PRIVACY-AWARE FEDERATED LEARNING IN HYBRID CLOUD-BASED HEALTH SURVEILLANCE SYSTEMS

Istamov Mirjahon Mo‘minjon ogli

Bahronov Shahzodjon Vahobjon ogli

Isoqov Diyorbek Dilshod ogli

In recent years, artificial intelligence (AI) and data analysis have begun to be widely used in the healthcare sector. However, the uniqueness of medical data lies in its sensitivity and personal nature. For this reason, ensuring confidentiality for information systems used in healthcare has become a top priority. Traditional data collection and centralized training methods pose serious risks to information security. To prevent such problems, solutions based on federated learning and hybrid cloud systems are being developed.

Federated learning is a decentralized machine learning technique that conducts training on local devices without sending users' data to a central server. The model is only sent to the server in the form of updated weights, where it is aggregated.

In medicine, patient information is confidential, and it is necessary to implement security measures when analyzing and making predictions based on it.

Federated training offers the following advantages:

- Maintaining confidentiality: data remains on local devices.
- Reduction in data transmission costs.
- Interoperability: different hospitals can work on a common model.
- High flexibility: the ability to work with data of various formats and from different locations.

A hybrid cloud is an infrastructure that combines private and public cloud technologies. It integrates the advantages of both technologies to create a flexible, cost-effective, and secure system.

Cloud computing servers provide computing resources such as storage, databases, networking, software, and analytics as services over the Internet.

Cloud computing services can be offered in various models, including public, private, and hybrid, each with its own unique advantages and compromises (which are outside the scope of this article).

Cloud enterprises do not have to manage the underlying hardware infrastructure of their applications, allowing them to focus on their core business, leading to faster innovations and growth.

Key advantages of hybrid cloud include data sovereignty and compliance:

Hybrid cloud enables organizations to keep sensitive data stored locally while utilizing cloud resources for less critical workloads.

Legacy system integration: Enterprises can maintain existing local systems while gradually transitioning to cloud-based solutions.

Customized security: Hybrid cloud enables businesses to implement customized security measures for various types of data and applications.

Optimized resource allocation: Organizations can allocate workloads between on-premises and cloud environments based on cost and security requirements.

Medical data, such as patient histories, genetic information, or diagnostic results, can be stored in a private cloud, while the public cloud is used for model computation and testing.

This approach ensures the following:

- Enhances confidentiality and security.
- Allows for rational use of resources.
- Strengthens system integration among various medical institutions.

Differential privacy is a technique that enables user data to be hidden to the extent that it cannot be separated from the model. In federated learning, this technique is applied by adding noise to local model updates.

This guarantees that:

- Individual user data cannot be viewed.
- Although the model is globally beneficial, it does not violate local privacy.

Data is analyzed in encrypted form using homomorphic encryption, and encrypted results are obtained. This is used in federated learning to transmit model weights in a protected manner.

Real-time monitoring systems, such as heart rate, blood pressure, or sugar levels.

Advantages of the federated monitoring system:

- The ability to train the AI model on the medical devices themselves.
- The system continues to operate even in the case of interruptions.

Google Fit and Apple Health applications are attempting to train various SI models federatively based on user personal data. This experience is also being adapted in the healthcare sector.

OpenMined is an open-source federated learning library.

With the help of PySyft, decentralized training systems in healthcare are being developed.

Future Prospects In the future, the following is expected in healthcare systems:

Automated medical diagnosis with the help of artificial intelligence. Expanding medical monitoring capabilities at home.

Creating global health monitoring systems.

Developing universal protocols suitable for federated learning for all medical systems.

Data stored in the cloud can be lost due to hardware failures, human errors, or other technical issues. Data loss is one of the problems encountered in cloud computing. Nowadays, many confidential data leaks are also known as such. It is known that a user's confidential information can fall into the hands of someone else from the platform and that the user does not have full control over their database indicates a threat to their data. Thus, if the security of the cloud service is compromised by hackers, hackers can access the user's confidential information or personal files.

In summary, through federated learning and hybrid cloud technologies in healthcare systems, it is possible to provide not only highly accurate analyses but also complete protection of personal data. Approaches that emphasize privacy are not only a technological but also a moral necessity.

REFERENCES

1. Threats: Concepts, Methodologies, Tools, and Applications: IGI Global, 2018, pp. 268 285

2. C.Vidal and K.K. Choo, “Situatsional Crime Prevention and the Mitigation of Cloud Computing threats”, in International conference on Security and privacy in Communication Systems, 2017: Springer, pp. 218-233

3. Турдиева Г. С. Сетевые атаки и использование защиты от них //Universum: технические науки. – 2022. – №. 2-1 (95). – С. 60-62.

4. Йулдашева, Г., & Йўлдошева, М. (2022). Использования информационных технологий в организациях. Scientific progress, 3(3), 477-480.