International Journal of Research in Artificial Intelligence and Data Science (IJRAIDS)
ISSN: 3139-7174/ Volume 1 Issue 2 April – June 2026
Paper Id: IJRAIDS -V1I2P102/ Page No: 07-18

International Journal of Research in Artificial Intelligence and Data Science

Original Article

Fusion of Edge AI and Federated Learning in Smart Cities

Mrs.D. Jayasree[1], D. Deepika[2], N. Prabha devi[3]

[1]*Assistant Professor, Mangayarkarasi college of Mangayarkarasi College Engineering, Paravai, Madurai, Tamil Nadu India.*

[2,3]*Students Mangayarkarasi college of Mangayarkarasi College Engineering, Paravai, Madurai, Tamil Nadu, India*

Received Date: 18 March 2026 | Revised Date: 02 April 2026 | Accepted Date: 14 April 2026

Abstract

The emergence of smart cities has necessitated the development of data processing systems that are real-time, decentralized, and privacy-conscious. This paper analyzes the integration of Edge Artificial Intelligence (Edge AI) with Federated Learning (FL) as an innovative approach to enhance data management, security, and decision-making in intelligent urban environments. Edge AI enables localized data analysis with reduced latency, whilst Federated Learning safeguards data privacy by facilitating model training without necessitating centralized data storage. This combination fixes big difficulties with scalability, latency, and privacy. But there are a lot of challenges that make it challenging to employ this integration in real life. For example, devices aren't all the same, data isn't all the same, communication is slow, and coordinating in real time is hard. Also, limitations including limited edge resources, privacy-utility trade-offs, and concerns about how well models can be comprehended might make smart city services less effective and less obvious. The paper examines the design, applications, advantages, challenges, and prospective developments of this integration within the context of smart cities. The growth of smart cities has made it very important to have data processing systems that are real-time, decentralized, and keep people's privacy safe. As cities depend more on smart devices and networked sensors, Edge Artificial Intelligence (Edge AI) and Federated Learning (FL) together offer a new way to undertake safe, scalable, and efficient urban data analytics. Edge AI lets you process data quickly and close to where it came from. This speeds up decision-making and cuts down on the requirement for cloud infrastructure. Federated Learning, on the other hand, lets several devices or organizations train a model simultaneously without having to share raw data. This maintains people's privacy and meets the standards for protecting data.

Keywords

Edge AI, federated learning, smart cities, privacy protection, decentralized intelligence, real-time processing, and city infrastructure.

Introduction

One of the most major technological changes of the 21st century is the switch from conventional cities to smart cities. Smart cities use the latest technology, such as sensors, data analytics, cloud computing, and artificial intelligence (AI), to make city services work better, improve infrastructure, and make life better for people who live there. This transformation is happening because cities are growing quickly and their operations are becoming more complicated. These developments need clever, scalable systems that can make judgments on the spot. Smart cities are based on the idea of the Internet of Things (IoT). It helps devices talk to one other and collect, share, and analyze data in sectors including traffic control, environmental monitoring, public safety, energy management, and healthcare. But delivering data to centralized cloud servers for processing hasn't worked well for city services that need to change quickly and are sensitive to delay. People are often worried about the safety and privacy of their data when they process it on the cloud, which usually causes delays and utilizes too much bandwidth. Edge Artificial Intelligence (Edge AI) is a new type of computing that has been created to solve these challenges. Edge AI is putting AI algorithms right on edge devices so that choices can be made faster by processing data close to where it comes from. This makes the system work better, less reliant on central servers, and less prone to experience delays. Edge devices, on the other hand, often don't have a lot of processing power or storage capacity, which can make AI models that are already in use less complicated and less powerful. Federated Learning (FL) was created because more and more people want to keep their information safe. Federated Learning (FL) is a means to train machine learning models on many different devices or servers while keeping the raw data in one location. You can only send model updates between devices and the central server, not data. This design makes better use of bandwidth and

This is an open access article under the CCBY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/2.0/)

decreases the risk to privacy. Combining Edge AI and Federated Learning is a good technique to deal with the reality that smart city surroundings have a lot of various sorts of data and are spread out. Edge AI lets you make inferences in real time and close to where you are, and FL makes sure that several nodes may learn together without putting critical data at risk. They work together to tackle some of the major flaws with traditional smart city systems, like how well they can develop, how long it takes to respond, and how safe the data is. This research investigates the synergistic integration of Edge AI with Federated Learning within the context of smart cities. It examines the technological underpinnings, proposes a stratified architectural framework, evaluates applications in specific domains, and enumerates the advantages and technical challenges associated with them. As cities become more connected and full of data, combining these two ideas is a long-term strategy to make cities that are smart, robust, and respect people's privacy. One of the most crucial technological changes of the 21st century is the shift from conventional cities to smart cities. Smart cities use the latest technology, such as sensors, data analytics, cloud computing, and artificial intelligence (AI), to improve the lives of their residents, their infrastructure, and the services they provide. This trend is happening because more people are moving to cities and cities are becoming more complicated to run. Cities require systems that are smart, can grow, and can make decisions in real time.

Smart cities are based on the idea of the Internet of Things (IoT). It lets devices talk to each other and share information in areas including traffic control, environmental monitoring, public safety, energy management, and healthcare. But the typical design that sends data to centralized cloud servers for processing doesn't work for urban services since they need to be able to change quickly and are sensitive to latency. Processing in the cloud usually takes longer, utilizes too much bandwidth, and makes customers worry about the safety and privacy of their data.

Edge Artificial Intelligence (Edge AI) is a novel technique to compute that can help with these issues. Edge AI puts AI algorithms directly on edge devices, which lets choices be made faster by analyzing data closer to where it originates from. This means that the system doesn't need as many centralized servers, has less latency, and is more responsive. But edge devices usually don't have a lot of processing power or storage capacity, which can make AI models that are already in use less powerful and less complicated.

Federated Learning (FL) was also created since it is becoming more and more important to secure people's privacy. Federated Learning (FL) is a means for several devices or servers to work together to train machine learning models while keeping the raw data in one place. The central server and devices only provide model updates, not data. This design not only protects privacy better, but it also makes the most of bandwidth.

Combining Edge AI and Federated Learning creates a useful way to deal with the different and spread-out nature of smart city environments. Edge AI lets you make conclusions in real time and in a certain area. FL lets numerous nodes learn together without putting important data at risk. They work together to solve some of the major difficulties with traditional smart city technologies, such as how well they perform, how long it takes for data to get to where it needs to go, and how safe it is.

This paper looks at how Edge AI and Federated Learning can work together to make smart cities better. It talks about the technological foundations, recommends a layered architectural model, looks at how it can be used in several sectors, and talks about the pros and cons of these uses. As cities become more connected and full of data, combining these two ideas is a long-term method to construct smart cities that are smart, respect people's privacy, and are robust.

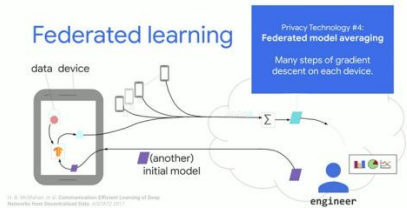

Figure 1. Edge Ai & Fl Overview

Background and Literature Review

You need to know a lot about the core technologies and recent research in this area to be able to mix Edge AI with Federated Learning (FL) in smart cities. Smart cities use smart systems and real-time data to make city services work better and make life better for people who live there. The Internet of Things (IoT), cloud computing, AI, and distributed computing models are all emerging technologies that are making this transition happen. As these cities transform, millions of sensors and gadgets are making more and more data at a faster and more varied rate. This highlights how limited centralized processing is and how crucial it is to create smart, decentralized systems.

Edge AI is when machine learning algorithms are used directly on devices at the edge of the network, which is close to where the data is stored. By not having to transfer data to centralized servers for processing, this technique cuts down on latency, boosts privacy, and makes systems more reliable. Small devices can now execute real-time inferencing thanks to the development of fast hardware accelerators like GPUs and AI-specific chips like Google's Edge TPU. This is especially helpful for apps that need to respond quickly, such those that manage traffic or keep people safe. Lightweight neural networks like MobileNet, TinyML, and quantized models have made it even easier to employ AI at the edge.

Google announced Federated Learning (FL) in 2016. It changes the way machine learning models are taught in a big way. FL is different from regular centralized learning since it lets several decentralized edge nodes work together to train a single model, each with its own local data. The best thing about FL is that it keeps data private by making sure that raw data never leaves the device it is on.

This is very crucial in smart cities, where things like health records, location data, and surveillance footage need to be kept safe. There are several varieties of FL, such as horizontal federated learning, vertical federated learning, and federated transfer learning. These types of FL can be used for different ways of splitting data between nodes.

Previous research has shown that Edge AI and FL can significantly improve areas including healthcare, finance, and autonomous systems. FL has been used in healthcare to train diagnostic models using data from several facilities while protecting patient privacy. In finance, FL has been used to make fraud detection systems that don't violate the privacy of each organization. Edge AI has also been utilized in smart grid systems to plan maintenance ahead of time and in self-driving cars to find things in real time. Even though these advances have been made, the combination of Edge AI with FL for comprehensive smart city applications is still in its early phases. This means that there is still a lot of potential for new ideas.

Edge AI and FL work well together because they both have strengths that make them work well together. Edge AI lets people make choices on their own, whereas FL enables people learn together without placing all the information in one place. They can work together to fix problems with latency, privacy, and scalability in smart cities. As research in this area progresses, it is imperative to examine novel architectures, communication protocols, and security measures that will enhance the usability and safety of these technologies. This part sets the stage for the architectural models and applications that will be spoken about in the later parts of this study.

A. Edge Artificial Intelligence

Edge Artificial Intelligence Edge AI is the use of AI algorithms on edge devices, which are things like sensors, cell phones, and embedded systems. Because it is so close to data sources, it is easy to make judgments rapidly and requires less bandwidth. Recent advances in lightweight neural networks and hardware accelerators have made it possible to use Edge AI.

B. Federated Learning

Federated Learning Federated Learning is a decentralized form of machine learning that trains models on numerous devices without transferring data from one device to a central server. Google suggested FL in 2016. It secures data privacy and minimizes the cost of sending data. There are other kinds of FL, like horizontal FL, vertical FL, and federated transfer learning.

C. Related Work

Related Work Many studies have looked into FL in healthcare and banking, as well as Edge AI in self-driving cars and smart grids. Nonetheless, their convergence within the context of smart cities remains little analyzed. The goal of this study is to combine both technologies into one system.

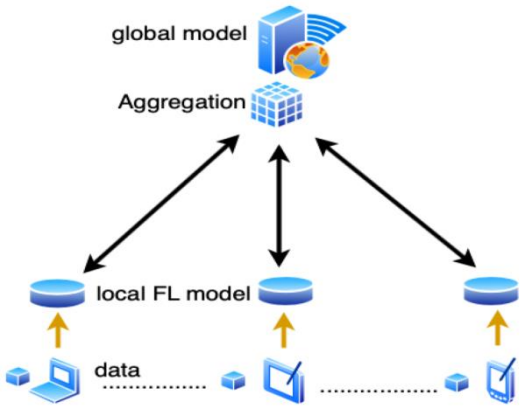

Figure 2. Background & Literature Review

Architectural Framework

Smart cities use a multi-layered design to combine Edge AI and Federated Learning (FL) in a way that keeps privacy, efficiency, and scalability while yet allowing for decentralized intelligence. This design works because it can process and learn from data at or near the source. This means it doesn't rely as much on centralized infrastructures. Some of the primary layers that make up this architecture include the perception layer, the edge intelligence layer, the federated learning layer, and the application layer. To make sure that data is safely and rapidly collected, analyzed, and acted on, each layer has a separate function to do.

A. Layered Architecture

a) Perception Layer

The perception layer is responsible for collecting and sensing real-time data from IoT devices such as cameras, environmental sensors, and wearable health monitors. This layer initiates the flow of data and provides the foundation for services that know what's going on around them.

b) Edge Intelligence Layer

This layer is made up of edge devices, such gateways and microcontrollers, that have modest AI models embedded into them. They accomplish things like processing, analyzing, and making conclusions straight away, which enables them respond rapidly and takes some of the work off the central systems.

c) Federated Learning Layer

The application layer is the top layer that runs smart city apps including intelligent transport systems, energy management, public safety analytics, and tailored healthcare. It gets data from the edge and federated layers.

d) Application Layer

The topmost layer that utilizes the outputs from the edge and federated layers to power smart city applications such as intelligent transport systems, energy management, public safety analytics, and personalized healthcare.

B. Communication Protocols

Communication Protocols For federated learning processes to operate together to update global models, communication needs to be fast and reliable. Here are some common ways to talk to one other:

- MQTT and CoAP for lightweight messaging between constrained devices.
- 5G and LPWAN for long-distance and high-bandwidth communication needs.
- Edge-to-cloud orchestration protocols manage tasks between servers in the center and edge nodes.

C. Security Mechanisms

In a distributed architecture, it is highly crucial to maintain data private and the model's integrity. Some sophisticated security measures are:

D. Differential Privacy

makes local model changes less clear by adding noise to them. This makes it harder to figure out what sensitive information is.

- Secure Multi-party Computation:(SMPC) and Homomorphic Encryption make it possible to safely gather model updates without needing to decrypt sensitive parameters.
- Blockchain Integration: Integrating blockchain to make sure that audit trails for changes to models and interactions with devices are obvious and can't be modified.

This architectural framework gives smart cities a safe and versatile platform for developing smart services. It combines the finest features of Edge AI and FL to build intelligence that is local, respects your privacy, and grows with the requirements of cities.

E. Layered Architecture

- The proposed architecture includes:
- Perception Layer: Edge sensors and IoT devices that collect data in real time.
- Edge Intelligence Layer: Edge nodes employ modest AI models to make choices based on data from their own locations.
- Federated Learning Layer: Getting models from edge nodes and keeping them up to date while protecting privacy.
- Application Layer: Smart city services that employ the outputs, including keeping an eye on pollution and traffic.

Applications in Smart Cities

Edge AI and Federated Learning (FL) work together to make a lot of smart city apps possible by giving them intelligence with minimal latency and keeping data private. These are the primary places where this combo is really helpful:

A. Smart Traffic and Transportation Management

- Real-time Traffic Flow Optimization: Real-time Traffic Flow Optimization: Edge AI lets you look at video of intersections in real time so that you can modify the timing of traffic lights. FL enables you train on traffic data from different intersections without having to put all the video feeds in one place.
- Autonomous Vehicle Coordination: Edge AI takes data from sensors on an autonomous vehicle, and FL helps all the vehicles in a fleet learn from each other to improve route planning and threat detection.
- Public Transit Scheduling: Edge nodes on buses and trains look at how many people are riding, and FL uses models from all throughout the transport network to adjust schedules on the fly.

B. Intelligent Energy Management

- Smart Grids: Edge AI incorporated into smart meters tells you how much energy your home consumes, and FL makes forecasts about how much energy the whole city will need without sharing your personal usage data.
- Demand Response Systems: Utility firms may be able to manage load well by keeping an eye on and projecting power demand in real time.
- Renewable Integration: FL-trained predictive models can indicate when solar and wind energy will be available, and Edge AI helps you store and balance energy on-site.

C. Smart Waste Management

- Dynamic Waste Collection: Edge cameras on bins check how full they are, and FL trains models in different communities to determine the optimum ways to pick up rubbish.
- Recycling Analysis: Edge AI sorts and classifies recyclables in real time, and FL makes the process more accurate without submitting images to a central server.

D. Public Safety and Surveillance

- Finding Anomalies: Edge cameras can see unusual things happening in real time. Federated Learning teaches models that can recognize behavior in different areas without showing private video.
- Edge sensors can immediately discover gas leaks, fires, or floods, and FL helps emergency departments work together to develop risk models. This is useful in case of a disaster.
- Crime Pattern Analysis: FL helps police stations safely share data trends so they can find patterns that cross regions without infringing the law.

E. Smart Healthcare Services

- Edge AI-powered wearables keep track of vital signs locally so that patients can be monitored from afar. FL trains health risk prediction models in many hospitals or homes while safeguarding private medical information.
- Epidemiological Surveillance: FL enables numerous local clinics learn about how outbreaks spread during a pandemic without giving away any patient information.

F. Environmental Monitoring

- Air Quality Management: Distributed air sensors check for pollutants in the vicinity. FL makes pollution predictions better without giving up raw geographic data.
- Tracking Noise Pollution: Edge microphones detect decibel levels, and models taught through FL help municipal planners discover and modify places that are too loud.

G. Smart Water Management

- Edge-based acoustic sensors can discover leaks in real time, and FL enables you see how people use things in different areas without giving up information about specific homes.
- Forecasting Consumption: FL uses data on how much water people in the area are using to help them prepare for future water needs, which helps them plan resources better.

H. Urban Mobility-as-a-Service (MaaS)

- Shared Micro-Mobility Optimization: Edge AI keeps track of how often bikes and scooters are used and predicts when they will need maintenance. This is called shared micro-mobility optimization. FL, on the other hand, studies at how people utilize cars in different cities to discover the optimum areas to install and use them.
- Ride-sharing Platforms: Using FL-trained predictive matching models improves the accuracy of connecting riders and drivers and cuts down on wait times, all without putting trip information in one place.

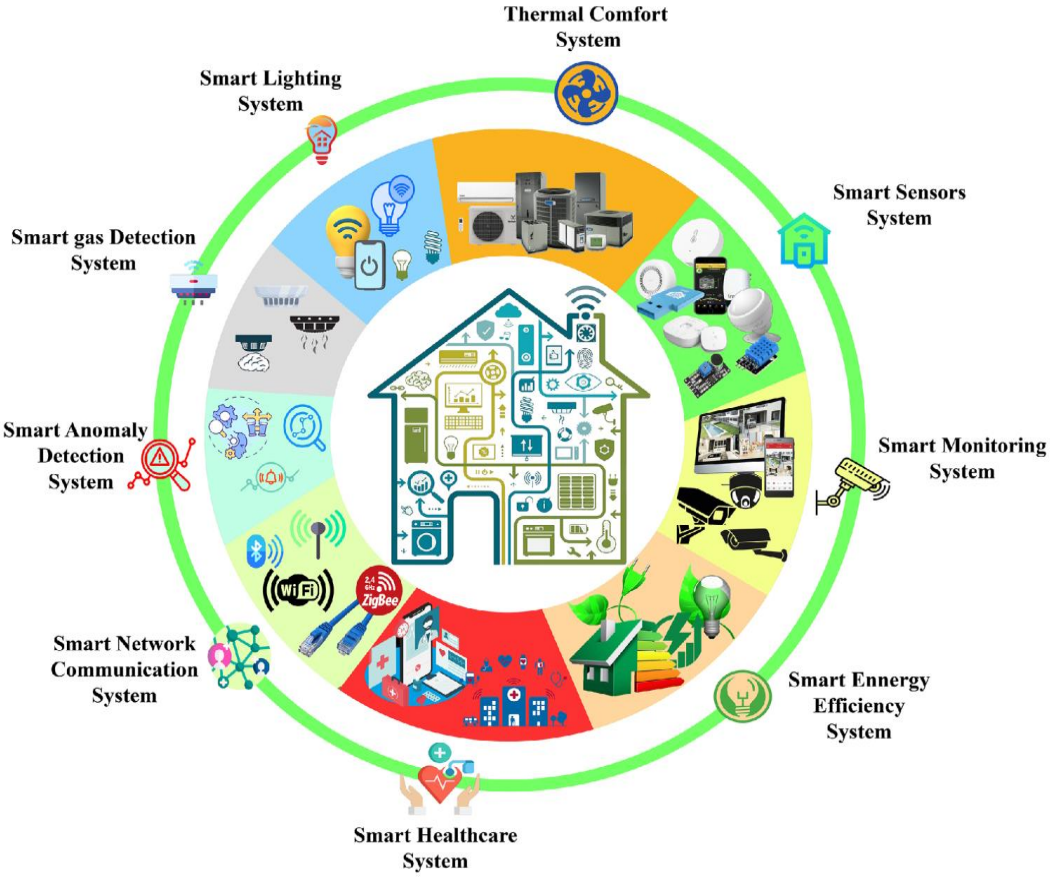

Figure 3. Applications In Smart Building Ecosystems

Privacy-Preserving Smart City Services using Federated Learning and Edge Computing

As smart cities use more and more data, keeping people's privacy safe while giving them smart services is now a primary priority. Cities collect a lot of private information every day, such as location and movement patterns, health care indications, energy use, and video from surveillance cameras. This is because there are so many AI-enabled sensors, connected gadgets, and city infrastructure. These databases are vital for making cities work better and delivering people better services. However, putting them all in one place raises a lot of worries, such illegal access, data breaches, and the inappropriate use of personal information. Using Federated Learning (FL) and Edge Computing together is a revolutionary technique to offer smart city services that keep people's privacy safe. This architecture concept ensures both operational efficiency and data safety by bringing computation closer to the data source and letting model training happen across many computers without having to store raw data in one place. Instead of on the cloud, edge computing analyzes data on smart devices or gateways, such traffic cameras, wearables, and environmental sensors. This makes cloud-based processes take less time and use less bandwidth.

These edge devices work with FL to train models by delivering only encrypted or camouflaged model updates instead of personal or raw data. This makes sure that personal data stays on the device, which is in line with guidelines and standards like GDPR, HIPAA, and national privacy laws that say you should only keep the data you need. In a smart healthcare system, for instance, hospitals and clinics can work together to develop a model that guesses what diseases people might have without ever exposing their personal information. Similarly, public transportation can use mobility patterns from different locations to discover the optimal routes and cut down on traffic without having to keep track of where each user has been.

One of the most fascinating uses of this technology is for real-time surveillance and public safety. In this case, video feeds from edge devices are looked at right away to discover suspicious behavior, accidents, or crowd formation. Edge AI doesn't transfer unprocessed video to a central control center. Instead, it looks at the video on-site and only shares alerts or anonymized metadata that are important. FL takes this to the next level by using thousands of cameras to constantly improve the detection models through distributed learning, all while keeping people's privacy safe in public settings. Managing energy is another key thing to think about. Smart meters in homes and businesses keep track of how much electricity is used in great detail. In the past, giving utility companies this information caused privacy concerns since it might be used to figure out how people live and act. You can train personalized energy usage models right on the meters with FL and Edge AI. This helps balance the loads on the grid, guess when demand will be highest, and recommend strategies to save energy, all without disclosing how each family consumes energy. Federated architectures can be used by citizen feedback platforms, digital complaint systems, and e-governance apps to learn from what people say while keeping their identities hidden and making sure they don't get profiled.

It's not straightforward to add privacy-preserving features to smart cities, though. To protect your model updates against reverse engineering or inference assaults, you need to deploy Privacy-Enhancing Technologies (PETs) including differential privacy, secure multiparty computation (SMPC), and homomorphic encryption. These strategies employ arithmetic to keep persons from being re-identified by model gradients or update patterns. Also, trust management between federated nodes, especially in urban networks with multiple agencies, demands strong mechanisms for authentication, audits, and incentives. You may make these stronger by employing federated frameworks based on blockchain. Also, the fact that devices have different capabilities, data is spread out in different ways, and connectivity conditions are different makes things more complicated from a technical point of view. This is why it's necessary to make lightweight, fault-tolerant algorithms that perform in a wide range of edge cases. To solve these difficulties, cities need to spend money on standardization, open protocols, and working together across industries. They also need to talk to people about AI use and data stewardship in a way that makes people trust them. In conclusion, federated learning and edge computing are a powerful, safe, and privacy-respecting platform for the next generation of smart city services. Cities should foster ethical AI innovation that puts people first by integrating intelligence to local infrastructure and making sure that personal data never leaves where it came from.

A. Benefits of Integration

Edge Artificial Intelligence (Edge AI) and Federated Learning (FL) together could change the game for smart cities since they give you a strong blend of real-time intelligence, data privacy, and scalable learning. One of the best things about this is that it helps you make decisions with very little delay right at the source of the data. This means that things like traffic lights, security cameras, and environmental sensors in cities can respond right away when things change. This intimacy not only makes things operate better, but it also means that less cloud infrastructure is needed, which cuts down on network congestion and energy use. The architecture maintains strict privacy standards and global legislation like the GDPR by storing sensitive data, such as personal health records, location information, or video feeds, on local devices. FL helps you train models on different devices at the same time without sending raw data. This lowers security risks and retains data sovereignty. The integrated design makes it easy to add new devices and districts without putting too much stress on the central servers. You can also modify services by utilizing models that are specific to the area, such as traffic patterns in a certain neighborhood or energy use habits in a single family. This way, you still get the benefits of global learning. This decentralized form also makes the system stronger, so that services keep running even when there are difficulties with devices or connections. The framework helps save money and energy by cutting down on the number of data centers needed and enabling edge devices run on batteries. It can work with many different suppliers and devices because it is modular and supports open standards. This stops cities from being stuck with one vendor and gives them long-term freedom. The design also makes the system safer by limiting access to data and offering tamper-proof ways to combine models, such blockchain-based audits. You can use ethical AI strategies to keep an eye on bias and make improvements to make things fairer in certain instances with the framework. This ensures ensuring that AI is used in a fair and responsible way. Edge AI and Federated Learning work together to give cities the tools they need to

build smart, flexible, and long-lasting ecosystems that place both public trust and operational performance first. This opens the door to a new era of safe, responsive, and personalized urban innovation.

Limitation

- Constrained Model Complexity: Because the technology at the edge is constrained, only lightweight models can be used. This makes it harder for advanced AI applications to work.
- Edge nodes may not always be active or may drop out due to power loss, network failure, or local processing priorities. This makes it less likely that training will work.
- High Energy Use: Constant training and communication drain the batteries of mobile or low-power devices, making them less usable over time.
- cy-Utility Trade-off: When you use things like differential privacy and encryption, models become less accurate, which makes smart city services less useful.
- Difficulty in Model ValidationIt is challenging to assess how well a model works over the complete network when you can't get to the raw data in one spot.
- People usually think of federated models as black boxes, which makes it hard to make key decisions in the public sector that need to be obvious.
- Not enough help for updating edge devices Managing firmware and model updates in real time across a large fleet of edge devices is hard to do both logistically and technically.
- Vulnerability to Concept Drift: Trained models can quickly become ineffective in cities where things change quickly, such traffic or pollution patterns that alter with the seasons.
- Limited Dataset Diversity on Individual NodesEdge devices may only capture a small part of the complete data spectrum, which makes local training less effective.
- Absence of Economic Models: There are no clear incentive structures in place to get third-party data providers to maintain contributing data.
- Legal and Ethical Ambiguities: In many locations, there are still problems regarding who owns data, who is responsible for it, and who is liable in federated environments.
- Integration Complexity with Legacy Systems: Many existing urban infrastructures lack compatibility and flexibility to support federated and edge-based AI systems.

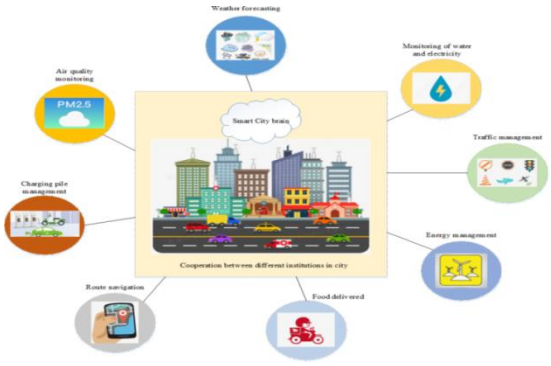

Figure 4. Limitations in smart-city edge ai & federated learning

Blockchain-Integrated Federated Learning For Secure Smart City Data Collaboration

A. Decentralized Trust Framework

- Blockchain is a decentralized, trustless ledger that allows smart city stakeholders to collaborate securely in an immutable manner.
- Federated learning model aggregation does away with the need for a single trusted authority.

B. Immutable Model Update Logs

- Changes to a model in the FL process are kept on the blockchain in a form that can't be modified, which makes it easy to completely trace and audit.
- In a federated setup, it helps detect updates that are dangerous or poisoned.

C. Smart Contracts for Automation

- Smart contracts can let devices or organizations automatically collect, check, and share incentives.

- Helpful for interacting with more than one organization (such healthcare providers, utilities, and traffic authorities) without having to do anything by hand.

D. Enhanced Data Integrity and Accountability

- Cryptographic verification of participants and their changes makes sure that model contributions are honest.
- Participants are accountable for their actions, which promotes honesty.

E. Incentivization for Collaboration

- You can utilize blockchain to construct token-based or reputation-based incentive schemes that get edge devices or institutions to exchange data and models.
- Encourages more people to get involved, especially private groups and regular people.

F. Cross-Organizational Collaboration

- Lets different groups, like hospitals, universities, and city departments, operate together safely without giving out private information.
- Promotes a unified strategy for addressing urban challenges while maintaining data borders between jurisdictions.

G. Secure Aggregation with Confidentiality

- You can use Zero-Knowledge Proofs (ZKPs) or Secure Multiparty Computation (SMPC) to encrypt and check model updates on-chain.
- Keeps data private while making sure the model converges in a way that is dependable.

H. Federated Learning Version Control

- You can keep track of different versions of models and training iterations with blockchain.
- If you detect any difficulties or poisoning attacks, it helps you go back to prior versions.

I. Resilience to Byzantine Participants

- Blockchain consensus methods can assist get rid of or punish problematic (Byzantine) nodes that communicate model changes that hurt the system.
- Strengthens and makes the results of federated learning more dependable.

J. Interoperability Across Smart City Domains

- Blockchain can act as a unified layer that makes it easier for different businesses to work together, such as transportation, energy, public safety, and healthcare.
- It makes it easier to train models and communicate information between fields.

Future Directions

- Advanced Federated Optimization Techniques: The development of adaptable and efficient FL algorithms (including FedOpt, FedBN, and FedDyn) to address the variability in devices and data within extensive metropolitan implementations.
- Cross-Silo and Cross-Device Federated Learning: Investigating hybrid FL systems that integrate cross-device (smartphones, sensors) and cross-silo (institutions, utility firms) training to enhance collaboration in smart cities.
- Design of hierarchical systems that let model orchestration and dynamic offloading happen across edge, fog, and cloud layers.
- Federated Reinforcement Learning: This is the use of reinforcement learning in FL at the edge so that it can always adjust to changes in urban environments (such managing traffic or using energy).
- Autonomous FL Scheduling and Task AllocationIntelligent orchestration of model updates, training cycles, and resource distribution based on energy availability, device health, and network conditions.
- Blockchain-Enabled Federated Learning: Using blockchain or distributed ledger technology to create clear, safe ways for participating edge nodes to work together and get rewards.
- Privacy-Enhancing Technologies (PETs) More use of homomorphic encryption, secure multiparty computation (SMPC), and differential privacy in Edge-FL to make privacy less of a problem.
- htweight and Energy-Aware AI ModelsDevelopment of TinyML or compressed models specifically intended for ultra-low-power edge devices.
- Regulatory Frameworks and Ethical Guidelines: Setting up national and international rules that make it possible to use federated edge AI in smart city infrastructures in a way that is ethical, fair, and respects privacy.

- Personalization and Transferability of Models: Examining the modification of global models for local contexts while preventing overfitting and bias, especially in heterogeneous urban populations.
- Federated models that are easy to explain and understand: Making FL models transparent and easy to understand will assist develop trust, governance, and public responsibility in crucial urban applications.
- Digital Twin Integration: Using FL-powered edge intelligence to feed data into city-wide digital twins for simulation, forecasting, and real-time administration of cities.
- Standardization and Open Architecture DevelopmentContributing to open standards (like IEEE and ETSI) that make it easier for different vendors and industries to work together, share data, and use tools.
- Resilient and Self-Healing SystemsDesigning federated edge networks that can fix themselves when there are problems, attacks, or hardware failures without needing help from a central authority.
- Education and Workforce Development: Programs to teach municipal workers, developers, and politicians about Edge AI and FL technologies so that they can be used in the future.

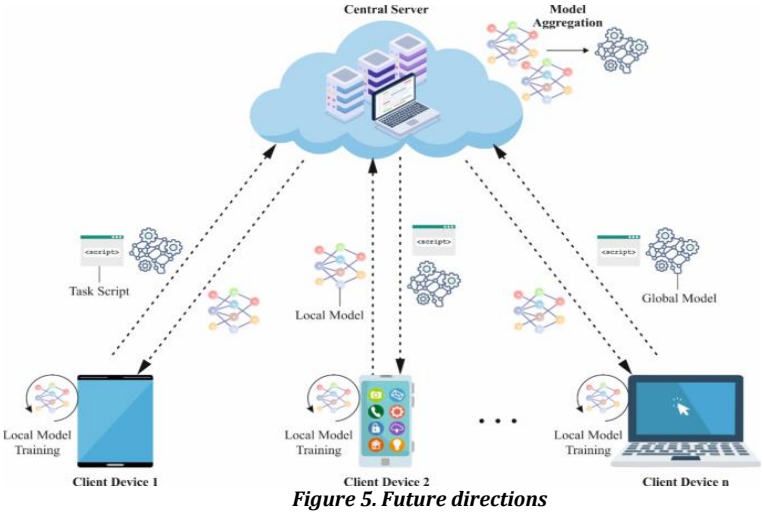

Figure 5. Future directions

Conclusion

Smart cities that use both Edge Artificial Intelligence (Edge AI) and Federated Learning (FL) are making a big stride toward building smart, privacy-protecting, and responsive urban infrastructures. As cities around the world keep growing and going digital, the challenges with traditional cloud-based models, such too much latency, not enough bandwidth, and privacy concerns, have become clearer. Edge AI solves these problems by letting equipment like sensors, surveillance systems, and connected cars work in real time in metropolitan areas. This feature makes it easier to make quick judgments, puts less stress on the network, and provides local systems greater freedom. But Edge AI's potential is restricted by problems like not having enough processing power, data being spread out, and devices not learning together. Federated Learning works well with Edge AI because it lets different nodes work together to build a model without having to send raw data to a central server. This technique protects data privacy and follows the rules, but it also makes AI models stronger and more accurate by using collective intelligence. When you combine Edge AI with FL, you get a synergistic approach that uses the best features of both systems and fixes their shortcomings. They work together to build smart city apps that can grow, change, and be safe. You may use these apps for a lot of things, like keeping an eye on the environment, managing energy, controlling traffic, and keeping people safe. This integrated strategy also has a number of benefits, including less latency, more system resilience, more customisation, and better compliance with data governance frameworks. Even with these benefits, there are still some problems, such as model convergence concerns in heterogeneous contexts, edge devices' limited resources, communication overhead, and the necessity for strong security and standards processes. To solve these problems, we need to keep doing research across disciplines, make lightweight algorithms that protect privacy, and make ethical and legal frameworks that allow for responsible use. There will be FL systems based on blockchain, reinforcement learning at the edge, and edge-to-cloud hierarchies that vary how much computing power is needed depending on the situation. As digital infrastructure becomes increasingly important in modern cities, Edge AI and FL will help make cities that are not just smarter but also safer, fairer, and more focused on the needs of the people who live there. Ultimately, the adoption of this fusion will enable municipalities to leverage distributed intelligence while safeguarding individual privacy, promoting real-time responsiveness, and guaranteeing sustainable scalability—facilitating the emergence of a new generation of intelligent and resilient urban ecosystems.

References

[1] Abadi, M., et al. (2016). TensorFlow: A way to do machine learning on a massive scale. OSDI.
[2] Aazam, M., & Huh, E.-N. (2015). Using fog computing and smart gateways to communicate for the "cloud of things." Future Generation Computer Systems, 74, 14–20.
[3] Aledhari, M., Razzak, R., Hu, C., and Muhammad, G. (2020). Federated learning: An overview of facilitating technologies, protocols, and applications. IEEE Access, 8, 140699–140725.
[4] Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing: a place for analytics and the Internet of Things. Big Data and IoT, 2(1), 13–17.
[5] Bonawitz, K., et al. (2019). System design for large-scale federated learning. SysML Conference.
[6] Cao, K., Liu, Y., Meng, G., and Sun, Q. (2020). A summary of research on edge computing. IEEE Access, 8, 85714–85728.
[7] , M., et al. (2021). A survey on federated learning: the shift from centralized to decentralized on-site learning and beyond. IEEE Internet of Things Journal, 8(7), 5476–5497.
[8] , B., Solmaz, G., Cirillo, F., Bauer, M., & Kovacs, E. (2015). Building a big data platform for smart cities: Lessons learned and experiences from Santander. IEEE International Congress on Big Data, 592–599.
[9] Dinh, C. T., et al. (2020). Designing and analyzing an optimization model for federated learning across wireless networks. IEEE INFOCOM.
[10] EdgeX Foundry. (2023). platform for edge computing that is open. https://www.edgexfoundry.org/
[11] The European Telecommunications Standards Institute (ETSI). (2019). Multi-access Edge Computing (MEC): A Framework and Reference Architecture.
[12] Gai, K., Qiu, M., Zhao, H., Tao, L., & Zong, Z. (2016). A dynamic, energy-aware, cloudlet-based mobile cloud computing platform for environmentally friendly computing. Journal of Network and Computer Applications, 59, 46.
[13] Google AI Blog. (2017). Federated Learning: Collaborating on machine learning without consolidating all training data in a single location. https://ai.googleblog.com/2017/04/federated-learning-collaborative.html
[14] Gupta, H., Dastjerdi, A. V., Ghosh, S. K., and Buyya, R. (2017). iFogSim: A set of tools for modeling and simulating ways to manage resources in the Internet of Things, Edge, and Fog computing environments. Software: Practice and Experience, 47(9), 1275–1296.
[15] Hinton, G., et al. (2015). Extracting the information from a neural network. arXiv preprint arXiv:1503.02531.
[16] IEEE P2413. (2019). Draft Standard for an Architectural Framework for the Internet of Things (IoT).
[17] Jiang, W., et al. (2020). Federated learning through over-the-air computation. IEEE Transactions on Wireless Communications, 19(3), 2022–2035.
[18] **Kang**, J., et al. (2019). A combined optimization strategy for merging reputation and contract theory to create an incentive mechanism for dependable federated learning. IEEE Internet of Things Journal, 6(6), 10700–10714.
[19] Kim, H., et al. (2020). Federated learning that uses compressive sensing to save on communication. IEEE Transactions on Neural Networks and Learning Systems, 32(5), 2041–2055.
[20] Konečný, J., et al. (2016). Federated optimization is optimization that happens outside of the data center. arXiv preprint number 1511.03575.
[21] Li, Q., Diao, Y., Chen, Q., and He, B. (2021). A survey of federated learning on non-IID data silos. arXiv preprint arXiv:2106.06843.
[22] Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Issues, strategies, and prospective trajectories. IEEE Signal Processing Magazine, 37(3), 50–60.
[23] Lim, W. Y. B., et al. (2020). A comprehensive survey of federated learning in mobile edge networks. IEEE Communications Surveys & Tutorials, 22(3), 2031–2063.
[24] Lin, X., et al. (2021). A study on federated learning for edge computing: Research challenges and forthcoming goals. IEEE Internet of Things Journal, 8(4), 2826–2849.
[25] Liu, Y., et al. (2020). An examination of edge computing systems and instruments. Proceedings of the IEEE, 108(8), 1475–1492.
[26] Lu, Y., and Dullerud, G. (2019). Data privacy in federated learning with blockchain-based architecture. IEEE Globecom Workshops.
[27] McMahan, H. B., et al. (2017). Learning deep networks from distributed data without wasting time on communication. AISTATS, 1273–1282.
[28] Mohammadi, M., Al-Fuqaha, A., Guizani, M., and Oh, J.-S. (2018). Semisupervised deep reinforcement learning to help IoT and smart city services. IEEE Internet of Things Journal, 5(2), 624–635.
[29] Nguyen, D. C., et al. (2021). Federated learning and blockchain come together in edge computing: pros and cons. IEEE Internet of Things Journal, 8(16), 12806–12825.
[30] Nikouei, S. Y., et al. (2018). As an edge service, a lightweight CNN can find people in real time. IEEE IoT Journal, 6(3), 6344–6354.
[31] Ni, J., Lin, X., and Shen, X. (2020). Federated learning for industrial AI that works well and keeps your information safe. IEEE Transactions on Industrial Informatics, 16(8), 5636–5644.
[32] OpenAI. (2023). ChatGPT and AI models that create things. https://openai.com/research
[33] Qi, Q., Tao, F., Hu, T., and Zhang, M. (2021). Digital twin in smart manufacturing. Journal of Manufacturing Systems, 58, 208–219.
[34] Rahman, M. A., et al. (2020). Federated learning with differential privacy: An analysis of algorithms and efficacy. IEEE Transactions on Information Forensics and Security, 15, 3452–3465.
[35] Rieke, N., et al. (2020). The future of digital health with federated learning. npj Digital Medicine, 3(1), 1–7.

[36] Roman, R., and others (2018). Mobile edge computing, Fog et al.: An analysis and evaluation of security issues and challenges. Future Generation Computer Systems, 78, 680–698.
[37] Samarakoon, S., Bennis, M., Saad, W., and Debbah, M. (2018). Federated learning for V2V communications that are very reliable and have very little lag time. IEEE Transactions on Communications, 68(6), 3241–3255.
[38] Shokri, R., & Shmatikov, V. (2015). Deep learning that keeps your information safe. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 1310–1321.
[39] Shi, W., Cao, J., Zhang, Q., Li, Y., and Xu, L. (2016). Edge computing: Concepts and challenges. IEEE Internet of Things Journal, 3(5), 637–646.
[40] Sun, Y., et al. (2021). Federated learning that saves energy in edge computing: a technique to learn and talk at the same time. IEEE Transactions on Mobile Computing.
[41] Tang, J., et al. (2020). Deep reinforcement learning for the management of smart cities. IEEE Wireless Communications, 27(2), 92–99.
[42] Tseng, F. H., et al. (2020). Edge AI for predicting traffic in smart cities in real time. IEEE Access, 8, 211017–211027.
[43] Varghese, B., and Buyya, R. (2018). Cloud computing for the future generation: new trends and research projects. Future Generation Computer Systems, 79, 849–861.
[44] Wang, H., et al. (2020). Adaptive federated learning in edge computing systems with constrained resources. IEEE Journal on Selected Areas in Communications, 39(1), 190–205.
[45] Wang, S., et al. (2021). A comprehensive examination of the intersection of edge computing and deep learning. IEEE Communications Surveys & Tutorials, 22(2), 869–904.
[46] Xiao, Y., et al. (2020). Federated learning on medical data that keeps your information safe. Journal of Biomedical Informatics, 108, 103500.
[47] Xu, J., et al. (2021). Edge learning for IoT: From hype to reality. IEEE Communications Magazine, 59(1), 102–108.
[48] Yang, Q., Liu, Y., Chen, T., and Tong, Y. (2019). Federated machine learning: Its principles and implementations. ACM Transactions on Intelligent Systems and Technology, 10(2), 1–19.
[49] Zhang, K., and others (2021). Edge AI: Using edge computing to make deep neural network inference faster when needed. IEEE Transactions on Wireless Communications, 20(1), 126–137.
[50] Zhou, Z., Chen, X., Li, E., Zeng, L., Luo, K., & Zhang, J. (2019). Edge intelligence: Using edge computing to make the last mile of AI conceivable. Proceedings of the IEEE, 107(8), 1738–1762.