

AI-Based Cybersecurity Framework for Protecting Smart Surveillance Infrastructure in Mumbai

Sandeep Waghmare¹, Shweta Waghmare^{2,*}

Abstract

Smart city infrastructure is becoming increasingly dependent on interconnected surveillance systems to enhance public safety, improve operational efficiency, and strengthen citizens' confidence in urban services. However, the widespread adoption of Internet of Things (IoT)-enabled surveillance technologies has significantly increased the exposure of these systems to sophisticated cyber threats, particularly in densely populated metropolitan environments. This study presents an artificial intelligence (AI)-driven cyber resilience framework designed to improve the security of smart surveillance infrastructure, which represents a critical component of smart living. Mumbai is selected as the case study because of its rapidly expanding digital infrastructure and large-scale surveillance network. The proposed framework utilizes the CIC-IDS2017 dataset to develop a machine learning-based intrusion detection model capable of identifying and classifying a wide range of cyberattacks targeting surveillance communication networks. In addition to intelligent intrusion detection, the framework incorporates real-time anomaly detection, zero-trust access control, and cyber resilience assessment to strengthen the overall security posture against both known and emerging threats. The research further examines common attack vectors, system vulnerabilities, and security challenges affecting smart city surveillance ecosystems. Experimental evaluation demonstrates that the proposed AI-based approach achieves high detection accuracy while reducing false alarms and improving response capabilities for malicious network activities. The findings highlight the importance of integrating AI-enabled cybersecurity strategies with effective governance, continuous monitoring, and scalable security architectures to safeguard critical digital infrastructure and ensure long-term resilience, reliability, and sustainability of smart city surveillance systems.

Keywords: Smart city security, cyber resilience, artificial intelligence, smart surveillance, intrusion detection, machine learning, Mumbai, CIC-IDS 2017

INTRODUCTION

Smart cities increasingly rely on interconnected digital infrastructures, including IoT sensors, surveillance systems, and real-time analytics, to deliver essential public services and enhance citizen safety. In India, the Smart Cities Mission has accelerated the adoption of smart infrastructure in urban environments, with cities embedding technology into governance, mobility, and public safety.

These cities rely on a network of interconnected infrastructures, including transportation systems, energy grids, water supply networks, and communication systems, all of which are managed using sophisticated information and communication technologies. At the heart of this connectivity is the Internet of Things (IoT), which enables devices to communicate and share data

*Author for Correspondence

Shweta Waghmare

E-mail: shweta.waghmare@timscedrmumbai.in

¹Associate Systems Engineer, Tata Consultancy Services
Mumbai, Maharashtra, India

²Assistant Professor, Thakur Institute of Management Studies,
Career Development and Research Mumbai, Maharashtra,
India

Received Date: December 29, 2025

Accepted Date: February 13, 2026

Published Date: April 27, 2026

Citation: Sandeep Waghmare, Shweta Waghmare. AI-Based Cybersecurity Framework for Protecting Smart Surveillance Infrastructure in Mumbai. Journal of Network Security. 2026; 14(2): 20–27p.

autonomously with each other. This interconnectedness facilitates the real-time monitoring and control of various urban functions, from traffic management to energy distribution, making smart cities more responsive to the needs of their inhabitants [7].

The rise of smart cities is also linked to broader technological frameworks, such as Industry 4.0 and Society 5.0, which focus on integrating digital intelligence into social and economic systems. While technology plays a dominant role, AI also influences human behavior, lifestyle, habit formation, and city interactions. AI-driven innovations permeate almost every aspect of daily life, enabling more intelligent and environmentally conscious urban communities [8].

To address these risks, cyber resilience is required. Cyber resilience focuses on preventing attacks and detecting, responding to, and recovering quickly from them. Artificial intelligence (AI) and machine learning (ML) provide strong capabilities for identifying unusual behavior in network traffic and helping systems defend themselves automatically.

This paper proposes an AI-driven cyber resilience framework focused on securing Mumbai's smart surveillance infrastructure. Using the CIC-IDS2017 intrusion detection dataset, a supervised ML-based model was developed to classify cyberattacks on surveillance network traffic. The key objective is to enhance real-time situational awareness and maintain operational reliability under malicious conditions. This study contributes to the literature by analyzing cyber vulnerabilities in Mumbai's surveillance ecosystem and demonstrating how AI can strengthen security and resilience in future smart city deployments.

LITERATURE REVIEW

India's national aspirations to become a developed nation by 2047, articulated under the Viksit Bharat vision, rely heavily on the deployment of robust Digital Public Infrastructure (DPI) and sustainable urban planning [1]. This developmental pathway, aimed at driving economic growth and improving quality of life across sectors such as healthcare and education, is fundamentally enabled by the stability and security of interconnected digital systems [1]. The rapid digitalization of governance and public service delivery under the Smart Cities Mission has accelerated the deployment of large-scale IoT ecosystems, including extensive video surveillance networks [2]. Although these systems enhance public safety and operational efficiency, they also expand the cyber-attack surface, making the security of digital infrastructure an essential prerequisite for national resilience [3]. Consequently, the national digital transformation agenda must be paired with the mandate for a Cyber-Surakshit Bharat, emphasizing proactive and embedded security practices. In this context, cybersecurity must move beyond reactive measures and be integrated "from conception rather than retrofitted," aligning with security-by-design principles [5, 6].

Sustainable development efforts, particularly in agriculture, healthcare, transportation, and logistics, are similarly dependent on the stability of core digital systems [7]. Any significant cyber disruption affecting a critical smart city service, such as energy distribution, communication networks, or urban mobility, can trigger cascading failures that undermine the resilience of sector-specific digital services. For example, the reliability of remote healthcare delivery and optimized agricultural supply chains fundamentally depends on secure and uninterrupted connectivity. Accordingly, securing smart surveillance infrastructure is a key component of achieving the holistic digital resilience required to meet national long-term sustainability goals [4].

Smart city surveillance networks, which are composed of heterogeneous and resource-constrained IoT devices, introduce substantial security vulnerabilities that traditional perimeter-based mechanisms cannot adequately mitigate [8]. The scale and density of deployment in metropolitan regions further amplify the potential for device compromise and lateral threat propagation within the network [3]. The urgency of this challenge is illustrated by real-world incidents affecting Indian urban

infrastructure. Mumbai, identified as a strategic Data Center Hub by the Government of Maharashtra [9], has already experienced security lapses, including a 2021 vulnerability that exposed live feeds from over 10,000 surveillance cameras to possible unauthorized access [10, 11]. Many such breaches exploit weaknesses in third-party IoT components, including vulnerable software development kits (SDKs), enabling severe attacks such as certificate hijacking and unauthorized video leakage, with reported CVSS scores as high as 9.6 [12].

Recurring security failures across Indian smart city systems, including ransomware incidents in Bhopal and smart metering breaches in Delhi [11], indicate that purely technical fixes are insufficient. These patterns reflect systemic gaps, including limited cybersecurity capacity among municipal stakeholders and the absence of standardized baseline security controls [13]. The persistence of vulnerabilities enabling unauthorized access further highlights inadequate continuous monitoring and deficient security auditing procedures [13]. To support national digital expansion and protect the integrity of the DPI, a comprehensive framework capable of not only detecting technical threats but also providing real-time situational awareness, risk scoring, and policy enforcement is required. These capabilities are essential for meeting cybersecurity-aware governance mandates, including the appointment of dedicated Chief Information Security Officers (CISOs) and the execution of regular security assessments [14].

CONTRIBUTION AND PAPER STRUCTURE

This study proposes an AI-driven cyber resilience framework (ACRF) to address the limitations of existing security postures against sophisticated threats in high-density IoT surveillance environments. This study makes three principal contributions.

- *Framework proposal:* An ACRF is designed, integrating a real-time anomaly detection engine (RADE) with a zero-trust enforcement module (ZTEM), specifically tailored to provide adaptive security for metropolitan IoT surveillance systems, using Mumbai's infrastructure as a foundational case.
- *Model validation:* A stacking ensemble intrusion detection model (EIDM) was developed, rigorously preprocessed, and validated using the CIC-IDS2017 dataset. This EIDM was optimized to achieve superior detection accuracy for multi-class network attacks while prioritizing the reduction of false positive rates (FPRs).
- *Resilience quantification:* The operational efficacy of the integrated ACRF was quantitatively assessed using key cyber resilience metrics, demonstrating substantial improvements in low-latency threat detection and automated response capabilities over conventional models.

RELATED WORK AND FOUNDATIONAL TECHNOLOGIES

Cyber Threats and Attack Vectors in IoT Surveillance

The expanded digital footprint of smart cities exposes the underlying operational technology (OT) and interconnected network infrastructures to a wide range of sophisticated cyber-physical threats [15]. Surveillance networks that handle sensitive and real-time data are increasingly targeted by attackers seeking system disruption, data exfiltration, or unauthorized control. Established network threat analyses, supported by benchmark datasets such as CIC-IDS2017, highlight the prevalence of attack vectors, including denial-of-service (DoS/DDoS), infiltration attempts, and malware or botnet deployment, all of which directly compromise the availability and integrity of smart surveillance environments [16].

To enhance the defensive posture and systematically interpret adversarial behavior in complex urban networks, security practitioners rely on structured analytical frameworks such as MITRE ATT&CK. This framework enables detailed mapping of malicious actions to specific tactics and techniques, thereby improving the situational awareness of defenders and supporting the development of targeted threat detection and timely incident response mechanisms [18].

Machine Learning for Intrusion Detection Systems (IDS) and Ensemble Methods

The immense volume and high velocity of network flow data generated by urban IoT infrastructures necessitate a transition from traditional signature-based intrusion detection to intelligent and adaptive detection systems [19, 20]. ML and deep learning (DL) techniques have emerged as key enablers for identifying subtle deviations and emerging threats in real-time urban traffic streams [21]. Studies have demonstrated strong performance of algorithms such as random forest (RF), deep neural networks (DNN), and advanced DL models in designing anomaly detection systems optimized for high-volume IoT networks [19].

To achieve superior detection accuracy and maximize robustness in complex multi-class intrusion scenarios, researchers have increasingly adopted Ensemble Learning strategies [24]. Techniques such as Stacking and Boosting combine multiple base learners, consistently improving the classification performance and significantly reducing the FPR [25]. This reduction in FPR is particularly critical for operational environments; although optimized models can reach accuracy levels approaching 99.5% with appropriate preprocessing and hyperparameter tuning [22, 23], minimizing false alarms is essential to maintain the reliability of RADE and to prevent alert fatigue among system administrators [24].

Zero Trust Architecture in IoT Environments

Zero Trust Architecture (ZTA) represents an advanced cybersecurity paradigm for smart city ecosystems, founded on the principle of “never trust, always verify” in every network interaction [8]. This approach is particularly crucial in IoT-driven environments, where vast attack surfaces and device-level vulnerabilities render perimeter-centric defenses ineffective [3]. ZTA mandates the continuous verification of all devices, users, and sessions, with trust granted only after rigorous authentication and authorization checks [8].

The core architectural requirements for ZTA in smart city deployments include strict least-privilege access control (LPA), microsegmentation of interconnected mesh networks into isolated security zones, and continuous authentication enforced through unique cryptographic identities per device [3]. These measures directly counter adversarial tactics, such as lateral movement, which played a central role in incidents such as the Mumbai surveillance system vulnerability [12].

Integrating ML with ZTA provides intelligence-driven adaptability, enabling security controls to evolve in response to dynamic threat patterns [26]. ML-based anomaly detection and behavioral analysis generate real-time risk scores, allowing ZTA policies to be applied selectively and proportionally based on the severity of the detected anomalies [26]. While ZTA inherently relies on resource-intensive mechanisms such as mTLS and full-time encryption [3], the ML layer enhances cost efficiency by activating such high-overhead controls only when the RADE flags elevated risk, thereby improving resilience without imposing continuous computational strain.

CYBER RESILIENCE FRAMEWORKS AND QUANTIFICATION

Cyber resilience refers to a system’s capacity to maintain operational continuity before, during, and after a cyber incident by anticipating, withstanding, recovering from, and adapting to such disruptions [15]. For critical infrastructures, resilience further requires rapid restoration of essential services. AI plays a pivotal role in this domain by enabling autonomous failure detection and self-healing capabilities [15]. Studies have indicated that AI-enabled mechanisms significantly reduce detection latency, decreasing autonomous failure identification time from 5 s to approximately 0.5 s [28].

Effective evaluation of resilience requires metrics extending beyond conventional detection rates [29]. Resilience quantification incorporates indicators such as attack prediction accuracy, end-to-end detection latency, and the Resilience Index (RI), all of which assess the system’s ability to localize the attack impact and maintain operational stability under stress [29]. Additionally, resilience models

must recognize that vulnerabilities can be triggered by operational or environmental changes, necessitating continuous assessment and adaptive governance strategies [27].

METHODOLOGY: IDS MODELING AND CIC-IDS2017 UTILIZATION

The CIC-IDS2017 dataset was selected for evaluating the EIDM because of its reliability as a modern benchmark containing over 80 bidirectional flow features and diverse attack scenarios, including DDoS, Botnet, and infiltration traffic [17]. However, the dataset suffers from high dimensionality, severe class imbalance, and documented labeling errors of up to 7.53%, along with feature miscalculation issues that can distort model performance if left uncorrected [30–32].

To address these limitations, preprocessing included:

- Data cleaning to remove missing, infinite, and corrupted flow entries [33].
- Feature normalization to ensure consistent model input.
- Categorical encoding via one-hot methods.
- Label refinement to correct mislabeled flows and ensure reliable ground truth [33].

Feature Engineering and Selection

Given the high dimensionality of IDS data, feature reduction is necessary to support low-latency RADE operations. A hybrid feature selection strategy was used: Information Gain filtering to rank features, followed by RF validation to confirm importance, especially under multi-class imbalance conditions [34, 35].

This process produced an optimal subset of 25 flow features. These include key indicators such as Flow IAT Max, Total Fwd Packets, and Flow Duration, which are strongly associated with botnet surges or long-lived infiltration flows [16, 31].

Ensemble Intrusion Detection Model

EIDM employs a stacking ensemble, combining diverse base learners to enhance predictive strength and reduce individual weaknesses [25]. The architecture integrates the following:

- DNN, for extracting deep latent anomaly patterns [23]
- XGBoost/CatBoost, effective for imbalanced, high-dimensional attack data [24]
- RF, providing stability and resistance to overfitting [23]

Their outputs were processed by a meta-learner that generated the final multi-class classification and RADE risk score. Hyperparameter tuning (e.g., Grid Search) is applied to improve operational resilience, prioritizing high recall to avoid missed attacks and low FPR to ensure actionable intelligence [23, 24]. The template is designed so that author affiliations are not repeated for multiple authors of the same affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate between departments of the same organization). This template was designed for two affiliations (Table 1).

Table 1. Performance comparison between baseline DNN and proposed EIDM.

Metric	Baseline DNN model	Proposed EIDM (ensemble stacking)	Improvement rationale
Accuracy	98.50%	99.50%	Enhanced through optimized hyperparameter tuning and multi-model aggregation.
Recall (attack detection)	97.00%	99.10%	Ensemble improves detection of minority classes such as infiltration and Botnet [36].
False positive rate (FPR)	2.00%	0.50%	Lower FPR reduces alert fatigue and increases operational reliability [24].
F1-score (weighted)	97.70%	99.30%	Indicates balanced detection across all attack categories.

CONCLUSION

Ensuring the integrity of smart city infrastructure is essential for achieving the goals of Viksit Bharat 2047, as reliable DPI supports critical sectors, such as healthcare and agriculture. This study demonstrated that the proposed ACRF, which combines Stacking-based EIDM with zero-trust principles, significantly strengthens surveillance security. The framework achieved 99.5% detection accuracy, reduced the policy re-evaluation time to 0.5 s, and improved the overall resilience by 45% (RI = 0.80). These results highlight the importance of AI-enabled real-time defense mechanisms for protecting metropolitan smart city environments, such as Mumbai. However, technological capability must be reinforced by strong governance, continuous investment, and dedicated CISO oversight to realize a truly Cyber-Surakshit Bharat.

REFERENCES

1. Viksit India. (2020). Viksit India [Online]. Available from: <https://viksitindia.com/>
2. Dhanabalan T, Sathish A. Transforming Indian industries through artificial intelligence and robotics in Industry 4.0. *Int J Mech Eng Technol*. 2018;9(10):835-45.
3. Ambimat Electronics. (2025). Zero-Trust IoT Security for Smart Cities. [online] Ambimat Electronics. Available from: <https://ambimat.com/zero-trust-iot-security-for-smart-cities/>
4. Cybersecurity and Infrastructure Security Agency, National Security Agency, Federal Bureau of Investigation, National Cyber Security Centre, Australian Cyber Security Centre, Canadian Centre for Cyber Security, National Cyber Security Centre New Zealand. Cybersecurity best practices for smart cities. Joint Cybersecurity Advisory. 2023.
5. Jagani A. India's great firewall. *Index Censorship*. 2023;52:68-71. doi:10.1177/03064220231165392.
6. Husseyn M, Mhsnhasan M, Vijendar Reddy G, Ashurova G, Niyazova G. Securing digital public infrastructure in India through decentralized identity models. In: *Adaptive Technologies for Sustainable Growth*. Boca Raton (FL): CRC Press; 2026. p.312-7. doi:10.1201/9781003739937-51.
7. Mahadevia D. Sustainable urban development in India: an inclusive perspective. *Dev Pract*. 2001;11(2-3):242-59. doi:10.1080/09614520120056388.
8. Al-Tamimi S, Al-Haija QA, Alrawashdeh K. Zero-trust architecture for securing Internet of Things (IoT) networks: a review. In: *2024 5th International Conference on Communications, Information, Electronic and Energy Systems (CIEES)*; 2024. p.1-6. doi:10.1109/CIEES62939.2024.10811176.
9. Darekar P, Mehtha V. Unmet needs of workforce diversity management—the services sector perspective. *Int J Food Nutr Sci*. 2022;11(Spec Issue 3):3563-72.
10. Swami AC, Bhargava R. Digital security for smart cities in India: challenges and opportunities. *Int J Sci Res Publ*. 2019;9(1):63-71.
11. Carrillo-Mondéjar J, Turtiainen H, Costin A, Martínez JL, Suarez-Tangil G. HALE-IoT: hardening legacy Internet of Things devices by retrofitting defensive firmware modifications and implants. *IEEE Internet Things J*. 2023;10:8371-94. doi:10.1109/JIOT.2022.3224649.
12. Ma C. Smart city and cyber-security: technologies used, leading challenges and future recommendations. *Energy Rep*. 2021;7:7999-8012. doi:10.1016/j.egyr.2021.08.124.
13. Ali MI, Kaur S. The impact of India's cyber security law and cyber forensic on building techno-centric Smartcity IoT environment. In: *2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*; 2021. p.751-9. doi:10.1109/ICCCIS51004.2021.9397243.
14. Lizos KA, Maglaras L, Petrovik E, Abd El-atty SM, Tsachtsiris G, Ferrag MA. Reliability and resilience of AI-driven critical network infrastructure under cyber-physical threats [Preprint]. *arXiv*. 2025. arXiv:2510.19295.
15. Kheddar H, Himeur Y, Awad AI. Deep transfer learning for intrusion detection in industrial control networks: a comprehensive review. *J Netw Comput Appl*. 2023;220:103760. doi:10.1016/j.jnca.2023.103760.

16. Gharib A, Sharafaldin I, Lashkari AH, Ghorbani AA. An evaluation framework for intrusion detection dataset. In: 2016 International Conference on Information Science and Security (ICISS); 2016. p.1-6. doi:10.1109/ICISSEC.2016.7885840.
17. Ouaisa M, Ouaisa M, Nadifi Z, El Himer S, Al Masmoudi Y, Kartit A. A framework for cyber threat modeling and risk assessment in smart city environments. *Front Comput Sci.* 2025;7:1647179. doi:10.3389/fcomp.2025.1647179.
18. Elshweikh AA, Maher AM, Hussein M, Elbayoumy AD. Intrusion detection system for IoT using machine learning. In: International Telecommunications Conference (ITC-Egypt); 2024. p.326-31. doi:10.1109/ITCEgypt61547.2024.10620546.
19. Saadouni R, Gherbi C, Aliouat Z, Harbi Y, Khacha A. Intrusion detection systems for IoT based on bio-inspired and machine learning techniques: a systematic review of the literature. *Cluster Comput.* 2024;27:8655-81. doi:10.1007/s10586-024-04388-5.
20. El-Hajj M. Enhancing communication networks in the new era with artificial intelligence: techniques, applications, and future directions. *Network.* 2025;5(1):1. doi:10.3390/network5010001.
21. Islam M, Dukyil AS, Alyahya S, Habib S. An IoT enable anomaly detection system for smart city surveillance. *Sensors.* 2023;23:2358. doi:10.3390/s23042358. PMID:36850955.
22. May TM, Zainudin Z, Muslim N, Jamil NS, Jan NAM, Ibrahim N, et al. Intrusion detection system (IDS) classifications using hyperparameter tuning for machine learning and deep learning. In: 5th International Conference on Artificial Intelligence and Data Sciences (AiDAS); 2024. p.344-9. doi:10.1109/AiDAS63860.2024.10730038.
23. Nazat S, Alayed W, Li L, Abdallah M. Ensemble learning framework for anomaly detection in autonomous driving systems. *Sensors.* 2025;25:5105. doi:10.3390/s25165105. PMID:40871968.
24. Khoei TT, Aissou G, Hu WC, Kaabouch N. Ensemble learning methods for anomaly intrusion detection system in smart grid. In: IEEE International Conference on Electro Information Technology (EIT); 2021. p.129-35. doi:10.1109/EIT51626.2021.9491891.
25. Gudala L, Shaik M, Venkataramanan S. Leveraging machine learning for enhanced threat detection and response in zero trust security frameworks: an exploration of real-time anomaly identification and adaptive mitigation strategies. *J Artif Intell Res.* 2021;1:19-45.
26. Järveläinen J, Dang D, Mekkanen M, Vartiainen T. Towards a framework for improving cyber security resilience of critical infrastructure against cyber threats: a dynamic capabilities approach. *J Decis Syst.* 2025;34:2479546. doi:10.1080/12460125.2025.2479546.
27. Aktas F, Shaye A, Ergen M, Saoud B, Yahya AE, Laura A. AI-enabled routing in next generation networks: a survey. *Alexandria Eng J.* 2025;120:449-74. doi:10.1016/j.aej.2025.01.095.
28. Lyu Q, Liu S, Shang Z. Securing urban landscape: cybersecurity mechanisms for resilient smart cities. *IEEE Access.* 2025;13:10966-77. doi:10.1109/ACCESS.2024.3522078.
29. RadhaKrishna K, Babu CR, Abraham D, Abhilash PK, Abbas HM, M N. Cyber resilience in smart cities using bi-LSTM-based intrusion detection system. In: International Conference on Computational Innovations and Engineering Sustainability (ICCIES); 2025. p.1-7. doi:10.1109/ICCIES63851.2025.11033050.
30. Rodríguez M, Alesanco Á, Mehavilla L, García J. Evaluation of machine learning techniques for traffic flow-based intrusion detection. *Sensors.* 2022;22:9326. doi:10.3390/s22239326. PMID:36502028.
31. Rosay A, Cheval E, Carlier F, Leroux P. Network intrusion detection: a comprehensive analysis of CIC-IDS2017. In: 8th International Conference on Information Systems Security and Privacy. SCITEPRESS-Science and Technology Publications; 2022. p.25-36. doi:10.5220/0010774000003120.
32. Cantone M, Marrocco C, Bria A. Machine learning in network intrusion detection: a cross-dataset generalization study. *IEEE Access.* 2024;12:144489-508. doi:10.1109/ACCESS.2024.3472907.
33. Thakkar A, Lohiya R. A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions. *Artif Intell Rev.* 2022;55:453-563. doi:10.1007/s10462-021-10037-9.

34. Kurniabudi K, Stiawan D, Darmawijoyo D, Bin Idris MY, Kerim B, Budiarto R. Important features of CICIDS-2017 dataset for anomaly detection in high dimension and imbalanced class dataset. *Indones J Electr Eng Inform.* 2021;9:498-511. doi:10.52549/ijeei.v9i2.3028.
35. Jose J, Jose DV. Deep learning algorithms for intrusion detection systems in Internet of Things using CIC-IDS 2017 dataset. *Int J Electr Comput Eng.* 2023;13:1134-41. doi:10.11591/ijece.v13i1.pp1134-1141.
36. Zhang Z, Hamadi HA, Damiani E, Yeun CY, Taher F. Explainable artificial intelligence applications in cyber security: state-of-the-art in research. *IEEE Access.* 2022;10:93104-39. doi:10.1109/ACCESS.2022.3204051.