залежать від відомих шаблонів і тому мають труднощі з ідентифікацією нових або несподіваних явищ. Евристичний аналіз дозволяє ширше узагальнювати, але часто пов'язаний з високим рівнем помилкових спрацьовувань, що знижує його практичну корисність. Моніторинг поведінки дозволяє фіксувати динамічні зміни в діяльності системи, але вимагає значних обчислювальних ресурсів і може уповільнювати роботу. Моделі машинного навчання забезпечують адаптивність і здатність навчатися на основі даних, але вимагають великих обсягів навчальної інформації та ретельного налаштування для уникнення помилок. Гібридні підходи намагаються поєднати сильні сторони декількох технік, але часто стикаються з труднощами в безперебійній інтеграції та оптимізації в рамках існуючих інфраструктур.

Через ці обмеження дослідники все більше зосереджуються на розробці фреймворків, що включають механізми автоматичного оновлення. Такі фреймворки розроблені як самоадаптивні, тобто вони можуть постійно розвиватися у відповідь на нові умови без необхідності ручного втручання. Адаптація в режимі реального часу є центральною особливістю цих систем, що дозволяє їм підвищити точність, зменшити кількість помилкових спрацьовувань та оптимізувати використання обчислювальних ресурсів.

Завдяки інтеграції інтелектуальних механізмів оновлення інформаційні інфраструктури можуть досягти вищого рівня стабільності та ефективності. Це не тільки підвищує загальну продуктивність комп'ютерних систем, але й гарантує, що вони залишатимуться актуальними та ефективними в середовищах, де зміни відбуваються постійно. Здатність до автоматичної еволюції, без залежності від застарілих статичних методів, робить ці технології основою майбутнього розвитку інформаційних систем.

Постійна еволюція обчислювальних середовищ вимагає рішень, які є гнучкими, інтелектуальними та здатними до адаптації в режимі реального часу. Використовуючи адаптивні фреймворки, дослідники та розробники можуть створювати системи, які є не тільки більш точними та ефективними, але й більш стійкими та масштабованими. Це є вирішальним кроком на шляху до комп'ютерних систем наступного покоління, де адаптивність та автоматизація є необхідними для довгострокової надійності та успіху.

Ключові слова: комп'ютерні системи, виявлення загроз, машинне навчання, інформаційні технології, автоматичне оновлення