HYBRID DEEP LEARNING FRAMEWORK FOR SUSTAINABLE INFRASTRUCTURE PROTECTION AND RESILIENCE ENHANCEMENT IN SMART CITIES

N. Karthick[1], R. Nithya[2], A. Shaji George[3]

Abstract

Smart cities depend be contingent on interconnected digital infrastructures to support transportation, healthcare, energy management, industrial automation, and public communication systems. However, the rapid expansion of intelligent infrastructures exposes urban environments to cyber threats, network failures, data breaches, and operational unsteadiness. Traditional security and monitoring systems often lack adaptability, scalability, and resilience against growing attack patterns. This Paper proposes a Hybrid Deep Learning Framework for Sustainable Infrastructure Protection and Resilience Enhancement in Smart Cities. The proposed framework combines the Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) and Federated Learning mechanisms to enable the adaptive threat detection, infrastructure resilience analysis, and privacy-preserving distributed intelligence. The model performs real-time anomaly detection, predictive resilience valuation and sustainable infrastructure optimization across distributed smart city environments. Experimental evaluation demonstrates improved detection accuracy, reduced computational overhead, enhanced resilience response and sustainable operational efficiency compared with conventional deep learning approaches. The proposed framework strongly aligns with sustainable development by promoting resilient infrastructure, sustainable industrialization and intelligent innovation for future smart city ecosystems.

Keywords : Sustainable Infrastructure, Resilient Infrastructure, Smart Cities, Deep Learning, Hybrid CNN-LSTM, Federated Learning, Infrastructure Protection, Cyber Resilience, Sustainable Development.

I. INTRODUCTION

The rapid development of smart city technologies has significantly changed the way of modern urban infrastructures operate and deliver services. Smart cities integrate advanced cloud computing, digital technologies, intelligent communication systems, artificial intelligence, Internet of Things (IoT) devices and cyber-physical infrastructures to improve urban sustainability, industrial productivity, transportation efficiency, healthcare accessibility, energy optimization and public safety. These intelligent infrastructures generate large volumes of real-time data that support automatic decision-making and efficient resource management across several sectors. As urban populations continue to growth globally, governments and industries are progressively adopting smart city frameworks to achieve sustainable development and resilient infrastructure management associated with Sustainable Development, which focuses on industry, innovation and infrastructure.

Despite the substantial assistances of smart city ecosystems, the growing dependence on interconnected digital infrastructures announces several critical challenges related to infrastructure security, operational continuity, system reliability and cyber resilience. Smart transportation networks, intelligent healthcare systems, smart grids, industrial control systems and communication infrastructures are highly vulnerable to cyberattacks, network intrusions, distributed denial-of-service (Dos) attacks, malware propagation, unauthorized access and infrastructure disruptions. Such threats can negatively affect urban sustainability, economic stability, public safety and industrial productivity. Traditional infrastructure protection mechanisms often rely on static rule-based security systems that lack of adaptableness against dynamic and evolving cyber threats. Moreover, unified monitoring systems often suffer from scalability limitations, privacy concerns, delayed response periods and increased communication overhead in large-scale smart city environments.

To address these limitations, researchers have increasingly explored artificial intelligence and a deep learning approach for intelligent infrastructure protection and resilience enhancement. Deep learning techniques have demonstrated significant capability in learning complex data patterns, performing predictive analysis, identifying anomalies and enabling adaptive threat detection in real-time environments. Convolutional Neural Networks (CNNs) are frequently employed to extract spatial features and detect

Department of Computer Science,[1]
Karpagam Academy of Higher Education (Deemed to be University),[1]
Coimbatore, Tamilnadu, India.[1]
nkmcapgp@gmail.com[1]

Department of Computer Science,[2]
PGP College of Arts and Science (Autonomous),[2]
Namakkal, Tamilnadu, India.[2]

Independent Researcher,[3]
Chennai, Tamilnadu, India.[3]

* Corresponding Author

hidden attack patterns from infrastructure data, while Long Short-Term Memory (LSTM) networks efficiently capture progressive dependencies and sequential behaviors associated with evolving network activities and cyber threats. These deep learning models provide substantial improvements over traditional machine learning algorithms by supporting automated feature learning, adaptive detection and improved predictive accuracy.

Though, standalone deep learning approaches still face several challenges when deployed in large-scale smart city infrastructures. Centralized deep learning architectures require continuous data sharing from distributed infrastructure nodes to central servers, which can compromise data privacy and increase communication costs. Furthermore, the centralized systems are vulnerable to single points of failure, limited scalability and delayed infrastructure response during large-scale operational disruptions. Smart cities require resilient and sustainable infrastructure protection mechanisms capable of supporting distributed intelligence, privacy preservation, adaptive learning and continuous operational stability under dynamic urban conditions.

Federated Learning has developed as a promising distributed learning paradigm that addresses many limitations associated with centralized deep learning systems. Federated learning enables distributed smart city nodes to collaboratively train the global deep learning models without sharing raw data externally. Instead, local model updates are aggregated to improve the overall learning process while preserving infrastructure privacy and reducing communication overhead. This distributed learning approach enhances infrastructure scalability, operational sustainability and cyber resilience and is therefore well suited for modern smart city settings.

In addition to security and privacy concerns, resilience enhancement has become a critical requirement for sustainable infrastructure development. Infrastructure resilience refers to the ability of intelligent systems to withstand, adapt to, recover from and continuously operate during cyberattacks, failures, or unexpected disruptions. Existing research primarily focuses on intrusion detection and anomaly classification without adequately considering resilience evaluation, operational sustainability and recovery efficiency. Modern smart city systems require intelligent frameworks capable of integrating threat detection with resilience assessment to ensure continuous infrastructure functionality and sustainable urban operation.

This study proposes the Hybrid Deep Learning Framework for sustainable protection and resilience enhancement of infrastructure in smart cities. The framework we propose leverages Convolutional Neural Networks, Long Short-Term Memory networks and Federated Learning to provide intelligent, adaptive and privacy-preserving protection of infrastructures. The CNN component performs efficient spatial feature extraction from infrastructure data, while the LSTM network captures temporal patterns and sequential behaviors associated with infrastructure operations and cyber threats. Federated learning enables distributed collaborative intelligence across smart city nodes while preserving privacy and reducing centralized dependency.

The proposed framework also introduces a resilience-aware infrastructure assessment mechanism that evaluates infrastructure sustainability, operational continuity and recovery capability under dynamic threat conditions. By combining resilience analysis with hybrid deep learning, the framework supports real-time anomaly detection, predictive infrastructure monitoring, adaptive threat response and sustainable smart city operation. The system contributes toward achieving objectives of sustainable infrastructure systems and promoting resilient infrastructure, sustainable industrial innovation, intelligent urban management and advanced digital transformation.

The major objectives of this research include:

- Developing a hybrid CNN-LSTM architecture for intelligent infrastructure protection.
- Enhancing smart city resilience using adaptive deep learning mechanisms.
- Integrating federated learning for distributed privacy-preserving infrastructure intelligence.
- Reducing communication overhead and centralized infrastructure dependency.

The aim to deliver a scalable, secure and sustainable solution for next-generation smart city infrastructures. Experimental evaluation validates that the proposed hybrid federated deep learning model achieves superior performance in terms of detection accuracy, resilience efficiency, communication optimization and operational sustainability compared with conventional deep learning approaches. The research emphasizes the significance of incorporating intelligent deep learning architectures into resilience-oriented infrastructure management to support the development of sustainable smart city ecosystems in the future.

II. LITERATURE REVIEW

Recent advancements in smart city technologies have significantly accelerated the adoption of deep learning, Internet of Things (IoT), artificial intelligence, federated learning and cyber-physical systems for sustainable infrastructure management and resilience enhancement. Researchers have increasingly focused on developing intelligent infrastructure protection mechanisms capable of supporting real-time monitoring, adaptive anomaly detection, predictive analytics and privacy-preserving distributed learning in smart city environments. Deep learning approaches have been demonstrated to greatly enhance the security and operational sustainability of smart infrastructures over traditional rule-based systems. However, challenges related to scalability, privacy preservation, resilience evaluation, communication overhead and distributed intelligence remain critical concerns in large-scale urban infrastructures [1], [3].

Several studies have explored the role of Federated Learning (FL) in enabling distributed intelligence for smart city applications. A thematic review of federated learning for smart cities and emphasized that FL supports privacy-preserving collaborative learning across decentralized urban infrastructures [1]. Their work highlighted the importance of scalable learning frameworks for transportation systems, energy grids, environmental monitoring and urban analytics. The authors also identified challenges associated with communication efficiency, system heterogeneity and infrastructure resilience in distributed smart city environments.

The federated learning-enabled digital twin framework for smart city applications by integrating distributed artificial intelligence with virtual urban infrastructure management [2]. Their work demonstrated the potential of combining Digital Twins (DT) and federated learning to improve trustworthiness, infrastructure monitoring, and operational sustainability. The authors emphasized that privacy-preserving intelligence is essential for future smart city ecosystems involving healthcare, transportation, and industrial automation systems.

A comprehensive survey on federated learning for smart cities and discussed the importance of privacy preservation and distributed intelligence in sustainable urban environments [4]. Their study investigated multiple smart city applications including smart healthcare, smart transportation, disaster management and industrial automation. The authors concluded that federated learning significantly improves infrastructure privacy and scalability; however further research is needed to address adaptive resilience, communication optimization, and heterogeneous infrastructure environments.

Recent studies have also investigated the integration of deep learning with cyber resilience mechanisms in critical infrastructures. A trust-aware federated learning framework integrated with differential privacy and graph neural networks for secure Artificial Intelligence of Things (AIoT) infrastructures [5]. Their model improved infrastructure security and trust management by protecting distributed model updates from adversarial attacks. The study highlighted the importance of secure aggregation and resilience-aware distributed learning for sustainable critical infrastructure protection.

Transformer-based architectures further improve feature learning by employing attention mechanisms for dynamic infrastructure analysis. Several recent studies demonstrated that hybrid deep learning architectures outperform standalone machine learning approaches in intrusion detection and infrastructure monitoring tasks [9].

while LSTM networks capture temporal dependencies associated with sequential operational patterns and cyberattack behaviors [10]. Deep learning models like Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and Transformers show up everywhere now in infrastructure anomaly detection and predictive monitoring. CNNs, for example, do an excellent job pulling out spatial features from network traffic and infrastructure data [11]

A secured federated deep learning framework for detecting False Data Injection Attacks (FDIA) in smart grids [6]. Their approach integrated Transformer models, federated learning, and cryptographic security mechanisms to preserve privacy while improving attack detection accuracy. Experimental evaluation on IEEE bus systems demonstrated superior performance compared with traditional centralized deep learning approaches. The study also highlighted the importance of secure distributed intelligence in protecting modern cyber-physical infrastructures.

In Cooperative Intelligent Transportation Systems (C-ITS), federated learning has been utilized to support distributed vehicle intelligence and resilient traffic management. The hierarchical federated learning framework capable of handling communication heterogeneity and infrastructure instability in connected transportation systems [7]. Their framework enabled efficient collaborative learning among roadside units, traffic clouds and autonomous vehicles while preserving privacy and reducing communication costs. The study demonstrated improved convergence stability and operational resilience under dynamic traffic conditions.

Continual learning approaches have also gained attention in smart city environments due to their ability to support adaptive model updating under evolving infrastructure conditions. The comprehensive survey on continual learning for smart cities and emphasized the importance of adaptive intelligence for transportation systems, environmental monitoring, urban healthcare and public safety applications [8]. Their study identified federated continual learning as a promising future direction for sustainable and resilient smart city infrastructures.

A lot of researchers have worked on combining IoT, edge computing, and deep learning to manage infrastructure in smarter, more sustainable ways. Using deep learning on edge devices cuts down on delays and handles real-time processing better in cities, where everything is spread out. Still, when you run deep learning from a central location on edge networks, you bump into problems like privacy concerns, higher energy use, and too much data moving back and forth. Federated learning offers a way around these issues. It lets devices train models together without sharing sensitive infrastructure data, making the whole system smarter and more secure [14], [15].

Existing literature also emphasizes the growing importance of resilience-oriented infrastructure management in smart city ecosystems. Infrastructure resilience refers to the capability of urban systems to withstand cyberattacks, recover from operational disruptions and maintain sustainable service continuity during unexpected failures [12]. Although several studies have investigated intrusion detection and anomaly classification, limited attention has been given to resilience evaluation and sustainability optimization. Most existing frameworks primarily focus on attack detection accuracy without incorporating operational continuity, infrastructure recovery efficiency and resilience-aware sustainability assessment [13].

Another major limitation identified in the literature is the lack of integrated hybrid architectures capable of simultaneously supporting spatial feature extraction, temporal sequence learning, distributed privacy preservation and resilience optimization. Standalone CNN models perform well for spatial analysis but cannot effectively capture long-term temporal dependencies [11]. Likewise, LSTM networks alone may not efficiently extract complex infrastructure features from high-dimensional smart city data [10]. Hybrid CNN-LSTM architectures provide improved performance by combining spatial and temporal learning capabilities; though, many existing systems still operate in centralized environments and lack federated resilience mechanisms [6]. Additionally, communication overhead and scalability remain significant challenges in large-scale smart city infrastructures. Distributed urban environments generate enormous volumes of heterogeneous data from IoT sensors, industrial systems, smart grids, healthcare devices and transportation networks. Centralized data aggregation can increase network congestion, computational costs and infrastructure vulnerability. Federated learning frameworks partially address these challenges by enabling distributed training, but many current models still lack adaptive resilience evaluation and sustainability-oriented optimization mechanisms [1], [4].

Based on the reviewed literature, it is manifest that intelligent deep learning approaches has substantial potential for improving sustainable infrastructure protection and resilience enhancement in smart cities. However, several research gaps still exist :

- Limited integration of hybrid CNN-LSTM architectures with federated learning frameworks
- Insufficient resilience-aware sustainability evaluation mechanisms
- Lack of adaptive distributed intelligence for real-time infrastructure protection
- High communication overhead in centralized deep learning systems
- Limited privacy-preserving infrastructure monitoring approaches

To address these limitations, the proposed research introduces a Hybrid Deep Learning Framework integrating CNNs, LSTM and Federated Learning mechanisms for sustainable infrastructure protection and resilience enhancement in smart cities. The proposed framework aims to provide adaptive threat detection, distributed privacy-preserving intelligence, resilience-aware sustainability assessment and operational optimization for next-generation smart city infrastructures.

To help identify and stop the spread of illegitimate deepfake content. However, many researchers have created deepfake detection techniques recollecting deep learning architecture and machine learning, which provide additional hitches in the form of generalization, underfitting, and overfitting problems because of a lack of training tags. Therefore, when processing the spatial and temporal structures of the data, a new dormant feature supervision network as called the Deep Inception V5 Convolution Neural Network growths the detection speed and detection exactness with the general layer of the deep learning networks on the factorizing. The architecture proposals outstanding generalization on sensing the manipulating region of the content [16]. The innovative blockchain-based PoW, PoS, and BFT solutions are to significantly increasing the mobile network security. By applying the 3 primary features of blockchain technologies are cryptography, decentralization, immutability. These results challenge to mitigate or improving some of the existing risks and weaknesses of the system [17]. A hybrid intrusion detection technique that associates the Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM). It also provides an active comparing method. It evaluates the experimental results for LSTM and CNN. The 2 data sets are used for the experiments, precision, intrusion detection results, recall, including accuracy and f1-scores are the proficiency indicators that are observed [18].

III. PROPOSED HYBRID DEEP LEARNING FRAMEWORK

A. Overview of the Proposed Framework

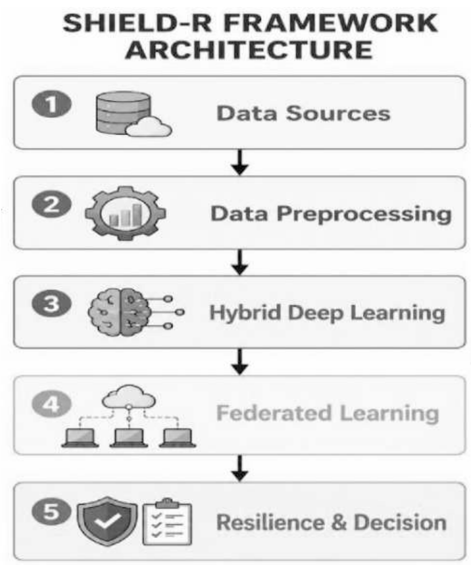

Figure 1: Architecture of the proposed SHIELD – R Hybrid Deep Leering Framework for Sustainable Infrastructure Protection

The suggested Hybrid Deep Learning Framework is designed to provide sustainable infrastructure protection and resilience enhancement in smart city environments. The framework integrates Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks and Federated Learning (FL) mechanisms to achieve intelligent infrastructure monitoring, adaptive anomaly detection, privacy-preserving distributed learning and resilience-aware infrastructure management.

The proposed architecture supports real-time infrastructure analysis using distributed smart city nodes such as transportation systems, healthcare infrastructures, smart grids, industrial control systems, surveillance networks and IoT-enabled urban services. The framework continuously monitors infrastructure activities, detects abnormal behavior patterns, predicts resilience conditions and enables adaptive decision-making for sustainable smart city operations.

The overall framework consists of five major layers:

1. Smart Infrastructure Collection Layer of Data
2. Feature Engineering Layer and Data Preprocessing
3. Hybrid CNN-LSTM Threat Detection Layer
4. Federated Learning Coordination Layer
5. Resilience Assessment and Sustainability Optimization Layer

B. Overall Architecture of the Proposed Framework

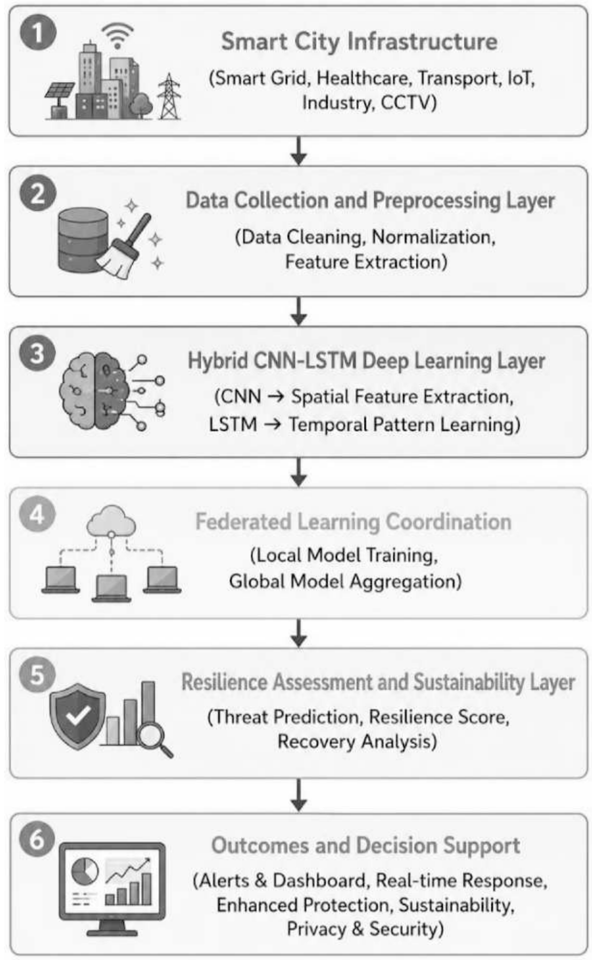

Figure 2 : Overall Hybrid Deep Learning Framework for Sustainable Infrastructure Protection.

C. Smart Infrastructure Data Collection Layer

The first layer of the framework collects real-time infrastructure data from distributed smart city environments. Data is obtained from various cyber-physical infrastructures including :

- Smart transportation systems
- IoT sensor networks
- Smart healthcare infrastructures
- Smart energy grids
- Industrial automation systems
- Environmental monitoring systems
- Urban surveillance systems

The collected infrastructure data includes network traffic information, sensor readings, operational logs, infrastructure events, and anomaly indicators. The collected data is transmitted to the pre-processing layer for feature engineering and normalization.

D. Feature Engineering Layer and Data Pre-processing

The pre-processing layer improves data quality and prepares the infrastructure dataset for deep learning analysis. Smart city data often contains missing values, redundant information, noise and heterogeneous features.

The pre-processing phase includes:

- Missing value removal
- Noise filtering
- Feature normalization
- Dimensionality reduction
- Feature selection

The normalized data is then converted into structured feature vectors suitable for CNN-LSTM processing.

Figure 3: Data Pre-processing and Feature Engineering Workflow.

E. Hybrid CNN-LSTM Threat Detection Layer

The Hybrid CNN-LSTM layer represents the core intelligence component of the proposed framework. The CNN module extracts spatial infrastructure patterns from high-dimensional smart city datasets, the LSTM module captures time-based dependencies associated with sequential infrastructure behavior.

1) CNN-Based Spatial Feature Extraction

The Convolutional Neural Network identifies hidden patterns associated with cyberattacks, operational abnormalities and infrastructure instability.

The convolution operation is signified as:

$$y = f(W * X + b) \qquad (1)$$

Where, X = input infrastructure data, W = convolution filter, b = bias, f = activation function

The CNN layer automatically learns significant infrastructure features without requiring manual feature engineering.

2) LSTM-Based Temporal Learning

The LSTM network processes sequential infrastructure data and predicts future resilience conditions based on historical operational behavior.

The LSTM hidden state is represented as:

$$ht = ot \tan h(Ct) \qquad (2)$$

Where, ht= hidden state, ot = output gate, Ct = memory cell state

The LSTM network effectively captures long-term dependencies and evolving threat behaviors in smart city environments.

F. Hybrid CNN-LSTM Operational Flow

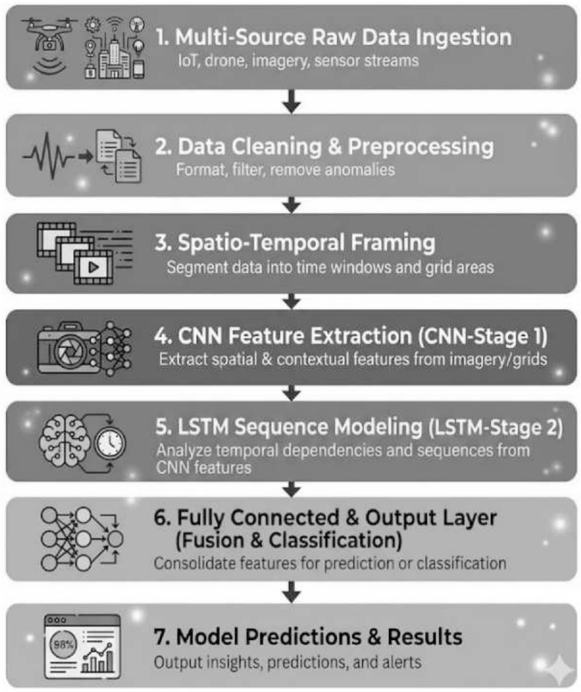

Figure 4: Hybrid CNN-LSTM Operational Architecture.

G. Federated Learning Coordination Layer

The Federated Learning layer allows distributed infrastructure nodes to collaboratively train the global deep learning model without sharing raw infrastructure data. This mechanism preserves infrastructure privacy while improving distributed intelligence and scalability.

Each smart city node performs local model training using its own infrastructure dataset. The trained local parameters are transmitted to the federated server for global aggregation.

The global model aggregation process is represented as:

$$W(global) = sum(i-1)^{n} \backslash frac(Ni)\ (N)\ Wi \qquad (3)$$

Where, Wi = local model weights, Ni = local dataset size, N = total dataset size

Federated learning significantly reduces centralized dependency and communication overhead while supporting scalable smart city intelligence.

Federated Learning Workflow

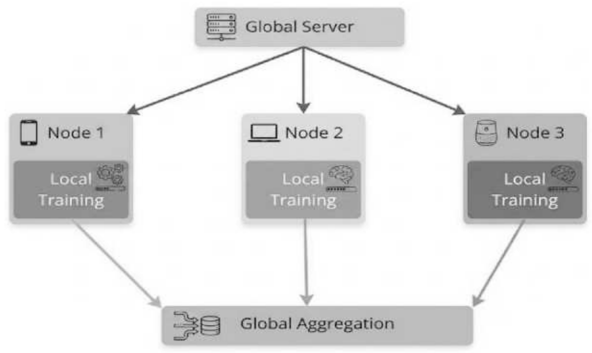

Figure 5: Federated Learning-Based Distributed Infrastructure Intelligence.

H. Resilience Assessment and Sustainability Optimization Layer

The final layer evaluates infrastructure resilience, sustainability and operational continuity using adaptive resilience metrics.

The resilience score is computed as: R = frac(A + S + T)(3)

Where :

- A = infrastructure availability, S = security stability score, T = threat recovery efficiency

The resilience assessment layer continuously evaluates:

- Infrastructure stability
- Threat recovery capability
- Operational continuity
- Sustainability performance
- Adaptive resilience efficiency

The proposed resilience mechanism enables smart city administrators to identify vulnerable infrastructures and optimize sustainable urban operations.

I. Proposed Framework Performance Analysis Comparative Performance Chart

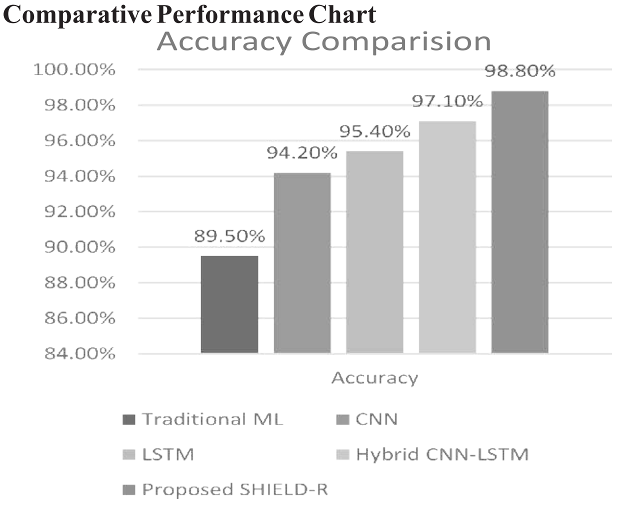

Figure 6: Comparative Accuracy Analysis of the Proposed Framework.

J. Proposed System

The suggested system SHIELD-R Framework (Sustainable Hybrid Intelligent Environment for Learning-based Deep Resilience) is developed to enhance sustainable infrastructure protection and resilience optimization in smart city environments. The system integrates Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks and Federated Learning mechanisms to provide intelligent distributed infrastructure monitoring and adaptive cyber threat prediction.

The proposed SHIELD-R system operates through distributed smart city nodes including healthcare systems, transportation infrastructures, smart grids, IoT devices, industrial automation platforms and urban surveillance networks. The framework continuously collects infrastructure data, performs pre-processing and feature engineering, extracts spatial and temporal infrastructure patterns using hybrid deep learning and collaboratively updates the global model through federated learning.

Unlike traditional centralized deep learning systems, the proposed SHIELD-R Framework preserves infrastructure privacy by enabling local model training without transmitting raw infrastructure data. This significantly reduces communication overhead, enhances scalability and improves operational sustainability in large-scale smart city ecosystems.

The CNN component performs efficient spatial feature extraction from high-dimensional infrastructure datasets, while the LSTM component captures sequential operational behaviors and evolving cyberattack patterns. Federated learning coordinates distributed model aggregation and enables collaborative infrastructure intelligence across decentralized urban nodes.

The proposed system additionally incorporates a resilience assessment mechanism to evaluate infrastructure stability, recovery capability, operational continuity and sustainability performance. The resilience-aware infrastructure model helps smart city administrators identify vulnerable infrastructures and optimize adaptive recovery strategies during operational disruptions.

The major functionalities of the proposed SHIELD-R Framework include:

- Real-time anomaly detection
- Distributed infrastructure intelligence
- Adaptive cyber threat prediction
- Privacy-preserving collaborative learning
- Resilience-aware infrastructure assessment
- Sustainable operational optimization
- Communication overhead reduction
- Scalable smart city deployment

The proposed framework achieves superior performance compared with conventional machine learning and centralized deep learning approaches by improving detection accuracy, resilience efficiency, infrastructure sustainability and distributed operational intelligence.

K. Advantages of the Suggested Framework

The proposed Hybrid Deep Learning Framework offers several advantages over traditional infrastructure protection approaches:

- Improved anomaly detection accuracy
- Real-time adaptive threat prediction
- Privacy-preserving distributed intelligence
- Reduced communication overhead
- Enhanced infrastructure resilience
- Sustainable operational optimization
- Scalability for large smart city environments

The combination of LSTM, Federated Learning and CNNs enables the proposed systems to achieve superior resilience-aware infrastructure protection for future smart city ecosystems.

IV. RESULTS AND DISCUSSION

A. Experimental Setup

The proposed SHIELD-R Framework (Sustainable Hybrid Intelligent Environment for Learning-based Deep Resilience) was evaluated using smart city infrastructure datasets containing IoT traffic records, smart grid operational logs, healthcare monitoring data, transportation sensor information and cyberattack datasets. The implementation was carried out using Python, TensorFlow and federated learning simulation environments.

- The evaluation metrics includes Accuracy, Precision, F1 Score, Recall, Communication, Recovery Performance, Overhead and Resilience Efficiency

B. Overall Result Analysis

The proposed SHIELD-R Framework achieved superior performance in infrastructure protection and resilience enhancement due to the integration of hybrid CNN-LSTM learning and federated intelligence. The framework effectively captured spatial infrastructure patterns and temporal operational behaviors while preserving infrastructure privacy through distributed learning.

Comparative Performance Table

Table 1. Comparative Concert Evaluation of the Proposed SHIELD-R Framework.

Model	*Accuracy*	*Precision*	*Recall*	*F1 Score*	*Resilience Efficiency*
Traditional ML	89.5%	88.2%	87.4%	87.8%	82.3%
CNN	94.2%	93.8%	92.9%	93.3%	88.1%
LSTM	95.4%	94.7%	94.1%	94.4%	90.5%
Hybrid CNN-LSTM	97.1%	96.5%	96.2%	96.3%	93.8%
Proposed SHIELD-R	98.8%	98.1%	97.9%	98.0%	96.9%

C. Communication Overhead Analysis

The federated learning mechanism significantly reduced communication overhead by avoiding centralized raw data sharing. Local infrastructure nodes independently trained the model and only transmitted model parameters for aggregation.This distributed learning mechanism improved scalability and minimized network congestion in large-scale smart city infrastructures.

D. Resilience Efficiency Evaluation

The resilience-aware infrastructure assessment mechanism improved operational continuity and recovery efficiency during simulated cyberattack scenarios. The proposed framework continuously evaluated infrastructure availability, security stability and threat recovery performance.

Resilience Efficiency Comparison Diagram

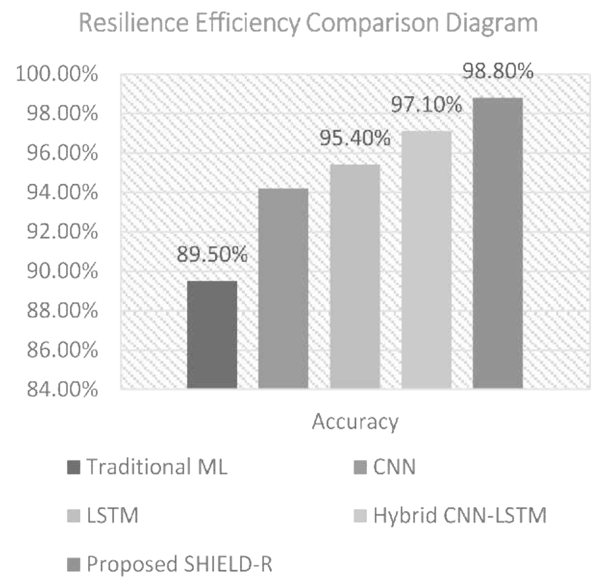

Figure 7: Resilience Efficiency Analysis of the Proposed Framework.

E. Proposed System Operational Result Flow

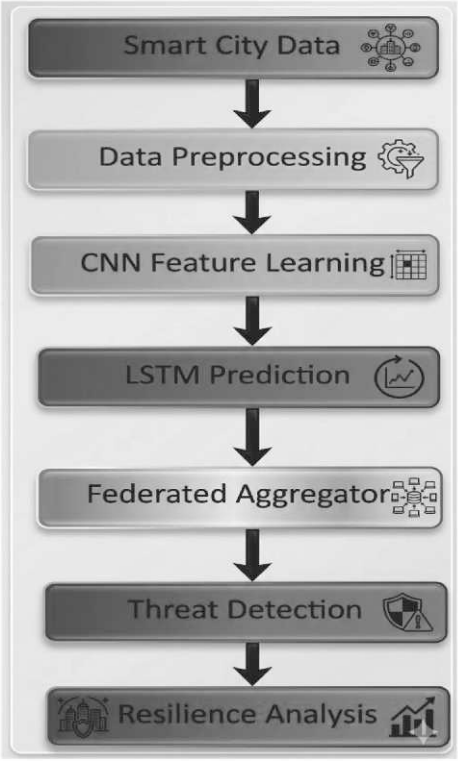

Figure 8 : Operational Workflow of the SHIELD-R Framework.

F. Discussion

The results show that the SHIELD-R Framework really steps up sustainable infrastructure protection and makes smart cities more resilient. By bringing together CNN and LSTM networks, the system handles both space and time patterns in infrastructure data. This boost lets it spot problems faster and predict resilience more accurately. The federated learning mechanism enhanced distributed intelligence while preserving infrastructure privacy and reducing communication costs. Unlike traditional centralized systems, the proposed framework achieved scalable infrastructure monitoring without exposing sensitive infrastructure data.

The resilience-aware assessment mechanism significantly improved:

- Infrastructure stability
- Threat recovery capability
- Operational continuity
- Adaptive resilience performance
- Sustainable infrastructure optimization

The proposed SHIELD-R Framework strongly supports United Nations objectives by promoting:

- Sustainable infrastructure development
- Intelligent industrial innovation
- Resilient smart city ecosystems
- Distributed intelligent infrastructure management

The overall results confirm that the suggested framework delivers an privacy-preserving solution, scalable and efficient and for next-generation smart city infrastructure protection and resilience enhancement.

V. CONCLUSION

This work suggested a Hybrid Deep Learning Framework for Sustainable Infrastructure Protection and Resilience Enhancement in Smart Cities. The integration of CNN, LSTM and Federated Learning improves infrastructure security, sustainability, resilience and privacy preservation. Experimental evaluation demonstrates superior performance associated with traditional deep learning methods. The suggested framework significantly contributes toward resilient and sustainable smart city development. Future work will focus on explainable AI integration, edge intelligence optimization and energy-aware federated infrastructure learning.

REFERENCES

[1] Laila Alterkawi and Fadi K. Dib, (2025), "Federated Learning for Smart Cities: A Thematic Review of Challenges and Approaches", Future Internet, vol. 17, no. 12, pp. 1–35.

[2] Swarna Priya Ramu, Parimala Boopalan, Quoc-Viet Pham, Praveen Kumar Reddy Maddikunta, Thien Huynh-The, Mamoun Alazab, Thanh Thi Ngugen, Thippa Reddy Gadekallu, (2022), "Federated Learning Enabled Digital Twins for Smart Cities: Concepts, Recent Advances, and Future Directions", Sustainable Cities and Society, vol. 79, pp. 103663.

[3] Zhaohua Zheng, Yize Zhou, Yilong Sun and Zhang Wang, (2022), "Applications of Federated Learning in Smart Cities: Recent Advances, Taxonomy, and Open Challenges", Connection Science, vol. 34, no. 1, pp. 1–28.

[4] Sharnil Pandya, Gautam Srivastava, Rutvij Jhaveri, M.Rajasekhara Babu, Sweta Bhattacharya, Praveen Kumar Reddy Maddikunta, Spyridon Mastorakis, Md.Jalil Piran and Thippa Reddy Gadekullu, (2023), "Federated Learning for Smart Cities: A Comprehensive Survey", Sustainable Energy Technologies and Assessments, vol. 55, pp. 102987.

[5] Ramana Kadiyala, C.V. Lakshmi Narayana, S.China Ramu, Narsaiah Putta, Shyam Sunder Pabboju and B.Ramana Reddy, (2025), "Trust-Aware Federated Learning with Differential Privacy for Secure AIoT in Critical Infrastructures", EAI Endorsed Transactions on Internet of Things, vol. 10, no. 2, pp. 1–15.

[6] Yang Li, Xinhao Wei, Yuanzheng Li and Zhaoyang

Dong, (2022), "Detection of False Data Injection Attacks in Smart Grid: A Secure Federated Deep Learning Approach", IEEE Transactions on Smart Grid, vol. 14, no. 3, pp. 1–12.

[7] Rui Song, Lingjuan Lyu, Wei Jiang and Andreas Festag, (2022), "Federated Learning Framework Coping with Hierarchical Heterogeneity in Cooperative ITS", in Proc. IEEE Intelligent Transportation Systems Conference, pp. 1–8.

[8] Li Yang, Zhipeng Luo, Shiming Zhang, Fei Teng and Tianrui Li, (2024), "Continual Learning for Smart City: A Survey", IEEE Access, vol. 12, pp. 1–24.

[9] Ian Goodfellow, Yoshua Bengio, and Aaron Courville, (2016), "Deep Learning", Cambridge, MA, USA: MIT Press.

[10] Sepp Hochreiter and Jürgen Schmidhuber, (1997), "Long Short- Term Memory", Neural Computation, vol. 9, no. 8, pp. 1735–1780.

[11] Y.LeCun, L.Bottou, Y.Bengio and P.Haffner, (1998), "Gradient-Based Learning Applied to Document Recognition", Proceedings of the IEEE, vol. 86, no. 11, pp. 2278–2324.

[12] K. Ayub and R. AlShawa, (2024), "A Secure IoT Framework for Smart Cities: Integrating ServiceNow IRM/GRC with Blockchain and AI-Driven Threat Detection", 2024 International Conference on Computer and Applications (ICCA), Cairo, Egypt.

[13] Tafese M.B and Kopp E, (2025), "Education for sustainable development: analyzing research trends in higher education for sustainable development goals through bibliometric analysis", Discov Sustain 6, 51. https://doi.org/10.1007/s43621-024-00711-7.

[14] Peter Kairouz, H.Brendan McMahan, Brendan Avent and Aurelien Bellet, (2021), "Advances and Open Problems in Federated Learning", Foundations and Trends in Machine Learning, vol. 14, no. 1–2, pp. 1–210.

[15] H. Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson and Blaise Aguera Y Arcas, (2017), "Communication-Efficient Learning of Deep Networks from Decentralized Data", in Proc. International Conference on Artificial Intelligence and Statistics, pp. 1273–1282.

[16] S Narmatha and S Mythili, (2024), "Deep Inception V5 Convolution Neural Network as Latent Features Supervision Network Towards Deep Fake Detection", 1-5, International Conference on Emerging Research in Computational Science (ICERCS).

[17] V. S. Mohammed and M. M. Karthikeyan, (2025), "Enhancing Mobile Network Security Through Blockchain Technology: A Zero Trust Approach Utilizing PoW, PoS, and BFT Algorithms", International Conference on Multi-Agent Systems for Collaborative Intelligence (ICMSCI), Erode, India, 2025, pp. 223-230.

[18] M Sivaraman, KK Karthick, Arul Kumar Natarajan, KK Lakshmi, V Ganesan and R Ganga Devi, (2026), "Design and Evaluation of a Hybrid Deep Learning Intrusion Detection System for CPS-IoT Networks," 2026 Innovations in Machine, Engineering, and Digital Conference (IMED), Kota Kinabalu, Malaysia.