Chapter X

Federated learning for Secure Smart Cities using IoT.

Apurba Koirala[1], Aaryan Shrestha[2], Hrigdev Singh[3], Jonathan Atrey[4], Rajeshkannan Regunathan[5]

[1,2,3,4,5] School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India

Abstract

Limitations of data storing and processing in traditional machine learning have led to constraints in creating high-scalability models. In addition, several security areas may be compromised when accessing and utilizing data. Recent advances in machine learning have resulted in the conception of Federated machine learning to address these difficulties. There are significant issues regarding security, such as the disclosure of private or sensitive information. At times, centralized databases may experience a breach, putting the stored data in danger, or there can be interceptions by hackers during data transmission. As a result, we use Federated learning to address these issues. The decentralized architecture offered by federated learning has allowed us to create more scalable models with definite architectures while incrementing various security aspects of training data.

The combination of federated learning along with data gathered from today's Internet-of-Things has resulted in several studies that may be beneficial concerning different research perspectives in smart cities. In the proposed book chapter, an exhaustive inquiry is carried out to summarize the most recent research on using federated learning in various smart city-related domains. A comprehensive knowledge of the recent advances in federated learning across multiple industries. A brief history, explanation, and overview of the most critical technologies crucial to federated learning come next, along with applications in the context of smart cities.

Federated learning has the potential to transform how we live, work, and interact in our urban surroundings by combining the power of advanced technology with a privacy-preserving approach, ushering in a new era of collaborative intelligence and invention.

Keywords: Smart Cities, Decentralized Environment, Federated Learning, IoT

Introduction

In the twenty-first century, urbanization has surged, with cities now housing more than half of the world's population. As these urban areas continue to grow, there is a greater need for efficient, sustainable, and intelligent solutions to manage resources and improve the quality of life for their residents. Smart cities are a technologically driven approach that merges advanced digital technologies, big data analytics, and networked systems to produce more efficient, sustainable, and citizen-centric urban settings.

Smart cities use the Internet of Things (IoT), artificial intelligence (AI), and other emerging technologies to improve public services, improve infrastructure, and promote innovation. These advances not only improve transportation, energy management, and trash disposal systems but also improve urban people’s safety, health, and overall well-being. Yet, the data privacy and security risks that these breakthroughs raise must not be overlooked. Because the smart city ecosystem is heavily reliant on data collection and processing, there is an increasing demand for technologies that can manage sensitive data while retaining the benefits of collaborative intelligence. This is where federated learning comes into play.

Federated learning is a decentralized machine learning technique that allows AI models to learn from distributed datasets while maintaining data privacy. Local devices or edge nodes do model training using their own data in this system, and only model updates are exchanged with a central server. This reduces the need for raw data transfer, lowering privacy concerns and bandwidth costs. Smart cities may harness the power of AI while protecting the privacy and security of their inhabitants' data by employing federated learning.

Federated learning has numerous advantages in the context of smart cities. It fosters the development of customised, context-aware solutions by enabling smooth collaboration among multiple stakeholders, including government agencies, private firms, and citizens. This shared intelligence enables city planners and policymakers to make data-driven decisions, improving resource allocation and assuring the city's resilience to challenges like climate change, population expansion, and economic volatility.

Furthermore, federated learning allows incorporating a wide range of data sources, from traffic sensors to healthcare records, without disclosing sensitive information. This enables smart cities to fully utilize their data, resulting in more accurate and robust AI models. Improvements in predictive analytics and real-time decision-making capabilities have improved many elements of urban living, ranging from traffic management and public safety to environmental monitoring and healthcare services.

Research Contributions

The authors' primary goal in the proposed book chapter is to investigate the various uses of federated learning in the context of smart cities, with a particular emphasis on its integration with Internet of Things (IoT) devices. The major goal is to evaluate the dependability of federated learning in terms of time, cost, scalability, and security. Following an introduction that establishes the significance of federated learning, the proposed study goes into the numerous types of federated learning, their requirements, and their restrictions. This basic understanding prepares readers for the chapter's focus, which is the use of federated learning in IoT and smart cities. Before reaching their conclusions, the authors discuss the challenges that must be overcome as well as the future scope of federated learning in smart cities, providing readers with a thorough understanding of the subject. Finally, the authors give their conclusions based on the many findings from the various use cases and recent empirical research discussed throughout the chapter, shining light on the consequences and prospects of federated learning in smart city applications.

Incorporating Federated Learning in Smart Cities

As we move deeper into the world of smart cities, federated learning will continue to open new avenues for innovation and growth. By encouraging a synergistic link between technology and urban development, we can ensure that future cities are prepared to face the difficult problems that lie ahead.

Transportation systems are one crucial area where federated learning may have a substantial influence. With the growth of self-driving cars and intelligent traffic management, there is a greater demand for real-time data processing and decision-making. Federated learning can aid in the development of a cooperative network of automobiles, traffic lights, and infrastructure, allowing them to learn from each other's experiences while retaining privacy. This collaborative strategy can result in more efficient traffic flow, less congestion, and lower emissions, eventually leading to a cleaner and more sustainable urban environment.

Federated learning has the potential to transform the way medical data is processed and evaluated in the field of healthcare. Federated learning can significantly improve the accuracy of disease prediction, early diagnosis, and personalized treatment plans by allowing hospitals, clinics, and research institutions to share AI model updates without exposing sensitive patient information. This approach can also help cities better prepare for and respond to outbreaks, epidemics, and other health emergencies.

Another domain in which federated learning can be useful is energy management. Federated learning can assist improve energy distribution and consumption by combining data from several sources, such as smart meters, weather trends, and energy usage behaviours. This might result in more efficient energy consumption, less strain on the power system, and a smaller carbon impact on the city.

Finally, federated learning can help improve public safety and security in smart cities. Federated learning can help build a safer and more resilient urban environment by enabling multiple stakeholders, such as law enforcement agencies, private security corporations, and people, to share information and work on AI models without risking privacy violations. This can lead to more successful crime prevention initiatives, emergency response plans, and overall increased citizen safety.

Preliminary concepts about Federated Learning

Aggregation cycle

When working with a federated learning network, the following are the major steps:

Network Configuration
First, specific nodes are assigned to collect all local outputs and updates from each participating node. Following this, a central point for data collection is chosen, and the rest of the network relies on local nodes to process their training data using local models. Consequently, the central data collection point selects a number of sub-nodes that are suitable for the given task and integrates them into the Federated Learning network.

Local node training
Once the local nodes and central collection point have been established, the central server disseminates a model containing all necessary parameters to initiate local data training within each node. The individual nodes then train their respective models, generating updates that may include values such as weights or other forms of unprocessed data. These updates are subsequently uploaded to the network and forwarded to the central collection point.

Aggregating Updates
The central collection point receives updates from all the trained local nodes and proceeds to combine these updates to produce a consolidated model. This final model is generated by averaging the parameters obtained from the local nodes within the federated network, and updating the weights based on the data associated with the central server.

Iterative Process until Optimal Model
After the first network iteration, the central server updates the final model and redistributes the resulting combined parameters back to the local nodes for the subsequent iteration of local data training. This cycle of local training and aggregation continues through multiple iterations, with the updated model being shared and refined until an optimal model is achieved. Each iteration allows the local nodes to further refine their models based on the aggregated parameters, gradually improving the performance and accuracy of the global model.

Throughout this iterative process, local nodes maintain their data privacy, as only model updates and not raw data are shared with the central server. This ensures that sensitive information remains protected, while still allowing the network to benefit from the collective intelligence of all participating nodes.

Once the optimal model has been attained, the central server can halt the iterative process, and the final model can be deployed for the desired application. This Federated Learning approach enables the development of robust and accurate models without compromising data privacy and security, making it particularly suitable for scenarios where data protection is a top priority.

Figure 1 illustrates a federated model that communicates with the central server by distributing a model containing global parameters for every local node to train with, which are then fine-tuned based on local data processing. The figure also demonstrates the transfer of each local node's modifications to the central server and the distribution of a refreshed global model after the central server has combined the incoming parameters.

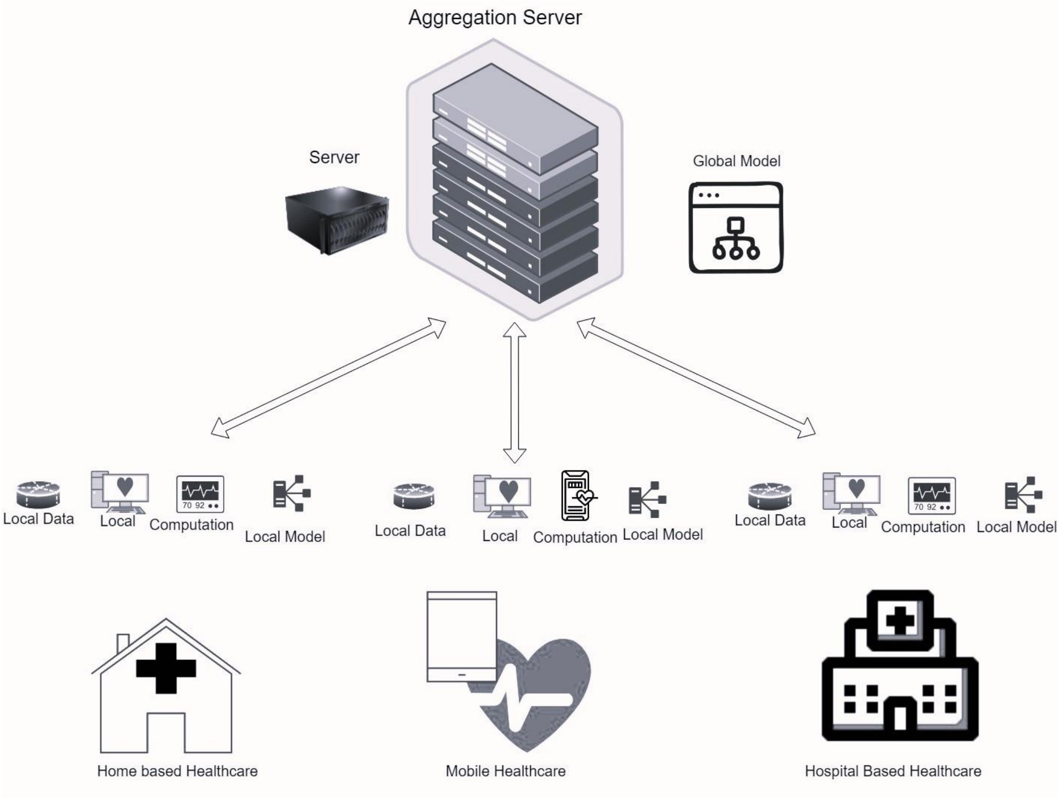

Figure 1. FL Architecture.

FedAvg

Federated averaging (FedAvg) is a communication strategy that provides efficiency for a large sample space of clients holding distributed data for training models. Clients in FedAvg secure their data by training them locally and not sharing the actual data while generating a global model by submitting their parameters to an aggregation server. Most deep learning applications rely heavily on the variation of their related stochastic gradient descent (SGD). Hence, while developing FedAvg, or federated averaging technique, writers in [1] used federated optimization to apply SGD to an instance. Every round of communication in this example employs a single batch of gradient computation. This method is efficient; nevertheless, training a good model requires a significant number of iterations. Hence, [1] used large batch synchronous SGD, similar to the trials in [2]. To execute this strategy, a group of clients is chosen each round, and the gradient of loss is computed depending on the data that these clients have. This is known as FederatedSGD or FedSGD. Given such a set of FedSGD, the proportion of clients is regarded as a variable C equivalent to 1, and a fixed learning rate 'η' is utilized by each client for computing the average gradient 'g' at the local models 'w.' The Central server combines gradients and performs an update. Each locally trained client performs a single gradient descent step on the current model using local data, and the server then uses the weighted average of the resulting model as its parameters. Following that, the local clients can be repeated several times before proceeding to the next stage, which entails determining the weighted average. FedAvg, or the federated averaging algorithm, is the name given to this approach. **Figure 2** is an illustration of the FedAvg algorithm.

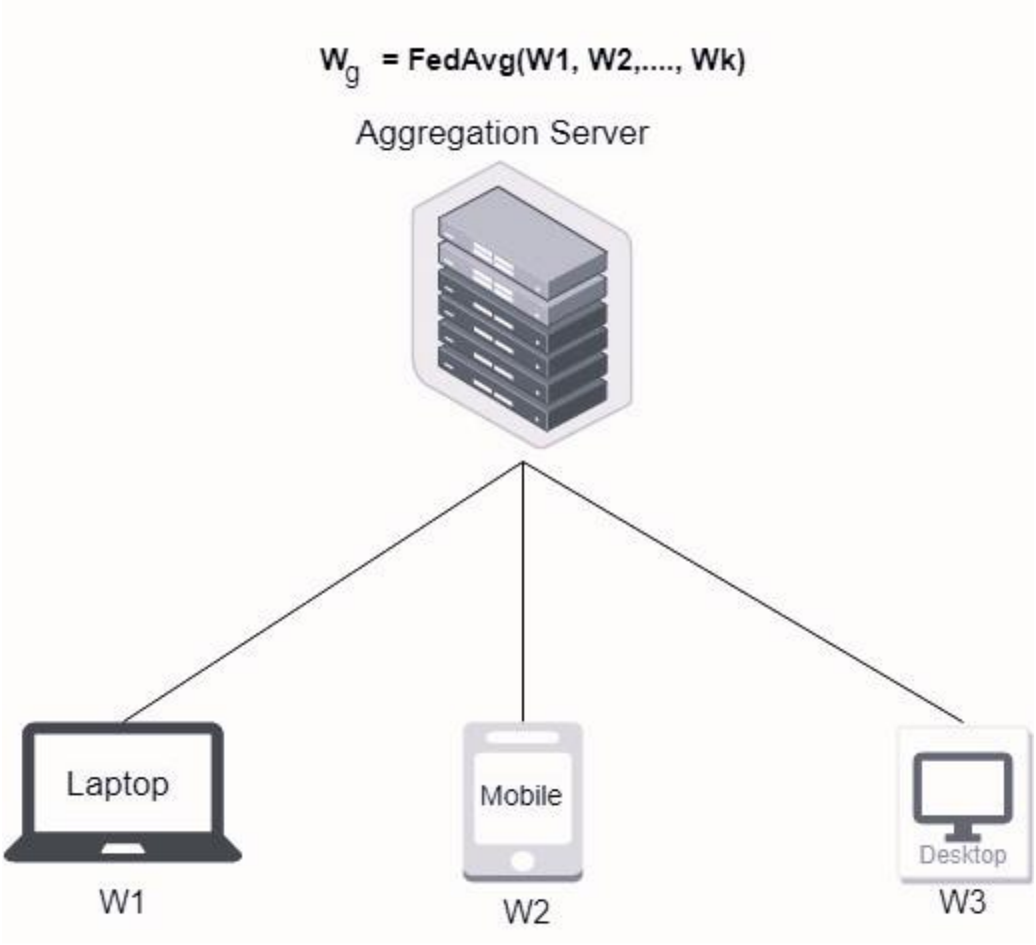

Figure 2. FedAvg.

Drawbacks of Traditional Machine Learning

Traditional Machine Learning has various constraints, some of which are not suitable for training data in a smart environment. They are as follows:

Adversarial attacks

Traditional machine learning algorithms can be vulnerable to adversarial attacks, where an attacker can manipulate the input data in a way that the model misclassifies the data. For example, an attacker can modify the pixels in an image slightly to make it look different from the original, but still be misclassified by the machine learning model.

Data poisoning
Traditional machine learning algorithms can be susceptible to data poisoning attacks, where an attacker injects malicious or incorrect data into the training dataset to influence the model's behavior. This can result in the model making incorrect predictions or decisions.

Model inversion
Traditional machine learning models can also be vulnerable to model inversion attacks, where an attacker can use the output of the model to reconstruct sensitive information about the input data. This can be particularly problematic in applications such as credit scoring or medical diagnosis, where the input data is sensitive.

Model stealing
Attackers can also steal the machine learning model itself, which can be valuable intellectual property. They can do this by reverse-engineering the model's architecture or by exploiting weaknesses in the model's training process.

Lack of explainability
Traditional machine learning models can sometimes lack transparency and explainability, which can make it difficult to identify and mitigate vulnerabilities or biases in the model.

Motivation for Federated Learning

To eradicate the above-listed issues raised by traditional machine learning that are not suitable for highly scalable modelling training such as smart cities, we utilize federated machine learning. Federated machine learning offers a distributed and secure training environment to train data at local entities. To combat these drawbacks federated learning can be used. In federated learning, the model is trained locally in the user’s device. Then the model updates are sent to the aggregation server where a global model is created. The advantage of federated learning is that it can allow multiple parties to collaborate on training a machine learning model, without compromising the privacy and security of their data. This can be particularly useful in applications such as healthcare or finance, where sensitive data must be protected. Federated learning can also be more efficient and scalable than traditional machine learning approaches since the data is distributed across multiple devices or servers, reducing the need to transfer large amounts of data to a central location. In addition, federated learning can help to mitigate issues such as bias or overfitting that can arise when training machine learning models on centralized datasets.

Federated learning (FL) algorithms can overcome some of the security drawbacks of traditional machine learning algorithms.

Data privacy
FL allows for the training of a machine learning model using data that is distributed across multiple devices without requiring the data to be shared to a third-party entity. This means that sensitive data can be kept private, reducing the risk of data breaches or leaks.

Data security

FL can also help to enhance data security by ensuring that the data is kept on the local device or server and only model updates are sent to the central server. This can reduce the risk of data theft or data tampering by malicious actors.

Adversarial attacks

FL can also be used to defend against adversarial attacks, where attackers attempt to manipulate the input data in a way that the model produces incorrect predictions. In FL, each local device or server trains the model on its own data and sends only the model updates to the central server. This can make it more difficult for attackers to launch adversarial attacks as they would need to compromise multiple devices or servers simultaneously.

Data poisoning

FL can also mitigate the risk of data poisoning attacks by utilizing different security protocols on each local node. By implementing varying security measures, the risk of an attacker injecting malicious or incorrect data into the training dataset to influence the model's behaviour is reduced significantly.

Explainability

FL can also help to improve the explainability of the machine learning model by allowing for the analysis of the model updates and training data on each device or server. This can help to identify potential biases or errors in the model, as well as improve the transparency of the model's decision-making process.

Figure 3 is a diagrammatic representation of the difference between traditional machine learning and federated machine learning.

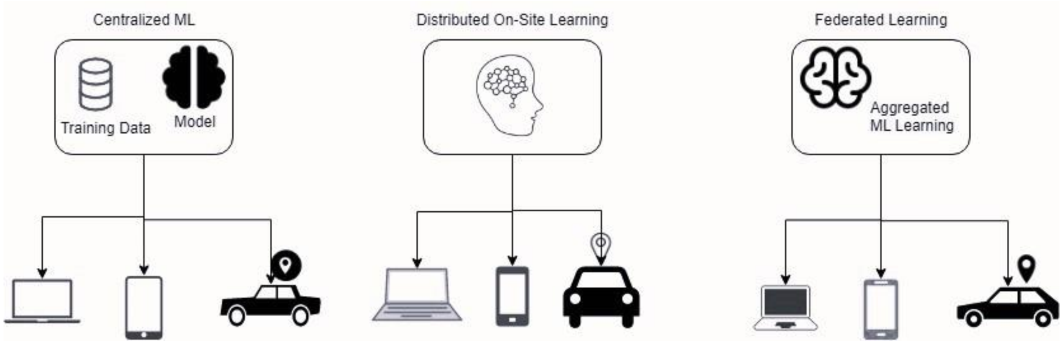

Figure 3. Traditional vs Federated Machine Learning.

Literature Survey

Federated learning has emerged as a promising approach for enabling machine learning on dispersed data sources while maintaining the confidentiality and safety of the nodes that take part in the process. This is especially important in smart cities, which are characterized by the production of massive amounts of sensitive data by a wide variety of IoT devices, such as sensors, cameras, and drones. Federated learning makes it possible for various devices to work together on training machine learning models without having to share their raw data. As a result, the risk of data breaches is reduced, and the privacy of the persons and organizations involved is preserved.

Table 1. Summary of a few included articles

Reference No.	Observations	Drawbacks
[3]	The paper highlights the challenges and opportunities of using federated learning in smart city sensing.	No specific drawbacks were mentioned in the paper.
[4]	The paper provides a comprehensive review of the applications of federated learning in various domains.	The paper lacks specific validation of Federate Learning for Smart Cities.
[5]	The paper presents recent advances, taxonomy, and open challenges in the application of federated learning in smart cities.	The paper lacks a detailed discussion of privacy and security challenges.
[6]	The paper discusses the application of federated learning in healthcare informatics.	The paper lacks a specific focus on smart cities and IoT.
[7]	The paper provides a comprehensive survey of the application of federated learning in smart cities.	The paper lacks a detailed discussion of challenges in implementing federated learning in smart cities.
[8]	The paper discusses the application of federated learning in IoT and identifies its challenges and opportunities.	The paper lacks a specific focus on smart cities.
[9]	The paper presents a method for exploiting unlabeled data in smart cities using federated learning.	The paper lacks a comprehensive discussion of privacy and security challenges.
[10]	The paper presents a method for water consumption forecasting in smart cities using federated learning.	The paper lacks a detailed discussion of the implementation challenges.
[11]	The paper discusses the impact of federated learning on smart buildings	The paper lacks a specific focus on IoT and smart cities.
[12]	The paper provides a comprehensive survey of the applications of federated learning in accelerating the Industrial Internet of Things	No specific drawbacks were mentioned in the paper
[13]	The paper proposes a privacy-preserving blockchain-based federated learning framework for IoT devices.	The proposed framework may require significant computational resources for blockchain operations.
[14]	The paper discusses the challenges and opportunities of providing trustworthy and sustainable smart city services at the edge.	No specific drawbacks were mentioned in the paper.
[15]	The paper provides an overview of the concepts, taxonomies, challenges, and open issues in using federated learning-based AI approaches in smart healthcare.	No specific drawbacks were mentioned in the paper.

[16]	The paper presents a survey on the fusion of federated learning and the Industrial Internet of Things.	No specific drawbacks were mentioned in the paper.

Paper [17], written by Al-Huthaifi et al., offers a comprehensive review of the difficulties associated with maintaining privacy and security when federating learning used in smart cities. The authors examine a variety of privacy and security problems, including as data leakage, model poisoning, and adversarial attacks, and present a set of recommended procedures and potential solutions as a means of mitigating these dangers. In addition to this, they offer an overview of the most recent federated learning algorithms and frameworks for smart cities, highlighting both the virtues and limitations of each.

Utomo et al. present their idea for a federated and trustworthy AI architecture for smart cities in paper number [19]. The authors concentrate on the difficulties associated with assuring the trustworthiness of federated learning models and present a set of design principles that can be used to construct trustworthy federated learning systems. In addition to this, they emphasize the significance of governance and legislation in guaranteeing the ethical application of federated learning in smart cities.

Pothole detection is another important application of federated learning in smart transportation, as discussed in paper [20] by Alshammari et al. The authors present a federated learning-based, three-dimensional pothole detection system that makes use of data collected by numerous sensors and cameras that are mounted on automobiles. They show that their method is effective in detecting potholes and demonstrate how federated learning can be used to overcome the difficulties of data heterogeneity and privacy protection in the context of smart transportation.

In paper [21], Liu et al. present a federated learning-based architecture for aerial-ground air quality sensing in smart cities. This framework is described in more detail in the study. The authors offer a federated learning strategy to train a machine learning model that predicts the air quality index. The authors deploy swarms of unmanned aerial vehicles (UAVs) to collect data on the air quality in various areas. They show that their strategy is effective in lowering the amount of overhead communication and maintaining the privacy of the participating nodes in the network.

Alsamhi et al. present an assessment of collaborative smart drones and IoT for improving the smartness of smart cities in their [22]. The authors examine a variety of uses of drones and the Internet of Things in smart cities, such as traffic control, emergency response, and environmental monitoring. They also highlight the issues of data privacy and security that are present in these applications. In addition to this, they highlight the potential of federated learning for enabling collaborative drone and IoT applications and propose a set of research goals for future work.

Paper [23] by Rieke et al. investigates the potential of federated learning to shape the future of digital health. The authors highlight the possibility of federated learning to enable collaborative machine learning on dispersed health data while maintaining the patients' right to privacy and keeping their data secure. They also highlight the difficulties associated with the heterogeneity of data and the lack of interoperability in digital health, and they suggest several methods to overcome these problems.

A federated learning strategy is proposed by Choudhury et al. in paper [24] as a method for predicting adverse medication reactions based on dispersed health data. The authors present evidence that their method is effective in demonstrating an improvement in the accuracy of the prediction of adverse medication reactions while maintaining the confidentiality of the participating institutions and patients.

The authors of the paper [25] "Privacy-Preserving Traffic Flow Prediction: A Federated Learning Method" (Liu et al) suggest a privacy-preserving Federated Learning approach for traffic flow prediction. In this research, a novel FL technique for model training and aggregation is presented. This approach protects both the privacy and the security of the data.

The paper written by Zhang et al. and titled "FASTGNN: A Topological Information Protected Federated Learning Method for Traffic Speed Forecasting", [26], presents a federated learning method that keeps topological information intact and is used for traffic speed forecasting. The authors offer an FL algorithm that aims to protect the privacy of the participating nodes.

According to the findings presented in the paper [18], federated learning has several key applications in smart cities. One of these applications is the prediction of air quality. The authors provide an overview of federated learning approaches for air quality index prediction and compare their performance with centralized learning approaches. They also explore the difficulties associated with predicting air quality, such as data heterogeneity and protecting individuals' privacy, and they provide a series of ways to overcome these problems.

In their article number [27], Saputra and colleagues applied federated learning to predict energy demand in electric car networks. The authors used a centralized learning architecture with secure aggregation to address the challenges of data heterogeneity and privacy protection. In paper number [28], Zhang and colleagues developed a privacy-protecting hybrid federated learning architecture for the identification of financial crime. The authors struck a balance between the competing values of data privacy and model accuracy by employing a hybrid approach that combined centralized and federated learning.

Rahman and colleagues studied the use of federated learning as an intrusion detection method in IoT networks in paper number [29]. The authors examined the efficacy of three distinct methods, namely centralized learning, on-device learning, and federated learning, and compared their results regarding accuracy and privacy.

In general, the studies that were examined for this literature review illustrate the promise of federated learning for making smart cities that use IoT more secure while also protecting residents' privacy. They demonstrate how federated learning may be used to meet the difficulties of data heterogeneity, privacy protection, and security in a variety of smart city applications. Some examples of these applications include predicting air quality, traffic flow, energy demand, and financial crime detection.

Future Scope and Challenges

Communication Issues in FL-based Environment

Communication, which is important for FL users, and embedded servers are critical in FL-supported healthcare services. Effective communication resource allocation increases learning results dramatically. This is especially significant if many IoT devices must be deployed on the aggregation server for prolonged link-template upgrades and low link sample deployments. In this instance, the aggregation server can choose a suitable collection of IoT devices based on an effective planning policy, as documented in several previous research [30][31][32][33]. Another major connection issue is the dynamic and rapid changing of the radio channel between the IoT device and the aggregation server, which impacts the reliability and quality of training updates. One possible approach is to address the impact of user disruption [34][35] as well as more dependable design goals such as device downtime and availability.

Specifications for Deployment

Although the literature has numerous promising health outcomes supported by FL, there are no standard and universal results for comparing the efficacy of different methods to the same condition. Various blockchain frameworks have been proposed for FL systems, such as removing the need for a central server and handling IoT device update locally. Nevertheless, comparing these techniques is challenging since they are advised for various (status) circumstances and utilize different network parameters/datasets to evaluate performance. There are additional critical concerns to consider about the universality and standardization of communication protocols, device hardware, deployment situations, and integration approaches. Recently, IEEE Std 3652.1-2020 gave guidelines on the architecture and design views of FL [36], as well as the FL rating table and performance data system.

Quality of Federated Training Data

Variations in computer power and data quality between hospitals can significantly impact educational quality. In this scenario, one viable option is to provide incentives for hospitals and medical institutions to use high-quality data for teaching and to submit trustworthy changes to a single server. Blockchain and game theory are two essential instruments for building stimulation mechanisms [37] [38] [39]. By flexibly customizing learning demands, the FL format should be easily adaptable and adaptive for nurses, physicians, and patients (e.g., changing data types, changing learning rates, changing, or regressing the classification of learning objectives). These modifications may have an impact on FL models and default learning patterns (in FL users and embedded servers), necessitating the creation of an adaptable FL methodology. AI is a potential approach since it can increase the flexibility of FL models to future occurrences by using previous data. As a result, DRL [40] employs a classic way to generate an incentive mechanism in the event of poor performance when the opportunity is significant enough.

Confidential Dataset concerns

Different customers may have distinct data types, such as text, photos, sound, and time series, and varied data content, such as blood type, heart rate, facial image, and body temperature, in some treatment situations. Almost all FL approaches in the literature, as is customary, are based on a single data set with a restricted number of characteristics. A novel heterogeneous FL strategy should be devised, with a central server exploring this heterogeneity via the unique construction of the entire [41]. Participants in this activity must give a final approach that allows them to employ a diverse collection of models without having to integrate data in one spot.

FL integrated advanced networks

Although 5G networks have not yet reached full availability or commercial deployment, they do exist. Numerous research and development efforts are in progress for emerging 6G wireless technologies [42]. With 6G and Industry 5.0, a variety of applications become possible, such as intelligent healthcare, smart grids, holographic television, and personalized body area networks. Furthermore, several cutting-edge technologies, including blockchain, compression sensors, terahertz and visible light communication, 3D networking, quantum communication, and large-scale intelligent surfaces, are being introduced to meet the stringent requirements of 6G.

Questions arise regarding how Federated Learning capabilities will be incorporated into future 5G/6G medical devices and how 6G devices, like smart implants and wearable devices, will be utilized in various FL-based healthcare and novel health services that 6G will enable. For instance, future e-health services will be enhanced by AI and Federated Learning capabilities to improve quality of life and reduce hospital admissions [43]. These questions provide an exciting avenue for further research.

FL's Provable Privacy

Although FL offers great promise to secure users' data privacy, the high sensitivity of health data raises a variety of privacy concerns that must be addressed carefully, particularly in the context of smart healthcare. Federated Learning privacy problems, according to [44], may be classed as the member's last attack, inadvertent information leaking, and generative antagonism. An attacker, for example, may utilize the global FL template to see if a sample of data exists in the FL health dataset. When a patient's gadget communicates local model updates to central servers in hospitals and healthcare institutions, patient information is also acquired. There is also a sophisticated encryption technology being developed for securing personal information for medical Care systems and ensuring differential confidentiality. Additional research into the use of differential confidence to increase the secrecy of the FL system is being considered[45][46].

Cyber defense aspects

In an FL-based smart care system, multiple client participants can behave as attackers, sending toxic model updates or disinformation to undermine model integration. When learning local data, an attacker might infect data attribute information or modify local updates while moving templates between local clients and central servers. Remote attackers can utilize their assaults on the server to obtain information about the accumulated global pattern, resulting in serious privacy problems such as information breaches. Fixing these security flaws is a significant concern for smart FL-based healthcare systems. Various options, such as the use of differential confidentiality [47], should be investigated to safeguard the training dataset against data corruption. Furthermore, by encrypting local updates and sharing keys between the client and a central server, the creation of a secure integration technique [48] is a viable option to create a double-mask structure to protect clients from data fabrication and assaults.

IIDness issue of data

Inconsistencies in medical data sets that might lead to learning FL in training are major challenges that must be addressed to obtain the necessary learning performance in FL-based medical systems. A hospital, for example, may have a higher frequency of a certain type of regional disease than another hospital in a different geographical location. Participation in federal data education is challenging in this scenario since label distribution differs by the medical institution. If this does not resolve the inconsistency problem, it may worsen or possibly depart from learning the data. As a result, solutions to non-IID challenges, such as producing new subsets of data sets for fair distribution to consumers, should be created to successfully shape data in FL-based smart healthcare. Another intriguing technique is to execute the mobility of characteristics amongst diverse consumers by modifying the distribution of characteristics on the customer side before averaging local models. To examine non-IID data in the FL-based smart care sector, quantitative measures such as standard deviation, a curvature of label/function distribution, and accuracy and accuracy for homogenous sections are required [49].

Conclusion

Federated learning is a rapidly growing area of research, and its combination with the medical Internet of Things could significantly transform the safety of healthcare data. The proposed book chapter aims to assess whether federated learning is a highly reliable topic in terms of enhancing the confidentiality and security of data for intelligent urban environments and if it can contribute to developing a more scalable model for handling sensitive information. The proposed book chapter explores some of the most crucial real-world implementations that have been examined and simulated for research purposes. In concluding the book chapter, vital discussions regarding the challenges faced by federated learning frameworks, as well as the future prospects of federated learning in healthcare settings, are presented. In summary, this topic possesses substantial research potential, with the capability to develop advanced AI methodologies in the future.

References

[1] McMahan, Brendan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera y Arcas. "Communication-efficient learning of deep networks from decentralized data." In Artificial intelligence and statistics, pp. 1273-1282. PMLR, 2017.

[2] Chen, Jianmin, Xinghao Pan, Rajat Monga, Samy Bengio, and Rafal Jozefowicz. "Revisiting distributed synchronous SGD." arXiv preprint arXiv:1604.00981 (2016).

[3] Jiang, Ji Chu, Burak Kantarci, Sema Oktug, and Tolga Soyata. "Federated learning in smart city sensing: Challenges and opportunities." *Sensors* 20, no. 21 (2020): 6230.

[4] Li, Li, Yuxi Fan, Mike Tse, and Kuo-Yi Lin. "A review of applications in federated learning." *Computers & Industrial Engineering* 149 (2020): 106854.

[5] Zheng, Zhaohua, Yize Zhou, Yilong Sun, Zhang Wang, Boyi Liu, and Keqiu Li. "Applications of federated learning in smart cities: recent advances, taxonomy, and open challenges." *Connection Science* 34, no. 1 (2022): 1-28.

[6] Xu, Jie, Benjamin S. Glicksberg, Chang Su, Peter Walker, Jiang Bian, and Fei Wang. "Federated learning for healthcare informatics." *Journal of Healthcare Informatics Research* 5 (2021): 1-19.

[7] Pandya, Sharnil, Gautam Srivastava, Rutvij Jhaveri, M. Rajasekhara Babu, Sweta Bhattacharya, Praveen Kumar Reddy Maddikunta, Spyridon Mastorakis, Md Jalil Piran, and Thippa Reddy Gadekallu. "Federated learning for smart cities: A comprehensive survey." *Sustainable Energy Technologies and Assessments* 55 (2023): 102987.

[8] Zhang, Tuo, Lei Gao, Chaoyang He, Mi Zhang, Bhaskar Krishnamachari, and A. Salman Avestimehr. "Federated learning for the internet of things: applications, challenges, and opportunities." *IEEE Internet of Things Magazine* 5, no. 1 (2022): 24-29.

[9] Albaseer, Abdullatif, Bekir Sait Ciftler, Mohamed Abdallah, and Ala Al-Fuqaha. "Exploiting unlabeled data in smart cities using federated edge learning." In *2020 International Wireless Communications and Mobile Computing (IWCMC)*, pp. 1666-1671. IEEE, 2020.

[10] Hanjri, Mohammed El, Hibatallah Kabbaj, Abdellatif Kobbane, and Amine Abouaomar. "Federated Learning for Wa Mitra, Angan, Yanik Ngoko, and Denis Trystram. "Impact of federated learning on smart buildings." In *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*, pp. 93-99. IEEE, 2021.ter Consumption Forecasting in Smart Cities." *arXiv preprint arXiv:2301.13036* (2023).

[11] Zhou, Jiehan, Shouhua Zhang, Qinghua Lu, Wenbin Dai, Min Chen, Xin Liu, Susanna Pirttikangas, Yang Shi, Weishan Zhang, and Enrique Herrera-Viedma. "A survey on federated learning and its applications for accelerating industrial internet of things." *arXiv preprint arXiv:2104.10501* (2021).

[12] Zhao, Yang, Jun Zhao, Linshan Jiang, Rui Tan, Dusit Niyato, Zengxiang Li, Lingjuan Lyu, and Yingbo Liu. "Privacy-preserving blockchain-based federated learning for IoT devices." *IEEE Internet of Things Journal* 8, no. 3 (2020): 1817-1829.

[13] Jararweh, Yaser, Safa Otoum, and Ismaeel Al Ridhawi. "Trustworthy and sustainable smart city services at the edge." *Sustainable Cities and Society* 62 (2020): 102394.

[14] Rahman, Anichur, Md Sazzad Hossain, Ghulam Muhammad, Dipanjali Kundu, Tanoy Debnath, Muaz Rahman, Md Saikat Islam Khan, Prayag Tiwari, and Shahab S. Band. "Federated learning-based AI approaches in smart healthcare: concepts, taxonomies, challenges and open issues." *Cluster Computing* (2022): 1-41.

[15] Boopalan, Parimala, Swarna Priya Ramu, Quoc-Viet Pham, Kapal Dev, Praveen Kumar Reddy Maddikunta, Thippa Reddy Gadekallu, and Thien Huynh-The. "Fusion of federated learning and industrial Internet of Things: A survey." *Computer Networks* (2022): 109048.

[16] Ramu, Swarna Priya, Parimala Boopalan, Quoc-Viet Pham, Praveen Kumar Reddy Maddikunta, Thien Huynh-The, Mamoun Alazab, Thanh Thi Nguyen, and Thippa Reddy Gadekallu. "Federated learning enabled digital twins for smart cities: Concepts, recent advances, and future directions." *Sustainable Cities and Society* 79 (2022): 103663.

[17] Rasha, Al-Huthaifi, Tianrui Li, Wei Huang, Jin Gu, and Chongshou Li. "Federated Learning in Smart Cities: Privacy and Security Survey." *Information Sciences* (2023).

[18] Le, Duy-Dong, Anh-Khoa Tran, Minh-Son Dao, Mohamed Saleem Haja Nazmudeen, Viet-Tiep Mai, and Nhat-Ha Su. "Federated Learning for Air Quality Index Prediction: An Overview." In *2022 14th International Conference on Knowledge and Systems Engineering (KSE)*, pp. 1-8. IEEE, 2022.

[19] Utomo, Sapdo, A. John, Adarsh Rouniyar, Hsiu-Chun Hsu, and Pao-Ann Hsiung. "Federated Trustworthy AI Architecture for Smart Cities." In *2022 IEEE International Smart Cities Conference (ISC2)*, pp. 1-7. IEEE, 2022.

[20] Alshammari, Sami, and Sejun Song. "3Pod: Federated Learning-based 3 Dimensional Pothole Detection for Smart Transportation." In *2022 IEEE International Smart Cities Conference (ISC2)*, pp. 1-7. IEEE, 2022.

[21] Liu, Yi, Jiangtian Nie, Xuandi Li, Syed Hassan Ahmed, Wei Yang Bryan Lim, and Chunyan Miao. "Federated learning in the sky: Aerial-ground air quality sensing framework with UAV swarms." *IEEE Internet of Things Journal* 8, no. 12 (2020): 9827-9837.

[22] Alsamhi, Saeed H., Ou Ma, Mohammad Samar Ansari, and Faris A. Almalki. "Survey on collaborative smart drones and internet of things for improving smartness of smart cities." *Ieee Access* 7 (2019): 128125-128152.

[23] Rieke, Nicola, Jonny Hancox, Wenqi Li, Fausto Milletari, Holger R. Roth, Shadi Albarqouni, Spyridon Bakas et al. "The future of digital health with federated learning." *NPJ digital medicine* 3, no. 1 (2020): 119.

[24] Choudhury, Olivia, Yoonyoung Park, Theodoros Salonidis, Aris Gkoulalas-Divanis, and Issa Sylla. "Predicting adverse drug reactions on distributed health data using federated learning." In *AMIA Annual symposium proceedings*, vol. 2019, p. 313. American Medical Informatics Association, 2019.

[25] Liu, Yi, J. Q. James, Jiawen Kang, Dusit Niyato, and Shuyu Zhang. "Privacy-preserving traffic flow prediction: A federated learning approach." *IEEE Internet of Things Journal* 7, no. 8 (2020): 7751-7763.

[26] Zhang, Chenhan, Shuyu Zhang, J. Q. James, and Shui Yu. "FASTGNN: A topological information protected federated learning approach for traffic speed forecasting." *IEEE Transactions on Industrial Informatics* 17, no. 12 (2021): 8464-8474.

[27] Saputra, Yuris Mulya, Dinh Thai Hoang, Diep N. Nguyen, Eryk Dutkiewicz, Markus Dominik Mueck, and Srikathyayani Srikanteswara. "Energy demand prediction with federated learning for electric vehicle networks." In *2019 IEEE global communications conference (GLOBECOM)*, pp. 1-6. IEEE, 2019.

[28] Zhang, Haobo, Junyuan Hong, Fan Dong, Steve Drew, Liangjie Xue, and Jiayu Zhou. "A Privacy-Preserving Hybrid Federated Learning Framework for Financial Crime Detection." *arXiv preprint arXiv:2302.03654* (2023).

[29] Rahman, Sawsan Abdul, Hanine Tout, Chamseddine Talhi, and Azzam Mourad. "Internet of things intrusion detection: Centralized, on-device, or federated learning?." *IEEE Network* 34, no. 6 (2020): 310-317.

[30] Xu, Bo, Wenchao Xia, Jun Zhang, Tony QS Quek, and Hongbo Zhu. "Online client scheduling for fast federated learning." IEEE Wireless Communications Letters 10, no. 7 (2021): 1434-1438.

[31] Xia, Wenchao, Tony QS Quek, Kun Guo, Wanli Wen, Howard H. Yang, and Hongbo Zhu. "Multi-armed bandit-based client scheduling for federated learning." IEEE Transactions on Wireless Communications 19, no. 11 (2020): 7108-7123.

[32] Luo, Siqi, Xu Chen, Qiong Wu, Zhi Zhou, and Shuai Yu. "HFEL: Joint edge association and resource allocation for cost-efficient hierarchical federated edge learning." IEEE Transactions on Wireless Communications 19, no. 10 (2020): 6535-6548.

[33] Yang, Howard H., Zuozhu Liu, Tony QS Quek, and H. Vincent Poor. "Scheduling policies for federated learning in wireless networks." IEEE transactions on communications 68, no. 1 (2019): 317-333.

[34] Bonawitz, Keith, Vladimir Ivanov, Ben Kreuter, Antonio Marcedone, H. Brendan McMahan, Sarvar Patel, Daniel Ramage, Aaron Segal, and Karn Seth. "Practical secure aggregation for federated learning on user-held data." arXiv preprint arXiv:1611.04482 (2016).

[35] So, Jinhyun, Başak Güler, and A. Salman Avestimehr. "Turbo-aggregate: Breaking the quadratic aggregation barrier in secure federated learning." IEEE Journal on Selected Areas in Information Theory 2, no. 1 (2021): 479-489.

[36] Qiang, Fan, Tong Lixin, and Lv Richard. "White paper-IEEE federated machine learning." (2021): 1-18.

[37] Xu, Jie, Heqiang Wang, and Lixing Chen. "Bandwidth allocation for multiple federated learning services in wireless edge networks." IEEE Transactions on Wireless Communications (2021).

[38] Kang, Jiawen, Zehui Xiong, Dusit Niyato, Shengli Xie, and Junshan Zhang. "Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory." IEEE Internet of Things Journal 6, no. 6 (2019): 10700-10714.

[39] Sarikaya, Yunus, and Ozgur Ercetin. "Motivating workers in federated learning: A stackelberg game perspective." IEEE Networking Letters 2, no. 1 (2019): 23-27.

[40] Zhao, Jie, Xinghua Zhu, Jianzong Wang, and Jing Xiao. "Efficient client contribution evaluation for horizontal federated learning." In ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 3060-3064. IEEE, 2021.

[41] Choquette-Choo, Christopher A., Natalie Dullerud, Adam Dziedzic, Yunxiang Zhang, Somesh Jha, Nicolas Papernot, and Xiao Wang. "CaPC learning: Confidential and private collaborative learning." arXiv preprint arXiv:2102.05188 (2021).

[42] De Alwis, Chamitha, Anshuman Kalla, Quoc-Viet Pham, Pardeep Kumar, Kapal Dev, Won-Joo Hwang, and Madhusanka Liyanage. "Survey on 6G frontiers: Trends, applications, requirements, technologies and future research." IEEE Open Journal of the Communications Society 2 (2021): 836-886.

[43] Mucchi, Lorenzo, Sara Jayousi, Stefano Caputo, Elisabetta Paoletti, Paolo Zoppi, Simona Geli, and Pietro Dioniso. "How 6G technology can change the future wireless healthcare." In 2020 2nd 6G wireless summit (6G SUMMIT), pp. 1-6. IEEE, 2020.

[44] Mothukuri, Viraaji, Reza M. Parizi, Seyedamin Pouriyeh, Yan Huang, Ali Dehghantanha, and Gautam Srivastava. "A survey on security and privacy of federated learning." Future Generation Computer Systems 115 (2021): 619-640.

[45] Wu, Maoqiang, Dongdong Ye, Jiahao Ding, Yuanxiong Guo, Rong Yu, and Miao Pan. "Incentivizing Differentially Private Federated Learning: A Multidimensional Contract Approach." IEEE Internet of Things Journal 8, no. 13 (2021): 10639-10651.

[46] Kerkouche, Raouf, Gergely Acs, Claude Castelluccia, and Pierre Genevès. "Privacy-preserving and bandwidth-efficient federated learning: an application to in-hospital mortality prediction." In Proceedings of the Conference on Health, Inference, and Learning, pp. 25-35. 2021.

[47] Hu, Rui, Yuanxiong Guo, Hongning Li, Qingqi Pei, and Yanmin Gong. "Personalized federated learning with differential privacy." IEEE Internet of Things Journal 7, no. 10 (2020): 9530-9539.

[48] Fereidooni, Hossein, Samuel Marchal, Markus Miettinen, Azalia Mirhoseini, Helen Möllering, Thien Duc Nguyen, Phillip Rieger et al. "SAFELearn: Secure aggregation for private FEderated learning." In 2021 IEEE Security and Privacy Workshops (SPW), pp. 56-62. IEEE, 2021.

[49] Li, Qinbin, Yiqun Diao, Quan Chen, and Bingsheng He. "Federated learning on non-iid data silos: An experimental study." arXiv preprint arXiv:2102.02079 (2021).