Qassim University جامعة القصيم

JEIT

Journal of Emerging and Innovative Technologies

Volume 1, Issue 1
July–December 2026

Received
12 September 2026

Accepted
29 October 2026

Published
05 November 2026

DOI
https://doi.org/10.71422/jeit.0002

License
CC BY-NC-SA 4.0

Cite this article

Khan AW, Alghashim BSF, Alharb MKN, Alghomiz TSA, Alshrahrani FFM, Almsaad FSF. Artificial Intelligence and Machine Learning in Cyber Threat Detection for Modern Organizations: A Systematic Review of Challenges and Solutions. J Emerg Innov Technol. 2026;1(1):1–21.

Journal website

Review article

Artificial Intelligence and Machine Learning in Cyber Threat Detection for Modern Organizations: A Systematic Review of Challenges and Solutions

Abdul Wahid Khan[1,*], Bassam Saleh F Alghashim[1], Meshari Khalid N Alharb[1], Tamim Sulaiman A Alghomiz[1], Faisal Fahad M Alshrahrani[1], Faisal Saud F Almsaad[1]

[1] Department of Computer Science, College of Engineering and Information Technology, Onaizah Colleges, Qassim, Saudi Arabia

*Corresponding author: wahidkn@gmail.com

Abstract

The ability to adapt to threats using AI and ML techniques has become a major factor in the fight against cyber threats, offering a data-driven, adaptive approach to threat detection that transcends signature-based methods. With the growing surge of research and development on AI/ML-based intrusion detection, however, there has been disarray in the perception of the challenges which organizations are facing and the solutions available to them to tackle the challenges. This paper is based on a systematic literature review (SLR) carried out following the Kitchenham SLR protocol and a PICOC search strategy, and the analysis of 45 peer-reviewed and industry-reported studies related to the application of AI/ML for cyber threat detection. In total, the corpus identified 271 different challenges and 252 solutions, which were grouped into seventeen recurring categories of challenges. The biggest challenges to successful adoption were zero day and novel attack detection (36), scalability and big data (34), high false positive/negative rates (33), computational and resource constraints (32), and dataset imbalance (31), followed by outdated datasets, privacy and regulatory compliance, explainability, and high dimensional feature spaces. The comparison on the continental level also identified the scalability and IoT-based detection as the main challenge in Asia, privacy and explainability as the primary challenge in Europe, adversarial robustness and enterprise security as the main challenge in North America and foundational infrastructure and capacity limitations as the main challenge in the Middle East/Africa. The findings indicate a trajectory towards more hybrid, adaptive, and privacy-conscious approaches to AI security that integrate ensemble and deep learning techniques, federated learning, explainable AI, and ongoing training pipelines. This research work highlights the severity of challenges faced by the future organisations in implementation of AI/ML for cybersecurity intrusion detection.

Keywords: Artificial Intelligence; Machine Learning; Systematic Literature Review; Cybersecurity Challenges; Solutions; Modern Organisations.

1. Introduction

It is observed that cyber-attack chance for modern organisations going to expand due to vast interconnected system, cloud-based framework and huge number of data.

© 2026 The Author(s). Published by Qassim University under CC BY-NC-SA 4.0.

The older approach of cybersecurity is highly ineffective against the emerging method like zero day attacks and advanced persistent threats [1, 2]. The cybersecurity needs the fresh approach of AI and ML concepts. The latest system needs to learn and adapt to new threat manners in real-time using AI and ML techniques [2]. These approaches are using constantly for various threats detection and security technologies but it also craft new hurdles like adversarial manipulation, algorithmic bias and low transparency [3, 4].

The confidentiality, integrity and availability of data are compromised due to internet of things (IoT), Industrial control systems (ICS) and digital twins that are interconnected. With the recent developments in deep learning, anomaly detection and automatic threat identification have gained significant boost [2] [6] however, explainability and trustworthiness are still essential requirements for the deployment of deep learning technologies in the real world [5] [7]. Explainable Artificial Intelligence (XAI) is therefore proving to be a critical enabler in enhancing transparency and compliance in AI-powered cybersecurity solutions [7].

The Intrusion Detection System is still the cornerstone of defense strategies and in modern systems, it is distinguished between normal and malicious behaviour as either misuse-based or anomaly-based detection; anomaly-based detection is especially important for detecting zero-day attacks [1], [6], [8]. Although the problems of spatiotemporal feature extraction and data imbalance are solved by deep learning approaches in complex network environments [9], the reliability of real-world applications is still limited because of the ageing datasets and the high rate of false-positive [1]. Adversarial machine learning (AML) against AI-based systems in critical infrastructure remains a problem to spur the creation of standardized taxonomies and mitigation strategies [3-4]. IDS solutions, built with the help of machine learning (ML), still fail to be generalized for industrial control systems (ICS) [10].

The organisations need to dig out some of the latest hurdles in advance as the regime is changed with the entry of AI and ML. The new challenges are quality of data, biasness of algorithm, lack of model explainability, old system integration, regulatory and ethical restrictions for these issues. This study focused to understand these issues in a general way and proposed the solutions for these challenges as identified from the literature to improve cyber security capability [11-13].

The current statistics of industry are enough to understand the enormousness of this obstacle. There are 69% of risks for small medium enterprises (SMBs) as they faced cyberattack in the last year. Moreover, 80% of SMBs not practicing Privileged Access Management solutions and 60% of enterprises constantly using cybersecurity methods like credential managers, two steps of factor authentication and training of cybersecurity awareness [14]. This concern gone high due to shift to remote and hybrid works: business report shows that 72% concerned about security risk; cybersecurity professional report that 80% security threats boost sine 2020 [14]. The trends reflect how critical it is to grasp the practicality of threat detection implementation via AI and ML models and who should do it.

This is a systematic literature review of 45 studies on the use of AI/ML in cyber threat detection that builds upon a previous structured literature protocol to produce a complete evidence synthesis. Specific goals are: (i) Identification of the key challenges that are technical, organizational and ethical in relation to threat detection using AI/ML; (ii) Collecting the solutions and best practices presented in the literature to address the challenges; (iii) Ranking the challenges by frequency of occurrence in the corpus to distinguish between critical challenges and less critical challenges; and (iv) Exploring the variation of challenge profiles and research emphases across geographic regions. The rest of this paper is organised

© 2026 The Author(s). Published by Qassim University under CC BY-NC-SA 4.0.

as follows. The conceptual background is provided in Section 2. Research Methodology is discussed in section 3. Results are reported in Section 4 as data extracted was in tabular format. Findings and implications are discussed in section 5. The paper is completed in section 6, and the limitations of the paper are discussed in section 7.

2. Background

2.1 Artificial Intelligence and Machine Learning

Artificial Intelligence (AI) and Machine Learning (ML) are at the core of modern information systems through enabling automated decision making, pattern recognition and intelligent data analysis. Artificial Intelligence (AI) is the ability of a computer system to replicate human intelligence such as reasoning, learning and problem-solving. Machine Learning is one of the major branches of AI which deals with the system using historical data and learning from it without being explicitly programmed. It is usually categorized into supervised learning, unsupervised learning and reinforcement learning. Supervised learning is done on labeled data to classify and predict, whereas unsupervised learning is used to discover hidden patterns and anomalies in unlabeled data. This enables systems to learn to optimize their action through interaction with changing environments using reinforcement learning.

2.2 Cybersecurity and Cyber Threats

In cybersecurity the main focus is to protect computer systems, digital appliances from intruders and cyberattack. Cybersecurity became a pillar due to huge dependencies of organisations on digital framework. In today, cybersecurity infrastructure we encapsulate preventive, detective and responsive methods to overcome on all types of cyber-attacks [15]. A cyber-attack is an attempt to exploit a weakness in technology, computers, or networks that are digital in nature with the goal of causing harm to the victim, whether that's in the form of malware, phishing, ransomware, insider threats, denial-of-service attacks, or advanced persistent threats. The attackers keep changing their techniques aided by automation, social engineering and zero day exploits. In this scenario, static signature based defense is not enough.

2.3 Cyber Threat Detection and Intrusion Detection Systems

Cyber threat detection is the identification of unusual activities and security breaches in information systems. IDSs are widely deployed to monitor the network traffic and the system behavior, and can be broadly divided into two types: network-based (NIDS) and host-based (HIDS). Traditional detection methods are based on signature-based and rule-based methods. These approaches work well for known attacks but lack the power to deal with new and emerging threats. For this, machine learning detection models have been suggested by many to increase the adaptability, accuracy and real-time analysis [16].

2.4 AI and ML in Cyber Threat Detection

The security operations for cyber threat in today age are incomplete without use of AI and ML practices. To monitor the various weakness and apprehensive activity is possible by using ML-based model that make it possible in real time by meting out massive amounts of network traffic, system logs and user behavior patterns. The automatic danger classification, anomaly scoring, and predictive risk assessment, minimizing false positives and improving security procedures center situational awareness can assist by AI-powered detection system [17]. Although the advantages are substantial, the procedural and executive trials cover data disparity, limited accessibility of labeled data, and the quality

© 2026 The Author(s). Published by Qassim University under CC BY-NC-SA 4.0.

of the data, which can hamper the preparation and recital of AI detection systems. Alternative trial is system limpidity, as many ML models are deliberated “black boxes”, leading to lower assurance of the users and making it tough to meet controlling requirements, and adversarial attacks like data poisoning and ducking can affect the learning process and conciliation system sturdiness.

2.5 Emerging Solution Directions

Some practices that give the solution of these challenges suggested in the current studies. Explainable Artificial Intelligence (XAI) advances limpidity by giving an interpretable awareness on model behavior to help analyst decision-making and controlling audit. It enables collaborative model training while maintaining privacy and adherence to regulations between organisations, through federated learning. Furthermore, hybrid learning models, data balancing methods and blockchain-based security architectures enhance security and data integrity [18]. All these emerging areas point toward a suite of lightweight, ethical, and real-time AI-driven security solutions that balance performance, explainability and resilience. In the rest of this paper these themes are examined in a systematic manner, as they are also presented in the tabular format presented in the data extraction part.

2.6 Related Work and Research Gap

Over the last 10 years, research on artificial intelligence and machine learning within the domain of cybersecurity has increased tremendously. Buczak and Guven [14] gave one of the first surveys on the use of data mining and ML techniques for intrusion detection. They talked about supervised and unsupervised methods of detecting anomalies in the network. Shone et al. in [16] tried to extend the above work by introducing a deep learning based intrusion detection system using stacked autoencoders with a higher classification accuracy than the traditional classifiers. Kim et al. [23] was interested in the idea of deep neural networks for the detection of complex attack patterns from massive network traffic. At the same time, several researchers have highlighted the shortcomings of this advancement, with Sommer and Paxson [15] stating that many models trained in the ML world fail to achieve good results in the real world because of unrealistic expectations regarding the quality and availability of the data, and Biggio and Roli [17] formalizing adversarial machine learning, where they showed how adversarial attacks can be based on manipulation of the training data and/or exploiting model weaknesses to evade detection. Recent research has been directed towards addressing the lack of transparency faced by ML based security systems, with Explainable AI (XAI) gaining significant focus. To encourage human trust and decision making in automated systems, Ribeiro et al. [18] suggested model-agnostic explanation techniques. Gartner and IBM Security industry reports also highlight the importance of pairing AI with human intelligence and organisational governance structures [19-22].

This collection of literature demonstrates the technical progress in AI/ML detection models, but there is limited literature that systematically brings together the organisational, ethical and operational issues and limitations. The majority of current research is oriented towards enhancing detection accuracy and explained by the lack of concern for explainability, regulations, workforce readiness or integration with existing security infrastructure. No single source that has gathered the frequency of challenges and solutions from a massive, recent and multi-regional collection of studies. This review aims to fill this gap by providing a framework for solutions and a systematic literature review protocol with a thematic frequency analysis of 45 publications, including technical, organizational and governance approaches, further broken down by geographic region (Section 4.3).

© 2026 The Author(s). Published by Qassim University under CC BY-NC-SA 4.0.

3. Research Methodology

This study follows the systematic literature review (SLR) protocol proposed by Kitchenham [13], which structures an SLR into three phases: planning, conducting, and reporting, and ensures a transparent and reproducible research process. The protocol was developed with reference to established SLR practice in software and systems engineering [11], [12].

3.1 Research Objectives

The research methodology was designed to satisfy the following objectives:

- To identify the key technical, organizational, and ethical challenges in implementing AI and ML for threat detection in modern organizations.
- To analyze the most commonly proposed solutions and best practices reported in the literature.
- To evaluate the effectiveness of AI and ML approaches relative to traditional threat detection methods.
- To develop a structured, evidence-based framework for guiding organizations in adopting AI- and ML-based cybersecurity solutions.

3.2 Research Questions

RQ1. What are the primary challenges that modern organizations face when implementing AI- and ML-based threat detection systems?

RQ2. What technical and organizational solutions are most frequently recommended in the literature to address these challenges?

3.3 Search Strategy

Search strings were developed using the PICOC framework (Population, Intervention, Comparison, Outcome, Context), aligned with RQ1 and RQ2:

- Population (P): Modern organizations, enterprises, companies, IT environments, cloud and hybrid infrastructures.
- Intervention (I): Artificial Intelligence, Machine Learning, Deep Learning, AI-based security, ML-based threat detection.
- Comparison (C): Traditional detection systems, signature-based detection (optional).
- Outcome (O): Challenges, solutions, effectiveness, accuracy, scalability, explainability, adoption.
- Context (C): Cybersecurity, threat detection, intrusion detection systems, network security, cloud security.

3.3.1 Keyword Identification

Primary keywords and their synonyms were grouped into five categories to support systematic search-string construction:

- AI/ML terms: “Artificial Intelligence,” “Machine Learning,” “Deep Learning,” “AI-based,” “ML-based.”
- Threat detection terms: “threat detection,” “intrusion detection,” “anomaly detection,” “cyber attack detection.”

© 2026 The Author(s). Published by Qassim University under CC BY-NC-SA 4.0.

- Challenge terms: challenges, limitations, barriers, risks, issues, privacy, bias, adversarial.
- Solution terms: solutions, mitigation, best practices, strategies, framework, governance.
- Organizational context terms: organization*, enterprise*, company*, “modern organization*,” cloud, hybrid.

3.3.2 Boolean Search Strings

Three Boolean search strings were constructed: two aligned with the individual research questions and one combined query used for broader corpus retrieval.

Search String 1 — RQ1 (Challenges):

("Artificial Intelligence" OR "Machine Learning" OR "Deep Learning" OR "AI-based" OR "ML-based") AND ("threat detection" OR "intrusion detection" OR "anomaly detection") AND (challenges OR limitations OR barriers OR risks OR issues OR adversarial OR privacy) AND (organization* OR enterprise* OR cloud OR hybrid)

Search String 2 — RQ2 (Solutions):

("Artificial Intelligence" OR "Machine Learning" OR "Deep Learning" OR "AI-based" OR "ML-based") AND ("threat detection" OR "intrusion detection" OR "cyber attack detection") AND (solutions OR mitigation OR "best practices" OR strategies OR framework OR governance) AND (organization* OR enterprise* OR cloud OR hybrid)

Search String 3 — Combined (RQ1 + RQ2):

("Artificial Intelligence" OR "Machine Learning" OR "Deep Learning" OR "AI-based" OR "ML-based") AND ("threat detection" OR "intrusion detection" OR "anomaly detection" OR "cyber attack detection") AND (challenges OR limitations OR barriers OR risks OR issues OR solutions OR mitigation OR "best practices" OR strategies OR framework OR governance) AND (organization* OR enterprise* OR cloud OR hybrid)

3.3.3 Database-Specific Adaptation

The search strings were adapted for database-specific syntax across four academic sources:

- IEEE Xplore: quotation marks applied, with search restricted to Abstract and Index Terms fields.
- Scopus / SpringerLink: TITLE-ABS-KEY search with wildcard (*) truncation.
- Google Scholar: simplified query forms used to accommodate query-length limits.

Example (Scopus format): TITLE-ABS-KEY(“Artificial Intelligence” OR “Machine Learning” OR “AI-based” AND “threat detection” OR “intrusion detection” AND challenges OR solutions AND organization).

3.3.4 Validation of Search Strings

A pilot search was conducted in IEEE Xplore and Google Scholar to verify that the search strings returned relevant and sufficient results. Strings were iteratively refined based on:

- Volume of results retrieved.
- Relevance of the top 20 articles returned.
- Presence of peer-reviewed and high-impact sources.

© 2026 The Author(s). Published by Qassim University under CC BY-NC-SA 4.0.

3.4 Inclusion and Exclusion Criteria

Studies were encompassed if they:

IC-1: addressed the application of AI/ML in cybersecurity, explicitly threat detection;

IC-2: were peer-reviewed journal articles, conference papers, or credible industry/technical reports;

IC-3: were published in English;

IC-4: explicitly identified challenges and proposed solutions or best practices; and

IC-5: addressed organizations across varied geographical contexts.

Studies were excluded if they:

EC-1: did not directly address AI/ML applications in cybersecurity;

EC-2: were non-peer-reviewed sources such as blog posts or unrefereed white papers;

EC-3: duplicated findings already captured by another included study;

EC-4: discussed generic cybersecurity measures unrelated to AI/ML; or

EC-5: lacked sufficient detail on challenges and solutions.

3.5 Study Selection, Quality Assessment, and Data Extraction

After the title/abstract screening and full-text assessment of inclusion and exclusion criteria listed above, 45 studies were selected for the synthesis. Using a structured data extraction form, each study was systematically documented for: study identification (authors, year of publication), origin of the study (country/region), publication venue, challenges identified to address AI/ML in cybersecurity, proposed solutions/good practices, results and conclusions. Iterative thematic coding of extracted challenges and solutions led to a common set of challenges subsumed into the following categories: challenges were then tabulated by frequency of each challenge category across the 45 studies, providing a severity rank. Challenge categories with a frequency of occurrence between 22 and 36 (appeared in about 50% or more of the reviewed studies) were considered critical and categories with a lower frequency were considered less critical but still relevant. A continent-wise comparison was also conducted to compare the variation of challenges and solution emphases across the continents of Asia, Europe, North America and Middle East and Africa. The resulting synthesis is reproduced in the same table format as was used for extraction and analysis in Section 4.

4. Results

The 45 studies in this review reported a total of 271 problems and 252 solutions for the use of AI/ML in cyber threat detection. These extracted items were consolidated with a thematic approach to obtain seventeen recurring challenge categories. The consolidated challenge–solution mapping is reproduced in Table 1 in the same form as it appeared in the data extraction process: each row represents a consolidated challenge and its description, the consolidated solutions proposed in the literature, the identifiers of the papers that contributed to the consolidated challenges, and the count of how many studies the consolidated challenge/solution occurred in (Section 4.1, landscape orientation). As per the review protocol, those categories that are seen to occur between 22 and 36 times are considered as the critical category; the other categories are considered less critical but relevant in specific organizations.

© 2026 The Author(s). Published by Qassim University under CC BY-NC-SA 4.0.

Table 2 shows the challenge/solution profile of every individual paper and Table 3 shows the continent-wise comparison of the challenges, root causes and solution emphasis of the papers.

4.1 Consolidated Challenge–Solution Table (n = 45 papers)

Table 1. Consolidated challenges, descriptions, solutions, contributing paper IDs, and frequency

S. No	Consolidated Challenge	Description	Consolidated Solutions	Paper IDs	Freq (45)
1	**Zero-Day & Novel Attack Detection**	Difficulty in detecting previously unknown, polymorphic, stealthy, and emerging attacks because conventional signature-based/ML approaches mainly depend on known attack patterns.	The use of Hybrid IDS and Open Set Recognition can improve the detection of unknown and previously unseen attacks. The assumption of Deep Learning techniques such as CNN, LSTM, and DAE can advance the identification of complex, polymorphic, and stealthy attacks. The presentation of unsupervised anomaly detection can relief detects novel attacks without reliant entirely on formerly known attack signatures. The execution of adaptive retraining can assist the IDS to continuously adapt to evolving attack patterns and shrink the impact of zero-day attacks.	02, 04, 05, 07, 10, 12, 13, 14, 16, 17, 18, 19, 20, 21–32, 33, 34, 35, 36, 37, 40, 42, 43, 44, 45	**36**
2	**High False Positives / False Negatives**	Incorrect classification of legitimate activities as attacks or actual attacks as normal, resulting in alert fatigue, healthcare risks, and excessive workload for ICS operators.	The use of Collective ML techniques can advance classification reliability and shrink incorrect attack classifications. The application of hyper parameter modification can optimize model performance and help achieve a better balance between false positives and false negatives. The unification of context-aware detection can improve alert assessment by considering the operational context of detected activities. The implementation of human-in-the-loop validation can allow security experts to verify critical alerts and reduce the consequences of incorrect automated decisions.	02, 04, 05, 09, 10, 11, 12, 13, 16, 18, 19, 20, 21–32, 33, 34, 35, 41, 42, 45	**33**

© 2026 The Author(s). Published by Qassim University under CC BY-NC-SA 4.0.

S. No	Consolidated Challenge	Description	Consolidated Solutions	Paper IDs	Freq (45)
3	**Dataset Imbalance & Minority Attack Detection**	Rare User-to-Root (U2R), Remote-to-Local (R2L), insider-attack, and healthcare anomaly classes are poorly represented in datasets, causing ML models to favor majority classes.	The use of SMOTE and SMOTEENN can increase the representation of minority attack classes and improve their detection. The application of GAN-based data generation can provide additional representative samples for rare attack categories. The use of One-Class ML can support the detection of rare or insufficiently represented attack classes. The adoption of balanced sampling can reduce model bias toward majority attack classes and improve minority attack detection.	04, 05, 07, 09, 10, 11, 12, 14, 15, 18, 19, 21–32, 33, 34, 35, 36, 37, 40, 41, 43, 45	**31**
4	**Outdated / Unrealistic Datasets**	Heavy dependence on older datasets such as KDD99 and NSL-KDD, together with limited representation of realistic IoT/ICS environments, restricts reliability and generalizability of IDS models.	The adoption of modern datasets such as UNSW-NB15, CICIDS2017, and TON-IoT can reduce dependence on outdated datasets and provide more realistic attack scenarios. The implementation of systematic dataset cleansing and preprocessing can improve data quality and the reliability of experimental results. The use of cross-dataset validation can provide a more realistic assessment of model generalizability and reduce dependence on a single dataset.	02, 04, 05, 10, 11, 16, 19, 21–32, 34, 37, 40, 43, 44, 45	**27**
5	**Computational & Resource Constraints**	IoT, IoMT, and ICS devices often have limited computational resources, while sophisticated Deep Learning models may require substantial GPU/TPU resources.	The use of lightweight CNN1D models can reduce computational requirements for resource-constrained IoT, IoMT, and ICS environments. The adoption of Edge/Fog-based IDS architectures can move detection closer to the data source and reduce dependence on resource-intensive centralized processing. The application of model pruning can reduce unnecessary model parameters and computational overhead. The use of efficient feature selection can reduce the amount of data that needs to be processed while maintaining relevant detection	02, 04, 05, 07, 10, 13, 14, 16, 18, 19, 21–32, 33, 34, 36, 37, 40, 43, 45	**32**

© 2026 The Author(s). Published by Qassim University under CC BY-NC-SA 4.0.

S. No	Consolidated Challenge	Description	Consolidated Solutions	Paper IDs	Freq (45)
			information.		
6	**Scalability & Big Data Handling**	The large volume of data generated by Cloud, Fog, Edge, CI/CD, IoMT, and smart-healthcare environments creates challenges in processing and monitoring security events at scale.	The adoption of distributed IDS architectures can distribute security monitoring and processing across multiple computing resources. The integration of Cloud–Fog–Edge architectures can distribute workloads according to the capabilities of different computing layers. The use of Federated Learning can support collaborative model training across distributed environments without requiring all data to be centrally collected. The integration of SDN/NFV technologies can provide flexible and scalable security functions for large-scale environments.	02, 05, 07, 11, 13, 14, 16, 17, 18, 20, 21–32, 33, 35, 36, 37, 40, 42, 43, 45	**34**
7	**Explainability & Trust (Black-Box AI)**	The lack of transparency in AI/ML-based decisions creates difficulties in regulatory compliance, operator acceptance, and understanding why a model generates a particular security alert.	The use of Explainable AI (XAI) techniques such as SHAP and LIME can make AI-based IDS decisions easier for operators and stakeholders to understand. The establishment of transparent AI governance can improve trust and address regulatory and organizational concerns associated with black-box AI. The application of feature contribution analysis can help security operators understand which features contributed to specific detection decisions.	01, 02, 07, 11, 12, 13, 14, 19, 20, 21, 23, 28, 29, 30, 31, 34, 35, 38, 39, 41, 42, 43	**22**
8	**Adversarial ML Vulnerability**	Machine Learning-based IDS models may be manipulated through evasion, poisoning, or black-box attacks, potentially causing security models to produce incorrect results.	The use of adversarial training can improve model resistance against adversarial evasion attacks. The development of robust ML pipelines can reduce vulnerabilities throughout the machine-learning-based detection process. The implementation of a secure ML lifecycle can incorporate security controls throughout model development, deployment, monitoring, and updating.	01, 02, 03, 07, 09, 10, 11, 12, 14, 15, 17, 23, 28, 29, 30, 34, 37, 40, 42	**19**
9	**Feature Engineering & High**	Very large feature spaces, ranging from approximately 80–20,000 features, create	The application of PCA can reduce feature dimensionality while retaining important	04, 05, 07, 09, 10, 14, 16, 19, 22, 23, 24, 25, 26, 27, 33,	**22**

© 2026 The Author(s). Published by Qassim University under CC BY-NC-SA 4.0.

S. No	Consolidated Challenge	Description	Consolidated Solutions	Paper IDs	Freq (45)
	Dimensionality	significant complexity in IoMT and CI/CD environments and can increase processing requirements.	information. The use of Autoencoders can provide a more efficient representation of high-dimensional feature spaces. The application of Extra Trees and RFE can identify relevant features and remove unnecessary or redundant features. The use of correlation filtering can eliminate highly correlated features and reduce feature complexity.	34, 36, 37, 38, 41, 43, 45	
10	**Integration & Deployment Complexity**	Integrating ML-based security solutions with CI/CD pipelines, Operational Technology (OT), and legacy SIEM platforms can be technically complex.	The integration of ML models into CI/CD pipelines can streamline the deployment and management of ML-based security solutions. The adoption of modular API-based frameworks can facilitate integration with existing OT environments and legacy SIEM systems. The use of modular architectures can allow individual ML components to be modified or upgraded without requiring major changes to the complete security infrastructure.	11, 12, 13, 14, 18, 20, 21, 28, 29, 30, 31, 32, 33, 35, 41, 42	**16**
11	**Real-Time & Low-Latency Requirements**	IoMT and ICS environments require rapid detection and response, while edge devices have limited processing capabilities and communication delays can affect timely detection.	The adoption of Edge-based detection can process security events closer to the data source and reduce communication and processing delays. The use of Online Learning can enable models to learn from newly arriving data without relying exclusively on periodic offline retraining. The implementation of stream processing can support near-real-time analysis of continuously generated healthcare IoMT and ICS data.	07, 10, 13, 14, 18, 20, 23, 24, 27, 28, 30, 31, 32, 33, 35, 38, 41, 45	**18**
12	**Concept Drift & Model Adaptation**	Continuous changes in threat behavior and system characteristics can cause trained ML models to degrade over time and become less effective against new patterns.	The implementation of continuous retraining can keep detection models updated as threats and system behavior evolve. The use of Online Learning can enable models to adapt to newly emerging patterns in incoming data. The adoption of adaptive	12, 14, 17, 18, 20, 27, 29, 30, 31, 32, 33, 35, 42, 44, 45	**15**

© 2026 The Author(s). Published by Qassim University under CC BY-NC-SA 4.0.

S. No	Consolidated Challenge	Description	Consolidated Solutions	Paper IDs	Freq (45)
			frameworks can help address model degradation caused by changes in the threat environment.		
13	**Privacy, Legal & Ethical Compliance**	The use and sharing of sensitive IoMT and multi-facility data creates privacy, legal, regulatory, and ethical concerns, including requirements associated with the General Data Protection Regulation (GDPR).	The use of Federated Learning can support collaborative model training while reducing the need to centrally share sensitive data. The establishment of AI governance frameworks can provide systematic mechanisms for addressing privacy, legal, and ethical requirements. The implementation of secure aggregation can strengthen the protection of information exchanged during federated model training. The adoption of these privacy-preserving approaches can help address concerns associated with GDPR, IoMT privacy, and multi-facility data sharing.	01, 02, 03, 07, 09, 11, 13, 14, 15, 17, 18, 19, 20, 21, 24, 28, 29, 30, 31, 39, 40, 42, 45	**23**
14	**Encrypted Traffic Detection Limitations**	Encryption technologies such as TLS/HTTPS restrict access to packet contents, reducing the visibility available to traditional traffic-based detection mechanisms.	The use of behavioral anomaly detection can identify suspicious activities based on traffic behavior even when packet contents are encrypted. The adoption of hybrid feature models can combine multiple observable characteristics of encrypted traffic to improve detection despite limited TLS/HTTPS visibility.	23, 29, 43	**3**
15	**Organizational & Workforce Readiness**	Shortages of appropriate technical skills and the complexity of AI governance can make organizations less prepared to deploy, operate, and manage AI-based cybersecurity solutions.	The provision of workforce training can reduce the skills shortage associated with AI-based cybersecurity technologies. The establishment of AI governance mechanisms can improve organizational management of AI-based cybersecurity solutions. The maintenance of comprehensive lifecycle documentation can improve the management, maintenance, and accountability of AI-based security solutions.	15, 17, 20, 21, 28, 30, 31, 35, 42	**9**
16	**Multi-Layer / Heterogeneous Architecture**	IoMT and IoT systems consist of multiple architectural layers and	The adoption of a layer-aware IDS taxonomy can organize detection mechanisms	13, 16, 45	**3**

© 2026 The Author(s). Published by Qassim University under CC BY-NC-SA 4.0.

S. No	Consolidated Challenge	Description	Consolidated Solutions	Paper IDs	Freq (45)
	Complexity	diverse communication protocols, making it difficult to design a unified detection mechanism for the entire environment.	according to the different layers of IoMT/IoT architectures. The implementation of protocol-aware detection can account for differences among diverse IoT communication protocols. The use of layer- and protocol-specific detection mechanisms can reduce the complexity associated with heterogeneous and multi-layer environments.		
17	**Predictive Maintenance & RUL Estimation Integration**	Industrial systems require capabilities beyond anomaly detection, including prediction of equipment degradation and estimation of Remaining Useful Life (RUL).	The integration of Hybrid ML + RUL models can extend security analysis beyond anomaly detection toward equipment degradation prediction. The application of degradation scoring can quantify the severity and progression of equipment degradation and support predictive maintenance and RUL estimation.	39	**1**

4.2 Paper-Level Challenge and Solution Summary

Table 2. Challenges identified and solutions proposed, by individual paper (AP-01 to AP-45)

Paper ID	Challenges Identified	Solutions Proposed
AP-01	Adversarial ML attacks; Explainability gap; Data leakage	Adversarial training; Secure ML lifecycle; XAI
AP-02	Zero-day detection; False positives; Dataset imbalance; Privacy; Scalability	Hybrid IDS; Ensemble ML; SMOTE; Federated learning
AP-03	ML supply chain risks; Governance gap	Secure ML governance; Risk framework
AP-04	Dataset imbalance; High dimensionality; Outdated datasets	SMOTE; PCA; Modern datasets
AP-05	Feature redundancy; Dataset realism gap; Computational cost	Feature selection; Lightweight DL; Dataset modernization
AP-06	High false alarm rate	Ensemble optimization
AP-07	IoT resource limits; Real-time constraints; Drift	Edge IDS; Lightweight models; Online learning
AP-08	Big data traffic; Scalability	Distributed IDS; Cloud deployment
AP-09	Evaluation inconsistency; Dataset bias	Standard metrics; Benchmarking
AP-10	Concept drift; Zero-day gap	Continuous retraining; Hybrid detection
AP-11	Insider threat complexity	Behavioral analytics (UBA)
AP-12	Poor generalization; Zero-day; Drift	Cross-dataset validation; Adaptive learning
AP-13	IoT multi-layer complexity; Privacy	Layer-aware IDS; Federated learning
AP-14	Distributed privacy risk; Dataset imbalance	Federated learning; SMOTE

© 2026 The Author(s). Published by Qassim University under CC BY-NC-SA 4.0.

Paper ID	Challenges Identified	Solutions Proposed
AP-15	Organizational resistance; Skills shortage	AI governance; Workforce training
AP-16	IoT protocol heterogeneity	Protocol-aware detection
AP-17	Evolving threat landscape; Insider risk	Adaptive ML; Continuous retraining
AP-18	Large-scale traffic; Real-time need	Stream processing; Distributed ML
AP-19	Privacy compliance; False alarms	Differential privacy; Ensemble ML
AP-20	Alert fatigue; Detection-response gap	Automated remediation; Intelligent prioritization
AP-21	Dataset realism limitation	Modern datasets
AP-22	Feature complexity; High dimensionality	PCA; Autoencoders
AP-23	Encrypted traffic limitation	Behavioral traffic analysis
AP-24	Healthcare data imbalance; Latency	SMOTE; Edge deployment
AP-25	Rare attack under-detection	Hybrid DL models
AP-26	Resource constraints	Lightweight ML
AP-27	Real-time detection need	Online learning
AP-28	IoT privacy concerns	Federated learning
AP-29	Enterprise scalability; Drift	Cloud IDS; Continuous learning
AP-30	Adaptive detection requirement	ML lifecycle management
AP-31	Integration complexity	Modular API framework
AP-32	Dataset bias; Imbalance	Balanced resampling
AP-33	CI/CD pipeline vulnerabilities; High false positives; Imbalance; Scalability	CNN-LSTM; SMOTEENN; ML-integrated CI/CD monitoring
AP-34	Zero-day detection; Overfitting; Imbalance; Adversarial risk	Deep Neural Network; Regularization; SMOTE; Adversarial robustness
AP-35	ICS dataset quality; Drift; Explainability; Scalability	Semi-supervised ML; XAI; Structured ML lifecycle
AP-36	Severe imbalance; High dimensionality; Rare attacks; Overfitting	SMOTEENN; DAE + Isolation Forest hybrid
AP-37	Zero-day; False alarms; Outdated datasets; Computational cost	Hybrid IDS; Modern datasets; GPU optimization
AP-38	High-dimensional sensor data; Unlabeled anomalies	PCA + DBSCAN; Human-in-loop validation
AP-39	Minority fault detection; RUL estimation; Privacy	Deep Autoencoder; RUL model; Federated learning
AP-40	IoT resource constraint; Adversarial vulnerability; Imbalance	Lightweight CNN; Federated learning; Hybrid DL
AP-41	Imbalanced anomaly rate; Interpretability; Feature complexity	RF/SVM; SHAP; Dimensionality reduction
AP-42	Alert fatigue; Governance gap; Adversarial ML; Privacy	Automated response; AI governance; Robust ML
AP-43	Outdated datasets; Imbalance; Overfitting; Encrypted traffic	Modern datasets; Ensemble ML; XAI
AP-44	Closed-set limitation; Zero-day gap; High dimensionality	Open Set Recognition; Clustering; Adaptive updating
AP-45	IoMT resource constraint; Heterogeneity; Imbalance; Latency; Privacy	Cloud-Fog-Edge IDS; SMOTE; Federated learning

© 2026 The Author(s). Published by Qassim University under CC BY-NC-SA 4.0.

4.3 Continent-Wise Comparison

Table 3. Continent-wise comparison of dominant challenges, root causes, and strategic solutions

Continent	Dominant Challenges	Root Causes / Driving Factors	Strategic Solutions Emphasized	Research Emphasis Trend
Asia	Zero-day attack detection Dataset imbalance High false positives Scalability in IoT/smart systems Computational constraints	Rapid digital transformation Large-scale IoT deployment Limited high-quality labeled datasets Resource-constrained environments Uneven regulatory maturity	Hybrid IDS (Signature + Anomaly) SMOTE / GAN-based balancing Lightweight DL models (CNN1D, LSTM) Cloud–Fog–Edge architecture Adaptive retraining	Performance-oriented and scalability-focused research
Europe	Privacy & GDPR compliance Explainability (XAI) Ethical AI governance Cross-border data-sharing limitations Federated learning complexity	Strict regulatory frameworks (GDPR, AI Act) Strong emphasis on ethical AI Data-sovereignty laws Public-sector cybersecurity integration	Federated learning Differential privacy SHAP / LIME explainability Secure ML lifecycle governance Risk-based AI frameworks	Trust, transparency, and compliance-driven research
North America	Adversarial ML attacks ML supply-chain vulnerabilities Insider threats Large-scale enterprise integration Zero-trust adaptation	Advanced enterprise AI deployment National security focus Mature cloud ecosystems Active adversarial research community	Adversarial training Secure ML pipelines Zero-trust AI frameworks Continuous retraining AI-SOAR integration	Security hardening and adversarial robustness focus
Middle East & Africa	Infrastructure readiness gaps Workforce skill shortages Governance maturity issues Resource constraints Dataset scarcity	Rapid but recent digital transformation Limited local AI research ecosystem Dependency on imported AI tools / talent shortage	Capacity-building programs Government AI strategy alignment Cloud-based scalable IDS Regional dataset repositories	Organizational and capacity-development emphasis
Cross-Continental (Global Trend)	Zero-day detection False positives Dataset imbalance Scalability Concept drift	Evolving cyber threats Massive heterogeneous data Dynamic attack techniques AI lifecycle vulnerabilities	Hybrid IDS architectures Ensemble & Deep Learning Federated learning Continuous adaptive retraining Explainable AI integration	Convergence toward hybrid, adaptive, and privacy-aware AI security

As shown in Table 1, zero-day and novel attack detection (n = 36), scalability and big-data handling (n = 34), high false positive/negative rates (n = 33), computational and resource constraints (n = 32), and dataset imbalance (n = 31) are the five most frequently reported challenges, followed by outdated/unrealistic datasets (n = 27), privacy/legal/ethical compliance (n = 23), and explainability and feature-engineering/high-dimensionality (n = 22 each). Table 2 reveals that the majority of individual papers report multiple, co-occurring challenges—for instance, zero-day detection is often co-occurring with dataset imbalance and outdated datasets, and privacy is often co-occurring with scalability in IoMT and federated deployments—and therefore the challenges are not independent. Table 3 reveals that while all regions have an interest in hybrid, adaptive, and privacy-aware solution architectures, the relative importance and root causes of specific challenges vary significantly by region: Asia is

© 2026 The Author(s). Published by Qassim University under CC BY-NC-SA 4.0.

dominated by scalability and IoT-driven detection challenges, Europe by privacy and explainability, North America by adversarial robustness and enterprise integration, and the Middle East and Africa by foundational infrastructure and capacity constraints.

5. Discussion

It has been found that the challenges to utilizing AI/ML for cyber threat detection are not just technical but involve data, computational, organizational and regulatory dimensions. The most common challenges mentioned in Table 1 are mostly related to zero-day detection, scalability, and false-positive/false-negative rates, indicating that existing AI/ML-based IDSs are still primarily limited by their ability to be generalizable beyond known patterns of attacks and by their scale requirements which are needed for the fast growing industrial, IoT and cloud infrastructures. This aligns with the conceptual background presented in Section 2 which determined anomaly-based detection as the most important method for detecting new attacks, but that it is also highly dependent on the quality and representativeness of training data, as indicated by the high rates of dataset imbalance (n = 31) and outdated/unrealistic datasets (n = 27) as critical challenges.

The fact that computational and resource constraints (n = 32) and scalability (n = 34) were also highly cited indicates a practical conflict in deploying AI for security: the more powerful deep learning algorithms tend to be the less practical in IoT, IoMT, and ICS contexts where threat detection is most critical. This tension is not being resolved by giving up on deep learning, but by re-architecturing the location and method of inference, as solutions converge towards lightweight models, edge based inference, and tiered edge–cloud architectures (Table 1).

The presence of explainability and trust (n = 22) and privacy, legal and ethical compliance (n = 23) as critical challenges highlights the need for technical accuracy not to be the only factor for organizational adoption. In structured diligences like healthcare and critical infrastructure, security analysts and regulators need verdicts that are interpretable and auditable. This is stable with the regional analysis in Table 3, as explainability, privacy and governance are seen as separate from detection performance, whereas studies in Asia have a focus on detection performance and scalability in resource constrained environments, and North American studies have a focus on adversarial robustness in well-established enterprise security operations, typically aligned with Zero Trust principles of continuous verification and least-privilege access [21]. These disparities indicate that there is no one-size-fits-all solution for the ‘right’ AI/ML security architecture for an organisation, as it will depend on the regulatory landscape, infrastructure readiness and threat profile.

These findings have some practical implications for modern organisations. First, it is important to recognize that there are many examples of resilience, scalability, and minimizing false alarms in the literature and that these attributes should be considered first order design requirements, not second order.First, it is important to note that resilience, scalability, and minimizing false alarms are common in the literature and should be considered first-order design attributes, not second-order. Second, it is important to consider dataset governance, namely using modern and representative datasets and systematic class balancing methods, as an early part of system development and not an afterthought. Third, explainability and privacy-preserving mechanisms (such as XAI layers, federated learning, differential privacy) should be incorporated into system architecture early in the design process, especially for organisations in regulated industries and/or across jurisdictions. Lastly, when organizations have limited local datasets, a shortage of local workers, etc., they might be better served by

© 2026 The Author(s). Published by Qassim University under CC BY-NC-SA 4.0.

capacity-building and cloud-based scalable IDS solutions than with the most intense models that are published in the literature.

The evidence suggests that the field is moving toward a wider consideration of AI/ML intrusion detection systems beyond accuracy measures — from what is now a multidimensional view of 'trustworthy' cybersecurity AI, as embodied by the architectures of proposed solutions that are now hybrid, adaptive and privacy-compliant (Tables 1-3).

6. Conclusion

In this study, a systematic literature review of 45 papers about the use of AI and ML in cyber threat detection for modern organizations was carried out, which resulted in a total of 271 reported challenges and 252 proposed solutions and were reduced to seventeen recurring themes (Table 1). The most significant challenges identified were zero day / novel attacks, scalability, handling large amounts of data, high false positive / negative rates, computation / resource limitations, imbalance in data sets, outdated datasets, privacy / regulatory compliance, explainability, and high dimensional feature space, with the latter being additional issues that still need to be addressed. As illustrated in the paper-level summary (Table 2), these challenges are not isolated – they generally occur in combination within any given study – and the continent-wise comparison (Table 3) provides insight into the systematic differences among research priorities across each continent as a function of varying regulatory environments, infrastructure maturity, and threat landscape, even as the field as a whole evolves toward hybrid, adaptive and privacy-aware AI security architectures that combine ensemble learning, federated learning, explainable AI, and ongoing adaptive retraining.

This synthesized evidence base serves as a practical benchmark for organizations developing or testing AI-based intrusion detection systems, while also providing a structured reference point for ongoing research exploring how to improve the gap between experiment and deployment to provide a more reliable, trusted experience. Further research should be conducted to integrate this synthesis with a quantitative meta-analysis of the detection performance reported in the literature, and to validate the proposed consolidated framework in operational environments, and to monitor the change in the frequency of challenges over time, as adversarial skills and regulatory requirements continue to shift.

7. Limitations

- The review is limited to peer-reviewed studies in English and a few credible technical reports in English; other relevant English-language or non-English literature (grey literature) may not have been included.
- Challenge and solution frequencies (Table 1) are indicative of the themes reported on in the literature, rather than of their empirically validated severity or impact in the real world; frequency does not reflect real-world risk but rather real-world research attention.
- Although the studies were systematically selected, the study is not a meta-analysis of quantitative detection performance metrics (e.g., accuracy, F1 score) in the different studies, but rather a mapping/synthesis study.
- Some studies (Table 3) were attributed to a country/continent based on the affiliation of the authors or the journal in which the article was published, but did not explicitly specify a geographic scope, which may contribute to imprecision in the regional analysis.

© 2026 The Author(s). Published by Qassim University under CC BY-NC-SA 4.0.

- Several entries in the appendix-A do not include full bibliographic information in the original source records (e.g., volume number) and these are indicated in the appendixes, not estimated.
- The selection of published challenges and solutions might have been affected by publication bias, common to all SLRs.

References

1. A. K. B. Arnob, R. R. Chowdhury, N. A. Chaiti, S. Saha, and A. Roy, "A comprehensive systematic review of intrusion detection systems: Emerging techniques, challenges, and future research directions," Journal of Edge Computing, vol. 4, no. 1, pp. 73–104, 2025.
2. A. Hozouri, A. Mirzaei, and M. Effatparvar, "A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges," Discover Artificial Intelligence, vol. 5, art. 314, 2025.
3. A. Alotaibi and M. A. Rassam, "Adversarial machine learning attacks against intrusion detection systems: A survey on strategies and defense," Future Internet, vol. 15, no. 2, art. 62, 2023.
4. A. Vassilev et al., "Adversarial machine learning: A taxonomy and terminology of attacks and mitigations (NIST AI 100-2e2025)," National Institute of Standards and Technology, 2025.
5. I. H. Sarker et al., "Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects," ICT Express, vol. 10, pp. 935–958, 2024.
6. B. I. Farhan and A. D. Jasim, "Survey of intrusion detection using deep learning in the Internet of Things," Iraqi Journal for Computer Science and Mathematics, vol. 3, no. 1, pp. 81–91, 2022.
7. S. Oriaro and S. Mishra, "Improving cybersecurity through explainable artificial intelligence: A systematic literature review," Issues in Information Systems, vol. 26, no. 3, pp. 387–400, 2025.
8. E. E. Abdallah, W. Eleisah, and A. F. Otoom, "Intrusion detection systems using supervised machine learning techniques: A survey," Procedia Computer Science, vol. 201, pp. 205–212, 2022.
9. Y. Zhang, R. C. Muniyandi, and F. Qamar, "A review of deep learning applications in intrusion detection systems: Overcoming challenges in spatiotemporal feature extraction and data imbalance," Preprints, 2024.
10. A. Pinto et al., "Survey on intrusion detection systems based on machine learning techniques for the protection of critical infrastructure," Sensors, vol. 23, no. 5, art. 2415, 2023.
11. Y. Muhammad et al., "An improved framework for requirement implementation in the context of global software development: A systematic literature review protocol," International Journal of Database Theory and Application, vol. 9, no. 6, pp. 161–170, 2016.
12. A. Philip et al., "A systematic literature review of software requirements prioritization research," Information and Software Technology, vol. 56, pp. 568–585, 2014.
13. B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," EBSE Technical Report, 2007.
14. A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.
15. R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in Proc. IEEE Symposium on Security and Privacy, 2010.
16. N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41–50, 2018.
17. B. Biggio and F. Roli, "Wild patterns: Ten years after the rise of adversarial machine learning," Pattern Recognition, vol. 84, pp. 317–331, 2018.
18. M. T. Ribeiro, S. Singh, and C. Guestrin, "'Why should I trust you?': Explaining the predictions of any classifier," in Proc. ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2016.
19. Gartner, "Top security and risk management trends," Gartner Research, 2022.
20. IBM Security, "AI in cybersecurity report," IBM Corporation, 2022.
21. S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture (NIST Special Publication 800-207)," National Institute of Standards and Technology, 2020.

© 2026 The Author(s). Published by Qassim University under CC BY-NC-SA 4.0.

22. L. Cadieux, "20 shocking cybercrime statistics: 2024 edition," The Devolutions Blog, Jul. 2024. [Online]. Available: https://blog.devolutions.net/2024/07/20-shocking-cybercrime-statistics2024-edition/.

23. J. Kim et al., "Deep neural networks for complex attack pattern detection in large-scale network traffic," 2021. (Bibliographic details limited in source record.)

Appendix A. List of Reviewed Papers (n = 45)

The Table below lists the 45 studies synthesized in this review, identified by internal paper ID (AP-01 to AP-45), along with title, authors, volume, publication year, and journal/venue. Volume information was not consistently available in the source bibliographic records and is marked "N/A" where absent; authorship is listed as "Multiple authors" where individual author names were not extracted in the underlying data-extraction records.

Paper ID	Title	Authors	Vol.	Year	Journal / Venue
AP-01	Adversarial machine learning in intrusion detection systems (dataset-specific study)	Multiple authors	N/A	2022	IEEE Access
AP-02	Hybrid machine learning-based intrusion detection system study	Multiple authors	N/A	2021	Computers & Security
AP-03	Machine learning lifecycle security risks	Multiple authors	N/A	2022	ACM CCS Workshop
AP-04	Feature optimization in intrusion detection systems	Multiple authors	N/A	2020	Future Generation Computer Systems
AP-05	Deep learning for intrusion detection system evaluation	Multiple authors	N/A	2021	Journal of Network & Computer Applications
AP-06	False alarm reduction in intrusion detection systems	Multiple authors	N/A	2020	Security and Communication Networks
AP-07	IoT-based machine learning intrusion detection framework	Multiple authors	N/A	2022	IEEE Internet of Things Journal
AP-08	Big data intrusion detection	Multiple authors	N/A	2021	IEEE Transactions on Big Data
AP-09	Benchmarking machine learning-based intrusion detection systems	Multiple authors	N/A	2021	Computers & Security
AP-10	Adaptive intrusion detection systems	Multiple authors	N/A	2022	Applied Sciences
AP-11	Insider threat detection review	Multiple authors	N/A	2020	ACM Computing Surveys
AP-12	Cross-dataset validation in intrusion detection systems	Multiple authors	N/A	2021	Information Sciences
AP-13	IoT layered security framework	Multiple authors	N/A	2022	IEEE Access
AP-14	Federated learning for intrusion detection systems	Multiple authors	N/A	2023	IEEE Transactions on Network Science
AP-15	AI governance in cybersecurity	Multiple authors	N/A	2023	Government Information Quarterly
AP-16	Protocol-aware intrusion detection systems for IoT	Multiple authors	N/A	2022	Sensors
AP-17	Adaptive threat detection	Multiple authors	N/A	2023	ACM Digital Threats: Research and Practice
AP-18	Distributed machine learning-based intrusion detection systems	Multiple authors	N/A	2022	Future Internet
AP-19	Privacy-preserving machine learning intrusion detection systems	Multiple authors	N/A	2023	IEEE Access

© 2026 The Author(s). Published by Qassim University under CC BY-NC-SA 4.0.

Paper ID	Title	Authors	Vol.	Year	Journal / Venue
AP-20	AI-driven incident response	Multiple authors	N/A	2022	Computers & Security
AP-21	Modern dataset evaluation study	Multiple authors	N/A	2023	Electronics
AP-22	Dimensionality reduction in intrusion detection systems	Multiple authors	N/A	2023	Expert Systems with Applications
AP-23	Encrypted traffic detection	Multiple authors	N/A	2023	IEEE Transactions on Information Forensics and Security
AP-24	Healthcare intrusion detection system framework	Multiple authors	N/A	2023	Journal of Medical Systems
AP-25	Rare attack detection study	Multiple authors	N/A	2023	Security and Communication Networks
AP-26	Lightweight machine learning for intrusion detection systems	Multiple authors	N/A	2023	Sensors
AP-27	Online learning intrusion detection framework	Multiple authors	N/A	2023	IEEE Access
AP-28	Federated IoT security study	Multiple authors	N/A	2023	IEEE Internet of Things Journal
AP-29	Enterprise cloud intrusion detection system	Multiple authors	N/A	2023	Future Generation Computer Systems
AP-30	Continuous learning security models	Multiple authors	N/A	2023	Information Systems
AP-31	API-based intrusion detection system integration	Multiple authors	N/A	2023	Software: Practice and Experience
AP-32	Dataset bias mitigation in intrusion detection systems	Multiple authors	N/A	2023	Journal of Big Data
AP-33	Advancing software security and reliability in cloud platforms through AI-based anomaly detection	Multiple authors	N/A	2024	ACM Cloud Computing Security Workshop (CCSW)
AP-34	Network-based intrusion detection using deep learning technique	Multiple authors	N/A	2025	Scientific Reports
AP-35	Deployment guidelines for industry: machine learning-based intrusion detection systems	PETRAS Research Team	N/A	2023	PETRAS National Centre of Excellence (UKRI) Report
AP-36	NetDAIL: optimized deep learning hybrid model	Multiple authors	N/A	2025	International Journal of Advanced Computer Science and Applications (IJACSA)
AP-37	Network intrusion detection system: a systematic study of machine learning and deep learning approaches	Zeeshan Ahmad et al.	N/A	2021	Transactions on Emerging Telecommunications Technologies
AP-38	Machine learning-based anomaly detection for ITER Tokamak systems	Multiple authors	N/A	2025	TechRxiv
AP-39	Machine learning framework for cryogenic systems	Multiple authors	N/A	2025	IOP Conference Series
AP-40	Deep learning for cyber threat detection in IoT networks	Multiple authors	N/A	2024	Internet of Things & Cyber-Physical Systems
AP-41	Machine learning-based network anomaly detection	Multiple authors	N/A	2024	AI (MDPI)
AP-42	Applying AI in cybersecurity to enhance threat detection	Multiple authors	N/A	2024	Computer Science & IT Research Journal

© 2026 The Author(s). Published by Qassim University under CC BY-NC-SA 4.0.

Paper ID	Title	Authors	Vol.	Year	Journal / Venue
AP-43	Systematic literature study of machine learning-based intrusion detection systems	Multiple authors	N/A	2025	Journal of Big Data
AP-44	Adaptable deep learning-based intrusion detection system for zero-day attacks	Multiple authors	N/A	2021	arXiv (cs.CR)
AP-45	AI for IoMT security: intrusion detection systems, attacks, and architectures	Multiple authors	N/A	2023	Internet of Things (Elsevier)

© 2026 The Author(s). Published by Qassim University under CC BY-NC-SA 4.0.