CGC International Journal of Contemporary Technology and Research
ISSN: 2582-0486 (online) Vol-8, Issue-1

AI-Driven Cybersecurity for IoT Networks: A Review of Intrusion Detection, Federated Learning, and Emerging Challenges

Kartikay

Department of Computer Science and Engineering, CEC-CGC, Landran Mohali, Punjab, India

***Abstract*:** The emergence of the Internet of Things (IoT) has led to the appearance of new cybersecurity issues associated with the large number of connected devices, constrained computing capabilities, heterogeneity of communication protocols and cyber threats. Classical security methods like signature-based intrusion detection or static rules are not always able to recognize novel attacks and network anomalies. Thus, artificial intelligence (AI), machine learning (ML) and deep learning became essential tools for analyzing network traffic and detecting potential malicious activity. At the same time, AI-powered security systems may face some difficulties related to data imbalance, privacy issues, computational complexity, adversaries' manipulations, and generality of attacks recognition in IoT. This paper gives a survey of current literature on AI-based intrusion detection, datasets of IoT cybersecurity problems, federated learning and adversarial ML. Representative methods are compared and their pros and cons in resource constrained networks are highlighted. Conceptual architecture, which includes edge monitoring, collaborative model training, central coordination and manual investigation of incidents, is suggested. Open research directions are indicated and recommendation for future studies is given.

***Keywords*—**IoT, cybersecurity, intrusion detection system, AI, federated learning, edge computing, adversarial machine learning.

I. INTRODUCTION

The Internet of Things connects physical devices, sensors, industrial equipment, smart appliances, healthcare systems, and other network-enabled technologies. These devices generate continuous streams of operational and communication data that support automation, remote monitoring, and intelligent decision-making. However, widespread connectivity also increases the potential attack surface. Weak authentication, insecure firmware, exposed network services, inadequate encryption, and delayed security updates can enable attackers to compromise individual devices and move across connected systems.

Traditional cybersecurity mechanisms remain essential, but signature-based intrusion detection depends heavily on previously identified attack patterns. Such systems can struggle when network traffic differs from known signatures or when attackers modify their techniques. Machine learning provides an alternative by identifying patterns in network traffic, device behaviour, and system events. Deep learning extends this capability by learning more complex representations from large datasets [2], [4], [5], [10].

Despite these advantages, machine learning should not be treated as a complete replacement for established security controls. Models trained on one network may perform poorly in another because device types, traffic distributions, protocols, and attack frequencies differ. Research has also

demonstrated that unrealistic evaluation settings can overstate the practical effectiveness of intrusion detection models [3]. Therefore, cybersecurity solutions must be evaluated not only on classification accuracy but also on false-alarm rates, detection latency, resource consumption, privacy, and robustness.

In this review, artificial intelligence-based intrusion detection for Internet of Things is discussed. This paper will concentrate on traditional and deep-learning methods of artificial intelligence intrusion detection, datasets problems, federated learning, and adversarial attacks. In this work, we provide the following contributions:

1. Summary of the intrusion detection methods based on AI;
2. Comparison of representative datasets and learning techniques;
3. Privacy-preserving collaborative detection with the use of federated learning;
4. Conceptual architecture of the deployment of AI-based security systems within IoT and edge computing environment.

II. REVIEW METHODOLOGY

This work uses the narrative literature review method to assess the evolution, applications, and challenges related to the use of AI cybersecurity techniques in IoT environments. In particular, ML, deep learning, intrusion detection systems (IDSs), federated learning, adversarial machine learning, and cybersecurity dataset evaluation will be studied. The selection of these topics is due to their relevance as promising areas of research in the field of enhancing detection and preventing cyber attacks.

Previously published research articles, survey papers, conference proceedings, technical reports, and cybersecurity guidelines are used in this work. Special emphasis is placed on works describing how intrusion detection techniques operate, comparing different learning-based methods, benchmark datasets, and challenges related to the practical implementation. Machine learning for cybersecurity studies

are used as a basis for an understanding of the principles of detection and their weaknesses [2], [4], and IDS surveys give information about techniques and their evaluation as

© All Rights Reserved to CGCIJCTR

well as open problems [5]. Network intrusion detection datasets research papers are used to evaluate the reliability and reproducibility of experimental results [6].

These sources are grouped under five key themes within research. The first theme analyzes classical machine learning methods, such as decision trees, random forests, and support vector machines, which are typically applied to network traffic classification. The second theme deals with deep learning methods, such as neural networks and autoencoders that enable anomaly detection for more complex network behavior identification [10] [12]. The third theme covers benchmarking data sets, such as KDD Cup 99, UNSW-NB15, and CICIDS2017, and assesses their suitability for evaluating performance of the intrusion detection models [7] [9]. The fourth theme describes federated learning as a collaborative approach to model training without transferring raw data to a central storage [13], [14]. The last theme is dedicated to the adversarial machine learning, privacy risks, and security challenges [15] [17].

The selected studies are compared using common analytical dimensions, including research objective, detection approach, principal contribution, practical applicability, and reported limitations. For intrusion detection, particular consideration is given to the ability to recognise malicious traffic, identify previously unseen attacks, manage false alarms, and operate under resource constraints. For federated learning, the review considers privacy implications, communication requirements, differences between local datasets, and the risks associated with malicious model updates. For adversarial machine learning, the emphasis is on threats that manipulate inputs or training processes and the corresponding mitigation strategies.

Quality of the dataset and the approach used to evaluate the performance of a system is considered as a key factor during the analysis of the findings of the work. The fact that an IDS demonstrates high classification accuracy does not mean that this system will function properly in the real world environment where the evaluation dataset includes imbalanced classes, obsolete attack signatures or different traffic characteristics than those of the target environment. Thus, attention is paid to the aspects such as precision, recall, F1-measure, false positives, detection latency and computational cost.

In addition to this, the literature review looks into the connection between technical detection capabilities and risk management in cybersecurity. The NIST Cybersecurity Framework 2.0 is an example of risk-management oriented framework for structuring cybersecurity efforts, while the ENISA threat landscape reporting provides more information about threats and priorities regarding security [1], [25]. This information contributes to the analysis of how AI-based detection can be used in larger security contexts.

The final step is the synthesis of results obtained from the literature review in order to highlight existing limitations and future research directions. Among these are the lack of applicability of machine learning models to various network settings, low explainability, computational limits at the edge, privacy issues, vulnerability to adversarial attacks, and inadequate experimental evidence. With these limitations and opportunities in mind, the paper suggests a concept of a hybrid cybersecurity architecture based on edge-based intrusion detection, model refinement through federated learning, and human supervision of incident handling.

It should be noted that this study is not a systematic literature review or a meta-analysis. It does not imply the use of an exhaustive review of all publications available and a database-based study procedure with reporting of the number of screened articles and the number of aggregated experimental studies. Thus, the conclusions are drawn on the basis of qualitative analysis of the selected literature only. This will enable us to establish the grounds for further development of the subject matter.

Fig. 1. Literature review and synthesis workflow



III. AI- BASED INTRUSION DETECTION TECHNIQUES

Intrusion Detection Systems (IDS) scan either the network traffic, host activities or the activities in a computer system to detect any malicious behavior. IDS may be categorized into signature based, anomaly based or hybrid systems, based upon their method of detection. Signature based IDS detect malicious activities using pattern recognition while the anomaly based IDS detect abnormalities in activities.

A. Traditional Machine Learning

Traditional ML methods include decision trees, random forests, support vector machines, k-nearest neighbours, and ensemble classifiers. These techniques often rely on engineered features such as packet statistics, connection duration, protocol information, byte counts, and traffic rates. Their comparatively manageable computational requirements can make them suitable for edge deployments, depending on model size and feature extraction cost.

Buczak and Guven reviewed data-mining and machine-learning techniques for cybersecurity, highlighting the

© All Rights Reserved to CGCIJCTR

importance of data preparation, feature selection, and evaluation [2]. Khraisat et al. discussed IDS techniques, datasets, and persistent challenges, including detection of new attacks and the difficulty of comparing results across studies [5].

B. Deep Learning

Deep-learning methods can learn complex representations from traffic and event data. Convolutional neural networks, recurrent networks, autoencoders, and other neural architectures have been investigated for intrusion detection. Autoencoder-based systems can learn patterns associated with ordinary network activity and flag sufficiently large reconstruction errors as anomalies. Kitsune, for example, uses an ensemble of autoencoders for online network intrusion detection [12].

However, deep learning introduces challenges related to training-data requirements, computational overhead, model interpretability, and changing traffic distributions. High accuracy on a benchmark dataset does not guarantee equivalent performance in a real deployment. Sommer and Paxson highlighted the difficulties associated with applying machine learning to operational network intrusion detection, particularly the gap between controlled experiments and real-world traffic [3].

C. Hybrid Detection

A hybrid IDS can combine rule-based detection with ML classification and anomaly scoring. Known attack signatures can be handled through established rules, while learning-based components can identify unusual patterns that require further investigation. Such a design may improve operational flexibility, but its effectiveness depends on appropriate threshold selection, rule maintenance, integration, and evaluation.

IV. DATASETS AND EVALUATION CHALLENGES

Public datasets enable researchers to train and compare intrusion detection models. However, datasets differ in their traffic-generation procedures, attack categories, feature representations, collection periods, and class distributions. These differences can substantially affect experimental outcomes.

The KDD Cup 99 dataset is historically important, but its age and known limitations require caution when interpreting results [8]. UNSW-NB15 was developed to provide a more contemporary range of normal and malicious traffic patterns than older benchmark datasets [7]. CICIDS2017 offers labelled traffic involving multiple attack scenarios and has been widely used in intrusion detection research [9]. Ring et al. examined network-based IDS datasets and highlighted the importance of dataset selection and documentation [6].

Table I. Comparison of representative intrusion detection datasets

Dataset	Main characteristics	Potential use	Key limitation
KDD Cup 99 [8]	Historical benchmark with labelled connections	Baseline and reproducibility studies	Outdated traffic and known redundancy concerns
UNSW-NB15 [7]	Normal and malicious traffic across multiple categories	Classification and feature evaluation	Dataset-specific distribution may not represent deployment traffic
CICIDS2017 [9]	Labelled network traffic with multiple attack scenarios	Evaluation of supervised IDS models	Collection and labelling conditions affect generalisation
Operational IoT traffic	Device-specific traffic collected from a deployment	External and real-world validation	Collection can be costly and sensitive

A reliable evaluation should use separate training, validation, and test sets, with particular care to prevent leakage between them. Randomly splitting highly correlated records can produce overly optimistic results if similar flows or sessions occur in both training and testing data. Where possible, researchers should also conduct temporal or cross-environment evaluation.

Accuracy alone is insufficient for imbalanced cybersecurity datasets. A model can achieve high accuracy while missing rare but important attacks. Precision, recall, F1-score, false-positive rate, detection latency, and resource usage should therefore be reported. A confusion matrix can help explain whether the model is primarily missing attacks or generating excessive false alarms.

V. FEDERATED LEARNING FOR PRIVACY-AWARE CYBERSECURITY

Federated learning (FL) enables multiple participants to collaboratively train a machine learning model while retaining their local training data. A coordinating server distributes a global model to participating devices or edge gateways, which train the model using locally available datasets. The resulting model updates are transmitted to the

© All Rights Reserved to CGCIJCTR

server, aggregated, and redistributed to improve the global model. This approach reduces the need to transfer raw network records to a central location, supporting data confidentiality and privacy-aware cybersecurity [13], [14].

In IoT environments, participating organisations and edge gateways may have different devices, traffic patterns, and security requirements. Federated learning allows these participants to develop collaborative intrusion detection models without directly sharing their complete network datasets. For example, gateways in industrial and healthcare networks can contribute to a shared model for identifying suspicious traffic, unauthorised access attempts, and abnormal communication patterns. Existing research has examined federated learning applications in intrusion detection and privacy-preserving IoT security, highlighting its potential for distributed cybersecurity systems [21]–[24].

A typical federated learning-based cybersecurity architecture consists of IoT devices, edge gateways, a central coordination server, and a security monitoring module. IoT devices generate network traffic and operational data, which are analysed locally by their associated gateways. Each gateway extracts relevant features and trains a local model to distinguish normal network behaviour from potentially malicious activities. The gateways then transmit model updates to the coordination server, where the updates are aggregated using techniques such as Federated Averaging (FedAvg). The revised global model is distributed to participating gateways for subsequent training and local threat detection [13], [14].

Despite its privacy advantages, federated learning does not automatically guarantee complete data confidentiality. Model updates may reveal information about local training datasets, while malicious or compromised participants can submit manipulated updates to affect global model performance. Adversarial machine learning research highlights the importance of addressing such threats through appropriate detection and mitigation mechanisms [15]–[17]. Secure aggregation, differential privacy, participant authentication, and protected communication channels can strengthen the framework by reducing information exposure and limiting unauthorised participation. However, these mechanisms must be selected according to the system's security requirements and available computational resources.

Another challenge is the variation in local data distributions across participating IoT networks. Different gateways may observe different device types, traffic characteristics, and attack patterns, resulting in non-independent and identically distributed (non-IID) datasets. Consequently, a global model may perform differently across individual participants. Evaluating the model using precision, recall, F1-score, false-positive rate, and detection latency can help assess its effectiveness under different network conditions. Research on intrusion detection and machine learning also emphasises the importance of representative datasets and careful evaluation when developing reliable cybersecurity models [2], [5], [6].

Practical deployment must also consider communication overhead, intermittent connectivity, and limited device resources. A suitable approach is to perform federated learning primarily on capable edge gateways rather than on every constrained IoT sensor. Gateways can continue local monitoring using a previously validated model during temporary network interruptions and synchronise model updates when connectivity is restored. Model validation, version control, and rollback mechanisms can further reduce the risk of unreliable updates affecting security operations. In industrial IoT environments, combining federated learning with appropriate edge security mechanisms can support collaborative threat detection while maintaining local data control [24].

In conclusion, federated learning provides a promising approach to privacy-aware cybersecurity by enabling collaborative model training without routinely transferring raw network data to a central server. However, its effectiveness depends on addressing privacy leakage, malicious model updates, heterogeneous data distributions, and resource limitations. Integrating federated learning with secure aggregation, participant authentication, robust update validation, and continuous performance monitoring can improve the reliability of distributed intrusion detection. This approach can support scalable cybersecurity solutions for heterogeneous IoT environments while balancing data confidentiality, detection accuracy, and operational efficiency.

VI. ADVERSARIAL MACHINE LEARNING AND EMERGING THREATS

AI-based cybersecurity systems can themselves become targets. Adversarial machine learning studies how manipulated inputs, compromised training data, or other attacks can affect model behaviour. NIST's adversarial machine-learning taxonomy provides terminology for analysing attack and mitigation strategies [15].

Table II. AI-related threats and possible mitigation measures

Threat	Potential effect on IDS	Possible mitigation
Data poisoning	Corrupts training data or model behaviour	Data validation, trusted sampling and update screening
Evasion attacks	Changes malicious traffic to avoid detection	Robustness testing and complementary detection rules
Model or update leakage	Reveals information through model outputs or updates	Access controls, privacy assessment and secure aggregation

© All Rights Reserved to CGCIJCTR

Distribution shift	Reduces detection performance as traffic changes	Drift monitoring and controlled retraining
False-positive overload	Generates excessive alerts and burdens analysts	Threshold calibration and alert prioritisation

Adversarial attacks can undermine the assumption that training and deployment data follow similar distributions [16], [17]. Consequently, model evaluation should include more than clean test data. Robustness experiments should document the attack assumptions, perturbation methods, data conditions, and impact on detection metrics.

Human oversight remains important, particularly for high-impact responses such as blocking industrial devices or disrupting healthcare systems. AI outputs should support investigation and prioritisation rather than automatically triggering every possible defensive action.

VII. PROPOSED HYBRID CYBERSECURITY ARCHITECTURE

This review proposes a conceptual architecture that combines local traffic monitoring, edge-based detection, federated model improvement, and central security coordination. The architecture is a design proposal derived from the reviewed literature; it is not presented as a tested system.

Fig. 2. Conceptual hybrid AI-based IoT security architecture



The architecture contains four principal functions. First, IoT devices generate network and operational events. Second, an edge gateway extracts features and performs local inference, reducing the need to send all raw traffic to a central server. Third, a federated coordinator supports collaborative model improvement by aggregating validated updates from participating gateways. Fourth, a security team reviews alerts, manages policies, and supervises high-impact responses.

The design should include device authentication, encrypted communications, role-based access control, audit logging, model versioning, and a rollback mechanism. Local inference should remain available during temporary communication failures. The architecture also requires a fallback process for uncertain predictions, since false positives can interrupt legitimate services and false negatives can allow attacks to continue.

Table III. Proposed evaluation plan for the hybrid architecture

Evaluation dimension	Suggested measurement	Purpose
Detection effectiveness	Precision, recall, F1-score	Measure attack identification quality
False alarms	False-positive rate	Estimate operational alert burden
Response speed	Detection latency	Assess time sensitivity
Edge efficiency	CPU, memory and energy use	Assess suitability for IoT gateways
Privacy	Raw-data transfer and leakage assessment	Examine data exposure risks
Robustness	Performance under drift and poisoning tests	Assess resilience to changing or manipulated data

These measurements should be evaluated against a clearly defined baseline, such as a conventional ML classifier or a rule-based IDS. Results should be reported for each dataset and environment rather than combined in a way that hides differences. No numerical performance claims are made here because the proposed architecture has not been experimentally evaluated.

VIII. RESEARCH GAPS AND FUTURE DIRECTIONS

Several research gaps remain relevant to practical AI-driven IoT security.

A. **Generalisation across environments**: Models should be tested across different device types, network configurations, and time periods. Cross-dataset testing can help determine whether detection depends on general attack characteristics or dataset-specific patterns.

B. **Resource-efficient detection:** IoT gateways may have limited memory, processing capacity, and power. Future work should compare compact models, feature selection, quantisation, and selective inference while reporting actual hardware measurements.

C. **Trustworthy federated learning:** Research should evaluate secure aggregation, malicious-client detection, privacy leakage, and the impact of non-identically distributed data. The trade-off between communication cost and detection quality should also be measured [14], [21]–[24].

© All Rights Reserved to CGCIJCTR

D. **Explainability and operational usability:** Security analysts need meaningful explanations of alerts, including the traffic features or behaviours that contributed to a prediction. Explanation methods must be assessed for stability and usefulness rather than treated as inherently reliable.
E. **Reproducibility:** Studies should clearly report dataset versions, preprocessing, train-test splits, model parameters, baseline methods, and evaluation metrics. This would make comparisons more reliable and support independent validation.
F. **Alignment with risk management:** Technical detection should be integrated with governance, response, recovery, and organisational risk processes. Frameworks such as NIST CSF 2.0 provide a broader structure for connecting technical controls with cybersecurity risk management [1]. Threat landscape reporting, including ENISA's work, can help researchers understand evolving operational priorities [25].

IX. CONCLUSION

AI-driven intrusion detection offers useful capabilities for identifying suspicious activity in IoT networks, particularly when traditional signature-based mechanisms are insufficient to detect unfamiliar patterns. Traditional machine learning, deep learning, and anomaly detection each provide different trade-offs involving detection quality, computational cost, and interpretability. Public datasets support reproducible experiments, but their age, collection conditions, and distribution differences can limit the generalisability of reported results.

Federated learning provides a mechanism for collaborative model training without routinely centralising raw training records, although it introduces additional challenges involving malicious updates, privacy leakage, communication overhead, and heterogeneous data. Adversarial machine learning further demonstrates that security models require robustness assessment and ongoing monitoring.

The conceptual hybrid architecture presented in this review combines edge-based detection, federated model improvement, and human-supervised response. Future work should implement and evaluate this design using clearly documented datasets, realistic baselines, cross-environment testing, and measurements of detection performance, latency, resource consumption, privacy, and robustness. These steps are necessary to move AI-based IoT cybersecurity from promising experimental results toward dependable operational deployment.

REFERENCES

[1] C. Pascoe, S. Quinn, and K. Scarfone, "The NIST Cybersecurity Framework (CSF) 2.0," NIST Cybersecurity White Paper 29, National Institute of Standards and Technology, 2024, doi: 10.6028/NIST.CSWP.29.

[2] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Commun. Surveys Tuts., vol. 18, no. 2, pp. 1153–1176, 2016, doi: 10.1109/COMST.2015.2494502.

[3] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in Proc. IEEE Symp. Security and Privacy, 2010, pp. 305–316, doi: 10.1109/SP.2010.25.

[4] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," J. Netw. Comput. Appl., vol. 36, no. 1, pp. 16–24, 2013, doi: 10.1016/j.jnca.2012.09.004.

[5] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets and challenges," Cybersecurity, vol. 2, art. no. 20, 2019, doi: 10.1186/s42400-019-0038-7.

[6] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, "A survey of network-based intrusion detection data sets," Comput. Security, vol. 86, pp. 147–167, 2019, doi: 10.1016/j.cose.2019.06.005.

[7] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems," in Proc. Military Communications and Information Systems Conf. (MilCIS), 2015, doi: 10.1109/MilCIS.2015.7348942.

[8] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in Proc. IEEE Symp. Computational Intelligence for Security and Defense Applications, 2009, doi: 10.1109/CISDA.2009.5356528.

[9] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in Proc. Int. Conf. Information Systems Security and Privacy (ICISSP), 2018, pp. 108–116, doi: 10.5220/0006639801080116.

[10] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," J. Inf. Security Appl., vol. 50, art. no. 102419, 2020, doi: 10.1016/j.jisa.2019.102419.

[11] M. Macas, C. Wu, and W. Fuertes, "A survey on deep learning for cybersecurity: Progress, challenges, and opportunities," Comput. Netw., vol. 212, art. no. 109032, 2022, doi: 10.1016/j.comnet.2022.109032.

[12] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An ensemble of autoencoders for online network intrusion detection," in Proc. Network and Distributed System Security Symp. (NDSS), 2018, doi: 10.14722/ndss.2018.23204.

[13] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in Proc. 20th Int. Conf. Artificial Intelligence and Statistics (AISTATS), 2017, pp. 1273–1282.

[14] P. Kairouz et al., "Advances and open problems in federated learning," Found. Trends Mach. Learn., vol. 14, nos. 1–2, pp. 1–210, 2021, doi: 10.1561/2200000083.

[15] A. Vassilev, A. Oprea, A. Fordyce, and H. Andersen, "Adversarial machine learning: A taxonomy and terminology of attacks and mitigations," NIST AI 100-2 E2023, National Institute of Standards and Technology, 2024, doi: 10.6028/NIST.AI.100-2e2023.

[16] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," in Proc. Int. Conf. Learning Representations (ICLR), 2015.

[17] B. Biggio and F. Roli, "Wild patterns: Ten years after the rise of adversarial machine learning," Pattern Recognit., vol. 84, pp. 317–331, 2018, doi: 10.1016/j.patcog.2018.07.023.

[18] A. Kaur, Y. Kumar, and P. K. Singh, "Clustering IoT data using machine learning methods: A survey," in IoT, Big Data and AI for Improving Quality of Everyday Life: Present and Future Challenges. Singapore: Springer, 2023, pp. 39–57, doi: 10.1007/978-3-031-35783-1_3. [CGC Landran institutional publication record: Chandigarh Engineering College–CGC].

[19] K. Kaur, "A study of cyber security and cyber threats," CGC International Journal of Contemporary Technology and Research, vol. 3, no. 1, 2020. Affiliation: Department of Computer Science and Engineering, Chandigarh Engineering College, Landran, India. doi: 10.46860/cgcijctr.2020.12.26.154.

© All Rights Reserved to CGCIJCTR

[20] A. Kaur, Y. Kumar, and P. K. Singh, "IoT based framework for heart disease diagnose," in IoT, Big Data and AI for Improving Quality of Everyday Life: Present and Future Challenges. Singapore: Springer, 2023, pp. 59–73, doi: 10.1007/978-3-031-35783-1_4. [CGC Landran institutional publication record: Chandigarh Engineering College–CGC].

[21] A. Belenguer, J. A. Pascual, and J. Navaridas, "A review of federated learning applications in intrusion detection systems," Comput. Netw., vol. 258, art. no. 111023, 2025, doi: 10.1016/j.comnet.2024.111023.

[22] A. Vyas, P. C. Lin, R. H. Hwang, and M. Tripathi, "Privacy-preserving federated learning for intrusion detection in IoT environments: A survey," IEEE Access, vol. 12, pp. 127018–127050, 2024, doi: 10.1109/ACCESS.2024.3454211.

[23] H. Zhang, J. Ye, W. Huang, X. Liu, and J. Gu, "Survey of federated learning in intrusion detection," J. Parallel Distrib. Comput., vol. 195, art. no. 104976, 2025, doi: 10.1016/j.jpdc.2024.104976.

[24] S. Ali, Q. Li, and A. Yousafzai, "Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: A survey," Ad Hoc Netw., vol. 202, art. no. 103320, 2024, doi: 10.1016/j.adhoc.2023.103320.

[25] European Union Agency for Cybersecurity (ENISA), "ENISA threat landscape 2025," 2025. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscap

© All Rights Reserved to CGCIJCTR

© All Rights Reserved to CGCIJCTR