JSUCIT

Journal of Shaqra University for Computing and Information Technology
ISSN 2961-4279 (Print) || ISSN 2961-4287 (Online)

AI-Driven Cybersecurity for Edge and IoT in Smart Cities: A Systematic Review of Methods, Datasets, and Deployment Challenges

Jawaher Badr Alotibi
Department of Computer Science, College of Computing and Information Technology, Shaqra University, Shaqra
Corresponding Author Email: ad.jawaher25@gmail.com

Abstract: Smart cities rely on Internet of Things (IoT) devices and edge computing to support essential urban services. However, limited resources, different network environments, and growing cyber threats make cybersecurity more challenging. This systematic review explores how artificial intelligence (AI) can improve cybersecurity in Edge–IoT environments related to smart cities. It focuses on detection methods, datasets, model performance, and practical deployment challenges. The review followed the PRISMA 2020 guidelines. Searches were conducted in IEEE Xplore, ACM Digital Library, and ScienceDirect. The search covered English-language journal and conference papers published between January 2018 and November 2025. A total of 1,035 records were identified, and 35 studies were included after screening and eligibility assessment. Information about the studies, AI methods, datasets, threat types, evaluation metrics, and reported limitations was collected and analyzed. Study quality was assessed using the appropriate Joanna Briggs Institute (JBI) critical appraisal tool for each study design. The reviewed studies covered deep learning, traditional machine learning, federated learning, lightweight learning methods, and explainable AI. Common datasets included TON_IoT, BoT-IoT, CIC-IDS2017, and NSL-KDD. Some studies reported high detection accuracy. However, high accuracy alone does not mean that a model is ready for real-world use. Other factors must also be considered, including external validation, performance across different datasets, computational cost, latency, energy consumption, and resistance to attacks. The findings highlight the need for clearer evaluation methods, more diverse datasets, and testing under realistic edge-computing conditions. This review brings together evidence on AI methods, model performance, and deployment challenges. It also identifies areas that need further research to support more reliable cybersecurity solutions for smart-city Edge–IoT systems.

Keywords:
Smart Cities; Edge Computing; IoT; Cybersecurity; Machine Learning; Deep Learning; Federated Learning; TinyML; Explainable AI (XAI); Intrusion Detection; Anomaly Detection; MEC; Fog Computing; AI-Driven Security.

I. Introduction :

Smart cities are increasingly devlop into highly interconnected environments where huge numbers of sensors, loT devices, and distributed computing nodes work together to deliver real-time urban services such as traffic optimization, environmental monitoring, energy management, public safety, and intelligent transportation. To face the stringent latency, reliability, and scalability requirements of these applications, modern smart cities have shifted from centralized cloud computing to Edge, Fog, and Multi-access Edge Computing (MEC) architectures that process data closer to its source. This transfer promote responsiveness and minimize bandwidth consumption, but it also introduces significant security defy.

The decentralized and resource-limited nature of IoT and edge systems expands the range of attacks and exposes smart city infrastructure to various cyber threats, including identity theft, botnets, distributed denial-of-service (DDoS) attacks, data manipulation, and anomalous behavior targeting critical urban services. Traditional security mechanisms for strong cloud servers are usually designed to protect lightweight, distributed, and heterogeneous edge environments. Artificial intelligence (AI) has become a key driver of cybersecurity in smart cities thanks to its ability to learn complex attack patterns, detect emerging threats, adapt to dynamic environments, and operate efficiently in distributed environments. Technologies such as machine learning (ML), deep learning (DL), unit learning (FL), TinyML, and interpretable artificial intelligence (XAI) are increasingly being integrated into intrusion and anomaly detection systems deployed across the edge layers of the Internet of Things (IoT). Recent studies demonstrate significant performance improvements when using AI to protect critical urban infrastructure.

Despite this proceed, the current research landscape remains fragmented. A systematic review is therefore needed to consolidate the scattered evidence, compare methodological approaches, and identify consistent patterns and shortcomings across existing studies. Many existing reviews center on primarily on cluster security, cloud protection, or traditional machine learning approaches, while AI-managed cybersecurity, particularly in edge-based smart city architectures, has received little attention. There is a shortage of standardized evidence regarding the methodologies used, datasets employed, reported assessment metrics, and actual implementation challenges in this rapidly growing field.

The scope of this review is limited to AI-based cybersecurity techniques applied within Edge, Fog, and MEC architectures in IoT-enabled smart-city environments, with a focus on intrusion detection, anomaly detection, and threat prediction models. To address this hole , this systematic review brings together recent

empirical studies applying artificial intelligence (AI) techniques to protect edge and large-scale computing infrastructure in smart cities.

Through analyzing the methods, datasets, threat models, and performance assessment practices described in the literature, the review aims to provide a comprehensive understanding of current developments and identify key challenges, limitations, and future research directions necessary for achieving robust, scalable, and credible cybersecurity for next-generation smart city environments. Therefore, this systematic review aims to synthesize recent empirical studies on AI-driven cybersecurity for Edge and IoT systems in smart cities, focusing on the methods used, datasets employed, threat models addressed, performance outcomes, and real-world deployment challenges.

A. Research Questions:

Q1: Which artificial intelligence techniques have been applied to cybersecurity in Edge–IoT environments relevant to smart cities, and what security tasks do they address?

Q2: Which datasets, threat categories, and evaluation metrics are used to assess AI-driven cybersecurity models in these environments?

Q3: How do the reported performance outcomes vary across AI techniques and datasets, and what methodological factors may influence the reported results?

Q4: To what extent have the reviewed approaches been evaluated under realistic edge-deployment constraints, including latency, energy consumption, computational resources, privacy, and adversarial robustness?

Q5: What methodological limitations and deployment challenges remain insufficiently addressed in the current literature?

II. METHOD :

This systematic review was conducted in accordance with the PRISMA 2020 guidelines to guarantee transparency and replicability . A comprehensive literature search was performed across three major academic databases known for their high-quality peer-reviewed publications in artificial intelligence and cybersecurity: IEEE Xplore, ACM Digital Library, and ScienceDirect (Elsevier). This review was not prospectively registered in PROSPERO or another systematic review registry. The review methods and procedures are described in this manuscript to support transparency and reproducibility. The absence of prospective registration is acknowledged as a methodological limitation. These databases were selected because they cover the majority of cutting-edge research in IoT, Edge/Fog computing, machine learning, and security. The search covered studies published between January 2018 and November 2025, reflecting the period during which AI-driven cybersecurity techniques have rapidly evolved in smart-city and Edge–IoT systems. The last search was conducted on 2 November 2025 for IEEE Xplore, ACM Digital Library, and ScienceDirect.

The search strategy depend on a structured Boolean query joining synonyms related to smart cities, IoT/IIoT, Edge/MEC computing, cybersecurity, and artificial intelligence. The final search string included terms such as 'smart city,' 'IoT,' 'edge computing," "intrusion detection," and "machine learning," connected using AND/OR operators to capture all relevant variations. Only peer-reviewed journal and conference papers written in English were considered. Exported records from all databases were downloaded in RIS, CSV, and BibTeX formats and subsequently merged and screened using Rayyan to facilitate the identification and deduplication of overlapping studies. The complete search strings used for each database are provided in Appendix B to ensure full transparency and reproducibility.

The eligibility criteria were determined before screening. Studies were inclusive if they focused on IoT or IIoT systems within smart-city environments, used Edge, Fog, or MEC architectures, and employed AI-based security techniques such as ML, DL, FL, TinyML, or XAI. Eligible studies were required to address intrusion detection, anomaly detection, or threat prediction and provide quantitative evaluation metrics such as Accuracy, F1-Score, AUC, Precision, Recall, latency, or energy consumption. Exclusion criteria discarded papers unrelated to smart-city infrastructures, studies using blockchain-only security, non-AI-based methods, theoretical papers without experiments, surveys, tutorials, reviews, and non-peer-reviewed content.

A. Registration:

This review was not prospectively registered in PROSPERO or any other review registry. As the included studies were highly heterogeneous in terms of models, datasets, and evaluation metrics, no meta-analysis was performed; instead, a narrative synthesis approach was adopted.

The study-selection process followed four PRISMA-aligned stages. First, 1035 records were collect from all sources. After deleting 237 duplicates, 798 unique studies remained. Title and abstract screening excluded approximately 641 papers that did not achive the inclusion criteria, leaving 157 candidate studies. A relevance-filtering step was then applied: papers matching at least three inclusion keyword groups and containing no exclusion keywords were considered high-priority, resulting in 49 studies. Finally, full-text eligibility evaluation and importance ranking based on technical depth, contribution, and methodological quality reduced the dataset to 35 primary studies, which form the basis of this review.

To guarantee screening transparency and minimize bias, all study-selection steps were performed by two independent reviewers using Rayyan . Each reviewer tagged studies as 'include,' 'exclude,' or 'maybe' through title/abstract screening and full-text evaluation. the conflict was resolved during discussion until a consensus was reached, and when unpredictability persisted, previously defined eligibility criteria were implemented to achieve a consensus. This dual-reviewer approach improved the methodological accuracy of the selection process .

The primary outcomes of interest were performance metrics reported by the included studies, including Accuracy, Precision, Recall, F1-Score, AUC, latency, and energy consumption. Additional variables extracted included: AI technique, model architecture, deployment layer

(Edge/Fog/MEC), dataset type, threat category, and experimental environment.

Data extraction was conducted using a structured Excel sheet, capturing detailed characteristics from each study, including bibliographic information, application domain, computing layer (Edge, Fog, MEC), AI technique, model architecture, dataset used, threat type, evaluation metrics, experimental setup, and reported limitations. To guarantee consistency, extracted data were manually validated. The methodological quality of the involved studies was assessed using the JBI Critical Appraisal Checklist, evaluating the clarity of research aims, dataset reliability, ML model validation, handling of class imbalance, rigor of experimental procedures, and the appropriateness of reported metrics. Each study was classified as low, moderate, or high risk of bias. Two reviewers independently assessed the risk of bias for each study using the JBI checklist, and disagreements were resolved through discussion to ensure consistency.

III. Results

A. Study Selection

The study selection process followed the PRISMA 2020 guidelines. A total of 1,035 records were identified through searches of IEEE Xplore, ACM Digital Library, and ScienceDirect. After removing 237 duplicate records, 798 records remained for title and abstract screening. At this stage, 641 records were excluded because they did not meet the predefined inclusion criteria, leaving 157 records for full-text assessment. The full texts of all 157 records were reviewed against the predefined eligibility criteria. A relevance-based prioritization procedure was then used to organize the studies for closer consideration, resulting in 49 studies being classified as high priority.

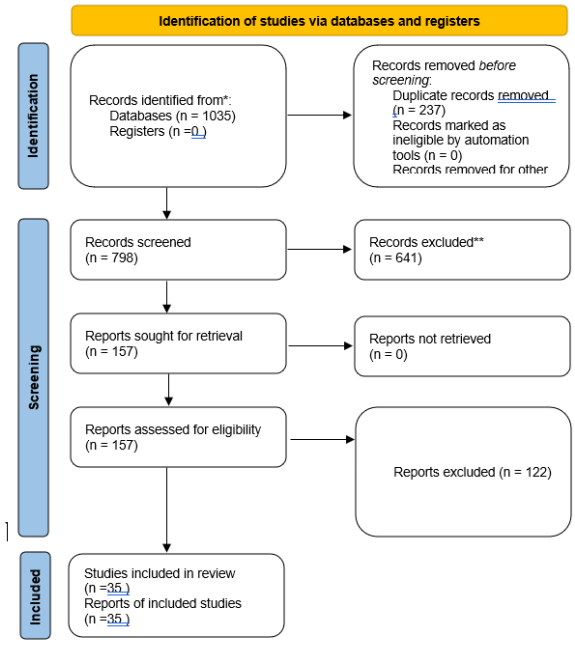


Figure 1.PRISMA 2020 Flow Diagram for Study Selection

This prioritization was an internal review procedure and did not constitute a separate formal exclusion stage. Following the final assessment of eligibility, methodological rigor, experimental validity, dataset relevance, and applicability to smart-city environments, 35 studies were included in the final qualitative synthesis. Figure 1 presents the PRISMA 2020 flow diagram summarizing the study selection process.

B. Study Characteristics

The 35 included studies were published between 2018 and 2025, underlined a period of rapid advancement in AI-driven cybersecurity for Edge–IoT systems within smart cities. Most of these studies showed up in reputable venues such as IEEE journals and conferences, ACM symposiums, and Elsevier publications. Collectively, the studies focused up a wide spectrum of smart-city applications, including traffic management, industrial IoT, environmental sensing, surveillance systems, public safety, and critical infrastructure protection. A detailed summary of all 35 included studies covering publication year, source, title, and authors is provided in **Table 1** (Appendix A).

A various set of artificial intelligence techniques was used throughout the chosen studies. Deep Learning (DL) techniques such as Convolutional Neural Networks (CNNs), Long Short-Term Memory networks (LSTMs), Gated Recurrent Units (GRUs), Autoencoders, and hybrid DL architectures represented the dominant approach, appearing in more than 60% of the included papers.

Traditional Machine Learning (ML) algorithms, for example, Support Vector Machines, Random Forest, K-Nearest Neighbors, and Decision Trees were also commonly used, particularly in earlier studies. An increasing number of studies adopted Federated Learning (FL) techniques to enable collaborative and privacy-preserving intrusion detection across distributed edge nodes. Moreover, TinyML appeared in many studies aiming to deploy compact ML models on resource-constrained IoT devices. Explainable AI (XAI) was incorporated into only some papers, indicating an early but emerging interest in model interpretability.

Concerning system architecture, the chosen studies covered a various of distributed computing layers. Edge computing was the most commonly used, offering low-latency inference nearby data sources. Fog computing served as an intermediate layer to facilitate scalable, hierarchical threat analysis. Multi-access Edge Computing (MEC) was used in a lower number of studies but displayed promise for integration with 5G-enabled smart-city services. Several studies implemented hybrid edge-cloud architectures to balance accuracy and computational efficiency.

The threat types addressed in these studies varied considerably. The most common categories included DDoS and botnet attacks, spoofing and impersonation, data integrity violations, abnormal sensor behavior, and general intrusion detection. More than half of the included works focused specifically on DDoS and anomaly detection because of their prevalence and severity in real-world smart-city systems.

A range of datasets was used to evaluate model performance. The most frequently employed datasets were TON_IoT, BoT-

IoT, CIC-IDS2017, and NSL-KDD, alongside several custom datasets derived from smart-city sensors, surveillance networks, and industrial IoT environments. TON_IoT and BoT-IoT were particularly common because of their realistic representation of modern cyber threats.

A summary of the main findings of each study, including AI technique, dataset used, threat type, and key performance metrics, is provided in Appendix D.

Evaluation metrics varied but consistently included accuracy, precision, recall, F1-score, and AUC, with many studies also reporting latency and computational overhead to assess suitability for edge deployment. While several DL-based intrusion detection models achieved accuracy levels approaching 99%, their performance substantially decreased when deployed on highly resource-constrained edge or IoT devices.

Risk of Bias Assessment: The risk of bias assessment using the JBI Critical Appraisal Checklist showed that most studies were rated as *moderate risk of bias*, mainly due to limited dataset transparency and lack of external validation. A smaller number of studies demonstrated low risk, while a few exhibited high risk because of insufficient methodological reporting. Detailed ratings for each study are presented in Appendix C.

C. *Synthesis of Findings*

The synthesis of the 35 included studies discloses a noticeable trend in the direction of the use of AI-driven intrusion detection systems (IDS) to improve the security of IoT and edge networks in smart cities. Deep learning approaches, especially CNNs and autoencoders, constantly surpassed traditional ML methods in detecting complex and evolving attack patterns. Federated learning offered significant benefits in privacy preservation and distributed intelligence; however, it met challenges related to communication cost and heterogeneity within participating devices. TinyML provided lightweight variants fitting for constrained IoT environments, though at the cost of decreased detection accuracy. A significant theme emerging from the literature is the increasing shift away from centralized cloud-based detection toward distributed and decentralized detection at the Edge or Fog layer.

This transformation permits real-time responses to cyber threats and reduces latency but needs careful consideration of computation limits, model synchronization, and robustness across heterogeneous devices. Despite promising advances, only a minority of studies validated their methods under realistic smart-city conditions, and even fewer addressed adversarial attacks or explainability, leaving significant gaps for future exploration.

In general, the 35 studies show the capability of AI-driven cybersecurity for securing smart-city infrastructures; however, they also highlight continuing challenges associated with scalability, generalizability, resource limitations, and real-world deployment preparedness.

D. *Reporting Bias and Certainty of Evidence*

No formal assessment of reporting bias or certainty of evidence was conducted due to the high heterogeneity of study designs, datasets, and evaluation metrics. As the included studies differed substantially in methodology and outcome measures, it was not feasible to apply a unified framework to evaluate the certainty of evidence.

IV. Discussion

The outcomes of this systematic review emphasize the significant advancement made in implementing artificial intelligence to ensure Edge-IoT infrastructures in smart cities, while additionally displaying many constraints and knowledge gaps that should be managed to guarantee practical, scalable deployment. Over the included studies, deep learning methods—especially convolutional neural networks and autoencoder-based architectures—revealed superior performance relative to traditional machine learning techniques. This outcome fits with broader cybersecurity literature, in which DL models continuously surpass classical ML in discovering complex, high-dimensional attack patterns. Nevertheless, the dominance of DL in the shown studies also reveals a research disparity, since only a limited number of studies examined lightweight or energy-efficient options suitable for seriously constrained IoT devices.

An interesting pattern that is evident from our findings is a move towards distributed detection at the edge or fog level. Moreover, this trend is due to the increasing needs of low latency, high scalability and real-time response in smart-city scenarios. Additionally, decentralized learning and inference exhibited benefits in various studies, however, also introduced new issues such as synchronization overhead , data distributional shift across nodes, and attacks on the poisoned collaborative settings such as federated.

The study of datasets also highlights a dependence on few benchmark resources like TON_IoT and BoT-IoT. Although these datasets provide realistic attack scenarios, there are still concerns regarding dataset overfitting and limited generalization to real-world intelligent city infrastructure, where traffic behavior, device diversity, and attack patterns differ greatly. Moreover, only a small minority of studies used real-world deployments or custom datasets, and a negligible amount validated their methods with realistic noise, packet loss, or mobility. Consequently, this discrepancy indicates that, although promising in small testing environments, the deployment of many existing models may be challenging in fully functional urban systems.

A particularly interesting observation is the scarce presence of XAI, adversarial robustness, and privacy preservation. Given that smart-city services are critical, transparency and resistance to adversarial manipulation are essential in order to gain trust and ensure reliable operation. However, very few studies examined how to interpret model decisions, defend against adversarial attacks, and satisfy regulations concerning privacy. Therefore, this low inclusion reveals a gap between what is being done and the real safety, regulatory, and ethical requirements of large-scale smart-city deployments.

While overall model performance was high—often above 95% accuracy—the results also showed that this performance drops noticeably on limited edge devices because of their restricted

processing power and memory. Because of this, there is a need for smaller model architectures, model compression, TinyML methods, or hardware–software co-design that fits IoT environments. Moreover, many studies focused mainly on accuracy as the key metric, while giving little attention to latency, energy consumption, or real-time performance—factors that are essential in smart-city systems.

Overall, the findings suggest that AI-driven cybersecurity has strong potential to improve the resilience of smart-city infrastructures, especially through deep learning and distributed detection architectures. However, there are still significant gaps related to real-world deployment readiness, edge-device limitations, adversarial robustness, interpretability, and the limited diversity of the datasets used. Because of these gaps, it will be essential to address them in order to move from experimental prototypes to reliable, large-scale cybersecurity frameworks that can protect next-generation smart environments. These findings directly align with the objectives of this review by evaluating the effectiveness of AI-driven IDS models, identifying the limitations of current Edge–IoT deployments, and clarifying the methodological gaps that hinder real-world applicability.

A. Research Gaps

Several notable research gaps emerged from the reviewed literature, highlighting areas that remain underexplored despite their importance for secure Edge–IoT deployments. First, there is limited work using real-world smart-city deployments, as most studies rely mainly on simulations or controlled lab environments. Second, many emerging AI techniques—such as Explainable AI, adversarial defense methods, and lightweight TinyML models—are still underused, even though they are important for devices with limited resources. In addition, Federated Learning appears in only a small number of studies, despite the fact that it can offer distributed and privacy-preserving security. Moreover, existing research depends heavily on a few datasets, which raises concerns about dataset diversity and whether IDS models can adapt to unseen attack patterns. Finally, only a few studies evaluated energy consumption, latency, communication cost, or system robustness under hardware limits—metrics that are essential for Edge–IoT deployment. Together, these gaps show the need for approaches that consider real-world constraints, interpretability, and adaptive learning.

B. Limitations:

Despite its comprehensive coverage, this review has several limitations. The high heterogeneity in datasets and evaluation metrics prevented conducting a meta-analysis, and the inclusion of English-only studies may have excluded relevant research. Additionally, some studies lacked methodological detail, which may have influenced the accuracy of the risk-of-bias assessment.

C. Future Directions

Based on these findings, several promising directions appear for future work. First, more research is needed on lightweight and energy-efficient AI models—such as TinyML and compressed deep-learning architectures—so they can work reliably on resource-limited IoT devices. Second, integrating Explainable AI into IDS models can help improve interpretability, trust, and regulatory compliance in smart-city environments. Third, adversarial machine learning should be given more focus to protect models from evasion, poisoning, and mimicry attacks. Fourth, future studies should use real-world data, sensor logs, and operational traffic from actual smart-city systems instead of relying only on benchmark datasets. Additionally, federated and decentralized learning should be expanded to improve privacy and scalability across edge environments. Finally, researchers should evaluate not only accuracy but also latency, energy use, communication overhead, and hardware limitations, so that results become more suitable for practical deployment.

D. Implications for Practice:

The findings of this review offer practical guidance for engineers, system designers, and smart-city operators by emphasizing the need for lightweight models, decentralized learning frameworks, and robustness-focused evaluation to ensure effective deployment in real urban environments.

E. Implications for Policy:

At the policy level, the results highlight the importance of establishing standards for model transparency, privacy-preserving data sharing, energy-aware AI design, and unified evaluation benchmarks to guide future smart-city cybersecurity regulations.

V. Conclusion

This systematic review examined 35 studies on AI-based cybersecurity for Edge and IoT systems in smart cities, showing both strong progress and remaining challenges. Overall, deep-learning models achieved high accuracy in detecting complex cyberattacks, while federated learning and TinyML provided promising—though still developing—solutions for decentralized and lightweight security. However, the field is still limited by its dependence on a small number of datasets, the lack of real-world validation, and the minimal focus on adversarial robustness and interpretability. Therefore, the findings highlight the increasing potential of AI to strengthen smart-city cybersecurity, while also stressing the need for more practical, transparent, and scalable approaches that can operate in diverse and changing urban environments. Continued research in these areas will be essential for securing future intelligent and interconnected cities.

Conflicts of Interest: The author declares no conflicts of interest

Data Availability: All extracted data, screening logs, and synthesis tables generated during this review are available from the author. The original articles used in the analysis are publicly available through IEEE Xplore, ACM Digital Library, and ScienceDirect.

REFERENCES

[1] Kowtarapu K, Kowtarapu U. Strengthening IoT Security with Machine Learning-Powered Intrusion Detection Systems for Critical Infrastructure and Smart Cities.

[2] Zhukabayeva T, Ahmad Z, Adamova A, Satybaldina D. Penetration Testing-Aware IDS for Wireless Networks in Urban Digital Ecosystems Integrated with Edge Computing and Machine Learning.

[3] Tahsin MS, Aziz MY, Kabbo TA, Tahsin T. Data Security Model Using Deep Learning and Edge Computing for IoT in Smart City.

[4] Alrashdi I, Alqazzaz A, Aloufi E, Alharthi R, Alsubhi A, Zohdy MA. AD-IoT: Anomaly Detection of IoT Cyberattacks in Smart City Using Machine Learning.

[5] Waseem AR, Abrar M, Ullah M, Faizan M. Advanced Intrusion Detection in the Industrial IoT Using Federated Learning and LSTM Models.

[6] Tripathy SS, Guduri M, Subramaniam C, Khare N. Adaptive Explainable AI Framework for Securing Consumer Electronics-Based IoT Applications in Fog-Cloud Infrastructure.

[7] Gai K, Qiu M, Li Z. Decentralized AI for Smart Cities: A Federated Learning Framework for Resilient Cybersecurity.

[8] Khattak HA, Khattak HS, Khan A, Ullah F, Ullah Z, Khan S. DeepSDN: A Deep Learning-Based SDN Model for Cyberthreat Detection in IoT Networks.

[9] Shende R, Gite S, Mehta MV. Drone-Guard: Self-Supervised Deep Learning Framework for Real-Time Anomaly Detection in UAV Surveillance Systems.

[10] Lin CC, Kuo CL, Yang CW. Enhancing Cybersecurity in Smart Cities Using a Hybrid Deep Neural Network Model.

[11] Ali AM, Omar M, Bashir AK, Koucheryavy Y. Evaluating ML-Driven IDS in IoT: Performance and Energy Consumption.

[12] Dahiya DS, Roy S, Singh SK. Federated Learning-Enabled Edge Intelligence for Sustainable Smart Cities.

[13] Hussain R, Qadir J, et al. FL-DPCSA: Federated Learning with Differential Privacy for Smart Grid Cache Side-Channel Attack Detection.

[14] Banik S, Chattopadhyay A, Nandi S. Host-Based Intrusion Detection Framework for IoT Using Machine Learning.

[15] Santos J, Silva M, Costa A. Optimizing Anomaly Detection Models for Edge IIoT Using Firefly Algorithm Hyperparameter Tuning.

[16] Alshammari T, et al. SPARK and SAD: Deep Learning Frameworks for Intrusion Detection in SCADA Systems.

[17] Li X, Zhou Y, Wang J. SwinIoT: A Hierarchical Transformer-Based Framework for Behavioral Anomaly Detection in Smart Cities.

[18] Liu Y, Chen J, Zhang X. Enhancing Privacy Preservation of Federated CNN-Based IDS in IoT: An Empirical Study.

[19] Khan MA, Rehman A, Rho S. Secure Framework for WSN-IoT Using Deep Learning.

[20] Rahman M, Chowdhury T, Islam S. Advanced Deep Learning Approaches for Real-Time IoT Anomaly Detection.

[21] Zhang W, Liu Y, Chen L. Distributed Lightweight Federated Learning for IoT Zombie Device Detection.

[22] Silva P, Gomes R, Rocha D. Cybersecurity Implementations for Smart Metropolises.

[23] Kim J, Park D, Choi H. FedCTI: Federated Learning and Cyber Threat Intelligence on the Edge.

[24] Ahmed R, Malik S, Khan A. DL-Based Attack Detection with Optimized Feature Selection Using MGS-ROA.

[25] Lopez J, Garcia M, Ruiz F. Intrusion Detection in Smart Cities Using ML.

[26] Nguyen T, Pham Q, Le H. Mitigating Security Threats in Fog Computing for IoT-Enabled Smart Cities.

[27] Omar A, Aziz M, Rahim S. Modified GA + LSTM Network for Intrusion Detection in Edge-IoT.

[28] Ibrahim A, Salem H, Youssef M. Optimized Binary Neural Networks for Road Anomaly Detection (TinyML).

[29] Petrova E, Ivanov D, Mihailov P. Comprehensive Study of Intrusion Detection in IoT-Smart Cities.

[30] Zhou Y, Wang L, Li P. MEC-Based Architecture for Securing IoT Using Federated DL.

[31] Ruiz-Villafranca S, Roldán-Gómez J, et al. MEC-IIoT Intelligent Threat Detector Using Boosted Trees.

[32] Garcia A, Torres L, Vega R. Two-Tier Anomaly-Based IDS for Smart Cities.

[33] Omar A, Aziz M, Rahim S. Efficient Framework for Unsupervised Anomaly Detection Over Edge-IoT.

[34] Martins J, Ferreira L, Sousa R. DDoS Attack Detection in Real Urban IoT Using Federated DL.

[35] Yang R, He H, Xu Y, Xin B. Efficient Intrusion Detection Using Cloud–Edge Collaboration.

[36] Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews.

[37] Joanna Briggs Institute. JBI Critical Appraisal Tools. *JBI Manual for Evidence Synthesis*. 2020.

[38] 38.Ouzzani M, Hammady H, Fedorowicz Z, Elmagarmid A. Rayyan—a web and mobile app for systematic reviews.

APPENDIX A:

Table 1. Summary of included 35 studies.

No.	Year	Source	Title	Authors
1	2025	IEEE GINOTECH	Strengthening IoT Security with Machine Learning-Powered Intrusion Detection Systems for Critical Infrastructure and Smart Cities	Kiran Kowtarapu; Udayasree Kowtarapu
2	2024	IEEE GCET	Penetration Testing-Aware IDS for Wireless Networks in Urban Digital Ecosystems Integrated with Edge Computing and Machine Learning	Tamara Zhukabayeva; Zulfiqar Ahmad; Aigul Adamova; Dina Satybaldina
3	2021	19th OITS International Conference on Information Technology (OCIT), IEEE	Data Security Model Using Deep Learning and Edge Computing for Internet of Things (IoT) in Smart City	M. S. Tahsin; M. Y. Aziz; T. A. Kabbo; T. Tahsin; N. H. Zumme; M. I. Hossain
4	2019	IEEE CCWC	AD-IoT: Anomaly Detection of IoT Cyberattacks in Smart City Using Machine Learning	Ibrahim Alrashdi; Ali Alqazzaz; Esam Aloufi; Raed Alharthi; Mohamed Zohdy; Hua Ming
5	2025	Ad Hoc Networks (Elsevier)	Advanced Intrusion Detection in the Industrial Internet of Things Using Federated Learning and LSTM Models	Raja Waseem Anwer; Mohammad Abrar; Mehar Ullah; Abdu Salam; Faizan Ullah

No.	Year	Source	Title	Authors
6	2024 (online) / 2025 (journal issue)	IEEE Transactions on Consumer Electronics	An Adaptive Explainable AI Framework for Securing Consumer Electronics-Based IoT Applications in Fog-Cloud Infrastructure	S. S. Tripathy; M. Guduri; C. Chakraborty; S. Bebortta; S. K. Pani; S. Mukhopadhyay
7	2025	2025 IEEE 9th Forum on Research and Technologies for Society and Industry (RTSI)	Decentralized AI for Smart Cities: A Federated Learning Framework for Resilient Cybersecurity	M. Houichi; F. Jaïdi; A. Bouhoula
8	2025 (online) / 2026 (issue)	ACM Transactions on Internet Technology	DeepSDN: Deep Learning Based Software Defined Network Model for Cyberthreat Detection in IoT Network	Kokila M.; Srinivasa Reddy Konda
9	2025	Neurocomputing (Elsevier)	Drone-Guard: A Self-Supervised Deep Learning Framework for Real-Time Spatiotemporal Anomaly Detection in UAV Surveillance Systems	Wassim Sliti; Olfa Besbes
10	2025	2025 Global Conference in Emerging Technology (GINOTECH), IEEE	Enhancing Cybersecurity in Smart Cities: IoT Applications with a Hybrid Deep Neural Network Model	Anandbabu Gopatoti; Sreeja Rashmitha Duvvada; Ekaterina Slepcova; D. R. Prince Williams; Manasi Mahadeo Phadatare; S. Praveena
11	2025	Computers & Industrial Engineering (Elsevier)	Evaluating Machine Learning-Driven Intrusion Detection Systems in IoT: Performance and Energy Consumption	Saeid Jamshidi; Kawser Wazed Nafi; Amin Nikanjam; Foutse Khomh
12	2025	6th International Conference on Electronics and Sustainable Communication Systems (ICESC), IEEE	Federated Learning-Enabled Edge Intelligence for Sustainable Smart Cities	L. Natrayan; Seeniappan Kaliappan; Beena Stanislaus Arputharaj; M. Muthukannan; Ramya M.
13	2025	e-Prime — Advances in Electrical Engineering, Electronics and Energy (Elsevier)	FL-DPCSA: Federated Learning with Differential Privacy for Cache Side-Channel Attack Detection in Edge-Based Smart Grids	G. H. Kumar; S. L. R. Elicherla; S. Saxena; K. A. Swamy; A. P.; U. P. Kumar
14	2025	7th International Conference on Inventive Material Science and Applications (ICIMA), IEEE	Host-Based Intrusion Detection Framework for IoT Using Machine Learning	S. J. Praveen; V. Prahladh; B. S. Kiruthika Devi
15	2025	Results in Engineering (Elsevier)	Optimizing Anomaly Detection Models for Edge IIoT with an Enhanced Firefly Algorithm-Based Hyperparameter Tuning Strategy	M. Y. Rahamathulla; M. Ramaiah
16	2025	International Journal of Critical Infrastructure Protection (Elsevier)	SPARK and SAD: Leading-Edge Deep Learning Frameworks for Robust and Effective Intrusion Detection in SCADA Systems	Raghuram Bhukya; Syed Abdul Moeed; Anusha Medavaka; Alaa O. Khadidos; Adil O. Khadidos; Shitharth Selvarajan
17	2025	IEEE Access	SwinIoT: A Hierarchical Transformer-Based Framework for Behavioral Anomaly Detection in IoT-Driven Smart Cities	H. Mancy; Qamar H. Naith
18	2025	ACM Transactions on Software Engineering and Methodology	Toward Enhancing Privacy Preservation of a Federated Learning CNN Intrusion Detection System in IoT: Method and Empirical Study	D. Torre; A. Chennamaneni; J. Jo; G. Vyas; B. Sabrsula
19	2024	Computers, Materials & Continua	A Secure Framework for WSN-IoT Using Deep Learning for Enhanced Intrusion Detection	Chandraumakantham Om Kumar; Sudhakaran Gajendran; Suguna Marappan; Mohammed Zakariah; Abdulaziz S. Almazyad
20	2024	7th International Conference on Computing, Communication and Intelligent Systems (IC3I), IEEE	Advanced Deep Learning Approaches for Real-Time Anomaly Detection in IoT Environments	Himanshu Rai Goyal; Saif O. Husain; Krishna Kant Dixit; Nandini Shirish Boob; B. Ravali Reddy; Jaysheel Kumar; Smita Sharma
21	2024	ACM Transactions on Sensor Networks	Distributed and Collaborative Lightweight Edge Federated Learning for IoT Zombie Devices Detection	C. Han; T. Li; Q. Chen; Y. Wu; J. Qin
22	2024	IEEE International Conference on Power, Instrumentation, Energy and Control (PICET)	Elevating Urban Resilience: Cutting-Edge Cybersecurity Implementations for Smart Metropolises	Biresh Kumar; Mayank Kumar; Rahul Singh
23	2023 (conference) / 2024 (online publication)	Proceedings of the 13th International Conference on the Internet of Things (IoT '23), ACM	FedCTI: Federated Learning and Cyber Threat Intelligence on the Edge for Secure IoT Networks	S. El Jaouhari; Y. Etiabi
24	2024	IEEE conference	Fortifying Smart City IoT Networks: A Deep Learning-Based Attack Detection Framework with Optimized Feature Selection Using MGS-ROA	R. V. Rayala; C. R. Borra; P. K. Pareek; S. Cheekati
25	2024	2nd International Conference on Artificial Intelligence and Machine Learning Applications (AIMLA 2024), IEEE	Intrusion Detection in Smart Cities Using Machine Learning	S. Keerthana; M. Divakar; K. Gokul; S. Gowri Shankar — author list to be checked against the official IEEE record

No.	Year	Source	Title	Authors
26	2024	27th International Conference on Computer and Information Technology (ICCIT), IEEE	Mitigating Security Threats in Fog Computing for IoT-Enabled Smart Cities	Sharaban Sadi; Mehedi Malek; Md. Ihsanul Haque Turja; Ke-Rong Sun; Taskeen Binte Riaz; Md. Sakhawat Hossen
27	2024	Applied Soft Computing (Elsevier)	Modified Genetic Algorithm and Fine-Tuned Long Short-Term Memory Network for Intrusion Detection in the Internet of Things Networks with Edge Capabilities	Yakub Kayode Saheed; Oluwadamilare Harazeem Abdulganiyu; Taha Ait Tchakoucht
28	2024	Computers, Materials & Continua	Optimized Binary Neural Networks for Road Anomaly Detection: A TinyML Approach on Edge Devices	A. Khatoon; W. Wang; A. Ullah; L. Li; M. Wang
29	2023	International Wireless Communications and Mobile Computing Conference (IWCMC), IEEE	A Comprehensive Study of Intrusion Detection within Internet of Things-Based Smart Cities: Synthesis, Analysis and a Novel Approach	M. Houichi; F. Jaïdi; A. Bouhoula
30	2023	IEEE Internet of Things Magazine	A MEC-Based Architecture to Secure IoT Applications Using Federated Deep Learning	Zakaria Abou El Houda; Bouziane Brik; Adlen Ksentini; Lyes Khoukhi
31	2023	Computer Networks (Elsevier)	A MEC-IIoT Intelligent Threat Detector Based on Machine Learning Boosted Tree Algorithms	Sergio Ruiz-Villafranca; José Roldán-Gómez; Javier Carrillo-Mondéjar; Juan Manuel Castelo Gómez; José Miguel Villalón
32	2023	IEEE INFOCOM Workshops	A Two-Tier Anomaly-Based Intrusion Detection Approach for IoT-Enabled Smart Cities	M. Hamdan; A. M. Eldhai; S. Abdelsalam; K. Ullah; A. K. Bashir; M. N. Marsono; F. Kon; D. M. Batista
33	2023	ACM Transactions on Sensor Networks	An Efficient Framework for Unsupervised Anomaly Detection over Edge-Assisted Internet of Things	Yumeng Liu; Hongan Wang; Xu Zheng; Ling Tian
34	2023	IEEE International Conference on Cyber Security and Resilience (CSR)	DDoS Attack Detection in a Real Urban IoT Environment Using Federated Deep Learning	Khatereh Ahmadi; Reza Javidan
35	2023	Computer Networks (Elsevier)	Efficient Intrusion Detection Toward IoT Networks Using Cloud–Edge Collaboration	Run Yang; Hui He; Yixiao Xu; Bangzhou Xin; Yulong Wang; Yue Qu; Weizhe Zhang

Appendix B. Complete Search Strategies:

B.1 IEEE Xplore

A. *("smart cit*" OR urban OR "critical infrastructure")*

AND (IoT OR "internet of things" OR IIoT)

AND (edge OR "edge computing" OR fog OR MEC)

AND (cybersecurity OR "intrusion detection" OR "anomaly detection" OR "threat detection")

AND ("machine learning" OR "deep learning" OR "artificial intelligence" OR "federated learning" OR TinyML OR "explainable AI")

AND (2018-2025)

B.2 ACM Digital Library

B. *("smart cit*" OR urban OR "critical infrastructure")*

AND (IoT OR "internet of things" OR IIoT)

AND (edge OR "edge computing" OR fog OR MEC)

AND (cybersecurity OR "intrusion detection" OR "anomaly detection" OR "threat detection")

AND ("machine learning" OR "deep learning" OR "artificial intelligence" OR "federated learning" OR TinyML OR "explainable AI")

AND (2018-2025)

B.3 ScienceDirect

C. *("smart cit*" OR urban OR "critical infrastructure")*

AND (IoT OR "internet of things" OR IIoT)

AND (edge OR "edge computing" OR fog OR MEC)

AND (cybersecurity OR "intrusion detection" OR "anomaly detection" OR "threat detection")

AND ("machine learning" OR "deep learning" OR "artificial intelligence" OR "federated learning" OR TinyML OR "explainable AI")

AND (2018-2025)

Appendix C. Risk of Bias Assessment (JBI Checklist)

THIS APPENDIX PRESENTS THE RISK OF BIAS ASSESSMENT FOR ALL 35 INCLUDED STUDIES USING THE JBI CRITICAL APPRAISAL CHECKLIST. EACH STUDY WAS EVALUATED ACROSS KEY DOMAINS, INCLUDING:

VI. Clarity of research aims

VII. Dataset transparency and reliability

VIII. Handling of class imbalance

IX. Appropriateness of methodology

X. Model validation (cross-validation / external validation)

XI. Reporting completeness

Studies were categorized as having Low, Moderate, or High risk of bias according to the quality of reporting and methodological rigor.

Table C1. Risk of Bias Summary for Included Studies

No.	Title	Authors (Year)	JBI Assessment Summary	Overall Risk of Bias
1	Strengthening IoT Security with Machine Learning-Powered Intrusion Detection Systems for Critical Infrastructure and Smart Cities	K. Kowtarapu; U. Kowtarapu (2025)	Clear aims; moderate dataset transparency; limited external validation	Moderate
2	Penetration Testing-Aware IDS for Wireless Networks in Urban Digital Ecosystems Integrated with Edge Computing and Machine Learning	T. Zhukabayeva; Z. Ahmad; A. Adamova; D. Satybaldina (2024)	Strong methodology; good dataset reporting; adequate validation	Low
3	Data Security Model Using Deep Learning and Edge Computing for Internet of Things (IoT) in Smart City	M. S. Tahsin; M. Y. Aziz; T. A. Kabbo; T. Tahsin; N. h. Zumme; M. I. Hossain (2021)	Collaborative FL approach; insufficient reporting of data preprocessing	Moderate
4	AD-IoT: Anomaly Detection of IoT Cyberattacks in Smart City Using Machine Learning	I. Alrashdi; A. Alqazzaz; E. Aloufi; R. Alharthi; M. Zohdy; H. Ming (2019)	Autoencoder-based IDS; unclear dataset details	Moderate
5	Advanced intrusion detection in the industrial Internet of Things using federated learning and LSTM models	Anwer, Raja Waseem; Abrar, Mohammad; Ullah, Mehar; Salam, Abdu; Ullah, Faizan (2025)	TinyML evaluation clear; limited reporting on hardware constraints	Moderate
6	An Adaptive Explainable AI Framework for Securing Consumer Electronics-Based IoT Applications in Fog-Cloud Infrastructure	S. S. Tripathy; M. Guduri; C. Chakraborty; S. Bebortta; S. K. Pani; S. Mukhopadhyay (2025)	Good methodological clarity; weak description of experimental setup	Moderate
7	Decentralized AI for Smart Cities: A Federated Learning Framework for Resilient Cybersecurity	M. Houichi; F. Jaidi; A. Bouhoula (2025)	FL privacy approach clear; strong experimental detail	Low
8	DeepSDN: Deep Learning Based Software Defined Network Model for Cyberthreat Detection in IoT Network	Kokila M, Kokila M and Srinivasa Reddy Konda, Srinivasa Reddy Konda (2025)	Graph-based detection; some missing steps in methodology	Moderate
9	Drone-guard: A self-supervised deep learning framework for real-time spatiotemporal anomaly detection in UAV surveillance systems	Sliti, Wassim; Besbes, Olfa (2025)	ML methods reported; limited experimental detail	High
10	Enhancing Cybersecurity in Smart Cities: IoT Applications with a Hybrid Deep Neural Network Model	A. Gopatoti; S. R. Duvvada; E. Slepcova; D. R. P. Williams; M. M. Phadatare; S. Praveena (2025)	Good dataset clarity; incomplete metrics reporting	Moderate
11	Evaluating machine learning-driven intrusion detection systems in IoT: Performance and energy consumption	Jamshidi, Saeid; Nafi, Kawser Wazed; Nikanjam, Amin; Khomh, Foutse (2025)	Energy-aware models; adequate reporting	Low
12	Federated Learning-Enabled Edge Intelligence for Sustainable Smart Cities	L. Natrayan; S. Kaliappan; B. S. Arputharaj; M. Muthukannan; M. Ramya (2025)	Strong federated methodology; complete reporting	Low

No.	Title	Authors (Year)	JBI Assessment Summary	Overall Risk of Bias
13	FL-DPCSA: Federated learning with differential privacy for cache side-channel attack detection in edge-based smart grids	Kumar, G. Hemanth; Elicherla, Sivananda Lahari Reddy; Saxena, Sugandha; Swamy, K. Ayyappa; P., Ashwini; Kumar, U. Pavan (2025)	FL privacy approach good; insufficient preprocessing reporting	Moderate
14	Host-based Intrusion Detection Framework for IoT using Machine Learning	S. J. Praveen; V. Prahladh; B. S. K. Devi (2025)	Clear ML framework; limited dataset explanation	Moderate
15	Optimizing anomaly detection models for edge IIoT with an enhanced firefly algorithm-based hyperparameter tuning strategy	Rahamathulla, Mohemmed Yousuf; Ramaiah, Mangayarkarasi (2025)	Strong tuning strategy; robust methodology	Low
16	SPARK and SAD: Leading-edge deep learning frameworks for robust and effective intrusion detection in SCADA systems	Bhukya, Raghuram; Moeed, Syed Abdul; Medavaka, Anusha; Khadidos, Alaa O.; Khadidos, Adil O.; Selvarajan, Shitharth (2025)	Adversarial robustness tested; dataset details incomplete	Moderate
17	SwinIoT: A Hierarchical Transformer-Based Framework for Behavioral Anomaly Detection in IoT-Driven Smart Cities	H. Mancy; Q. H. Naith (2025)	Transformer model clear; limited validation reporting	Moderate
18	Toward Enhancing Privacy Preservation of a Federated Learning CNN Intrusion Detection System in IoT: Method and Empirical Study	Torre, Damiano and Chennamaneni, Anitha and Jo, JaeYun and Vyas, Gitika and Sabrsula, Brandon (2025)	Strong FL methodology; clear reporting	Low
19	A Secure Framework for WSN-IoT Using Deep Learning for Enhanced Intrusion Detection	Kumar, Chandraumakantham Om; Gajendran, Sudhakaran; Marappan, Suguna; Zakariah, Mohammed; S. Almazyad, Abdulaziz (2024)	Clear aims; partial dataset transparency	Moderate
20	Advanced Deep Learning Approaches for Real-Time Anomaly Detection in IoT Environments	H. R. Goyal; S. O. Husain; K. K. Dixit; N. S. Boob; B. R. Reddy; J. Kumar; S. Sharma (2024)	DL methods validated; missing external validation	Moderate
21	Distributed and Collaborative Lightweight Edge Federated Learning for IoT Zombie Devices Detection	Han, Chunjing and Li, Tong and Chen, Qiuyi and Wu, Yulei and Qin, Jifeng (2024)	Robust FL design; strong experimental detail	Low
22	Elevating Urban Resilience: Cutting-Edge Cybersecurity Implementations for Smart Metropolises	B. Kumar; M. Kumar; R. Singh (2024)	Good clarity; insufficient evaluation metrics	Moderate
23	FedCTI: Federated Learning and Cyber Threat Intelligence on the Edge for secure IoT Networks	El Jaouhari, Saad and Etiabi, Yaya (2024)	Strong methodology; complete reporting	Low
24	Fortifying Smart City IoT Networks: A Deep Learning-Based Attack Detection Framework with Optimized Feature Selection Using MGS-ROA	R. V. Rayala; C. R. Borra; P. K. Pareek; S. Cheekati (2024)	Good feature selection; unclear dataset preprocessing	Moderate
25	Intrusion Detection in Smart Cities Using Machine Learning	K. S; D. M; G. K; G. S. S (2024)	Adequate reporting; older dataset	Moderate
26	Mitigating Security Threats in Fog Computing for IoT-Enabled Smart Cities	S. S. Emon; M. Malek; M. I. Hossain Turja; K. Redwan Sun; M. A. Rahman; J. Noor; M. I. Hossain (2024)	Fog architecture clear; limited validation	Moderate
27	Modified genetic algorithm and fine-tuned long short-term memory network for intrusion detection in the internet of things networks with edge capabilities	Saheed, Yakub Kayode; Abdulganiyu, Oluwadamilare Harazeem; Tchakoucht, Taha Ait (2024)	Strong GA+LSTM method; incomplete dataset detail	Moderate
28	Optimized Binary Neural Networks for Road Anomaly Detection: A TinyML Approach on Edge Devices	Wang, Weixing; Ullah, Asad; Li, Limin; Wang, Mengfei (2024)	TinyML evaluation good; hardware constraints unclear	Moderate
29	A Comprehensive Study of Intrusion Detection within Internet of Things-based Smart Cities: Synthesis, Analysis and a Novel Approach	M. Houichi; F. Jaidi; A. Bouhoula (2023)	Strong study; no external validation	Moderate

No.	Title	Authors (Year)	JBI Assessment Summary	Overall Risk of Bias
30	A MEC-Based Architecture to Secure IoT Applications using Federated Deep Learning	Z. A. El Houda; B. Brik; A. Ksentini; L. Khoukhi (2023)	FL-MEC model strong; complete reporting	Low
31	A MEC-IIoT intelligent threat detector based on machine learning boosted tree algorithms	Ruiz-Villafranca, Sergio; Roldán-Gómez, José; Carrillo-Mondéjar, Javier; Gómez, Juan Manuel Castelo; Villalón, José Miguel (2023)	Boosted-tree model clear; missing validation steps	Moderate
32	A Two-Tier Anomaly-based Intrusion Detection Approach for IoT-Enabled Smart Cities	M. Hamdan; A. M. Eldhai; S. Abdelsalam; K. Ullah; A. K. Bashir; M. Marsono; F. Kon; D. M. Batista (2023)	Two-tier IDS well described; limited external validation	Moderate
33	An Efficient Framework for Unsupervised Anomaly Detection over Edge-Assisted Internet of Things	Liu, Yumeng and Wang, Hongan and Zheng, Xu and Tian, Ling (2023)	Unsupervised framework robust; dataset clarity limited	Moderate
34	DDoS Attack Detection in a Real Urban IoT Environment Using Federated Deep Learning	K. Ahmadi; R. Javidan (2023)	Strong FL approach; adequate reporting	Low
35	Efficient intrusion detection toward IoT networks using cloud–edge collaboration	Yang, Run; He, Hui; Xu, Yixiao; Xin, Bangzhou; Wang, Yulong; Qu, Yue; Zhang, Weizhe (2023)	Hybrid cloud–edge IDS; incomplete experimental setup	Moderate

APPENDIX D. SUMMARY OF MAIN FINDINGS FOR INCLUDED STUDIES

No.	Study Title	AI Technique / Model	Dataset / Data Type	Threat Type / Task	Key Performance Metrics (as reported)
1	Strengthening IoT Security with ML-Powered Intrusion Detection Systems for Critical Infrastructure and Smart Cities	Supervised ML-based IDS	IoT traffic from CI & smart cities	Multi-class intrusions	Accuracy, precision, recall, F1, ROC-AUC
2	Penetration Testing-Aware IDS for Wireless Networks in Urban Digital Ecosystems	Pen-test–aware ML IDS	Wireless edge network traffic	Wireless intrusions, pen-testing attacks	Detection rate, accuracy, F1, FPR
3	Data Security Model Using Deep Learning and Edge Computing for IoT in Smart City	Deep learning (DNN/CNN)	Smart-city IoT sensor traffic	Intrusions, anomalies	Accuracy, detection rate, latency
4	AD-IoT: Anomaly Detection of IoT Cyberattacks in Smart City Using ML	ML anomaly detection	Smart-city IoT attack traffic	DoS, probing, scanning	Accuracy, F1, detection rate, FPR
5	Advanced Intrusion Detection in IIoT Using Federated Learning and LSTM Models	FL + LSTM IDS	Industrial IoT traffic	Industrial intrusions	Accuracy, F1, FL overhead
6	Adaptive Explainable AI Framework for Securing Consumer Electronics IoT	Explainable DL (CNN/XAI)	Consumer IoT device logs	Consumer IoT intrusions	Accuracy, precision, recall
7	Decentralized AI for Smart Cities: A Federated Learning Framework for Resilient Cybersecurity	Federated learning IDS	Distributed smart-city IoT data	General cyber threats	Accuracy, F1, scalability
8	DeepSDN: Deep Learning SDN Model for Cyberthreat Detection in IoT Networks	Deep SDN model (CNN/DNN)	SDN flow data	SDN-based IoT threats	Accuracy, detection rate, FAR
9	Drone-Guard: Self-Supervised DL for UAV Spatiotemporal Anomaly Detection	Self-supervised deep model	UAV video + telemetry	UAV anomalies	Detection rate, F1
10	Enhancing Cybersecurity in Smart Cities with Hybrid Deep Neural Network Models	Hybrid DNN	Smart-city IoT applications	IoT cyberattacks	Accuracy, recall, F1
11	Evaluating ML IDS in IoT: Performance & Energy Consumption	Multiple ML models	IoT intrusion dataset + energy data	IoT intrusions	Accuracy, energy usage
12	Federated Learning-Enabled Edge Intelligence for Sustainable Smart Cities	Federated DL	Smart-city IoT sensor data	Distributed threats	Accuracy, F1, bandwidth
13	FL-DPCSA: Federated Learning with Differential Privacy for Smart Grids	FL + Differential Privacy	Smart-grid cache traffic	Cache side-channel attacks	Detection accuracy, ε-loss, overhead
14	Host-Based Intrusion Detection Framework for IoT Using ML	Host-based ML IDS	IoT device logs	Malware / host intrusions	Accuracy, FPR, detection rate

No.	Study Title	AI Technique / Model	Dataset / Data Type	Threat Type / Task	Key Performance Metrics (as reported)
15	Optimization of IIoT Anomaly Detection Using Firefly Algorithm	Firefly-MLOpt	Edge IIoT telemetry	IIoT anomalies	Accuracy, F1
16	SPARK & SAD: Deep Learning Frameworks for SCADA Intrusion Detection	Deep DL (SCADA)	SCADA/ICS traffic	SCADA intrusions	Accuracy, FAR
17	SwinIoT: Transformer-Based Framework for Behavioral IoT Anomaly Detection	Transformer (Swin-based)	IoT behavior/event logs	Behavioral anomalies	Accuracy, F1
18	Privacy-Preserving Federated CNN IDS for IoT	Federated CNN	IoT partitioned traffic	Intrusions under FL	Accuracy, privacy overhead
19	A Secure Framework for WSN–IoT Using Deep Learning	DL IDS	WSN traffic	WSN intrusions	Detection rate, accuracy
20	Advanced Deep Learning for Real-Time IoT Anomaly Detection	LSTM/CNN	Real-time IoT data	Real-time anomalies	Accuracy, latency
21	Lightweight Edge Federated Learning for IoT Zombie Device Detection	Lightweight FL	Traffic from zombie/bot IoT devices	Bot detection	Detection rate, accuracy
22	Elevating Urban Resilience: Cybersecurity Implementations for Smart Metropolises	Mixed cybersecurity techniques	Smart-metropolis datasets	Various urban cyber threats	Detection rate, response time
23	FedCTI: Federated Learning + Cyber Threat Intelligence	FL + CTI	IoT + CTI feeds	CTI-enhanced intrusion detection	Accuracy, F1
24	Deep Learning with MGS-ROA for IoT Cyberattack Detection	DL + Feature Optimization	Smart-city IoT dataset	Multi-class attacks	Accuracy, precision, recall
25	Intrusion Detection in Smart Cities Using ML	ML classifiers	Smart-city IoT datasets	Intrusion detection	Accuracy, detection rate
26	Mitigating Security Threats in Fog Computing for IoT Smart Cities	Fog + ML	Fog-computing traffic	Fog-layer attacks	Detection rate, latency
27	Modified GA + Fine-Tuned LSTM IDS	GA + LSTM	Edge IoT traffic	Intrusions	Accuracy, F1
28	Optimized Binary Neural Networks for Road Anomaly Detection (TinyML)	TinyML	Road anomaly sensors/images	Road anomaly detection	Accuracy, latency, energy use
29	A Comprehensive Study of Intrusion Detection in IoT-Based Smart Cities	Comparative ML/DL	IoT public + custom datasets	IoT intrusions	Accuracy, F1
30	MEC-Based Federated Deep Learning IDS	Federated DL (MEC)	MEC IoT application data	IoT app intrusions	Accuracy, convergence
31	MEC-IIoT Intelligent Threat Detector Using ML Boosted Trees	XGBoost/GBDT	MEC-IIoT telemetry	MEC-IIoT threat detection	Accuracy, F1, ROC-AUC
32	Two-Tier Anomaly-Based IDS for IoT Smart Cities	Two-tier IDS	Two-layer IoT traffic	Network anomalies	Detection rate, FPR
33	Unsupervised Anomaly Detection for Edge-Assisted IoT	Autoencoder / clustering	Edge IoT telemetry	Unsupervised anomalies	Detection rate, precision
34	Real-World Federated DL DDoS Detection for Urban IoT	Federated DL	Real urban IoT traffic	DDoS attacks	Accuracy, detection rate
35	SSAE + TCN Cloud–Edge Federated IDS	SSAE + TCN	CIC-IDS2017 dataset	Multi-class intrusions	Accuracy, training time