



International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: <https://www.svedbergopen.com/>



Research Paper

Open Access

A Secure Edge-Cloud AI Framework Integrating Computer Vision, Signal Processing, and IoT Analytics for Intelligent Communication Systems

Muthukumaran P^{1*}, Vidhyashree S², Niladri Banerjee³, M. Dhanabal⁴, C J Harshitha⁵, Sitaram Satapathy⁶

^{1*}Assistant Professor, Electronics and Communications Engineering, RF Phase shifter, Sri Venkateswara College of Engineering, E-mail: muthu3nava@gmail.com

²Assistant Professor, Electronics and Communication Engineering, RF and Antenna Engineering, Veltech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College, E-mail: vidhyashree.s@velhightech.com
Orcid Id: 0000-0002-8357-0206

³Electronics And Communication Engineer, Techno Main Salt Lake, Pin code - 700116, India. E-mail: Niladribanerjee.in@gmail.com, Orcid: <https://orcid.org/0009-0004-0079-9251>

⁴Assistant Professor, Department of Mechanical Engineering, V.S.B. Engineering College, Karur- 639 111. E-mail: dhanabalm0101@gmail.com

⁵Assistant Professor, Computer Applications, Specialization in AI and Deep Learning Models, JSS Science and Technology, Mysuru, Karnataka, E-mail: harshi.cj@jssstuniv.in, Orcid Id: 0000-0002-7790-8805

⁶Assistant Professor, Department of Civil Engineering, Geotechnical Engineering, GIFT Autonomous, E-mail: sitaram.cet@gmail.com, Orcid: 0009-0000-8694-1861

ABSTRACT

The convergence of artificial intelligence, edge-cloud computing, and Internet of Things technologies provide new opportunities for developing responsive, secure, and resource-efficient intelligent communication systems. This study developed a secure edge-cloud AI framework integrating computer vision, signal processing, IoT analytics, adaptive workload allocation, and cybersecurity. The framework was evaluated using 1,200 multimodal observations across cloud-only, edge-only, and adaptive edge-cloud configurations. Statistical, correlation, security, and machine-learning analyses were performed to assess communication latency, throughput, energy consumption, quality of service (QoS), task success, and threat detection. Adaptive edge-cloud processing achieved the lowest mean latency (49.19 ms) and a 92.22% task-success rate while requiring substantially less energy than edge-only processing. Packet loss was negatively associated with QoS ($p = -0.503$), whereas signal quality showed a positive association ($p = 0.489$). The security mechanism achieved 93.42% detection accuracy and an F1-score of 86.77% across multiple cyberattack scenarios. Random Forest predicted QoS with an R^2 of 0.708, although task-success discrimination remained limited despite high classification accuracy. Overall, the findings demonstrate that security-aware adaptive edge-cloud intelligence can effectively balance latency, resource efficiency, communication quality, and cyber resilience, providing a scalable foundation for next-generation intelligent communication infrastructures and future AI-enabled network applications.

Keywords: Edge-cloud AI, intelligent communication systems, Internet of Things, signal processing, cybersecurity

Introduction

Distributed computing, Internet of Things (IoT), and Artificial Intelligence (AI) are changing the face of communication systems into intelligent infrastructures that can process heterogeneous information and make decisions in real time. They continuously produce visual, sensor, network and operational data that demand reliable processing to be able to assist automated services. Accuracy is crucial for the data generated from the IoT because inaccurate data could have a negative impact on downstream analytics and decision making (Liu et al., 2018). Predictive and prescriptive analytics also illustrate the shift from descriptive data analysis to predictive analysis and the identification of appropriate action steps based on these predictions (Rukh et al., 2023; Putri & Ainindhira, 2025). These capabilities offer a valuable basis for the intelligent communication environment, which demands quick and context-oriented reactions.

However, traditional cloud computing solutions offer significant computing power but are limited in that they are network dependent, can suffer delays as data is sent to and from distributed devices, and can require large bandwidth to transfer massive amounts of data from dispersed locations. To overcome these challenges, edge computing places computational resources closer to the data sources, thereby allowing for faster processing and reducing reliance on cloud-based resources with high latency (Khan et al., 2019). The new IoT-edge-cloud continuum also allows for the distribution of computational workloads between devices, edge and cloud resources as needed by applications and networks (Gkonis et al., 2023). Allocation of resources is still difficult due to the energy constraints, memory and computing power constraints of edge devices. Thus, it is crucial to have energy-aware hierarchical optimization across the device, edge, and cloud layers for efficient distributed computing (Cong et al., 2020). A hybrid fog-edge architecture has also been shown to enhance latency while ensuring resilience in real-time IoT applications (Islam et al., 2025).

Edge-cloud communication systems can be further enhanced by combining complementary information sources and thereby boosting multimodal intelligence. The computer vision can be used to extract contextual information from images and video, and the signal processing can be used to extract properties of communication conditions, such as signal strength, noise, packet loss, etc. The sensor, traffic, device and resource information, is now combined in IoT analytics to enable system-level decisions. The deep-learning architectures for heterogeneous IoT sensors show that there is potential to fuse information from various sensing modalities to enhance intelligent inference at resource-limited devices (Yao et al., 2019). When coupled with the ability to adapt edge-cloud workload allocation, these features could help make decisions about processing that adapt to computational need and communication conditions.

Security is also paramount as the attack surface in distributed edge-cloud environments stretches from the IoT devices, communications, edge nodes and cloud infrastructure. Edge-assisted IoT architectures (Alwarafy et al., 2020) therefore, require fundamental security properties such as authentication, privacy, access control, data integrity, and secure communication. Coordinated cybersecurity mechanisms and secure communications are also required to support the operation of resilient distributed infrastructures under cyber threats that are continuously changing (Ayele et al., 2024).

However, due to these improvements, there has been a lack of research that has integrated computer vision, signal processing, IoT analytics, adaptive edge-cloud allocation, and cybersecurity in a single intelligent communication framework. The objective of this research is thus to (1) design a secure edge-cloud AI architecture that combines computer vision, signal processing and IoT analytics; (2) study the benefit of adaptive workload sharing for latency, communication efficiency and resource utilization; and (3) assess the performance of predictive, QoS and security under heterogeneous network and cyberattack settings. Finally, the proposed approach is integrated, which can be used as a basis for developing responsive, efficient, and resilient intelligent communication systems.

2. Materials and Methods

2.1 Research Design and Edge-Cloud Architecture

A quantitative experimental framework was designed to assess the security of artificial intelligence-based communication between IoT, edge, and cloud. The system comprised edge, cloud and a layer of devices that facilitated distributed data processing and intelligent workload management. The three configurations: cloud-only, edge-only, and adaptive edge-cloud were tested in heterogeneous network conditions. The adaptive architecture chose to distribute computational loads based on quality of communication, computational requirements, and available resources. This design allowed for the assessment of intelligence, communication efficiency, resource utilization and security to be evaluated simultaneously.

2.2 Dataset and Data Preprocessing

The experimental data set included 1200 observations and 33 variables including computer vision, communication signals, IoT activity, computational resources, cybersecurity conditions, and system outcomes. The image characteristics, processing time, inference confidence, SNR, RSSI, packet loss, jitter, and signal quality were considered in the visual and signal variables, respectively. We defined attributes of sensors as IoT and attributes of networks as data rate, workload allocation, throughput, bandwidth, and resource utilization. Screening for missing values, inconsistent observation and extreme values were done on the data. Categorical attributes were coded and continuous variables were normalized, when necessary, for statistical and machine-learning analyses.

2.3 Computer Vision, Signal Processing, and IoT Analytics

The performance of computer vision was evaluated using visual workload, inference confidence and inference time, and the performance of communication was evaluated using the signal-quality index, SNR, RSSI, packet loss, and jitter. These features were combined with measure of sensor activities and IoT data rate to build a multimodal model of system conditions. The relationship between signal quality, visual inference and communication performance was then investigated. A key advantage of the integrated feature space was that it allowed the framework to consider heterogeneous information when deciding on workload and system-performance.

2.4 Adaptive Edge-Cloud and Security Framework

The evaluation of adaptive workload management was done with the edge-cloud offload ratio and in addition, CPU utilization, memory usage, bandwidth utilization, throughput, energy usage, latency, and QoS were measured. Security analysis was done with normal traffic, DDoS attack scenarios, spoofing attack scenarios, man in the middle attack scenarios, and various levels of severity of the malware attack scenarios. Security performance was quantified with attack-detection status, detection confidence and encryption overhead. The adaptive framework was evaluated against the cloud-based and edge-based configurations and compared to see if the intelligent allocation reduced the communication and computational costs while still being threat resilient.

2.5 Statistical and Machine-Learning Analysis

The variables were characterized using descriptive statistics, and relationships among the variables of communication, resources, security and performance indicators were determined using correlation analysis. ANOVA and appropriate post-hoc analysis were used to assess the differences between the three computational configurations; otherwise, non-parametric statistics were used. Predictions of latency, QoS, task success, and security outcomes were made using regression and classification models. The accuracy, precision, recall, F1 score, ROC-AUC were applied to assess the predictive performance, and relevant error metrics were applied. The contribution of the vision, signal, IoT, security and adaptive-allocation components was quantified using ablation analysis, which was considered statistically significant at $p < 0.05$.

3. Discussion

Results show the proposed secure edge-cloud AI framework achieved a balanced solution for communication efficiency, computational performance and intelligent system operation. The adaptive edge-cloud processing results in the minimum communication latency (49.19ms), while edge-only processing and cloud-only processing results in 51.27ms and 69.67ms, respectively. The computed placement of the modules had significant impacts on communication responsiveness, with 42.8% of the latency variation explained by the framework mode (Xu et al., 2019). Next-generation communication networks, where AI-driven resource allocation and self-managed networks are anticipated to meet progressively demanding latency and service levels requirements are expected to be of particular interest (Raihan, 2023). Adaptive allocation distributes processing resources based on the operational conditions, rather than putting all resources in the cloud.

In the architecture comparison, it was also evident that there was a clear trade-off between performance and efficiency. The highest value for throughput (32.68 Mbps) and QoS (89.10) were achieved by the edge-only processing, which used an energy of 10.22 J, while the adaptive edge-cloud processing used an energy of 6.99 J. Cloud-only operation used less energy, but had significantly higher latency, and lower QoS. The adaptive architecture was thus one that struck a balance between responsiveness, service quality, throughput and energy use, instead of optimizing any one of these four metrics (Zhao et al., 2024). The optimization of multi-objectives is significant for 6G networks using AI, as future intelligent networks will require dynamically optimising the allocation of computational and communication resources in face of heterogeneous operating conditions (Raihan, 2023).

Signals processing results also confirmed the significance of the quality of communication. The signal quality had a positive correlation with QoS ($\rho = 0.489$) while the packet loss had a negative correlation with QoS ($\rho = -0.503$). An increase in jitters was correlated with an increase in latency ($\rho = 0.405$) and an increase in signal quality was correlated with a decrease in latency ($\rho = -0.393$). The results suggest that the real-time communication conditions must be taken into consideration in the edge-cloud workload allocation. Interestingly, there were very few relationships between the signal indicators and the vision confidence as well as the inference time, indicating that vision confidence and inference time were relatively stable across different communication quality. This separation may be useful for an edge based visual application that needs to have local intelligence even during temporary outages of the network.

The security component also performed well with an accuracy of 93.42%, precision of 87.80%, recall of 85.76%, an F1 score of 86.77%. The detection rate was more than 82% with each attack type evaluated, and the highest attack-severity level (Sirapangi & Gopikrishnan, 2024) achieved a detection rate of 95.39%. The results, however, show a correlation between attack severity and latency ($\rho = 0.346$) and attack severity and reduced QoS ($\rho = -0.199$), indicating that cybersecurity threats can have a direct impact on the performance of communications. Thus, it is essential to consider security analytics in the context of intelligent resource management in AI-native future networks, where resilience is to go hand in hand with computational efficiency increases (Raihan, 2023).

The mixed but informative results of predictive modeling were found. Random Forest had the best task-success accuracy with 91.74%, but the ROC-AUC value of 0.590 meant that it had poor discrimination power because of the high degree of imbalance. Thus, a high classification accuracy must be evaluated in conjunction with the class distribution. The performance of the QOS prediction, however, was much better, as the Random Forest model accounted for 70.76% of the variance in the test set. The conditions of communication were the most observed tasksuccess discriminators, with packet loss and signal quality being the biggest observed factors.

The overall results demonstrate the viability of the integration of signal processing, IoT analytics, computer vision, cybersecurity and adaptive edge-cloud allocation in intelligent communication systems. The framework is especially relevant for emerging architectures for 6G, which are driven by AI (Raihan, 2023). However, physical edge devices, real communications traffic, multimodal sensor streams, and experimentally generated cyberattacks must be used for validation. In addition, future research could explore federated learning, privacy-aware AI, mobility considerations in resource management, and large-scale deployments of 6G networks.

4. Conclusion

The current work aims at the design and assessment of a secure edge-cloud AI framework combining computer

vision, signal processing, IoT analytics, adaptive workload allocation and cybersecurity, for intelligent communication systems. The results showed that adaptive edge-cloud processing offered a good balance between responsiveness to communication, resource efficiency, and service quality, with communication latency significantly reduced compared with cloud-only processing and energy consumption considerably less than with edge-only processing. System performance metrics were important factors, where packet loss had a negative impact on the QoS, and higher signal quality improved the QoS and reduced the communication latency. The performance of the computer-vision inference was robust in the face of changes in network environment, which suggests that multimodal intelligence is feasible in distributed environments. The security mechanism showed high overall accuracy of attacks detection, and it kept the attacks detection good in DDoS, MITM, malware and spoofing scenarios, while the attacks severity raised negatively affected the communication performance. In addition, it was demonstrated that predictive modeling of QoS was effective while the classification of task-success should be interpreted with caution, due to class imbalance and limited discriminative power. Overall, the results show the benefits of integrated, intelligent, secure edge-cloud based communication infrastructures for responsive and resilient communication infrastructure. Future validation efforts should also include physical edge devices, real multimodal IoT traffic, variable wireless environments and large-scale deployments to create generalizability and bring communication systems into the realm of practical use in the future.

References

1. Alwarafy, A., Al-Thelaya, K. A., Abdallah, M., Schneider, J., & Hamdi, M. (2020). A survey on security and privacy issues in edge-computing-assisted internet of things. *IEEE Internet of Things Journal*, 8(6), 4004-4022.
2. Ayele, E. D., Gonzalez, J. F., & Teeuw, W. B. (2024). Enhancing cybersecurity in distributed microgrids: A review of communication protocols and standards. *Sensors*, 24(3), 854.
3. Cong, P., Zhou, J., Li, L., Cao, K., Wei, T., & Li, K. (2020). A survey of hierarchical energy optimization for mobile edge computing: A perspective from end devices to the cloud. *ACM Computing Surveys (CSUR)*, 53(2), 1-44.
4. Gkonis, P., Giannopoulos, A., Trakadas, P., Masip-Bruin, X., & D'Andria, F. (2023). A survey on IoT-edge-cloud continuum systems: Status, challenges, use cases, and open issues. *Future Internet*, 15(12), 383.
5. He, J. (2025). Low-latency Adaptive Communication Protocols for Ultra-dense Network Environments. *Journal of ICT Standardization*, 13(2), 157-180.
6. Hohenstein, J., Kizilcec, R. F., DiFranzo, D., Aghajari, Z., Mieczkowski, H., Levy, K., ... & Jung, M. F. (2023). Artificial intelligence in communication impacts language and social relationships. *Scientific reports*, 13(1), 5487.
7. Islam, U., Alatawi, M. N., Alqazzaz, A., Alamro, S., Shah, B., & Moreira, F. (2025). A hybrid fog-edge computing architecture for real-time health monitoring in IoMT systems with optimized latency and threat resilience. *scientific reports*, 15(1), 25655.
8. Kerr, A., Barry, M., & Kelleher, J. D. (2020). Expectations of artificial intelligence and the performativity of ethics: Implications for communication governance. *Big Data & Society*, 7(1), 2053951720915939.
9. Khan, W. Z., Ahmed, E., Hakak, S., Yaqoob, I., & Ahmed, A. (2019). Edge computing: A survey. *Future Generation Computer Systems*, 97, 219-235.
10. Liu, X., Tamminen, S., Su, X., Siirtola, P., Rönning, J., Riekkki, J., ... & Soininen, J. P. (2018, March). Enhancing veracity of IoT generated big data in decision making. In *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)* (pp. 149-154). IEEE.
11. Lovins, A. B. (2018). How big is the energy efficiency resource?. *Environmental Research Letters*, 13(9), 090401.
12. Putri, N., & Ainindhira, A. (2025). Beyond Descriptive Analytics: Predictive Models For Strategic Marketing Decisions. *Journal of Management and Informatics*, 4(2), 872-889.
13. Raihan, A. (2023). An overview of the implications of artificial intelligence (AI) in sixth generation (6G) communication network. *Research Briefs on Information and Communication Technology Evolution*, 9, 120-146.
14. Rukh, S., Oziri, S. T., & Seyi-Lande, O. B. (2023). Framework for enhancing marketing strategy through predictive and prescriptive analytics. *Shodhshauryam, International Scientific Refereed Research Journal*, 6(4), 531-569.
15. Sirapangi, M. D., & Gopikrishnan, S. (2024). Predictive health behavior modeling using multimodal feature correlations via Medical Internet-of-Things devices. *Heliyon*, 10(15).
16. Xu, Y., Chen, H., Zhang, W., & Hwang, J. N. (2019). Smart media transport: A burgeoning intelligent system for next generation multimedia convergence service over heterogeneous networks in China. *IEEE MultiMedia*, 26(3), 79-91.
17. Yao, S., Zhao, Y., Shao, H., Liu, D., Liu, S., Hao, Y., ... & Abdelzaher, T. F. (2019, April). Sadeepsense: Self-attention deep learning framework for heterogeneous on-device sensors in internet of things applications. In *IEEE INFOCOM 2019-IEEE Conference on computer communications* (pp. 1243-1251).

IEEE.

18. Zhao, L., Li, B., & Yuan, H. (2024). Cloud edge integrated security architecture of new cloud manufacturing system. *Journal of Systems Engineering and Electronics*, 35(5), 1177-1189.