Science Discovery Computers
2026, Vol. 1, No. 2, pp. 102–109
https://doi.org/10.11648/j.sdcomput.20260102.14

SciencePG
Science Publishing Group

Research Article

Privacy Preserving Federated Learning for Advanced Persistent Threat Detection in Smart City IoT Networks

Sachira Sakalasooriya*

School of Computing, Sliit City Uni, Colombo, Sri Lanka

Abstract

The increasing deployment of Internet of Things (IoT) devices in smart city infrastructures has significantly expanded the cyberattack surface, creating new opportunities for sophisticated cyber threats. Among these threats, Advanced Persistent Threats (APTs) pose a major security challenge because they operate stealthily, remain active over extended periods, and often evade traditional signature-based intrusion detection systems. At the same time, privacy concerns and the decentralized nature of smart city environments limit the effectiveness of conventional centralized security solutions. To address these challenges, this study proposes a privacy preserving federated learning framework for detecting APTs within smart city IoT networks. The proposed system combines distributed federated learning with a dual model detection architecture consisting of a federated XGBoost classifier and a locally trained Long Short Term Memory (LSTM) autoencoder. The federated model enables collaborative learning across multiple edge nodes without transferring raw data to a central server, thereby preserving user privacy and reducing communication overhead. Meanwhile, the LSTM autoencoder learns local behavioral patterns and identifies previously unseen anomalies. The Edge IIoTset dataset, containing approximately 2.2 million network flow records and fourteen attack categories, is employed to evaluate the proposed framework under realistic non-independent and identically distributed (non-IID) conditions. Experimental evaluation demonstrates that the integrated federated learning approach achieves high detection performance while maintaining low inference latency suitable for edge environments. The LSTM autoencoder achieves an F1-score of 0.93, while the federated XGBoost classifier effectively identifies known attack categories with minimal computational overhead. The layered detection strategy improves the identification of both known and unknown threats and maintains response times below 200 milliseconds on edge class devices. These findings indicate that privacy preserving federated learning can provide a scalable, efficient, and practical solution for securing smart city IoT infrastructures against sophisticated APT attacks.

Keywords

Advanced Persistent Threats, Cybersecurity, Edge Computing, Federated Learning, Internet of Things

1. Introduction

Smart cities rely on millions of interconnected Internet of Things (IoT) devices including traffic management systems, smart meters, surveillance units, and environmental sensors to enable automation and real time urban services. With an estimated 19.8 billion connected IoT devices deployed worldwide in 2025 and projections exceeding 40 billion by 2034 [1], this rapid expansion has outpaced the maturity of existing security mechanisms. Weak device authentication,

*Correspondence: Sachira Sakalasooriya (sachira.s@scu.lk)

Received: 16 June 2026; **Accepted:** 11 August 2026; **Published:** 26 November 2026

Copyright: © The Author(s), 2026. Published by Science Publishing Group. This is an **Open Access** article, distributed under the terms of the Creative Commons Attribution 4.0 License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

unencrypted communications, and heteroge neous protocols expose smart city IoT infrastructures to large scale cyberattacks such as distributed denial of service (DDoS) attacks, botnets and device takeovers [2]. Among these threats, Advanced Persistent Threats (APTs) represent one of the most critical risks to smart city networks. APTs are characterized by stealthy, multi-stage attack campaigns involving initial compromise, reconnaissance, lateral movement, per sistence and data exfilteration [3]. Their ability to blend with legitimate traffic and main tain long term presence makes them highly resistant to detection by traditional signature based intrusion detection systems. Although machine learning (ML) approaches have demonstrated improved detection capabilities, their effectiveness is often limited by the scale, complexity, and distributed nature of smart city IoT environments [4]. These challenges are further intensified by device heterogeneity, strict resource con straints, and siloed data sources distributed across multiple administrative domains. In addition, the limited availability of realistic APT datasets compels researchers to rely on centralized, outdated or attack specific datasets that inadequately capture multi stage and distributed APT behaviors [5]. This gap highlights the need for scalable, privacy preserving detection mechanisms capable of learning from decentralized and heteroge neous IoT data streams. Recent studies have explored ML and deep learning DL based approaches for APT detection, including intelligent ML classifiers [6] and deep maxout network architec tures [7], achieving promising performance under controlled experimental settings. However these methods predominantly depend on centralized training, which is often infeasible in smart city deployments due to privacy concerns, bandwidth limitations, and the decentralized nature of IoT data. Consequently, their scalability and real world applicability remain limited. To address these limitations, this paper develops a federated learning based frame work for APT detection in smart city IoT networks. Federated learning enables collab orative model training across distributed edge nodes without requiring raw data to be centralized, thereby enhancing privacy, scalability and robustness. Leveraging the Edge-IIoT set dataset, which is well suited for edge and federated learning experiments, this study investigates how federated learning can improve APT detection accuracy in decentralized smart city IoT environments. The proposed framework contributes a practical and distributed solution for detecting complex, multi stage APT behaviors across heterogeneous smart city infrastructures.

2. Literature Review

2.1. Smart City IoT Security Landscape and APT Challenges

The rapid proliferation of smart devices and advanced telecommunication net works has accelerated the transformation of traditional urban environments into smart cities. This evolution has resulted in a complex, highly interconnected, and heterogeneous Internet of Things (IoT) ecosystem, which introduces significant security challenges. Ensuring the stability and resilience of smart city infrastructures therefore requires the deployment of robust and adaptive security mechanisms. Existing literature identifies several critical considerations for se curing smart city IoT systems, including the integration of Artificial intelligence AI and machine learning ML techniques for real time threat detection, the adop tion of quantum resilient cryptographic mechanisms, and the evolving nature and sophisticated of cyber threats. These vulnerabilities position smart city IoT architectures as attractive targets for Advanced Persistent Threats (APTs), which exploit system weaknesses 3 through covert, multi stage attack campaigns. Such attacks remain undetected for extended periods while progressively comprising system components. Consequently, proactive and collaborative defense strategies, supported by continuous research and monitoring, are required to develop next generation security solutions capable of protecting smart city IoT infrastructures [9]. Smart city environments face substantial cybersecurity risks due to the large scale, diversity. And interconnectivity of deployed IoT devices. Vulnerabilities including insecure firmware, exposed interfaces, and weak encryption mechanisms enable attackers to establish persistent and covert access within IoT net works. These conditions necessitate the adoption of stronger security mechanisms, particularly ML based detection approaches capable of identifying stealthy and long term attacks while effectively operating at the scale and heterogeneity inherent to smart city IoT ecosystems [8]. IoT infrastructures rely heavily on wireless communication technologies and diverse device types, introducing vulnerabilities across multiple architectural layers, including the perception, network and application layers. IoT sensors frequently transmit personal or operational data, which may be intercepted or manipulated by adversaries. When combined with the complexity and size of smart city deployments, these vulnerabilities create an environment conducive to multi layered and persistent attacks. APTs, characterized by stealth, persistence and data exfiltration objectives, exploit these weaknesses to establish long term foot holds within networks. Accordingly, recent research emphasizes the necessity of security mechanisms that are resilient to APTs and capable of detecting com plex, multi stage attack behaviours [10].

2.2. ML and DL Techniques for IoT Intrusion and APT Detection

Extensive research has demonstrated the effectiveness of machine learning (ML) and deep learning (DL) techniques in detecting APTs within Smart City IoT networks. Traditional intrusion detection systems are generally in effective against behavior based and stealthy attacks. In contrast, ML and DL methods including support vector machines (SVMs), k-means cluster ing, and decision tree based classifiers are capable of

analyzing network traffic and system logs to identify anomalous patterns in real time. These approaches typically rely on feature engineering and expert annotated da tasets to accurately detect both known and previously unseen APT behav iors [12].

2.2.1. Deep Autoencoders and LSTM Networks

Neuschmied et al proposed a multi stage autoencoder based intrusion detection framework designed to identify APTs across different phases of the attack lifecycle. Their approach employs statistical feature analysis combined with DL based anomaly detection to differentiate between benign and malicious network traffic. By integrating multiple publicly available benchmark datasets, the study demonstrates that multi stage autoencoders are effective in detecting both known and zero day APT attacks. The results indicate strong performance in terms of accuracy and robustness. The authors further emphasize that capturing the sequential nature of APT activities such as reconnaissance, exploitation, and exfiltration significantly improves detection effectiveness compared to tradi tional single stage models, highlighting the suitability of DL techniques for identifying slow and stealthy APT behaviours [12]. Similarly, LSTM-based autoencoders have been applied to network anomaly detection in IoT and IIoT environments [21].

2.2.2. Hybrid CNN-LSTM Models

The increasing deployment of IOT devices in smart city environments has heightened exposure to sophisticated, multi stage APTs that evade signature based detection by blending into normal traffic over extended durations. Hybrid convolutional neural network and long short term memory (CNN-LSTM) archi tectures have been proposed to address this challenge by jointly capturing spa tial and temporal traffic characteristics. In such models, CNN layers extract lo cal spatial patterns, while LSTM layers model long term temporal dependencies. Experimental evaluations show that these hybrid frameworks achieve detection accuracy of up to 96.4% maintain low false positive rates, and exhibit inference latency suitable for edge computing deployments [11, 13, 20].

2.2.3. Ensemble and Boosting Methods

Ensemble learning techniques have also proven effective for APT detection in IOT environments. Saini et al introduced a hybrid ensemble approach that com bines random forest and XGBoost classifiers to detect anomalous network be havior. Their framework integrates both deep learning and traditional ML mod els, including convolutional neural networks and multilayer perceptrons, and is evaluated across multiple benchmark datasets such as CSE-CIC-IDS2018, CIC IDS2017, NSL-KDD, and UNSW-NB15. The proposed approach achieves de tection accuracy of up to 99.91% with low false positive rates, demonstrating the effectiveness of boosting and ensemble strategies for APT detection, partic ularly in heterogeneous smart city IOT environments [14].

2.3. Positioning Edge-IIoTset Within IoT Intrusion Datasets

Reliable evaluation of security mechanisms for IoT and Industrial IoT (IIoT) environments requires datasets that accurately capture device behavior, protocol diversity, and modern attack patterns. However, many publicly available datasets focus on limited attack types, lack real world diversity, or fail to represent complex multi stage threats such as APTs. Table 1 compares widely used IoT intrusion detection datasets and highlights the rationale for selecting the Edge IIoT dataset for this study.

Table 1. *Comparison of IoT based Cybersecurity datasets for federated and Edge Learning Applications.*

Dataset	Strengths	Limitations	Relevance to This Study
CICAPT-IoT [15]	Realistic APT attack chains, provenance based logging	Limited scale, centralized setup	Useful for APT analysis, but unsuitable for edge level learning
N-BaIoT [16]	High quality botnet traces, real IoT devices	Focused solely on botnets	Suitable for anomaly detection baselines
Bot-IoT [17]	High volume traffic, diverse attack types	Highly imbalanced, synthetic benign traffic	Appropriate for ML benchmarking but lacks realism
TON_IoT [18]	Distributed telemetry sources	No multi stage APT scenarios	Relevant for distributed detection
Edge-IoTSet [19]	Large scale (2.2M flows), 14 attack types, suitable for edge and federated learning	No explicit APT chains	Best fit for heterogeneous and distributed smart city environments

2.4. Summary of Identified Research Gaps

Although existing studies acknowledge the growing security challenges and APT risks faced by smart city IoT systems [8, 10], and demonstrate the effectiveness of ML and DL models such as autoencoders, LSTMs, CNN LSTMs, and ensemble methods [4, 14], most proposed solutions rely on centralized data collection and processing. Such approaches are impractical for large scale, heterogeneous and privacy sensitive smart city environments. Furthermore, the reviewed datasets including CICAPT IIOT, N BaIOT, Bot-IoT and TON-IOT lack sufficient scale, protocol diversity, distributed architecture, or realistic APT sequencing required to evaluate federated learning based intrusion detection frameworks [15, 18]. While Edge IIoT set addresses many of these limitations by providing large scale and heterogeneous IIoT traffic suitable for edge level experimentation, there remains a lack of federated learning frameworks specifically designed for APT detection in smart city IoT networks. This gap forms the central motivation for the proposed study.

3. System Model and Methodology

3.1. Federated Learning Framework

The proposed approach adopts an iterative and adaptive federated learning framework designed to evolve continuously in response to emerging cyber threats. Unlike traditional intrusion detection systems that rely on static, centralized training, the proposed framework emphasizes an agile learning paradigm in which intelligence is moved to the data sources rather than aggregating sensitive raw traffic at a central location. Each edge node continuously monitors local model performance using rolling validation windows and evaluates key detection metrics, including accuracy, precision, recall, and F1 score. Performance degradation is identified when the local F1 score remains below 0.85 for three consecutive days, prompting the affected edge node to request retraining. A federated retraining round is initiated when more than 30% of participating nodes signal degradation or when critical infrastructure subsystems explicitly request model updates. Incremental warm start updates are incorporated in each retraining cycle, allowing models to reuse previously learnt parameters and reducing convergence time by approximately 60-70%. This adaptive learning process enables the system to respond dynamically to evolving attack behavior.

3.2. Dataset and Realistic Partitioning

This study utilizes the Edge IIoT set dataset [19], which contains approximately 2.2 million network flow records collected from a realistic IIoT testbed. The dataset is highly imbalanced, consisting of nearly 1.6 million benign flows and over 600,000 malicious flows spanning fourteen distinct attack types, including multiple distributed denial of service variants, reconnaissance, backdoor attacks, SQL injection, cross site scripting, ransomware, man in the middle attacks, public Wi-Fi gateways exposed to diverse but less sophisticated threats, smart building servers exhibiting mixed protocol usage and moderate attack rates, and critical infrastructure nodes managing sensitive util ity operations where minimizing false positives is essential. The resulting non identically distributed (non-IID) data partitions accurately reflect real smart 7 city operational conditions, unlike the homogeneous data splits commonly assumed in prior federated learning studies.

3.3. System Architecture

The global model aggregation process is defined as:
Equation (1)

$$W_{t+1} = \Sigma_{k=1}^{K} (|D_k| / |D|) W_{t+1}^{k} \quad (1)$$

Where:
W_{t+1} = Global model weights after aggregation at round t+1
K = Total number of participating clients
D_k = Local dataset belonging to client k
$|D_k|$ = Number of samples in client k
D = Total dataset across all clients
|D| = Total number of samples across all clients
W_{t+1}^{k} = Updated local model weights generated at client k after local training

The proposed system architecture consists of a cloud assisted federation server operating within the fog computing layer and a network of twenty five distributed edge clients. The federation server is responsible for initializing global model parameters, selecting eligible edge clients for each training round based on connectivity and data quality, and aggregating encrypted local model updates using the Federated Averaging (FedAvg) algorithm.

The federation server never processes raw network traffic and receives only encrypted gradients or parameter updates, thereby ensuring end node data privacy. Edge clients are deployed across traffic cabinets, building level servers, utility substations, and public safety hubs. Each edge client locally collects network flows from approximately 50 to 500 IoT devices, performs feature preprocessing, trains local models, and executes real time threat detection using both global and subsystem specific intelligence.

3.4. Edge-Level Preprocessing Pipeline

Each edge client executes an autonomous preprocessing pipeline comprising data cleaning, feature extraction, normalization, and temporal segmentation. Duplicate and corrupted records are removed, while missing values are imputed using median or mode based strategies. Obvious benign traffic is filtered to reduce noise and computational overhead. A comprehensive feature set of sixty-one attributes is extracted, including flow duration, packet and byte counts, inter arrival times,

MQTT topic characteristics, Modbus function codes, HTTP request behaviors, temporal attributes, and rolling statistical summaries. Min max normalization is applied using locally computed parameters to preserve data privacy. Traffic flows are segmented using a sliding window of twenty timesteps with a 50% overlap, corresponding to approximately 100 to 200 seconds of activity, enabling the modeling of temporal dependencies characteristic of multi stage Advanced Persistent Threats (APTs).

3.5. Dual-Model Architecture

The proposed detection framework employs a dual model architecture that integrates a federated XGBoost classifier with a locally trained LSTM autoencoder. At the global level, the federated XGBoost model is used to classify known attack categories by aggregating intelligence learned across distributed edge clients. The model consists of 100 decision trees with a maximum depth of six and a learning rate of 0.1 local gradients are encrypted using homomorphic encryption and securely aggregated before updated parameters are redistributed to participating nodes. The resulting classifier outputs Ulti class predictions covering fourteen attack categories in addition to normal traffic. At the local level, each edge client trains an LSTM autoencoder to learn subsystem specific normal behavior and detect previously unseen or localized anomalies. The encoder comprises with three LSTM layers with 128,64, and 32 units, while the decoder reconstructs the input using 2 LSTM layers with 64 and 128 units. The autoencoder is trained exclusively on benign traffic using the Adam optimizer with a learning rate of 0.001 for fifty epochs and early stopping. Anomalous events are identified based on elevated reconstruction error, which increases significantly when unfamiliar traffic patterns are encountered. This dual model design addresses variability in baseline behavior across heterogeneous smart city subsystems and overcomes the limitations of relying on a single global detector.

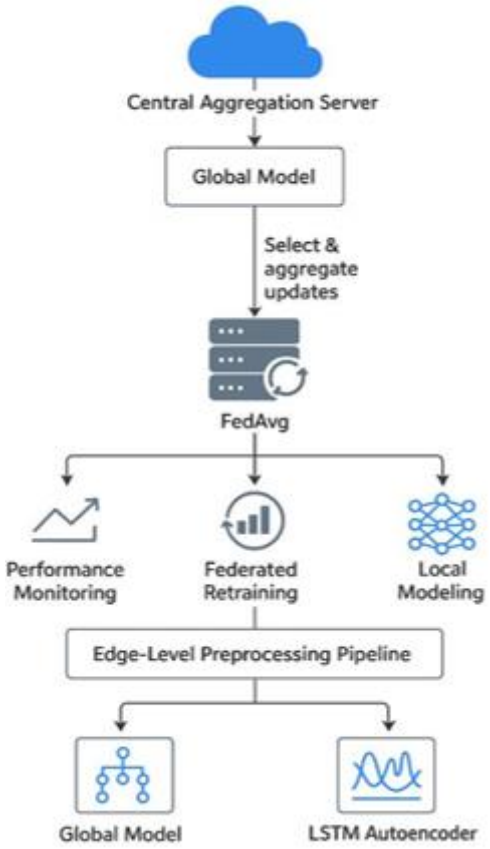


Figure 1. *Proposed End to End Federated Learning Pipeline with FedAvg and Edge Preprocessing.*

3.6. Real-Time Inference Pipeline

During real time operation, incoming network flows are processed through the local preprocessing pipeline and evaluated concurrently by both detection models. The federated XGBoost classifier performs multi class attack classification and outputs confidence scores, while the LSTM autoencoder computes reconstruction error for anomaly assessment. An alert is generated when the classifier confidence exceeds 0.8 or when the reconstruction error surpasses the 95th percentile of locally observed benign traffic. Events flagged by both

models are assigned the highest priority to facilitate efficient incident response and security triage.

3.7. Experimental Setup

Experiments are conducted using the Flower v1.5 federated learning frame work, with Raspberry Pi 4 devices configured as edge clients to emulate realistic computational constraints. Network conditions are designed to reflect urban communication environments, with an average bandwidth of approximately 10 Mbps and latency of 20ms. Evaluation metrics include accuracy, precession, recall, F1-score, and false positive rate for detection performance, time to convergence, communication overhead, and stability for federated learning efficiency, and inference latency, memory utilization, and energy consumption for real time feasibility. Baseline comparisons include centralized implementations of the proposed models, conventional intrusion detection techniques such as Random Forest and CNN- LSTM architectures, and federated learning configurations trained under IID data assumptions. These comparisons highlight the importance of realistic non IID data distributions, when evaluating federated intrusion detection systems for smart city IoT environments.

3.8. Privacy Considerations and Limitations

Gradient level differential privacy is applied to local model updates with a privacy budget of epsilon=1.0 to mitigate the risk of gradient inversion attacks, thereby preventing the federation server from reconstructing sensitive information from individual edge clients. Although the experimental setup with 25 edge clients effectively captures subsystem level heterogeneity, it does not fully reflect the scale of large smart city deployments, which may involve hundreds or thousands of distributed nodes. Furthermore, while the Edge IIoT set dataset provides a comprehensive and diverse representation of IoT and IIoT traffic, it remains synthetically generated, consequently, validation using real world smart city traffic is required in future work to further assess the robustness and generalizability of the proposed framework.

4. Results and Discussion

The proposed privacy-preserving federated learning framework demonstrates the capability to detect both known and previously unseen Advanced Persistent Threats within smart city IoT networks. The federated XGBoost classifier effectively identifies known attack categories through collaborative learning across distributed edge nodes, while the LSTM autoencoder captures subsystem-specific behavioral anomalies. Experimental observations indicate that the combined architecture achieves high detection performance while maintaining low computational overhead suitable for resource-constrained edge environments. The federated approach preserves data privacy because raw network traffic never leaves local devices during model training. Furthermore, the use of realistic non-IID data distributions enhances model robustness and reflects actual deployment conditions within heterogeneous smart city infrastructures. The achieved detection performance and low inference latency demonstrate the feasibility of implementing federated security intelligence in large-scale IoT ecosystems. Compared with traditional centralized intrusion detection systems, the proposed framework provides improved scalability, privacy protection, and adaptability to evolving attack behaviors.

5. Conclusion and Future Work

This study presented a privacy-preserving federated learning framework for Advanced Persistent Threat detection in smart city IoT environments. The proposed architecture integrates a federated XGBoost classifier with a locally trained LSTM autoencoder to provide both attack classification and anomaly detection capabilities. By enabling distributed model training without sharing raw data, the framework preserves privacy while supporting scalable deployment across heterogeneous smart city infrastructures.

Experimental evaluation using the Edge-IIoTset dataset demonstrated that the proposed approach achieves strong detection performance while maintaining inference latency suitable for edge computing environments. The layered detection strategy enhances the identification of both known and previously unseen cyber threats and improves resilience against sophisticated attack campaigns. The adoption of realistic non-IID data distributions further strengthens the practical applicability of the framework for real-world smart city deployments.

Future work will focus on validating the framework using real-world smart city traffic datasets, exploring advanced privacy-preserving mechanisms such as secure multiparty computation and homomorphic encryption, and scaling the architecture to support hundreds or thousands of distributed edge nodes. Additional investigation into adaptive federated aggregation algorithms and transformer-based threat detection models may further improve detection accuracy and system robustness against increasingly sophisticated APT behaviors.

Abbreviations

AI	Artificial Intelligence
APT	Advanced Persistent Threat
CNN	Convolutional Neural Network
DDoS	Distributed Denial of Service
DL	Deep Learning
FedAvg	Federated Averaging
FL	Federated Learning
FPR	False Positive Rate
IIoT	Industrial Internet of Things
IoT	Internet of Things
LSTM	Long Short-Term Memory

ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
SQL	Structured Query Language
XGBoost	Extreme Gradient Boosting

Acknowledgments

The author gratefully acknowledges the developers of the Edge-IIoTset dataset and the open-source federated learning research community for providing valuable resources that supported this work.

Author Contributions

Sachira Sakalasooriya: Conceptualization, Data curation, Formal Analysis, Investigation, Methodology, Software, Validation, Visualization, Writing – original draft, Writing – review & editing

Data Availability Statement

The data used in this study are available from the publicly accessible Edge-IIoTset dataset and related repositories cited in the reference section.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] R. Ahmad and I. Alsmadi, "Machine learning approaches to IoT security: A sys tematic literature review," Internet of Things, vol. 14, p. 100365, Jan. 2021, https://doi.org/10.1016/j.iot.2021.100365

[2] X. Liang and Y. Kim, "A survey on security attacks and solutions in the IoT network," IEEE Access, Jan. 2021, [Online]. Available: https://ieeexplore.ieee.org/document/9376174

[3] C. Gan, J. Lin, D.-W. Huang, Q. Zhu, and L. Tian, "Advanced persistent threats and their defense methods in industrial Internet of Things: A survey," Mathematics, vol. 11, no. 14, p. 3115, 2023, https://doi.org/10.3390/math11143115

[4] A. S. Al-Aamri, R. Abdulghafor, S. Turaev, I. Al-Shaikhli, A. Zeki, and S. Talib, "Machine learning for APT detection," Sustainability, vol. 15, no. 18, p. 13820, 2023, https://doi.org/10.3390/su151813820

[5] F. Farid, "A threat analysis framework for cyberattacks in smart cities," Ad vances in the Internet of Things, pp. 101–124, Jun. 2025, https://doi.org/10.1201/97810035066386

[6] S. H. Javed, M. B. Ahmad, M. Asif, S. H. Almotiri, K. Masood, and M. A. A. Ghamdi, "An intelligent system to detect advanced persistent threats in industrial Inter net of Things," Electronics, vol. 11, no. 5, p. 742, Feb. 2022, https://doi.org/10.3390/electronics11050742

[7] W. Rajeh et al., "Improved smart city security using a deep maxout network based intrusion detection system with walrus optimization," PeerJ Computer Science, vol. 11, p. e2743, Mar. 2025, https://doi.org/10.7717/peerj-cs.2743

[8] M. Alauthman, A. Aldweesh, and A. Al-Qerem, "IoT security challenges in mod ern smart cities," in Proc. Int. Conf. Comput. Commun. Robotics (ICCR)*, Feb. 2024, pp. 1–6, https://doi.org/10.1109/ICCR61006.2024.10533174

[9] F. Alzyoud, R. Al-Falah, M. Tarawneh, and O. Tarawneh, "Security challenges and solutions in smart cities," in Lecture Notes in Networks and Systems*, vol. 790, pp. 256–267, Jan. 2024, https://doi.org/10.1007/978-3-031-56950-0_22

[10] R. Sharma and R. Arya, "Security threats and measures in the Internet of Things for smart city infrastructure: A state-of-the-art," Trans. Emerg. Telecommun. Technol., vol. 34, no. 11, 2022, https://doi.org/10.1002/ett.4571

[11] Y. Chen et al., "Real-time inference with sub-35 ms latency processing over 1200 network flows using CNN–LSTM architecture for intrusion detection," IEEE Trans. Ind. Informatics, vol. 19, no. 3, pp. 2894–2903, Mar. 2023.

[12] H. Neuschmied, M. Winter, B. Stojanović, K. Hofer-Schmitz, J. Božić, and U. Kleb, "APT-attack detection based on multi-stage autoencoders," Applied Sciences, vol. 12, no. 13, p. 6816, Jul. 2022, https://doi.org/10.3390/app12136816

[13] E. Daisy, "Effectiveness of hybrid AI models (e.g., CNN–LSTM) in detecting advanced persistent threats," Jan. 2025, [Online]. Available: https://www.researchgate.net/publication/393862054

[14] N. Saini, V. B. Kasaragod, K. Prakash, and A. K. Das, "A hybrid ensemble machine learning model for detecting APT attacks based on network behavior anomaly detection," Concurrency Computat.: Pract. Exper., 2023, https://doi.org/10.1002/cpe.7865

[15] E. Ghiasvand, S. Ray, S. Iqbal, S. Dadkhah, and A. A. Ghorbani, "CICAPT IIoT: A provenance-based APT attack dataset for IIoT environments," arXiv: 2407.11278, Jul. 2024, https://doi.org/10.48550/arXiv.2407.11278

[16] Y. Meidan et al., "N-BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders," IEEE Perv. Comput., vol. 17, no. 3, pp. 12–22, Jul. 2018, https://doi.org/10.1109/MPRV.2018.03367731

[17] E. Özer, M. İskefiyeli, and J. Azimjonov, "Toward lightweight intrusion detec tion systems using optimal feature pairs from the Bot-IoT dataset," Int. J. Distrib. Sens. Netw., vol. 17, no. 10, Oct. 2021, https://doi.org/10.1177/15501477211052202

[18] N. Moustafa, "TON_IoT datasets: A distributed architecture for evaluating AI based security systems in IoT networks," Sustainable Cities and Society, vol. 72, p. 102994, May 2021, https://doi.org/10.1016/j.scs.2021.102994

[19] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning," *IEEE Access*, vol. 10, pp. 40281–40306, 2022. https://doi.org/10.1109/ACCESS.2022.3165809

[20] A. Kumar et al., "Smart framework for industrial IoT and cloud computing intrusion detection using CNN–LSTM GPU architecture," Journal of Sensors, 2023.

[21] P. K. Sharma and R. Kumar, "Network anomaly detection using LSTM-based autoencoder for IoT and IIoT networks," in *Proc. IEEE Int. Conf. Computing, Com munication and Networking Technologies (ICCCNT)*, 2021, pp. 1–6.