International Journal Of Artificial Intelligence And Engineering Innovation
VOL 01 | No. 1 | 2026
P-I-SSN: XXXXXXXXXX | E-I-SSN: XXXXXXXXXX

DEEP LEARNING APPROACHES FOR CYBERSECURITY THREAT DETECTION AND PREVENTION

Kinza Ishaq

BS, Department of CS Computer Science, The Cosmic Degree College (For Women) ,University of Okara

ABSTRACT

The rapid evolution of cyber threats has increased the need for intelligent, adaptive, and reliable cybersecurity mechanisms capable of detecting malicious activities and preventing security incidents. Traditional security approaches, including signature-based detection and predefined rules, remain valuable for identifying known threats but may struggle to recognize previously unseen attacks, sophisticated malware, and rapidly changing adversarial techniques. Deep learning (DL), a branch of artificial intelligence, offers advanced capabilities for automatically learning complex patterns from network traffic, system logs, executable files, user behavior, and other security-related data. This research examines the role of deep learning approaches in cybersecurity threat detection and prevention, focusing on convolutional neural networks, recurrent neural networks, long short-term memory networks, autoencoders, transformer architectures, and hybrid learning models. It explores their applications in network intrusion detection, malware classification, phishing identification, anomaly detection, distributed denial-of-service attack detection, and intelligent security monitoring. The study adopts a literature-based research approach to synthesize relevant research published between 2023 and 2025. Particular attention is given to detection performance, false-positive rates, computational efficiency, generalization to unseen threats, adversarial robustness, explainability, and practical deployment. The discussion indicates that deep learning can strengthen cybersecurity by improving automated pattern recognition and supporting faster identification of suspicious activities. However, effective implementation requires representative datasets, rigorous validation, continuous model monitoring, and integration with established security controls. The study concludes that deep learning should complement rather than replace conventional cybersecurity mechanisms, enabling a layered defense strategy that combines intelligent detection, human expertise, and carefully governed automated responses.

KEYWORDS:*Deep Learning, Cybersecurity, Threat Detection, Threat Prevention, Artificial Intelligence, Network Intrusion Detection, Malware Detection, Phishing Detection, Anomaly Detection, Convolutional Neural Networks, Recurrent Neural Networks, Transformers, Adversarial Robustness, Security Analytics, Automated Incident Response.*

INTRODUCTION

Cybersecurity has become a fundamental requirement for individuals, businesses, governments, and organizations that depend on digital infrastructure. The increasing use of cloud computing, Internet of Things (IoT) devices, online transactions, remote working platforms, and interconnected information systems has expanded the potential attack surface available to cybercriminals. Modern threats include malware infections, ransomware, phishing campaigns, unauthorized network access, credential theft, denial-of-service attacks, and exploitation of software vulnerabilities. These threats can compromise confidential information, disrupt essential services, damage organizational reputation, and create significant financial losses. Ali, A. H., Charfeddine, M., Ammar, B., Hamed, B. B., Albalwy, F., Alqarafi, A., & Hussain, A. (2024). found that Traditional security mechanisms remain important, particularly for detecting known malicious signatures and enforcing established security rules. However, attackers frequently modify their techniques to evade known detection patterns. Consequently, cybersecurity professionals increasingly require intelligent systems capable of analyzing complex data, identifying unusual behavior, and adapting to changing threat environments.Deep learning is a specialized branch of machine learning that

International Journal Of
Artificial Intelligence And
Engineering Innovation
VOL 01 | No. 1 | 2026
P-I-SSN: XXXXXXXXXX | E-I-SSN: XXXXXXXXXX

uses multilayer neural networks to learn increasingly complex representations from data. Unlike approaches that depend heavily on manually designed features, deep learning can automatically learn useful characteristics from network traffic, executable files, textual messages, system logs, and sequences of security events. Convolutional neural networks (CNNs) are useful for learning spatial or structured patterns, while recurrent neural networks (RNNs) and long short-term memory (LSTM) networks can model sequential relationships. Autoencoders learn compressed representations and may identify anomalies through reconstruction errors, while transformer architectures use attention mechanisms to represent relationships within sequences and other structured inputs. These capabilities make deep learning relevant to cybersecurity problems in which malicious behavior cannot always be identified through a single predefined rule. Nevertheless, the performance of a deep learning system depends on the quality of its training data, the suitability of its architecture, and the rigor of its evaluation.

Threat detection involves identifying activities, files, communications, or system behaviors that may indicate malicious intent or a security violation. Deep learning can support this process by classifying known attack categories, identifying deviations from normal behavior, and recognizing patterns associated with suspicious activities. In network intrusion detection, models can analyze traffic-flow characteristics to distinguish benign communications from potentially malicious connections. In malware detection, neural networks can learn patterns from executable files, byte sequences, API calls, or other representations of program behavior. Phishing detection models can examine textual characteristics, URLs, and message-related features, while log-analysis systems can identify unusual sequences of authentication events or administrative actions. Belenguer, A., Pascual, J. A., & Navaridas, J. (2025). Explained that These applications illustrate how deep learning can improve the automation of security analysis. However, a model's classification must be interpreted in context because legitimate activities can resemble malicious behavior, and sophisticated attacks may deliberately imitate normal system operations.Threat prevention extends beyond identifying suspicious activity to taking appropriate measures that reduce the likelihood or impact of a security incident. Deep learning systems can contribute to prevention by generating alerts, assigning risk scores, prioritizing suspicious events, and providing information to security orchestration and incident-response platforms. When integrated with firewalls, endpoint detection and response tools, intrusion prevention systems, and security information and event management platforms, predictive models can help organizations decide when to isolate a device, block a connection, request additional authentication, or investigate an event. However, automated responses must be designed carefully because incorrect predictions can interrupt legitimate business activities or deny access to authorized users. For this reason, high-impact actions should often require additional verification, explicit policy conditions, or human approval. Deep learning is most effective when it supports a layered defense strategy that combines detection, prevention, investigation, recovery, and conventional security controls.

Despite its potential, deep learning introduces several challenges that influence the reliability of cybersecurity systems. Training effective models may require large quantities of representative and accurately labelled data, yet real-world security datasets often contain class imbalance, outdated attack patterns, incomplete observations, or insufficient examples of emerging threats. Models may perform well on benchmark datasets but lose accuracy when deployed in networks with different traffic characteristics or operating conditions. Cyber attackers may also attempt to evade detection by manipulating inputs, exploiting

International Journal Of
Artificial Intelligence And
Engineering Innovation
VOL 01 | No. 1 | 2026
P-I-SSN: XXXXXXXXXX | E-I-SSN: XXXXXXXXXX

model weaknesses, or poisoning training data. In addition, deep learning models can require substantial computational resources, which may limit their suitability for resource-constrained devices or high-speed network environments. Limited interpretability can make it difficult for analysts to understand why an alert was generated. These issues demonstrate that detection accuracy alone is insufficient to establish whether a model is secure, practical, and suitable for operational deployment.This research investigates deep learning approaches for cybersecurity threat detection and prevention, emphasizing their architectures, application areas, benefits, limitations, and future development opportunities. It focuses on research published between 2023 and 2025 to examine recent developments in intelligent intrusion detection, malware analysis, anomaly detection, and security analytics. The study also considers the role of hybrid models, transformer-based approaches, privacy-preserving learning, explainable AI, and automated incident response. Its significance lies in examining deep learning not merely as a classification technique but as one component of a broader cybersecurity architecture. Maniriho, P., Mahmood, A. N., & Chowdhury, M. J. M. (2024). Elaborated on The research aims to identify the conditions under which deep learning can provide reliable security benefits, including appropriate dataset selection, robust evaluation, computational efficiency, and integration with existing defensive technologies. The findings are intended to inform researchers, cybersecurity practitioners, and organizations seeking to adopt intelligent security solutions while maintaining operational reliability and appropriate human oversight.

RESEARCH QUESTION

1. How can deep learning approaches improve cybersecurity threat detection and prevention, and what technical, operational, and security-related factors influence their accuracy, robustness, and effectiveness in real-world environments?

RESEARCH OBJECTIVES

1. To examine the principal deep learning architectures used for cybersecurity threat detection and prevention.

LITERATURE REVIEW

The development of deep learning has introduced new approaches to cybersecurity by enabling systems to learn complex patterns from large quantities of security-related data. Earlier security solutions relied heavily on predefined signatures, manually developed rules, and expert knowledge. Although these methods remain effective against recognized threats, their effectiveness can be limited when attackers modify malicious files, use unfamiliar communication patterns, or exploit vulnerabilities that have not yet been documented. Deep learning provides an alternative by learning representations from examples of benign and malicious behavior. Hore, S., Ghadermazi, J., Shah, A., & Bastian, N. D. (2024). Explains that These representations can be used to classify traffic, identify unusual events, and recognize patterns that may indicate security violations. Salem et al. (2024), in their review of AI-driven cybersecurity detection techniques, examine how artificial intelligence, including machine learning and deep learning, can support automated identification of cyberattacks. Recent research increasingly considers deep learning as part of a broader security architecture

International Journal Of
Artificial Intelligence And
Engineering Innovation
VOL 01 | No. 1 | 2026
P-I-SSN: XXXXXXXXXX | E-I-SSN: XXXXXXXXXX

rather than as an isolated classification method. An effective cybersecurity system must process data, identify potentially malicious activity, communicate alerts, and support an appropriate response. This broader perspective is important because a detection model that produces accurate classifications may still be unsuitable for operational use if it is too slow, difficult to maintain, or unable to integrate with existing security infrastructure. Wu, Zou, and Cao (2024) review the status, challenges, and future directions of deep learning-based intrusion detection models, emphasizing the importance of datasets and the continuing development of detection techniques. The literature therefore suggests that progress in deep learning must be evaluated in relation to both analytical performance and practical cybersecurity requirements.

Convolutional neural networks are designed to learn localized patterns and hierarchical representations from structured inputs. Although CNNs are widely associated with image processing, cybersecurity researchers can transform executable files, byte sequences, and selected network features into representations that can be processed by convolutional architectures. In malware detection, for example, an executable may be represented as a sequence of bytes or converted into a visualization-like matrix, allowing a CNN to learn patterns associated with different malware families. In network security, convolutional models can analyze selected traffic features to identify relationships associated with known attacks. Their ability to learn features automatically can reduce dependence on manual feature engineering and support the classification of complex inputs.Maniriho, Mahmood, and Chowdhury (2024) survey deep learning models for malware detection on desktop and mobile platforms, illustrating the range of neural architectures used to identify malicious software. Redhu et al. (2024) also review deep learning-powered malware detection and discuss the contribution of neural methods to cybersecurity. These studies provide a foundation for understanding why CNNs are frequently considered for malware classification and related pattern-recognition tasks.Nevertheless, CNN-based security models have limitations. Khraisat, A., Alazab, A., Alazab, M., Jan, T., Singh, S., & Uddin, M. A. (2025). revealed that Their results may depend on how input data are represented, which features are retained, and whether the training dataset adequately represents the malware families and attack patterns encountered during deployment. A model trained on one operating system or a limited set of malware samples may not generalize to a substantially different environment. Furthermore, classification confidence does not necessarily indicate that the model has correctly identified the underlying malicious behavior. CNNs should therefore be evaluated using independent test data, appropriate baselines, and security-specific assessments of false positives, false negatives, and performance on previously unseen samples.

Recurrent neural networks are designed to process sequential information, making them relevant to security tasks involving ordered events or time-dependent behavior. Network communications, authentication events, system logs, and sequences of application operations can contain temporal patterns that provide evidence of malicious activity. For example, repeated failed logins followed by an unusual successful authentication may be more suspicious when the events are considered together than when each event is evaluated independently. RNNs can model relationships between sequential observations, while long short-term memory networks use specialized gating mechanisms to retain relevant information over longer sequences.These architectures can support intrusion detection by learning relationships among network-flow records or system events. They may also help identify suspicious sequences associated with malware execution, unauthorized access, or command-and-control activity. Their principal advantage is the ability to consider temporal

International Journal Of
Artificial Intelligence And
Engineering Innovation
VOL 01 | No. 1 | 2026
P-I-SSN: XXXXXXXXXX | E-I-SSN: XXXXXXXXXX

context rather than relying solely on individual observations. However, sequential models require careful preparation of the input data, including the ordering of events, the selection of sequence lengths, and the handling of missing observations. In high-volume networks, long sequences can increase processing demands and delay the generation of alerts.A further limitation concerns changes in normal behavior. Enterprise traffic patterns may change because of software updates, new business applications, seasonal activity, or changes in user behavior. A sequential model that has learned an outdated representation of normal activity may generate excessive false alarms or miss new threats. Consequently, RNN and LSTM models should be evaluated under realistic temporal conditions, with training and testing periods separated appropriately. Their operational value depends on whether temporal information produces a meaningful improvement over simpler models and whether the resulting system can operate within the required detection latency.

Autoencoders are neural networks that learn to reconstruct input data through an internal representation. In anomaly detection, an autoencoder may be trained primarily on observations representing normal system activity. When an input differs substantially from the learned patterns, the model may produce a larger reconstruction error, which can be used as an anomaly score. This approach is attractive when complete labels for every possible attack are unavailable, a common limitation in cybersecurity because new threats emerge continuously and incident labels can be difficult to obtain.Anomaly-based detection can help identify deviations from expected behavior, including unfamiliar traffic patterns, unusual system activity, and unexpected changes in communication frequency. Unlike signature-based systems, anomaly detection does not necessarily require a predefined signature for each attack. However, an unusual event is not automatically malicious. Legitimate software deployments, unusual workloads, and authorized administrative activity may also differ from previously observed patterns. Makris, I., Karampasi, A., Radoglou-Grammatikis, P., Episkopos, N., Iturbe, E., Rios, E., ... & Sarigiannidis, P. (2025). Elaborated on If the anomaly threshold is set too low, the system may generate excessive false positives; if it is set too high, subtle malicious activities may remain undetected.Research on deep learning-based intrusion detection identifies anomaly detection as an important direction while highlighting the continuing challenges associated with datasets, model performance, and operational deployment (Wu et al., 2024). The literature suggests that autoencoders are most useful when their anomaly scores are combined with contextual information, risk prioritization, and further investigation. They should not be assumed to detect every zero-day attack merely because they do not depend exclusively on known signatures. Their effectiveness must be demonstrated against realistic benign variations and previously unseen malicious activity.

Transformer architectures use attention mechanisms to represent relationships between elements of a sequence or other structured input. In cybersecurity, these architectures may be applied to sequences of network events, system logs, code representations, malware characteristics, and security-related text. Their ability to consider relationships across an input can be useful when malicious behavior is distributed across multiple events rather than concentrated in a single feature. Transformer-based models may also support analysis of security reports and threat intelligence, where relationships between entities, indicators, and reported activities are important.The recent literature on deep learning-based network intrusion detection identifies transformer-based sequence models as one of the important categories of current research, alongside reconstruction methods, convolutional classifiers, and hybrid systems. This development reflects a broader interest in architectures that can represent complicated relationships within security data. Nevertheless, transformers may

International Journal Of
Artificial Intelligence And
Engineering Innovation
VOL 01 | No. 1 | 2026
P-I-SSN: XXXXXXXXXX | E-I-SSN: XXXXXXXXXX

require substantial computational resources and large quantities of suitable training data. Their effectiveness also depends on how security events are tokenized, represented, and organized.Another concern is that attention weights should not automatically be interpreted as complete or faithful explanations of model decisions. A transformer may produce a strong prediction without providing a sufficiently clear reason for a security analyst to act confidently. Researchers should therefore evaluate not only classification performance but also memory consumption, inference latency, calibration, and the usefulness of explanations. In resource-constrained environments, a smaller model may be preferable if it provides adequate detection capability with lower operational cost. Transformer-based security systems should be selected according to demonstrated requirements rather than novelty alone.

METHODOLOGY

This research adopts a structured literature-review methodology to investigate deep learning approaches for cybersecurity threat detection and prevention. The methodology is designed to identify relevant research, compare the principal neural network architectures, examine their cybersecurity applications, and synthesize the major challenges affecting their implementation. The review focuses on publications from January 2023 through December 2025, including peer-reviewed journal articles, conference papers, systematic reviews, and other credible scholarly publications. Relevant literature should be identified through academic databases such as IEEE Xplore, ACM Digital Library, Scopus, Web of Science, ScienceDirect, SpringerLink, and Google Scholar. The search strategy should combine terms such as “deep learning cybersecurity,” “deep learning intrusion detection,” “neural networks malware detection,” “transformer-based threat detection,” “deep learning anomaly detection,” “IoT intrusion detection,” “federated learning cybersecurity,” and “adversarial robustness of intrusion detection systems.” Boolean operators can be used to refine the searches. For example, “deep learning AND intrusion detection” can identify studies addressing network security, while “transformer OR LSTM AND malware detection” can help identify work involving specific architectures. The review should prioritize publications that clearly describe their research objectives, technical approaches, data sources, evaluation methods, findings, and limitations.The selection process should use predefined inclusion and exclusion criteria. Publications should be included if they fall within the specified period, address deep learning or a closely related learning framework in a cybersecurity context, and provide substantive information relevant to threat detection, prevention, robustness, or deployment. Studies concerning network intrusion detection, malware classification, phishing identification, IoT security, anomaly detection, federated intrusion detection, and intelligent security analytics are particularly relevant. Publications should be excluded if they have no meaningful cybersecurity application, duplicate another record, lack sufficient methodological detail, or do not meet the minimum scholarly credibility requirements. The review process should begin with title and abstract screening, followed by examination of the full text of potentially relevant studies. A data-extraction matrix should then record the authors, publication year, research objective, security problem, deep learning architecture, dataset, evaluation metrics, principal conclusions, and reported limitations. The extracted evidence should be grouped into themes covering neural architectures, application domains, performance assessment, adversarial robustness, privacy, explainability, and operational integration. This procedure will provide a consistent framework for comparing research that may differ substantially in experimental design and technical scope.

International Journal Of
Artificial Intelligence And
Engineering Innovation
VOL 01 | No. 1 | 2026
P-I-SSN: XXXXXXXXXX | E-I-SSN: XXXXXXXXXX

RESEARCH DESIGN

The study adopts a descriptive, comparative, and thematic research design to examine the role of deep learning in cybersecurity threat detection and prevention. The descriptive component explains the main neural network architectures and their intended security applications. The comparative component evaluates the strengths and limitations of CNNs, RNNs, LSTMs, autoencoders, transformers, and hybrid architectures in relation to different types of security data. The thematic component identifies recurring issues involving dataset quality, detection performance, generalization, adversarial robustness, privacy, explainability, and operational deployment. The research is cross-sectional because it synthesizes a defined body of literature published during the 2023–2025 period rather than tracking a particular cybersecurity system over time. Its principal unit of analysis is the scholarly publication or documented research contribution. This design is suitable for developing an integrated understanding of a diverse field in which different studies address different threats, use different datasets, and employ different evaluation methods. These dimensions are interdependent. A highly accurate model may still be unsuitable if it consumes excessive resources, fails under distribution changes, or produces alerts that security teams cannot investigate effectively.The research design also distinguishes threat detection from threat prevention. Detection involves recognizing suspicious activity, identifying likely attack categories, or assigning risk scores to events. Prevention involves using the resulting information to reduce the likelihood or impact of an attack through actions such as blocking malicious connections, restricting suspicious processes, isolating compromised devices, or requiring additional verification. These activities are related but not identical. A model may identify suspicious traffic accurately without having the authority or contextual information required to take a safe preventive action. Therefore, the framework evaluates deep learning as one element in a layered security system that includes conventional rules, access controls, endpoint protection, monitoring, incident-response procedures, and human expertise. The research design provides a basis for determining whether the literature supports not only the technical feasibility of deep learning but also its potential contribution to secure and dependable cybersecurity operations.

DATA ANALYSIS

The data analysis is based on qualitative synthesis of information extracted from the selected publications. The first stage involves organizing the literature according to the principal cybersecurity task, including network intrusion detection, malware detection, phishing identification, anomaly detection, IoT security, and collaborative security monitoring. The second stage classifies the studies according to the learning architecture employed, such as convolutional neural networks, recurrent networks, LSTMs, autoencoders, transformers, and hybrid models. The third stage records the types of data analyzed, including network-flow features, packet-derived information, executable files, API-call sequences, textual content, and system logs. The final stage identifies the evaluation measures, reported findings, methodological limitations, and practical implications of each study. This structured classification makes it possible to identify recurring patterns across the literature while retaining the differences between individual research settings.The comparative analysis should examine how each architecture addresses the characteristics of a particular security problem. CNNs are potentially useful when malicious patterns can be represented through structured features or local relationships. RNNs and LSTMs may be suitable for event sequences and time-dependent behavior, while autoencoders can support anomaly detection

International Journal Of
Artificial Intelligence And
Engineering Innovation
VOL 01 | No. 1 | 2026
P-I-SSN: XXXXXXXXXX | E-I-SSN: XXXXXXXXXX

when representative examples of normal activity are available. Transformers can model relationships across longer sequences or complex inputs, although they may require substantial computational resources. Hybrid models may combine different capabilities, but their additional complexity must be justified by measurable improvements. Federated learning provides a method for training across distributed data sources without routinely transferring all raw data to a central location; however, communication overhead, heterogeneous datasets, and malicious model updates remain concerns. These comparisons should be based on the tasks, data, and experimental evidence reported in the reviewed studies rather than assumptions that any particular architecture is universally superior.The quantitative findings reported in the literature should be interpreted using several complementary performance measures.

FINDINGS

The literature synthesis indicates that deep learning offers useful capabilities for recognizing complex patterns in cybersecurity data and supporting the automation of threat detection. CNNs, recurrent architectures, autoencoders, and transformers address different aspects of the detection problem, including structured feature analysis, temporal relationships, anomaly identification, and sequence modelling. The evidence reviewed suggests that architecture selection should be based on the characteristics of the threat, the available data, and the required operational performance. Rather than identifying a single model as the best solution for all cybersecurity tasks, the literature supports a task-specific approach in which the advantages and limitations of each architecture are assessed against suitable baselines and realistic evaluation conditions.A second major finding concerns the importance of data quality and generalization. Deep learning models depend on the quality and representativeness of the examples used during training. If a dataset contains outdated attack patterns, duplicate observations, missing categories, or unrealistic distributions, the resulting model may learn patterns that do not correspond to reliable indicators of malicious behavior. Strong performance on one benchmark dataset does not guarantee equivalent performance on another network or on future attack variants. Temporal validation, cross-dataset testing, careful prevention of data leakage, and evaluation on previously unseen samples are therefore important measures for assessing practical reliability. These findings suggest that improved data collection and experimental design may be as important as developing more complex architectures.A third finding concerns the continuing relevance of false positives and false negatives. Deep learning systems can help automate the classification of large volumes of security events, but incorrect alerts can impose substantial investigative costs. False negatives are equally concerning because undetected attacks may compromise sensitive information or remain active within an organization's infrastructure.

CONCLUSION

Deep learning has emerged as an important approach to cybersecurity threat detection and prevention because it enables automated analysis of complex security data and the identification of patterns associated with malicious activity. This research has examined the principal deep learning architectures, including convolutional neural networks, recurrent neural networks, LSTM networks, autoencoders, transformers, and hybrid models, together with their applications in intrusion detection, malware classification, phishing identification, anomaly detection, and IoT security. The literature indicates that these approaches can

International Journal Of
Artificial Intelligence And
Engineering Innovation
VOL 01 | No. 1 | 2026
P-I-SSN: XXXXXXXXXX | E-I-SSN: XXXXXXXXXX

contribute to more adaptive security monitoring by learning from network traffic, executable files, system logs, and other security-related information. However, the effectiveness of a model depends on the suitability of its architecture, the quality of its training data, and the extent to which its performance has been validated under realistic conditions.The study also highlights that threat detection and threat prevention are related but distinct objectives. Identifying a suspicious event does not automatically prevent an attack; the prediction must be translated into an appropriate defensive response. Integrating deep learning with firewalls, endpoint protection, intrusion prevention, security monitoring platforms, and incident-response procedures can help organizations respond more effectively to potential threats. At the same time, incorrect predictions can disrupt legitimate activity, increase investigative workloads, or allow malicious behavior to remain undetected. Organizations should therefore assess precision, recall, false-positive rates, inference latency, and computational requirements alongside overall accuracy. External validation, temporal testing, and assessment against previously unseen threats are also important for determining whether a model can operate reliably outside its development environment.In conclusion, deep learning can strengthen cybersecurity when it is deployed as part of a layered, carefully governed defense strategy rather than treated as a complete replacement for existing security mechanisms.

REFERENCES

Ali, A. H., Charfeddine, M., Ammar, B., Hamed, B. B., Albalwy, F., Alqarafi, A., & Hussain, A. (2024). Unveiling machine learning strategies and considerations in intrusion detection systems: a comprehensive survey. Frontiers in Computer Science, 6, 1387354.

Belenguer, A., Pascual, J. A., & Navaridas, J. (2025). GLow–Flower Ingurunean Oinarritutako Esamesa bidezko Ikasketa Estrategia Simulatua. IkerGazte. Nazioarteko ikerketa euskaraz, 3, 69-76.

Hore, S., Ghadermazi, J., Shah, A., & Bastian, N. D. (2024). A sequential deep learning framework for a robust and resilient network intrusion detection system. Computers & Security, 144, 103928.

Khraisat, A., Alazab, A., Alazab, M., Jan, T., Singh, S., & Uddin, M. A. (2025). Securing federated learning: a defense strategy against targeted data poisoning attack. Discover Internet of Things, 5(1), 16.

Makris, I., Karampasi, A., Radoglou-Grammatikis, P., Episkopos, N., Iturbe, E., Rios, E., ... & Sarigiannidis, P. (2025). A comprehensive survey of Federated Intrusion Detection Systems: Techniques, challenges and solutions. Computer Science Review, 56, 100717.

Maniriho, P., Mahmood, A. N., & Chowdhury, M. J. M. (2024). A survey of recent advances in deep learning models for detecting malware in desktop and mobile platforms. ACM Computing Surveys, 56(6), 1-41.