AI-Driven Privacy Enhancements in Microservices Architectures

Profile

Dileep Pandiya
Principal Engineer @ZoomInfo

18+ Years of Experience: ZoomInfo, Wayfair, Walmart, IBM

Expertise: Architecting and Design highly available, highly impactful cross industry software solutions.
Sales Technology, Retail, E-commerce

Author, Speaker and Mentor

Briefly.ai

ArchitectGPT

Why Data Privacy Matters Today

- Global Rise in Data Privacy Concerns
- Challenges in Microservices Architectures
- Heightened Risks for Privacy Violations

Credit : Samir Jadhav

Privacy Challenges in Microservices

- Complex Data Flows Across Services
- Lack of Centralized Control
- Increased Attack Surface

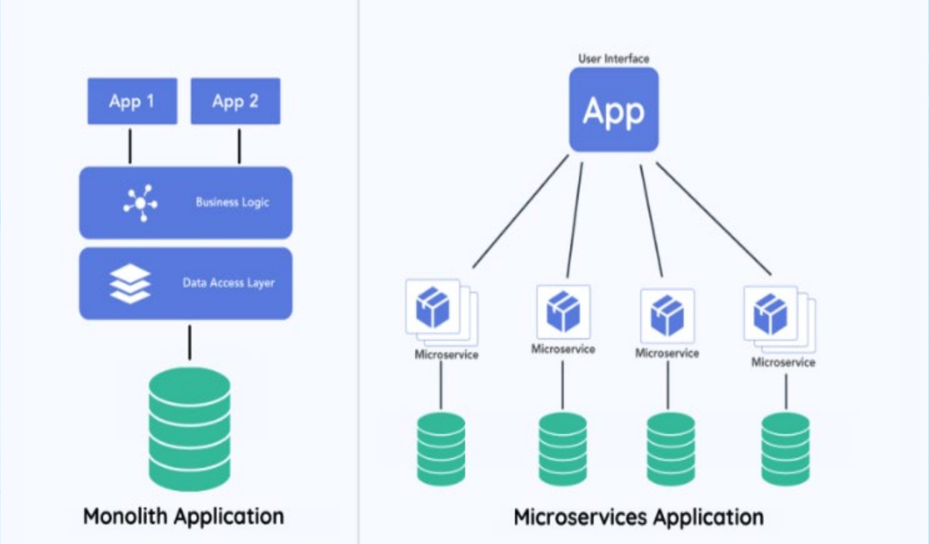
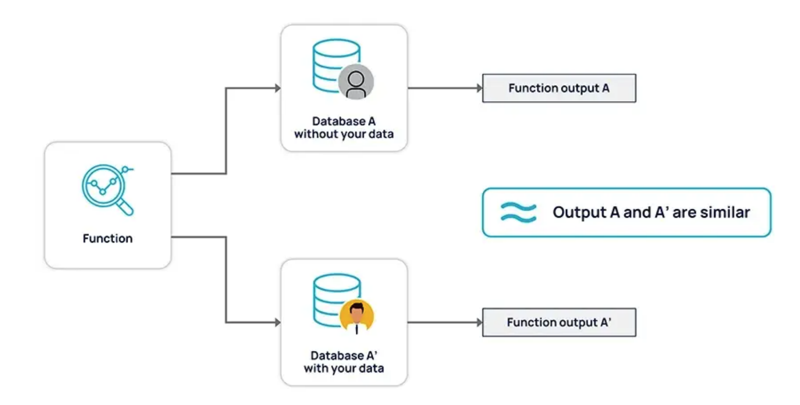


Image: Dev.to

AI for Differential Privacy in Distributed Architectures

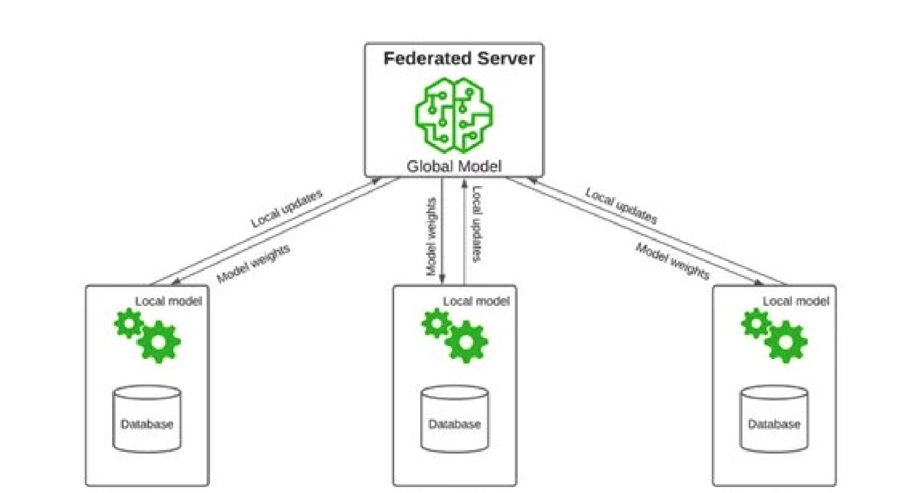
- What is Differential Privacy?
- AI's Role in Managing Differential Privacy
- How Differential Privacy Fits in Microservices
- Deep Learning with Differentially Private SGD (DPSGD), Apple Privacy



Credit : anonos.com

Federated Learning for Privacy

- What is Federated Learning?
- AI's Role in Privacy with Federated Learning
  - Decentralized Training
  - Secure Aggregation
  - Enhanced Privacy with Differential Privacy
- Federated Learning in Microservices Architectures



Credit : sparkd.ai

AI-Driven Data Anonymization in Microservices

- What is Data Anonymization?

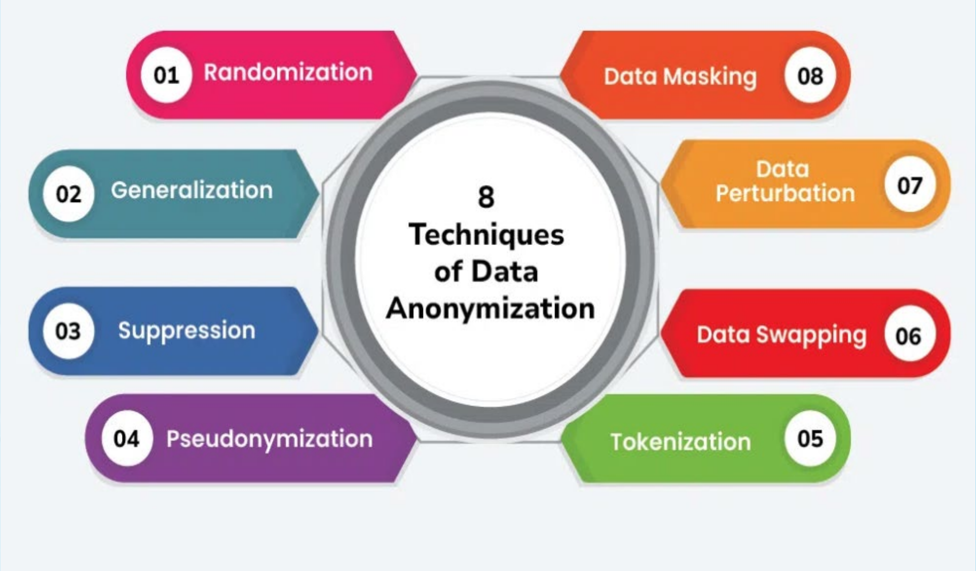
- AI’s Role in Data Anonymization

  - Automated Identification

  - Dynamic Anonymization

  - Scale

- Why Anonymization is Critical for Microservices



Real-Time Privacy Monitoring and Anomaly Detection

- Ensuring Consistent Privacy Compliance
- Spotting and Stopping Problems Fast
- Managing Complexity in Microservices

Automated Privacy Policy Enforcement

- **Ensuring Consistent Privacy Compliance**
  - *Automatic Policy Enforcement*
  - *AI's Precision*
- **Instant Remediation for Privacy Violations**
  - *Continuous Monitoring*
  - *Real-Time Corrections*
- **Handling Complex, Evolving Environments**
  - *Scaling Compliance*
  - *Adaptability to Regulatory Changes*

Conclusion & Key Takeaways

- **AI is Revolutionizing Privacy in Microservices**
  - AI brings **automation, real-time monitoring**, and **adaptive enforcement** of privacy policies, ensuring that microservices architectures stay compliant and secure without manual intervention.
  - These technologies help businesses scale their systems while maintaining high levels of data privacy, reducing risks associated with privacy violations.

- **Critical AI Techniques for Privacy**
  - **Differential Privacy**
  - **Federated Learning**
  - **Data Anonymization**
  - **Real-Time Monitoring and Enforcement**

- **Practical Applications Across Industries**

- **Adopting AI for Privacy Protection**

Thank You!

Email : dileeppandiya@hotmail.com
LinkedIn: https://www.linkedin.com/in/dileeppandiya/