Taking Computation to Data: Integrating Privacy-preserving AI techniques and Blockchain Allowing Secure Analysis of Sensitive Data on Premise

by

Jiahui Geng

Thesis submitted in full satisfaction of
the requirements for the degree
PHILOSOPHIAE DOCTOR (PhD)

Faculty of Science and Technology
Department of Electrical Engineering and Computer Science
September 2023

University of Stavanger
N-4036 Stavanger
NORWAY
www.uis.no

ISBN 978-82-8439-177-9
ISSN 1890-1387

PhD Thesis UiS no. 710

Abstract

With the advancement of artificial intelligence (AI), digital pathology has seen significant progress in recent years. However, the use of medical AI raises concerns about patient data privacy. The CLARIFY project is a research project funded under the European Union's Marie Skłodowska-Curie Actions (MSCA) program. The primary objective of CLARIFY is to create a reliable, automated digital diagnostic platform that utilizes cloud-based data algorithms and artificial intelligence to enable interpretation and diagnosis of whole-slide-images (WSI) from any location, maximizing the advantages of AI-based digital pathology.

My research as an early stage researcher for the CLARIFY project centers on securing information systems using machine learning and access control techniques. To achieve this goal, I extensively researched privacy protection technologies such as federated learning, differential privacy, dataset distillation, and blockchain. These technologies have different priorities in terms of privacy, computational efficiency, and usability. Therefore, we designed a computing system that supports different levels of privacy security, based on the concept: taking computation to data. Our approach is based on two design principles. First, when external users need to access internal data, a robust access control mechanism must be established to limit unauthorized access. Second, it implies that raw data should be processed to ensure privacy and security. Specifically, we use smart contract-based access control and decentralized identity technology at the system security boundary to ensure the flexibility and immutability of verification. If the user's raw data still cannot be directly accessed, we propose to use dataset distillation technology to filter out privacy, or use locally trained model as data agent. Our research focuses on improving the usability of these methods, and this thesis serves as a demonstration of current privacy-preserving and secure computing technologies.

Acknowledgements

I am thrilled to have successfully completed my doctoral thesis, and many memories from my journey are still fresh in my mind. From being accepted into the program to having my first paper accepted and visiting other schools, it has been an incredible experience.

I want to thank my supervisor, Prof. Chunming Rong, for giving me the opportunity to conduct research and guiding me on my research path for the past three years. I am also grateful to Prof. Martin Gilje Jaatun, Prof. Kjersti Engan, and other professors for their academic guidance, as well as Tom Ryen, the head of the department, for his ongoing support. My roommates, Saul Fuster Navarro, Luca Tomasetti, and Neel Kanwal, provided valuable feedback on my articles, and my colleagues, Prachi Vinod Wadatkar, Arian Baloochestani Asl, Thilina Dhanushka Kalahe Pathirana, and others, left me with happy memories of my doctoral life.

I would like to express my gratitude to Marie Curie, who not only demonstrated her brilliance in her time but also provided many students from developing countries with the opportunity to pursue their academic dreams. The Marie Curie program also encouraged me to collaborate across different countries, and I had the opportunity to be seconded to the University of Amsterdam in the Netherlands and the University of Granada in Spain, as well as the Technical University of Munich, Germany. These experiences left a deep impression on me.

I am fortunate to have the support of my wife Qing Li, who made my days brighter. I am deeply grateful to my family and friends for their unwavering support, encouragement, and understanding throughout my Ph.D. journey.

Jiahui Geng, September 2023

Contents

List of Papers

The following papers are included in this thesis:

- **Paper 1**

  OpenIaC: open infrastructure as code-the network is my computer
  Chunming Rong, Jiahui Geng, Thomas J. Hacker, Haakon Bryhni, Martin Gilje Jaatun
  Journal of Cloud Computing 11, no. 1 (2022): 1-13.
  doi = https://doi.org/10.1186/s13677-022-00285-7

- **Paper 2**

  Improved Gradient Inversion Attacks and Defenses in Federated Learning
  Jiahui Geng, Yongli Mou, Qing Li, Feifei Li, Oya Beyan, Stefan Decker, Chunming Rong
  IEEE Transactions on Big Data (2023).
  doi = https://doi.org/10.1109/TBDATA.2023.3239116

- **Paper 3**

  A Survey on Dataset Distillation: Approaches, Applications and Future Directions
  Jiahui Geng Zongxiong Chen, Yuandou Wang Herbert Woisetschläger , Sonja Schimmler, Ruben Mayer, Zhiming Zhao, Chunming Rong

Proceedings of the Thirty-Second International Joint Conference on Artificial Intelligence, IJCAI 2023, 19th-25th August 2023, Macao, SAR, China
doi = https://doi.org/10.24963/ijcai.2023/741

- **Paper 4**

Blockchain Empowered and Self-sovereign Access Control System
Jiahui Geng, Hanif Tadjik, Martin Gilje Jaatun, Chunming Rong
2022 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Bangkok, Thailand, 2022, pp. 74-82
doi = https://doi.org/10.1109/CloudCom55334.2022.00021

- **Paper 5**

Blockchain-based Cross-organizational Workflow Platform
Jiahui Geng, Ali Akbar Rehman, Yongli Mou, Stefan Decker, Chunming Rong
2022 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Bangkok, Thailand, 2022, pp. 74-82
doi = https://doi.org/10.1109/CloudCom55334.2022.00018

Chapter 1

Introduction

1 Research Background

The swift advancement of artificial intelligence (AI) techniques has ignited an innovative era, significantly enhancing efficiency across diverse domains. AI has revolutionized healthcare, enabling precise diagnoses, individualized treatment plans, and optimized resource allocation. Machine learning algorithms can examine vast quantities of medical data, such as electronic health records and medical imaging, identifying patterns and correlations that are challenging for humans to detect. These insights enable early disease detection, like cancer [18, 4], and advance precision medicine [10, 12, 11], greatly improving patient outcomes and overall healthcare efficiency. In finance, AI-driven fraud detection systems [15, 19] can pinpoint suspicious transactions and flag potential security breaches, safeguarding customers and financial institutions from financial losses. AI has also enhanced customer service with the deployment of intelligent chatbots [2], managing routine inquiries and reducing human agents' workload. Machine learning algorithms can also predict consumer preferences and suggest products [21], boosting conversion rates and customer satisfaction.

However, the absence of proper supervision and legal regulations makes it easy for commercial interests to abuse user data. Some privacy data is intentionally or unintentionally leaked, causing in-

calculable harm to users and even the entire country's security. For example, the famous Facebook-Cambridge Analytica data scandal [1] is that Cambridge Analytica, a British consulting company, obtained personal data of millions of Facebook users without their consent and used it for political advertising. In order to protect personal privacy data, many countries and regions are issuing data privacy protection regulations, clarifying the responsibilities and obligations of privacy protection. A key challenge is complying with data protection regulations like GDPR [2], HIPAA [3], and CCPA [4]. Adherence to these regulations can be labor-intensive and resource-demanding, especially for organizations operating in multiple jurisdictions with diverse legal requirements. The increasing reliance on data-driven decision-making across various industries has led to the widespread collection, storage, and analysis of sensitive data. Besides, many industries also restrict entities from sharing customer data externally, creating data silos. In light of this development, privacy-preserving and access control mechanisms have become crucial components for ensuring the ethical and secure handling of sensitive information.

1.1 Challenges of sensitive data analysis

The handling of sensitive data presents various challenges for organizations, stemming from the need to balance data privacy and security with the efficient utilization of information for decision-making. Managing sensitive data presents multiple challenges for organizations aiming to harmonize data privacy, security, and efficient information use for decision-making and innovation.

Data security and breach prevention are also significant challenges. With an evolving threat landscape, organizations must adopt robust cybersecurity measures to defend sensitive data against unauthorized access, breaches, and cyberattacks. This necessitates a proactive security approach, encompassing risk assessments, workforce training,

[1] `https://en.wikipedia.org/wiki/Facebook-Cambridge_Analytica_data_scandal`

[2] `https://gdpr.eu/`

[3] `https://www.hhs.gov/hipaa/index.html`

[4] `https://oag.ca.gov/privacy/ccpa`

and sophisticated encryption and access control methods.

Balancing access and control is another challenge faced by organizations. They must delicately navigate between permitting access to sensitive data for analysis and retaining control over its use. This entails implementing granular access controls, ensuring data traceability, and monitoring data usage to avert unauthorized access or misuse. Achieving the right balance is vital for promoting data-driven innovation while protecting sensitive information.

Maintaining data quality and integrity is crucial for accurate analysis and decision-making. However, it can be challenging due to data silos, inconsistent formats, and potential human errors during data entry and processing. Therefore, organizations must establish data governance frameworks and execute data validation and cleansing procedures to uphold data quality and integrity.

Lastly, sharing sensitive data across organizational boundaries introduces further challenges regarding privacy, security, and trust. Organizations need to develop mutually agreed-upon protocols, legal agreements, and technical solutions to enable secure data sharing while respecting privacy and ownership rights.

1.2 CLARIFY Project

Pathology involves specialists examining biopsies to confirm cancer diagnoses, but traditional methods face issues of subjectivity and discrepancies. Digital pathology addresses these challenges with improved management and interpretation of digitized samples, aided by advancements in scanning, storage, data transfer, and software for high-resolution Whole Slide Images. Digital pathology offers numerous advantages, including simplified case sharing among pathologists, accelerated case tracking, archival and retrieval, and enhanced diagnostic efficiency.

The CLARIFY Project [5] aims to create a multinational, multisectoral, and multidisciplinary doctoral training network to develop expertise in AI, cloud computing, and clinical pathology with a focus on digital pathology. The project will address the existing variability

[5] `http://www.clarify-project.eu/`

in cancer diagnosis by selecting specific and challenging cancer types to test the tools and methods developed by the network as illustrated in Figure 1.1. These cancer types include Triple Negative Breast Cancer (TNBC), High-Risk Non-Muscle Invasive Bladder Cancer (HR-NMIBC), and Spitzoid Melanocytic Lesions (SML).

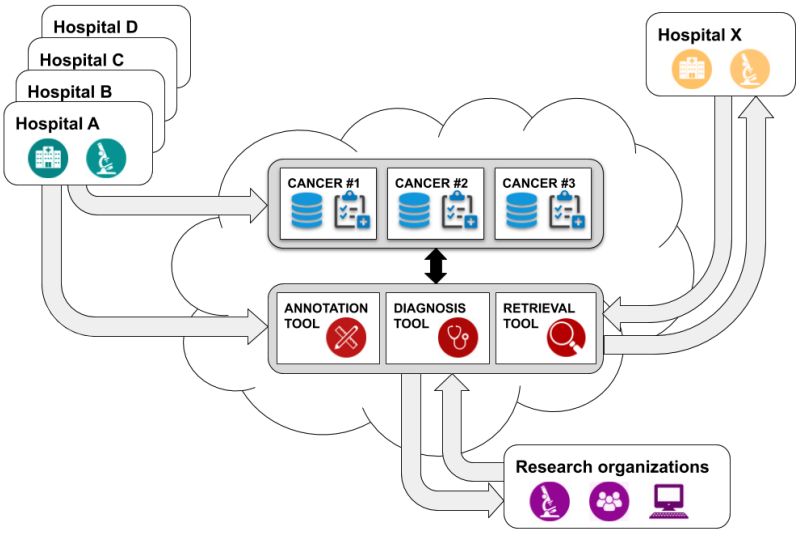


Figure 1.1: Overview of Claify Project.

2 Our Proposal: Trustworthy Open Infrastructure as Code

2.1 Motivation and Vision

In today's hyperconnected world, digital infrastructure underpins every facet of modern life. It is central to business competitiveness, enabling businesses to provide services globally, streamline operations, drive innovation, and adapt to changing market dynamics. For governments, digital infrastructure is vital for delivering public services efficiently, facilitating transparent governance, and fostering economic

growth. For individuals, it serves as a conduit for knowledge, communication, and opportunities, enabling access to education, healthcare, and various services.

The urgency for robust digital infrastructure has been particularly highlighted by the recent global pandemic, which has underscored the importance of connectivity and digital services. The era of digital transformation is upon us. With the rise of cloud computing, virtualization, and distributed systems, traditional methods of managing and provisioning computing infrastructure are being continually challenged. As companies adopt digital technologies at an unprecedented pace, the need for more streamlined, efficient, and robust infrastructure management practices is becoming increasingly apparent. This is where the concept of Infrastructure as Code (IaC) comes into play.

However, while the openness of these systems presents numerous advantages, it also introduces unique challenges, particularly in the domain of trust and security. Trust in Open Infrastructure refers to the confidence in the reliability, security, and ethical use of open-source tools and platforms that underpin the digital infrastructure of organizations. As systems become increasingly interconnected and data flows become more complex, the need for trustworthy open infrastructure becomes ever more critical. It ensures that while businesses leverage the benefits of open-source technologies - such as interoperability, transparency, and collaborative development - they also maintain robust security protocols, protect user data, and uphold ethical standards.

With this motivation, we propose OpenIaC (Open Infrastructure as Code), whose visions mainly include:

(i) Protection of data sovereignty
Establish a classification and classification authorization system for public data, enterprise data and personal data. Innovate new ways to register data property rights. According to the data sources and data generation characteristics, define the legal rights enjoyed by each participant in the process of data production, circulation and use respectively, and establish a property right operation mechanism with the separation of data resource holding right, data processing and use right, and data

product operation right.

(ii) Data access control

Protect data property rights and use data in a compliant manner. Establish a mechanism for the authorization of personal information data rights. Confidential public data will not be opened.

(iii) Strengthen the security and privacy protection in the process of data circulation.

Strengthen the convergence, sharing and open development, promote interconnection and interoperability, and break the "data silos". Encourage public data to protect personal privacy and ensure public security, in accordance with the requirements of "original data not out of the domain, data available but not visible", to provide the community with models, verification and other products and services. Innovative technical means to promote the anonymization and privacy of information processing.

(iv) Enabling federated computing

Federated computing involves the collaboration of multiple entities with a shared objective, emphasizing decentralized processing of hardware resources and data from diverse organizations. It enables efficient utilization of distributed workflows, where tasks are performed locally on devices or servers, rather than consolidating data centrally. This approach provides flexibility and customization options for real-world scenarios, unlike federated learning, which is limited to homogeneous data tasks. Notably, federated computing facilitates model iterations by different organizations, allowing continuous evolution and improvement through diverse datasets and expertise. This iterative process fosters efficient collaboration while safeguarding privacy by exchanging model updates instead of raw data. Furthermore, federated computing reduces reliance on centralized infrastructure, minimizes data transfers, and optimizes bandwidth utilization, making it well-suited for critical sectors like

healthcare, finance, telecommunications, and IoT, where privacy concerns and collaborative efforts among multiple organizations are paramount.

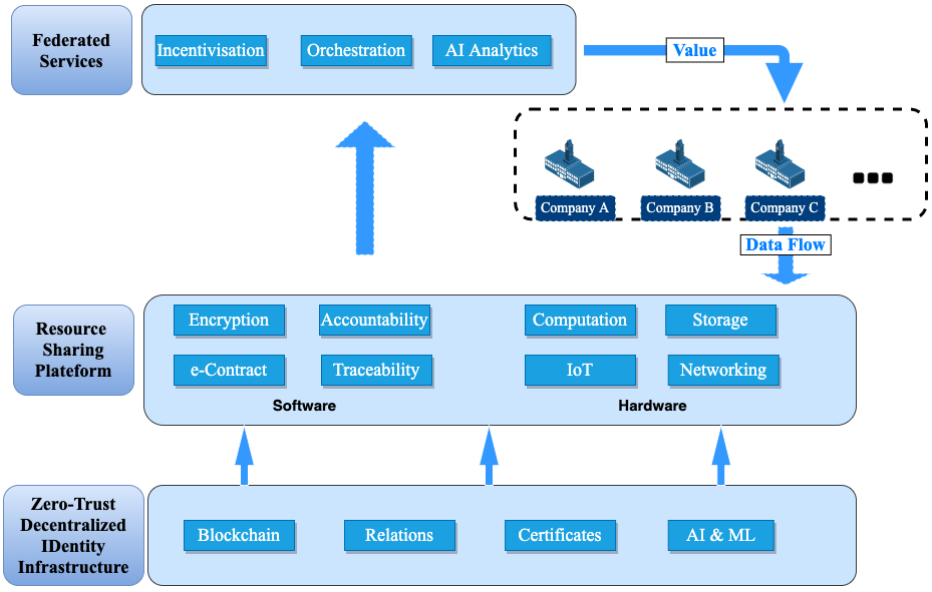


Figure 1.2: The vision of OpenIaC.

Figure 1.2 shows how OpenIaC builds open infrastructure and facilitates data flow between different entities. Based on a zero-trust network and a decentralized identity system, all services need to be developed on shared resources. The middle layer is a resource sharing platform. The general functions that need to be implemented include software and hardware resources to ensure cryptography, auditability and traceability. AI, incentives, and service orchestration will accelerate the flow and mutual transformation of data and value. IaC authorizes all computing resources, and preparation can be done through code.

OpenIaC is currently undergoing organized development, with updates on the project's progress available on the official website. For a more comprehensive understanding of the concept, interested individuals can refer to Prof. Chunming Rong's enlightening talk at TEDxYouth@Breiavatnet. Notably, the OpenIaC organization

successfully conducted a workshop at IEEE CloudCom 2022, further contributing to the project's growth and advancement. Figure 1.3 is the official logo for OpenIaC.

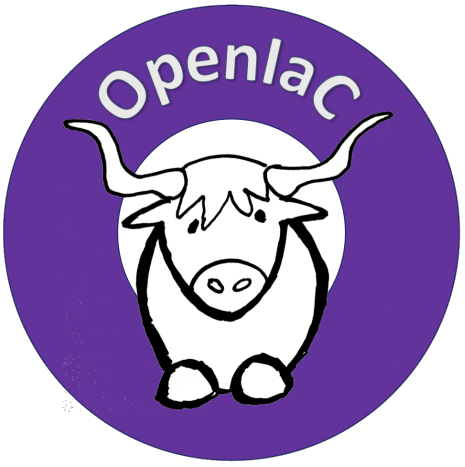


Figure 1.3: The logo of OpenIaC.

2.2 Research Objective and Questions

OpenIaC is an ambitious initiative that integrates diverse knowledge and technologies, such as virtualized resource management, identity and access management, IoT, artificial intelligence, and networking. Its future applications extend beyond the smart digital pathology domain outlined in the CLARIFY project, aiming to establish a comprehensive open platform. The realization of this vision relies on active participation from the entire community. In my doctoral research, I have primarily concentrated on enhancing privacy and security aspects within OpenIaC. To address these concerns, I will specifically investigate the following research questions:

(i) **RQ1: How to build machine learning systems that bring computation to data to preserve privacy?**
The landscape of privacy protection technologies is vast and diverse, with numerous methods and approaches designed to

safeguard sensitive information. In order to develop a comprehensive understanding of these privacy protection technologies, it is crucial to explore their respective advantages and disadvantages, as well as the limitations and capabilities they possess. To achieve this goal, different privacy protection technologies such as federated learning, differential privacy, dataset distillation, and blockchain need to be explored and comprehensively utilized.

(ii) **RQ2: How to achieve the balance between data utility and data privacy?**
Achieving a balance between data utility and data privacy is a critical challenge that organizations and researchers must address to fully leverage data-driven insights while protecting sensitive information.

Given that the CLARIFY project is primarily focused on the aided analysis of medical images, special attention must be paid to privacy protection technologies specifically tailored to image data. Medical image data often contains sensitive information about patients, and maintaining the confidentiality and integrity of such data is of paramount importance. As we delve into the image-related privacy protection technologies, we will consider various factors such as computational efficiency, scalability, and the level of privacy protection provided.

(iii) **RQ3: How to build blockchain system with flexible access control mechanism with trustworthy traceability?**
Data sovereignty is a crucial aspect of data security and privacy, emphasizing the rights of data owners to control the use and scope of their data. As a decentralized and immutable ledger, blockchain provides a transparent and secure way to store and track transactions. By utilizing smart contracts, blockchain can automate the enforcement of data usage policies and permissions. To address the challenges of securely sharing data and models within the CLARIFY project, it is essential to explore efficient ways of integrating blockchain technology with machine learning systems.

In summary, we will explore various methodologies to address privacy concerns, evaluating their effectiveness and suitability for different scenarios throughout the course of our research. By developing a deeper understanding of the complexities involved in creating a secure, privacy-focused data analysis system, we hope to contribute valuable knowledge and insights to the field, paving the way for more robust and efficient solutions in the future.

2.3 Prototype

Our research proposal introduces a prototype, as illustrated in Figure 1.4, designed to safeguard user data within a defined security perimeter. This approach addresses two primary federated computing needs: enabling external users to perform calculations on local infrastructure and sharing the value of user data beyond this boundary. This solution utilizes cryptography and machine learning technologies, specifically focusing on blockchain and decentralized identity application, as well as privacy-centric data value sharing via federated learning and dataset distillation.

In our OpenIaC framework, all users and data assets are catalogued in a blockchain ledger, capitalizing on its decentralization, transparency, and security for data management and sharing. Blockchain's inherent qualities such as unalterability and traceability provide a robust foundation for data provenance and integrity. Smart contracts enhance this by controlling access and enforcing data usage policies in line with regulations and organizational standards. Decentralized identity, an integral part of our system, ensures secure identities, promotes efficient cross-organizational collaboration, and tackles intricate data privacy and sovereignty issues. Data classification according to privacy and security needs is essential during its utilization. For sensitive data, processed information can be disseminated using techniques like dataset distillation and differential privacy, which sieve out sensitive details. Alternatively, the model can be used as a go-between, sharing itself instead of raw data, a tactic synonymous with federated learning, thereby ensuring data exchange while maintaining privacy and security.

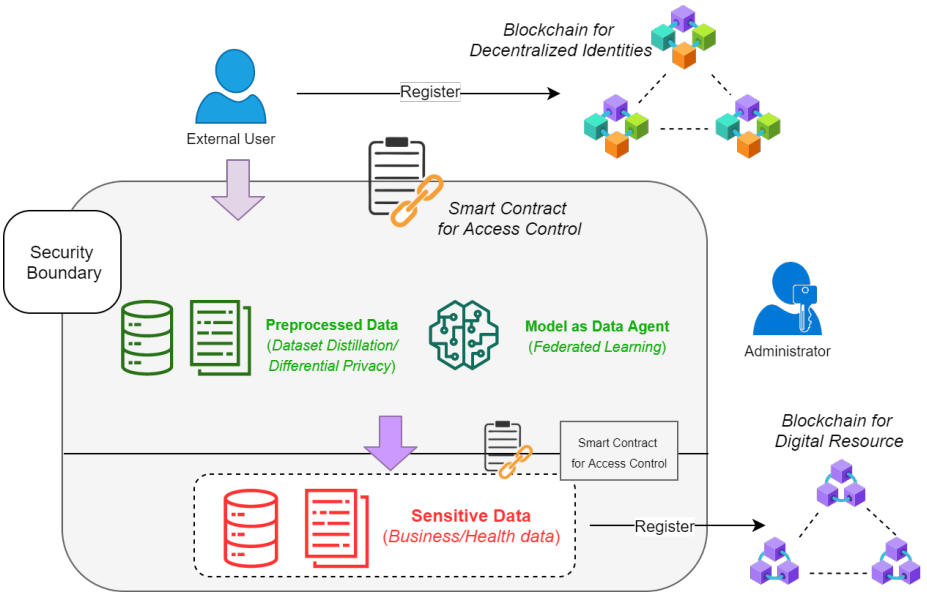


Figure 1.4: Prototype of OpenIaC

2.4 Research Publications

The content of this thesis is based on a number of papers. Some of these have been published, while others are currently under review. We list the publications that are directly relevant to this thesis below. The connection between research questions and publications is shown in Figure 1.5.

(i) **Geng, J., Mou, Y., Li, F., Li, Q., Beyan, O., Decker, S. and Rong, C., 2023, Improved Gradient Inversion Attacks and Defenses in Federated Learning. Published in IEEE Transactions on Big Data.**[8]
In this article, we investigate the gradient inversion attack in federated learning and propose a new attack method that includes zero-shot batch label inference and fidelity regularization techniques. Our approach can restore more details of training samples from gradient information. We extend our attack scenario to include shared model weights. We also propose some effective defense methods based on our experiments. Our

approach is simple and effective and does not compromise the model's utilization.

(ii) **J. Geng et al. A Comprehensive Study on Dataset Distillation: Performance, Privacy, Robustness and Fairness. Submitted to IEEE Transactions on Information Forensics and Security.[3]**
Dataset distillation is a promising technique that aims to reduce model training costs by learning from a smaller yet informative dataset. However, while many techniques have been proposed, most focus on improving the performance of new datasets and optimizing computational efficiency, with limited research on the security of this technology. In this article, we constructed a benchmark to evaluate the current mainstream dataset methods in terms of privacy, robustness, and fairness. Our research shows that when the compression rate is low, this method can be vulnerable to membership inference attacks, and the model may experience varying degrees of accuracy reduction across different categories.

(iii) **J. Geng et al. A Survey on Dataset Distillation: Approaches, Applications and Future Directions. Accepted by 2023 International Joint Conference on Artificial Intelligence (IJCAI 2023).[5]**
While there have been significant advancements in dataset distillation, there is currently no comprehensive overview available that summarizes its applications and progress. To address this gap, our paper presents a taxonomy of dataset distillation. Our survey aims to fill this void by first proposing a systematic taxonomy of dataset distillation, which characterizes existing approaches. We then provide a thorough review of the data modalities and related applications. Additionally, we highlight the challenges that researchers face in this field and discuss possible future directions for research.

(iv) **Mou, Y., Geng, J., Zhou, F., Beyan, O., Rong, C., Decker, S. (2023). pFedV: Mitigating Feature Distribution Skewness via Personalized Federated Learning with Variational Distribution Constraints. Published in The 27th Pacific-Asia Conference**

on Knowledge Discovery and Data Mining (PAKDD 2023).[14]
The statistical heterogeneity among the data sources, known as non-IID, is a common challenge that can lead to a performance degradation in federated learning. In this paper, we introduce pFedV, which leverages a variational inference approach by incorporating a variational distribution into neural networks and adding a KL-divergence term to the loss function during training. This approach constrains the output distribution of layers for feature extraction and personalizes the final layer of models. Our experimental results demonstrate the effectiveness of pFedV in mitigating feature distribution skewness in federated learning.

(v) **Geng, J., Kanwal, N., Jaatun, M.G. and Rong, C., 2021. Did-efed: Facilitating federated learning as a service with decentralized identities. Published in Evaluation and Assessment in Software Engineering (pp. 329-335).[6]**
We introduce DID-eFed, a Federated Learning as a Service (FLaaS) system that uses decentralized identities (DID) and a smart contract to facilitate FL. DID enables flexible and credible decentralized access management, while the smart contract streamlines the process and minimizes errors. We describe a scenario where DID-eFed enables FLaaS among hospitals and research institutions. Our proposed system provides a promising solution to the challenges of FLaaS in terms of privacy, security, and usability.

(vi) **Cantu, A., Geng, J. and Rong, C., 2022, December. NFT as a proof of Digital Ownership-reward system integrated to a Secure Distributed Computing Blockchain Framework. Published in 2022 IEEE International Conference on Cloud Computing Technology and Science (CloudCom) (pp. 97-104). IEEE.[1]**
This paper presents a blockchain-based infrastructure solution that enables companies to securely transmit and share information using the latest encryption and data storage technologies. The infrastructure converts unique digital assets into

non-fungible tokens (NFTs) to provide a trusted method of sharing data. By using a peer-to-peer file storage system called IPFS, and connecting all related elements through the application of the web. We demonstrate the feasibility and scalability of the proposed system.

(vii) **Rong, C., Geng, J. and Jaatun, M.G., 2022, December. Managing Digital Objects with Decentralised Identifiers based on NFT-like schema. Published in 2022 IEEE International Conference on Cloud Computing Technology and Science (CloudCom) (pp. 246-251). IEEE.[17]**
This paper proposes a new scheme that resembles Non-Fungible Tokens (NFT) and uses metadata to convert digital assets into digital object identifiers. The proposed scheme transforms digital objects requiring clear sovereignty into NFTs to ensure authenticity and unique ownership. Our scheme enables dynamic management of digital objects using smart contracts, providing a secure and efficient method for managing digital assets.

(viii) **Geng, J., Tadjik, H., Jaatun, M.G. and Rong, C., 2022, December. Blockchain Empowered and Self-sovereign Access Control System. Published in 2022 IEEE International Conference on Cloud Computing Technology and Science (CloudCom) (pp. 74-82). IEEE.[20]**
This paper presents the Self-Sovereign Identity-based, Decentralized, and Dynamic (SSIDD) access control system that uses blockchain technology to establish trust in untrusted data sharing networks while preserving user privacy. SSIDD authenticates users based on their Decentralized Identifiers (DID), which users control and can be resolved into a DID document stored on the blockchain. Smart contracts enable dynamic authorization processes, ensuring transparency in rules and agreements and traceability of records on the blockchain ledger.

(ix) **Rong, C., Geng, J., Hacker, T.J., Bryhni, H. and Jaatun, M.G., 2022. OpenIaC: open infrastructure as code-the network is my computer. Published in Journal of Cloud Computing,**

11(1), pp.1-13.[16]
This paper presents Open Infrastructure as Code (OpenIaC), an innovative approach that integrates advances in cloud computing and blockchain to address the needs of modern information architectures. OpenIaC provides a common open forum for building services based on the principles of Zero Trust Architecture (ZTA) among a federation of connected resources based on Decentralized Identity (DID). The main mission of OpenIaC is to enable secure and decentralized access to resources, ensuring trust and privacy in information architectures.

(x) **Mou, Y., Geng, J., Welten, S., Rong, C., Decker, S. and Beyan, O., 2022, February. Optimized Federated Learning on Class-Biased Distributed Data Sources. Published in Machine Learning and Principles and Practice of Knowledge Discovery in Databases: International Workshops of ECML PKDD 2021, Virtual Event, September 13-17, 2021, Proceedings, Part I (pp. 146-158). Cham: Springer International Publishing.[13]**
Federated learning often experiences performance degradation when training on non-i.i.d. data across participants, as opposed to centralized approaches. The class imbalance problem is a common issue in practical machine learning that leads to poor prediction on minority classes. To address this problem, we propose FedBGVS, which leverages a balanced global validation set to alleviate class bias severity. We refine the model aggregation algorithm using the Balanced Global Validation Score (BGVS). We evaluate our methods on classical benchmark datasets, such as MNIST, SVHN, and CIFAR-10, as well as a public clinical dataset, ISIC-2019.

(xi) **Geng, J., Rehman, A.A., Mou, Y., Decker, S. and Rong, C., 2022, December. Blockchain-based Cross-organizational Workflow Platform. Published in 2022 IEEE International Conference on Cloud Computing Technology and Science (CloudCom) (pp. 53-59). IEEE.[9]**
Organizations are increasingly adopting data-centric workflows, but traditional approaches often centralize data from different

organizations to the cloud, which can compromise data privacy and security. To address this challenge, we propose a workflow platform that allows for consuming distributed data while empowering data owners with control of their own data. Our platform leverages Kubernetes and JupyterFlow, and integrates blockchain technology to ensure security and privacy. The distributed ledger contains meta-data referring to the data in off-chain storage, reducing replication and network throughput. We also developed a JupyterHub extension to support data registration and query, and a RESTFul API to connect the web application with the blockchain network.

(xii) **Geng, J., Mou, Y., Li, F., Li, Q., Beyan, O., Decker, S. and Rong, C., 2021. Towards general deep leakage in federated learning. Published in International Workshop on Trustable, Verifiable, and Auditable Federated Learning in Conjunction with AAAI (Vol. 2022).[7]**
Federated learning (FL) offers an alternative to traditional central training by sharing and aggregating local models, rather than local data, to protect users' privacy and improve the performance of the global model. However, research has shown that attackers can still reconstruct private data using the shared gradient information, posing a security threat to FL. This on-the-fly reconstruction attack is a critical concern as it can occur at any stage of training, without requiring any relevant dataset or additional models to be trained. To address this challenge, we break through some of the unrealistic assumptions and limitations and extend the applicability of this reconstruction attack to a broader range of scenarios.

3 Thesis Outline

The rest part of this thesis is organized as follows. Chapter 2 presents the background of research and methodologies. Chapter 3 details demonstrates main research work during my Ph.D. program, the interrelationships between the different publications and how they

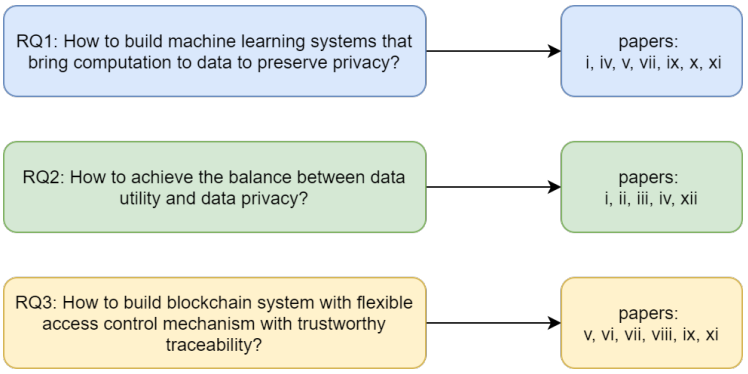


Figure 1.5: Relations between research questions and publications.

serve my research objectives. Chapter 4 concludes the thesis and discusses the potential future works. Five selected papers are available at the end of this thesis.

References

[1] Asahi Cantu, Jiahui Geng, and Chunming Rong. "NFT as a proof of Digital Ownership-reward system integrated to a Secure Distributed Computing Blockchain Framework." In: *2022 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*. IEEE. 2022, pp. 97–104.

[2] Hongshen Chen, Xiaorui Liu, Dawei Yin, and Jiliang Tang. "A survey on dialogue systems: Recent advances and new frontiers." In: *Acm Sigkdd Explorations Newsletter* 19.2 (2017), pp. 25–35.

[3] Zongxiong Chen, Jiahui Geng, Herbert Woisetschlaeger, Sonja Schimmler, Ruben Mayer, and Chunming Rong. "A Comprehensive Study on Dataset Distillation: Performance, Privacy, Robustness and Fairness." In: *arXiv preprint arXiv:2305.03355* (2023).

[4] Özgün Çiçek, Ahmed Abdulkadir, Soeren S Lienkamp, Thomas Brox, and Olaf Ronneberger. "3D U-Net: learning dense volumetric segmentation from sparse annotation." In: *Medical Image Computing and Computer-Assisted Intervention–MICCAI 2016:*

19th International Conference, Athens, Greece, October 17-21, 2016, Proceedings, Part II 19. Springer. 2016, pp. 424–432.

[5] Jiahui Geng, Zongxiong Chen, Yuandou Wang, Herbert Woisetschlaeger, Sonja Schimmler, Ruben Mayer, Zhiming Zhao, and Chunming Rong. "A Survey on Dataset Distillation: Approaches, Applications and Future Directions." In: *arXiv preprint arXiv:2305.01975* (2023).

[6] Jiahui Geng, Neel Kanwal, Martin Gilje Jaatun, and Chunming Rong. "DID-eFed: Facilitating Federated Learning as a Service with Decentralized Identities." In: *Evaluation and Assessment in Software Engineering*. 2021, pp. 329–335.

[7] Jiahui Geng, Yongli Mou, Feifei Li, Qing Li, Oya Beyan, Stefan Decker, and Chunming Rong. "Towards general deep leakage in federated learning." In: *arXiv preprint arXiv:2110.09074* (2021).

[8] Jiahui Geng, Yongli Mou, Qing Li, Feifei Li, Oya Beyan, Stefan Decker, and Chunming Rong. "Improved Gradient Inversion Attacks and Defenses in Federated Learning." In: *IEEE Transactions on Big Data* (2023).

[9] Jiahui Geng, Ali Akbar Rehman, Yongli Mou, Stefan Decker, and Chunming Rong. "Blockchain-based Cross-organizational Workflow Platform." In: *2022 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*. IEEE. 2022, pp. 53–59.

[10] John Jumper, Richard Evans, Alexander Pritzel, Tim Green, Michael Figurnov, Olaf Ronneberger, Kathryn Tunyasuvunakool, Russ Bates, Anna Potapenko, et al. "Highly accurate protein structure prediction with AlphaFold." In: *Nature* 596.7873 (2021), pp. 583–589.

[11] Neel Kanwal, Roger Amundsen, Helga Hardardottir, Emiel AM Janssen, and Kjersti Engan. "Detection and localization of melanoma skin cancer in histopathological whole slide images." In: *arXiv preprint arXiv:2302.03014* (2023).

[12] Neel Kanwal, Fernando Pérez-Bueno, Arne Schmidt, Kjersti Engan, and Rafael Molina. "The Devil is in the Details: Whole Slide Image Acquisition and Processing for Artifacts Detection, Color Variation, and Data Augmentation: A Review." In: *IEEE Access* 10 (2022), pp. 58821–58844.

[13] Yongli Mou, Jiahui Geng, Sascha Welten, Chunming Rong, Stefan Decker, and Oya Beyan. "Optimized Federated Learning on Class-Biased Distributed Data Sources." In: *Machine Learning and Principles and Practice of Knowledge Discovery in Databases: International Workshops of ECML PKDD 2021, Virtual Event, September 13-17, 2021, Proceedings, Part I*. Springer. 2022, pp. 146–158.

[14] Yongli Mou, Jiahui Geng, Feng Zhou, Oya Beyan, Chunming Rong, and Stefan Decker. "pFedV: Mitigating Feature Distribution Skewness via Personalized Federated Learning with Variational Distribution Constraints." In: *Advances in Knowledge Discovery and Data Mining*. Springer Nature Switzerland, 2023, pp. 283–294.

[15] Eric WT Ngai, Yong Hu, Yiu Hing Wong, Yijun Chen, and Xin Sun. "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature." In: *Decision support systems* 50.3 (2011), pp. 559–569.

[16] Chunming Rong, Jiahui Geng, Thomas J Hacker, Haakon Bryhni, and Martin Gilje Jaatun. "OpenIaC: open infrastructure as code – the network is my computer." In: *Journal of Cloud Computing* 11.1 (2022), pp. 1–13.

[17] Chunming Rong, Jiahui Geng, and Martin Gilje Jaatun. "Managing Digital Objects with Decentralised Identifiers based on NFT-like schema." In: *2022 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*. IEEE. 2022, pp. 246–251.

[18] Olaf Ronneberger, Philipp Fischer, and Thomas Brox. "U-net: Convolutional networks for biomedical image segmentation." In: *Medical Image Computing and Computer-Assisted Intervention–MICCAI 2015: 18th International Conference, Munich, Germany, October 5-9, 2015, Proceedings, Part III 18*. Springer. 2015, pp. 234–241.

[19] Iqbal H Sarker, Md Hasan Furhad, and Raza Nowrozy. "Ai-driven cybersecurity: an overview, security intelligence modeling and research directions." In: *SN Computer Science* 2 (2021), pp. 1–18.

[20] Hanif Tadjik, Jiahui Geng, Martin Gilje Jaatun, and Chunming Rong. "Blockchain Empowered and Self-sovereign Access Control System." In: *2022 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*. IEEE. 2022, pp. 74–82.

[21] Shuai Zhang, Lina Yao, Aixin Sun, and Yi Tay. "Deep learning based recommender system: A survey and new perspectives." In: *ACM computing surveys (CSUR)* 52.1 (2019), pp. 1–38.

Chapter 2

Background

1 Machine Learning Security and Privacy

With the popularity of machine learning systems, understanding the potential security and privacy attacks is crucial for individuals and organizations alike. In this section, I will introduce some basics of machine learning security and privacy, including common attack and defense methods.

1.1 Security and Privacy Attacks

Attacks can be categorized based on the target: security attacks, where the attacker aims to compromise the machine learning model by forcing it to make incorrect predictions, and privacy attacks, where the attacker attempts to infer the user's input data during either the training or inference phase.

Security Attacks

Based on their targets, security attacks can be categorized into three types: backdoor attacks, robustness attacks, and evasion attacks. Backdoor and evasion attacks both aim to hijack the model to make predictions according to the attacker's intention. Evasion attacks occur during the reasoning phase of the model, while backdoor and robustness attacks occur during the training phase, often using poisoned

data.

- Backdoor Attacks
  Backdoor attacks [20], also known as targeted attacks, involve embedding a backdoor in the model during the training process. In the inference process, the attacker can activate the backdoor by using a pre-set trigger. When the backdoor is not activated, the attacked model behaves similarly to a normal model. However, when the backdoor is triggered, the attacked model outputs results according to the attacker's intent.

- Robustness Attacks
  Robustness attacks, also known as untargeted attacks, aim to disrupt the functionality of a machine learning model with minimal cost, rendering it poorly trained and unable to perform effectively during the inference stage.

  Data poisoning is a common method in robustness attack where an attacker intentionally modifies the training data used to train a machine learning model to make it behave incorrectly. Data poisoning attacks can be carried out in various ways, such as by introducing incorrect or misleading data into the training dataset or by altering the existing data. For instance, an attacker may add malicious data to the training dataset that can cause the model to misclassify or misinterpret information during the inference.

- Evasion Attacks
  In evasion attacks [4], the attacker manipulates the input data to evade detection or classification, with the aim of tricking the model into making incorrect predictions or classifications. The attacker achieves this by adding small perturbations, or noise, to the original data, which can cause the machine learning model to misclassify the input. For instance, an attacker may subtly alter an image to make the model classify it as a different object.

Privacy Attacks

Privacy attacks in machine learning are a type of security attack that seeks to compromise the confidentiality and privacy of sensitive data used to train a model. These attacks aim to extract confidential information, including personal information, trade secrets, or sensitive data, from the model without authorization or knowledge.

- Membership Inference Attacks
  Membership inference attacks [31] are designed to identify whether a specific user or data record exists in a training dataset. These attacks usually assume that the attacker has access to some of the training data or data related to the training task.

- Data Reconstruction Attacks
  Data reconstruction attacks have two main goals: the first is to obtain users' private information directly, such as reconstructing their training data and labels [37, 38, 12, 13]. The second goal is to infer certain attributes of the training data that are unrelated to the task, but may inadvertently leak out [24, 15].

- Model Stealing Attacks
  Model stealing attacks [33] involve an attacker attempting to recreate a machine learning model that has been trained by someone else. This can be done by querying the model and using the responses to train a new model.

1.2 Common Protection Methods

Differential Privacy

Differential Privacy is a widely used privacy-enhancing technology that is based on information theory and probability theory. It provides a method for maximizing the accuracy of statistical database queries while minimizing the ability to identify individual query records. The concept of Differential Privacy was first proposed by Cynthia Dwork and others in 2006 [10]. Unlike previous privacy protection solutions such as K-Anonymity [32], L-Diversity [22], and T-Closeness [19], the main contribution of Differential Privacy is to provide a mathematical

definition of personal privacy leakage. Differential Privacy aims to provide maximum query result usability while ensuring that personal privacy leakage does not exceed a predetermined threshold.

Definition 1 (Differential Privacy)**.** *A random mechanism M provides (ϵ, δ)-differential privacy if for any two adjacent (only one record is different) data sets $x, x'$for any output set S, there should be:*

$$Pr[M(x) \in S] \leq \exp^{\epsilon} Pr[M(x') \in S] + \delta,$$

where ϵ is the privacy budget, representing probability of information accidentally being leaked.

Definition 2 (Sensitivity)**.** *If function f represents a mapping from a set to a numerical value, then the sensitivity Δf of this function can be defined as:*

$$\Delta f = max_{D,D'} \|f(D) - f(D')\|$$

where D and D' be two adjacent data sets (i.e., they differ by one individual's data point), and $\|\cdot\|$ is a norm function (e.g., L1-norm, L2-norm) that measures the distance between two vectors.

Differential Privacy for Deep Learning DP-SPG [1] and PATE [28] are two privacy-preserving machine learning algorithms used to protect sensitive data during the training process. DP-SPG, or Differentially Private Stochastic Proximal Gradient Descent, is a privacy-preserving optimization algorithm that employs differential privacy techniques to protect the privacy of sensitive data. It works by adding noise to the gradient of the model parameters during the training process to ensure that the privacy of each individual data point is preserved. On the other hand, PATE, or Private Aggregation of Teacher Ensembles, is a privacy-preserving machine learning algorithm that uses a teacher-student model to protect sensitive data. It involves training multiple models, known as teachers, on different subsets of the data and then aggregating the output of these models to form a single model, known as the student model. This aggregation process helps to protect the privacy of the sensitive data by preventing any single model from having access to the entire dataset. Additionally,

PATE uses differential privacy techniques to ensure that the aggregation process does not reveal sensitive information about individual data points.

Secure Multi-party Computation

Secure multi-party computation (SMPC) is a universal cryptographic primitive first proposed by Andrew Yao [36]. It enables computations to be distributed among multiple parties without revealing their original input data to each other. SMPC protocols allow data scientists and analysts to perform compliant, secure, and private computations on distributed data without exposing or moving the data. SMPC includes several branches, with current cryptography techniques such as oblivious transfer [18], garbled circuits [3], and secret sharing [17].

Secret-Sharing Secret-sharing (SS) is an important branch of modern cryptography, and a fundamental applied technology in multi-party secure computation and federated learning, as well as a crucial means for information security and data confidentiality. In practical applications, it plays a significant role in key management, digital signatures, identity authentication, error-correcting codes, bank network management, and data security. Secret-sharing was first proposed by Shamir [30], with the idea of dividing a secret into appropriate shares, where each share is managed by a different participant, and no single participant can recover the secret information alone. It requires collaboration between several participants to restore the secret message. Importantly, the secret can still be fully recovered even if some participants are not able to participate in the process within a certain range.

Shamir's secret sharing is an ideal (t, n)-threshold scheme, in which a secret S is divided into n data fragments, denoted as $S_1, S_2, ..., S_n$, known as secret shares. The scheme requires:

(i) Any t or more shares can be used to reconstruct the secret S.

(ii) Any $t-1$ or fewer shares reveal no information about the secret S.

The scheme is based on the Lagrange interpolation theorem, which states that t coordinate points are sufficient to determine a polynomial of degree less than or equal to $t-1$. For example, two points are sufficient to determine a line, three points are sufficient to determine a parabola, and four points are sufficient to determine a cubic curve, as shown in Figure2.1:

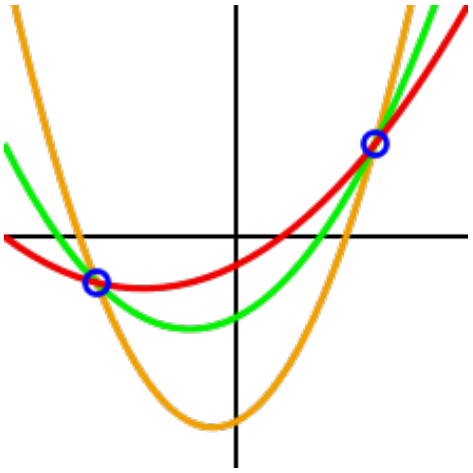


Figure 2.1: An infinite number of quadratic polynomials can be drawn through two points in the plane, but there is only one quadratic polynomial through three points.

Assuming that the secret S can be expressed as an element a_0, randomly select $t-1$ elements $a_1, a_2, \cdots, a_{t-1}$ to construct a polynomial:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots a_{t-1} x^{t-1}$$

Assume that t points are randomly selected on the polynomial curve, and the coordinates are: (x_i, y_i). Then in any subset of these points containing t points, and a_0 can be obtained by interpolation calculation:

$$a_0 = f(0) = \sum_{j=0}^{t-1} y_j \sum_{m=0, m\neq j}^{t-1} \frac{x_m}{x_m - x_j}$$

Based on the above principle, we can represent the Shamir's secret sharing scheme as two fundamental protocols.

- Secret Split Protocol

$$SS.share(S, t, U) = \{(u, S_u)\}_{u \in U}, \tag{2.1}$$

where the input S is the secret, U is the set of users, corresponding to the total number n of all users in the system, and t is the threshold of secret sharing.

- Secret Reconstruction Protocol

$$SS.recon(\{(u, S_u)\}_{u \in V}, t) \rightarrow S, \tag{2.2}$$

where the input $\{(u, S_u)\}_{u \in V}$ is the subset of secret shares, with $\|V\| \geq t$.

Homomorphic Encryption

Homomorphic Encryption (HE) is an encryption technique that allows specific algebraic operations to be performed on ciphertext, resulting in encrypted results that can be decrypted to the same result as if the operations were performed on plaintext. In other words, this technology enables operations such as searching and comparing to be performed on encrypted data, producing correct results without the need to decrypt the data during the entire processing. Its significance lies in fundamentally solving the confidentiality problem of delegating data and its operations to third parties, such as various cloud computing applications, including encrypted search, electronic voting, and multi-party computation. Currently emerging homomorphic encryption schemes can be divided into three types: partially homomorphic encryption (PHE) [25, 27], somewhat homomorphic encryption (SHE)[11] and fully homomorphic encryption (FHE) [14]. PHE supports one operation, such as addition or multiplication, on encrypted data, SHE supports a limited number of operations, and FHE supports an unlimited number of operations on encrypted data. Each scheme has its advantages and limitations, and the choice of which scheme to use depends on the specific application requirements and computational resources available.

2 Federated Learning

2.1 Federated Learning Basics

Federated learning was first proposed by a Google research group who pioneered the use of this technique to update language prediction models on smartphones [16]. Gboard users receive suggested word prediction from the model optimized based on not only the data stored on individual smartphones, but also on data from all smartphones using a technique called federated averaging (FedAvg [23]. The process does not require transferring data from any edge devices to a central server, as the models on each mobile device (such as a smartphone or tablet) are encrypted and uploaded to the cloud through federated learning. Finally, all encrypted models are aggregated into a global encrypted model, and the server in the cloud cannot access any data or models from individual devices. The aggregated model remains encrypted (using, for example, homomorphic encryption) and is then downloaded to all mobile devices. During this process, personal data on each device is not shared with other users or uploaded to the cloud.

Federated learning is essentially a type of distributed machine learning technology. We classify federated learning from two perspectives: the data features held by participants and the usage scenarios.

- Horizontal Federated Learning
  Horizontal federated fearning (HFL) also known as sample-partitioned federated learning, is suitable when the participants' data features in federated learning overlap, but the data samples they own are different. HFL requires that the data provided by each member has the same feature meaning and similar model parameter structure (which may be different in scenarios such as heterogeneous federated learning or federated multi-task learning). The federated model is generated by aggregating the parameters.

- Vertical Federated Learning
  Vertical federated learning (VFL) [35], also known as feature-partitioned federated learning, is a type of federated learning

that differs from horizontal federated learning in that it requires a significant overlap in data samples provided by each federated member, and that the features are complementary. The model parameters are stored in their corresponding federated members, and optimized using techniques such as federated gradient descent. VFL is suitable for scenarios where the customer groups are similar but the businesses differ significantly. For example, in risk scoring applications.

- Federated Transfer Learning
  Federated transfer learning (FTL) [21] is applicable when there is little overlap in data samples and data features among participating parties. FTL is a special form of knowledge transfer that does not require data sets to have the same feature meanings or share samples, and is a method of propagating knowledge across similar tasks.

A typical horizontal federated learning system is shown in Figure 2.2. This architecture is also known as the client-server or centralized architecture. In this system, federated learning participants with different data but the same features act as clients under the coordination of the server to collaboratively train a machine learning model. The training process of the horizontal federated learning system mainly includes the following four steps.

After setting up the connections and initializing the global model:

(i) The server will distribute the model by sending the initialized parameters to each stable connected client, including the current communication round number.

(ii) Clients will start local model training after receiving the model for several epochs.

(iii) After local training, clients will mask the model updates using technologies such as homomorphic encryption and secret sharing, and send the masked updates (encrypted model) back to the server.

(iv) The server utilizes secure aggregation, which aims to restrict the server's access to the individual client models and only allow it to observe the aggregated result. However, in situations where interpretability, or filtering out low-quality nodes is required, secure aggregation can be disabled to track each client's behavior.

(v) These steps will be iterated continuously until the loss function converges to an acceptable range or reaches the allowed maximum number of iterations.

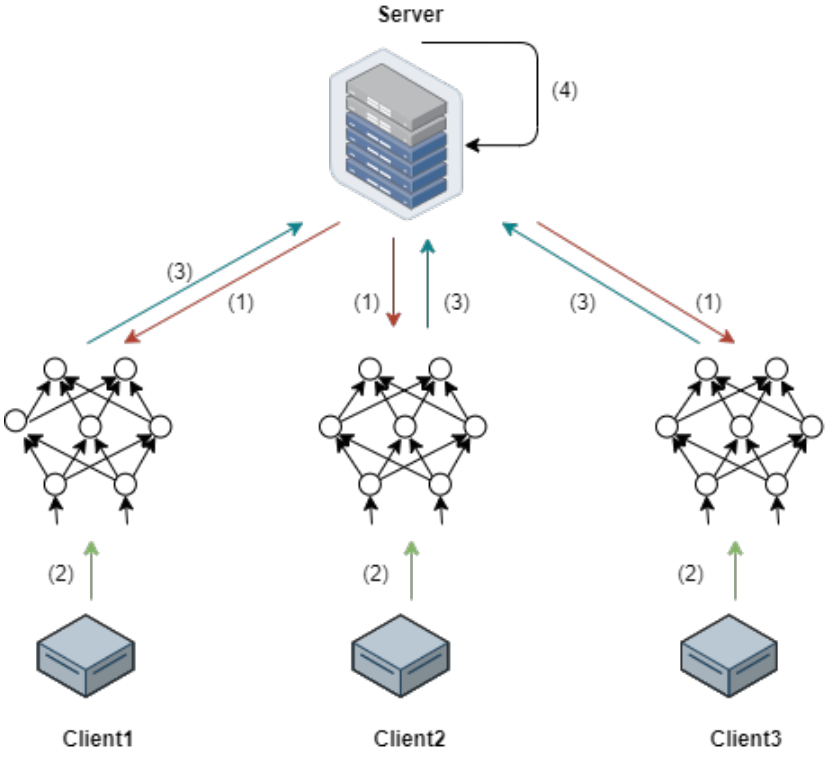


Figure 2.2: The architecture of horizontal federated learning.

2.2 Federated Learning Challenges

Federated learning is a collaborative machine learning approach designed for data security and privacy protection. To achieve data availability without data visibility, Federated learning systems need to balance performance, efficiency, privacy and security concerns. This includes the trade-off between model performance degradation due to data heterogeneity and the increased communication overhead introduced by encryption techniques. Additionally, the behavior of Federated learning participants is unknown, so system designs should be robust enough to handle potential issues such as machine offline status and malicious actors. As illustrated in Figure 2.3, We summarize the systematic challenges of federated learning into three main challenges: performance challenges, efficiency challenges, security and privacy challenges. The homomorphic encryption and secure multi-party computation introduced in the previous section can enhance the security of the federated learning system without affecting the performance of the model, but this method will reduce the computational efficiency. Differential privacy can also protect the privacy of federated learning, but it will damage the utilization of the model. Some acceleration methods such as hardware acceleration and asynchronous acceleration can improve the efficiency of the system, but cannot guarantee the privacy and security of the system.

Besides, federated learning, by decentralizing this process, could potentially reduce the need for such colossal centralized infrastructure. However, there's a trade-off: while reducing data center load, FL might increase the energy use of edge devices (like smartphones or IoT devices) as they now participate actively in the training process. It's crucial to balance these aspects to truly assess FL's net energy footprint. [29] proposes a methodology to estimate the ecological impact of federated learning experiments. Their scalability tests show that the training time increases linearly with the number of clients participating and the training time for the runs with DP is approximately three times longer than without DP.

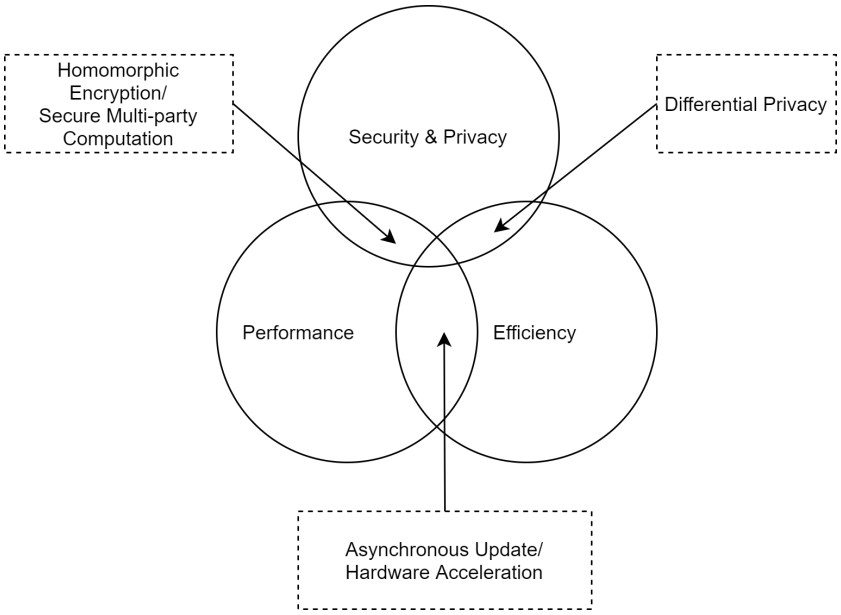


Figure 2.3: Federated learning challanges

3 Dataset Distillation

Dataset distillation [34] is a process of creating a smaller dataset from a larger one while maintaining its representativeness and retaining the essential information. Dataset distillation involves synthesizing new samples that capture the underlying patterns and structures in the training data. Dataset distillation can be especially useful in scenarios where the original dataset is too large or diverse, making it difficult to train a model effectively. By synthesizing new samples that capture the underlying patterns in the data, dataset distillation can help create a more representative and manageable dataset that can improve the performance of machine learning models.

4 Blockchain

4.1 Blockchain Basics

A blockchain is a chain-like data structure that combines data blocks in chronological order and ensures their immutability and non-falsifiability through cryptography, forming a distributed ledger. In a broad sense, blockchain technology utilizes the blockchain data structure to verify and store data, employs distributed node consensus algorithms to generate and update data, ensures secure data transmission and access through cryptography, and uses smart contracts composed of automated script code to program and operate data, creating a new distributed infrastructure and computing paradigm.

In simple terms, a blockchain is a chain of blocks linked in chronological order, as shown in Figure 2.4, with each block consisting of two parts: the block header and the block body. The block header is used to record the metadata of the current block, including the hash value of the parent block (each block is linked to its parent block through the hash value of the parent block), timestamp, Merkle Tree Root, and other information. The Merkle Tree is a binary tree, with each leaf being a transaction record. It is used to summarize all transactions in a block and the Merkle Tree Root is recorded in the block header. The Merkle Tree also generates a digital fingerprint of the entire transaction set and provides an efficient way to verify whether a certain transaction record exists in the block.

The core technologies of blockchain mainly include hash functions, digital signatures, P2P networks, consensus algorithms, and smart contracts, which ensure the decentralized, immutable, and traceable characteristics of blockchain. We will briefly discuss these technical solutions below.

- Hash Function
  A Hash function is a mathematical function that generates a fixed-size output (hash) from an input (data) of any size, creating digital fingerprints of data to ensure its integrity and authenticity in blockchain. In blockchain, hash functions are crucial for creating a unique digital signature of a block that is

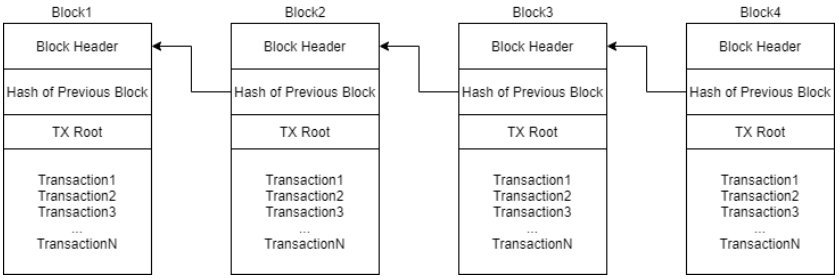


Figure 2.4: Data Structure of blockchain.

added to the blockchain, ensuring that each block is linked to the previous one in a tamper-proof way. Common hash algorithms used in blockchain include the MD series hash algorithm (such as MD2, MD4, and MD5), the Secure Hash Algorithm (SHA) hash algorithm (including SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512), and the SM3 hash algorithm.

- Digital Signature
  A Digital Signature is a cryptographic mechanism that provides authenticity and non-repudiation to digital documents, messages, and transactions. Digital signatures use public key cryptography to verify the identity of the sender and ensure that the content of the message or transaction has not been altered. In blockchain, digital signatures are used to verify the authenticity of transactions and ensure their immutability.

- P2P Network
  A Peer-to-Peer (P2P) Network is a decentralized network where all nodes have equal rights and responsibilities. In a P2P network, all nodes communicate directly with each other without relying on a central authority or server. In blockchain, P2P networks are used to distribute the blockchain's ledger across all nodes in the network, ensuring that each node has a copy of the same blockchain, and no single node has control over the entire network.

- Smart Contract
  Smart Contracts are self-executing contracts with the terms of

the agreement in forms of code. The code and the agreements contained therein exist on a decentralized blockchain network. Smart Contracts help to automate the execution of complex contractual agreements and facilitate transparent and secure transactions between parties on the blockchain network.

Blockchains can be divided into three categories based on their application scenarios and data read/write range: public blockchains, private blockchains, and consortium blockchains.

- Public Blockchains
  Public blockchains are open networks that allow for participation in transactions and consensus by anyone. Bitcoin [26] and Ethereum [5] are well-known examples of public blockchains. Public blockchains offer several advantages, including decentralization with no central control over user rights on the chain. Participants can join, read, and send transaction information, confirming its validity. Transaction data is publicly transparent, with low access barriers, and all participants can view the balance of all accounts and all transaction activity. Public blockchains also provide high security since information added to the blockchain through consensus is recorded by all nodes and cryptographically linked, making it difficult and costly to tamper with. However, public blockchains can be inefficient due to low access barriers and the need for confirmation of data values by a large number of nodes before adding them to the blockchain.

- Private Blockchains
  A private blockchain is a controlled-access blockchain system where read and write permissions are managed by a single organization. The organization determines the writing permissions for each node in the system and decides which information and data to make available based on specific circumstances. Transactions can also be restricted from querying. Despite this, a private chain maintains a common architecture for running multiple nodes. Advantages of private blockchains include extremely fast data processing and transaction speeds due to

centralized control. Transaction data is not publicly disclosed, which provides good data privacy. However, since permissions are completely controlled by a single organization, changes to the rules can lead to a decrease in trust and compromise the security and transparency of the blockchain.

- Consortium Blockchains
  Consortium Blockchains are a hybrid of public and private blockchains. Consortium blockchains are typically used by a group of companies or organizations that have a shared interest in a specific blockchain application. Consortium blockchains are permissioned, meaning that access is limited to a group of known and trusted participants, but they are not fully open to the public like public blockchains. Consortium blockchains are often used for cross-organization applications like supply chain management and other enterprise applications.

4.2 Common Blockchain Platformas

Hyperledger Fabric [2] and Ethereum are both blockchain platforms that enable the development of decentralized applications (dApps) and smart contracts. Hyperledger Fabric is a permissioned blockchain platform designed for enterprise use cases, while Ethereum is a public, permissionless blockchain platform used for a wide range of decentralized applications.

- Hyperledger Fabric
  Hyperledger Fabric is a permissioned blockchain platform that allows multiple organizations to collaborate and share data securely, while keeping their transactions private from unauthorized parties. Fabric uses a modular architecture and a pluggable consensus mechanism that allows organizations to customize their networks based on their specific needs. It also supports the execution of smart contracts using general-purpose programming languages, such as Go, Java, and Node.js. Fabric is well-suited for enterprise use cases, such as supply chain management, asset tracking, and identity management.

- Ethereum
  Ethereum is a public, permissionless blockchain platform that allows anyone to participate in its network and execute smart contracts. Ethereum uses a proof-of-work (PoW) consensus mechanism, which requires nodes to solve complex mathematical problems to add new blocks to the blockchain. Ethereum's smart contracts are written in Solidity, a programming language designed specifically for the Ethereum platform. Ethereum is popular for building dApps, decentralized finance (DeFi) applications, and non-fungible tokens (NFTs).

4.3 Fabric Performance Optimization

Hyperledger Fabric provides a modular and extensible architecture. This flexibility, however, means that optimal performance isn't always guaranteed out-of-the-box. Instead, achieving peak performance requires a nuanced understanding of various components and judicious tuning. [7] presents a formal definition of different types of transaction failures in Hyperledger Fabric and develops a comprehensive testbed and benchmarking system to evaluate the performance of the system. [6] aims to identify the factors affecting the acceptance of blockchain and proposes a framework to optimize blockchain performance by recommending appropriate configurations at different levels, including network, consensus, and smart contract levels. [8] develops a middleware system that can optimize the placement of data in a large-scale IoT system by using a neural network to make intelligent decisions.

4.4 Decentralized Identity

Decentralized identity techniques [9] use blockchain technology to enable individuals to own and control their digital identity without the need for a central authority or intermediary. By utilizing a secure, tamper-proof ledger, such as a blockchain-based distributed ledger, decentralized identity systems provide increased privacy and security, reduced risk of data breaches, and greater user control over their identity information. Decentralized identity systems are claim-

based, meaning that the identity information is not stored in the ledger but in a wallet managed by the user. By controlling what information is shared from the wallet to the requesting third party, users can better manage their identity and privacy online. Overall, decentralized identity techniques offer a more efficient, cost-effective, and user-controlled solution for managing digital identity.

A Decentralized Identifier (DID) is a new type of identifier that enables decentralized digital identity and consists of three parts: the DID URI scheme identifier, the identifier of the DID method, and the identifier specific to the DID method. The corresponding DID Document is a JSON document containing public key material, authentication descriptors, and service endpoints that enable a DID controller to prove control of the DID and authorize its use in specific services. DID Resolvers are servers that use DID drivers to provide a standard means of querying and resolving DID Identifiers across decentralized systems, returning the DID Document associated with the DID Identifier when queried.

References

[1] Martin Abadi, Andy Chu, Ian Goodfellow, H Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. "Deep learning with differential privacy." In: *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. 2016, pp. 308–318.

[2] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, et al. "Hyperledger fabric: a distributed operating system for permissioned blockchains." In: *Proceedings of the thirteenth EuroSys conference*. 2018, pp. 1–15.

[3] Mihir Bellare, Viet Tung Hoang, and Phillip Rogaway. "Foundations of garbled circuits." In: *Proceedings of the 2012 ACM conference on Computer and communications security*. 2012, pp. 784–796.

[4] Battista Biggio, Igino Corona, Davide Maiorca, Blaine Nelson, Nedim Šrndić, Pavel Laskov, Giorgio Giacinto, and Fabio Roli. "Evasion attacks against machine learning at test time." In: *Machine Learning and Knowledge Discovery in Databases: European Conference, ECML PKDD 2013, Prague, Czech Republic, September 23-27, 2013, Proceedings, Part III 13*. Springer. 2013, pp. 387–402.

[5] Vitalik Buterin et al. "A next-generation smart contract and decentralized application platform." In: *white paper* 3.37 (2014), pp. 2–1.

[6] Jeeta Ann Chacko, Ruben Mayer, and Hans-Arno Jacobsen. "How To Optimize My Blockchain? A Multi-Level Recommendation Approach." In: *Proceedings of the ACM on Management of Data* 1.1 (2023), pp. 1–27.

[7] Jeeta Ann Chacko, Ruben Mayer, and Hans-Arno Jacobsen. "Why do my blockchain transactions fail? a study of hyperledger fabric." In: *Proceedings of the 2021 international conference on management of data*. 2021, pp. 221–234.

[8] Syed Muhammad Danish, Kaiwen Zhang, and Hans-Arno Jacobsen. "BlockAIM: a neural network-based intelligent middleware for large-scale IoT data placement decisions." In: *IEEE Transactions on Mobile Computing* 22.1 (2021), pp. 84–99.

[9] Omar Dib and Khalifa Toumi. "Decentralized identity systems: Architecture, challenges, solutions and future directions." In: *Annals of Emerging Technologies in Computing (AETiC), Print ISSN* (2020), pp. 2516–0281.

[10] Cynthia Dwork. "Differential privacy." In: *Automata, Languages and Programming: 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings, Part II 33*. Springer. 2006, pp. 1–12.

[11] Junfeng Fan and Frederik Vercauteren. "Somewhat practical fully homomorphic encryption." In: *Cryptology ePrint Archive* (2012).

[12] Jiahui Geng, Yongli Mou, Feifei Li, Qing Li, Oya Beyan, Stefan Decker, and Chunming Rong. "Towards general deep leakage in federated learning." In: *arXiv preprint arXiv:2110.09074* (2021).

[13] Jiahui Geng, Yongli Mou, Qing Li, Feifei Li, Oya Beyan, Stefan Decker, and Chunming Rong. "Improved Gradient Inversion Attacks and Defenses in Federated Learning." In: *IEEE Transactions on Big Data* (2023).

[14] Craig Gentry. *A fully homomorphic encryption scheme*. Stanford university, 2009.

[15] Neil Zhenqiang Gong and Bin Liu. "Attribute inference attacks in online social networks." In: *ACM Transactions on Privacy and Security (TOPS)* 21.1 (2018), pp. 1–30.

[16] Andrew Hard, Kanishka Rao, Rajiv Mathews, Swaroop Ramaswamy, Françoise Beaufays, Sean Augenstein, Hubert Eichner, Chloé Kiddon, and Daniel Ramage. "Federated learning for mobile keyboard prediction." In: *arXiv preprint arXiv:1811.03604* (2018).

[17] Ehud Karnin, Jonathan Greene, and Martin Hellman. "On secret sharing systems." In: *IEEE Transactions on Information Theory* 29.1 (1983), pp. 35–41.

[18] Joe Kilian. "Founding crytpography on oblivious transfer." In: *Proceedings of the twentieth annual ACM symposium on Theory of computing*. 1988, pp. 20–31.

[19] Ninghui Li, Tiancheng Li, and Suresh Venkatasubramanian. "t-closeness: Privacy beyond k-anonymity and l-diversity." In: *2007 IEEE 23rd international conference on data engineering*. IEEE. 2006, pp. 106–115.

[20] Yiming Li, Yong Jiang, Zhifeng Li, and Shu-Tao Xia. "Backdoor learning: A survey." In: *IEEE Transactions on Neural Networks and Learning Systems* (2022).

[21] Yang Liu, Yan Kang, Chaoping Xing, Tianjian Chen, and Qiang Yang. "A secure federated transfer learning framework." In: *IEEE Intelligent Systems* 35.4 (2020), pp. 70–82.

[22] Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, and Muthuramakrishnan Venkitasubramaniam. "l-diversity: Privacy beyond k-anonymity." In: *ACM Transactions on Knowledge Discovery from Data (TKDD)* 1.1 (2007), 3–es.

[23] Brendan McMahan, 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*. PMLR. 2017, pp. 1273–1282.

[24] Luca Melis, Congzheng Song, Emiliano De Cristofaro, and Vitaly Shmatikov. "Exploiting unintended feature leakage in collaborative learning." In: *2019 IEEE symposium on security and privacy (SP)*. IEEE. 2019, pp. 691–706.

[25] Evgeny Milanov. "The RSA algorithm." In: *RSA laboratories* (2009), pp. 1–11.

[26] Satoshi Nakamoto. "Bitcoin whitepaper." In: *URL: https://bitcoin.org/bitcoin. pdf-(: 17.07. 2019)* (2008).

[27] Pascal Paillier. *Paillier Encryption and Signature Schemes.* 2005.

[28] Nicolas Papernot, Shuang Song, Ilya Mironov, Ananth Raghunathan, Kunal Talwar, and Úlfar Erlingsson. "Scalable private learning with pate." In: *arXiv preprint arXiv:1802.08908* (2018).

[29] René Schwermer, Ruben Mayer, and Hans-Arno Jacobsen. "Energy vs Privacy: Estimating the Ecological Impact of Federated Learning." In: *Proceedings of the 14th ACM International Conference on Future Energy Systems*. 2023, pp. 347–352.

[30] Adi Shamir. "How to share a secret." In: *Communications of the ACM* 22.11 (1979), pp. 612–613.

[31] Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov. "Membership inference attacks against machine learning models." In: *2017 IEEE symposium on security and privacy (SP)*. IEEE. 2017, pp. 3–18.

[32] Latanya Sweeney. "k-anonymity: A model for protecting privacy." In: *International journal of uncertainty, fuzziness and knowledge-based systems* 10.05 (2002), pp. 557–570.

[33] Florian Tramèr, Fan Zhang, Ari Juels, Michael K Reiter, and Thomas Ristenpart. "Stealing Machine Learning Models via Prediction {APIs}." In: *25th USENIX security symposium (USENIX Security 16)*. 2016, pp. 601–618.

[34] Tongzhou Wang, Jun-Yan Zhu, Antonio Torralba, and Alexei A Efros. "Dataset distillation." In: *arXiv preprint arXiv:1811.10959* (2018).

[35] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong. "Federated machine learning: Concept and applications." In: *ACM Transactions on Intelligent Systems and Technology (TIST)* 10.2 (2019), pp. 1–19.

[36] Andrew C Yao. "Protocols for secure computations." In: *23rd annual symposium on foundations of computer science (sfcs 1982)*. IEEE. 1982, pp. 160–164.

[37] Yuheng Zhang, Ruoxi Jia, Hengzhi Pei, Wenxiao Wang, Bo Li, and Dawn Song. "The secret revealer: Generative model-inversion attacks against deep neural networks." In: *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*. 2020, pp. 253–261.

[38] Ligeng Zhu, Zhijian Liu, and Song Han. "Deep Leakage from Gradients." In: *NeurIPS*. 2019.

Chapter 3

Research Contributions

1 Data Heterogeneity in Federated Learning

1.1 Research Problem

Data distribution patterns generated by various regions, devices, and users can differ, leading to client devices potentially exhibiting diverse data samples, labels, and distributions. Some may significantly deviate from the global data distribution, causing statistical heterogeneity, also known as non-independent and identically distributed (non-IID) data, in federated learning. Existing federated learning baseline methods fail to effectively address statistical challenges posed by non-IID data. Figure 3.1 demonstrates that bias occurs during model averaging when selected local models do not accurately represent the global data distribution. Aggregation strategy significantly slows down the convergence rate of the global model and reduces its accuracy, and may even cause the model to fail to converge.

In order to better study the statistical heterogeneity of data, we need to build non-iid datasets among clients. Compared with using datasets from real-world federated scenarios, partitioning a large dataset has the following advantages: It is difficult to evaluate the degree of data heterogeneity in a real federated dataset, but data partitioning strategies can easily quantify and control the level of local data heterogeneity. Second, partitioning strategies can easily set different numbers of clients. The use of data partitioning strategies

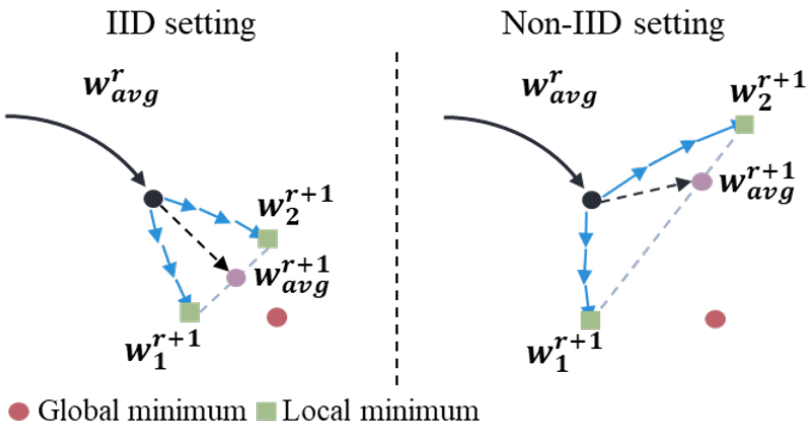


Figure 3.1: The impact of Non-IID data distribution on federated learning..

on widely used public datasets is more flexible, as these datasets already have a lot of study records as references.

The statistical heterogeneity of data across clients in federated learning can be broadly divided into:

- Imbalanced data volume among the clients
  This is the most common case of statistical heterogeneity in the data, which only considers the effect of different sample sizes owned by different participants on the final global model obtained through training.

- Imbalance class distribution among the clients
  Class distribution imbalance, also known as label distribution imbalance, can occur in the medical field when there are differences in the records of certain diseases between hospitals due to factors such as geographical location, diet, and living habits. It can also occur when a hospital has a specialist outpatient clinic, which attracts many patients with specific diseases. There are two ways to construct class distribution imbalance:

  - Imbalance distribution based on label categories
    In this scenario, each participant has data associated with a fixed label. Data with the same label will be partitioned

into the same subset, resulting in each participant being split into two or more subsets with different labels. For instance, when creating a federated dataset using CIFAR10 or MNIST, each client will have only two types of labels, thereby forming five clients. In an even more extreme case, each participant will have data only for a single label.

  - Imbalance distribution based on Dirichlet distribution
    The participants will allocate samples for each label according to the Dirichlet distribution, with a proportion determined by the concentration parameter. The Dirichlet distribution is commonly used as a prior distribution in Bayesian statistics and is used here to control label imbalance.

- Imbalanced feature distribution among the clients
  Unbalanced feature distribution is a common type of non-IID data. For instance, the size and color of blobs in a dog or cat's coat may vary across different regions. To simulate a skewed feature distribution, there are generally three settings: noise-based feature imbalance, synthetic feature imbalance, and real-world feature imbalance [4].

1.2 Our Contributions

To mitigate the impact of label distribution skewness, we propose to use a balanced global validation dataset to evaluate the performance of client models [5]. The dataset is created separately and only available on the server-side during model aggregation, ensuring data privacy protection. Our approach is straightforward and effective. Assume that the distributed datasets on K clients as $\mathcal{D}_1, \mathcal{D}_2, \cdots \mathcal{D}_K$. The objective of federated learning is to obtain the global optimum weight as follows:

$$w^* = \arg\min_{w} \sum_{k=1}^{K} \lambda_k \mathcal{L}_k(w) \tag{3.1}$$

where $\mathcal{L}_k(\cdot)$ is the local loss functions of different clients, and λ_k is the weight for client k with $\sum_k \lambda_k = 1$.

FedAVG algorithm calculates the weight for each client. Client k's weight is based on the ratio of their training samples to the total number of samples:

$$\lambda_k = \frac{|\mathcal{D}_k|}{\sum_i |\mathcal{D}_i|}. \tag{3.2}$$

However, this method ignores the quality difference of the models, We propose to alleviate the class bias severity by employing a balanced global validation set. After receiving models from selected clients, we obtain the validation scores s_k by evaluating the model's performance from client k on the balanced global validation dataset. Then we normalize the validation score as shown in Equation 3.4, where S_t is the set of selected clients in communication round t. The improved aggregation is formulated as:

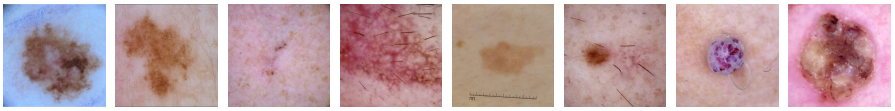
$$\lambda_k = \gamma \cdot (\tilde{s}_k - \frac{|\mathcal{D}_k|}{\sum_i |\mathcal{D}_k|}) + \frac{|\mathcal{D}_k|}{\sum_i |\mathcal{D}_i|}, \tag{3.3}$$

where the parameter γ determines the extent to which the balanced global validation score impacts model aggregation. When γ is set to 0, the FedBGVS algorithm aligns with FedAvg. $\tilde{s}_k$ the normalized score:

$$\tilde{s}_k = \frac{s_k}{\sum_{i \in S_t} s_i}. \tag{3.4}$$

Our approach is evaluated through experiments on classical benchmark datasets such as MNIST, SVHN, and CIFAR-10, as well as a public clinical dataset, ISIC-2019. ISIC-2019 is a public dataset of skin lesion images that was made available for the International Skin Imaging Collaboration (ISIC) 2019 Challenge. The dataset contains over 25,000 images from eight diagnostic categories, namely melanoma (MEL), melanocytic nevus (NV), basal cell carcinoma (BCC), actinic keratosis (AK), benign keratosis (BKL). dermatofibroma (DF), vascular lesion (VASC), and squamous cell carcinoma (SCC), as illustrated in Figure 3.2.

In order to construct the non-iid dataset, we follow the Dirichlet distribution $\mathcal{P}_Y \sim Dir(\beta)$ to sample images for four clients with the control vector β. Finally, the numbers of samples on all clients are the same. The proportion of each category in different clients is shown in Figure 3.3.



(a) (b) (c) (d) (e) (f) (g) (h)

Figure 3.2: ISIC 2019 dataset: (a) MEL, (b) NV, (c) BCC, (d) AK, (e) BKL, (f) DF, (g) VASC and (h) SCC

Due to the heterogeneity of data in the federated learning system, some participants can actually not benefit from federated learning. Personalization in federated learning addresses this issue by allowing the model to be customized for each client's data. We propose a novel personalization method pFedV [6] inspired by variational inference. We decouple the local model $f_{\theta_f}(\cdot)$ into a feature encoder $g_{\theta_g}(\cdot)$ and the classifier $h_{\theta_h}(\cdot)$, i.e., $f_x = h(g(x))$. The objective of standard variational inference is to minimize the Kullback–Leibler (KL) divergence between the variational distribution and the true posterior. This is equivalent to maximizing the evidence lower bound (ELBO), as shown below:

$$\text{ELBO} = \mathbb{E}_{z\sim q_\theta(\mathbf{z})} \log p(y|\mathbf{z}) - D_{KL}(q_\theta(\mathbf{z})||p(\mathbf{z})), \tag{3.5}$$

where z is the latent representation of model parameters and y is the output. $q_\theta(z)$ is the variational distribution. We assume the variational distribution of z follows a Gaussian distribution:

$$q(z) = \mathcal{N}(z|\mu_{\theta_g(x)}, \text{diag}(\sigma^2_{\theta_g}(x))). \tag{3.6}$$

We replace the log-likelihood in Equation 3.5 with the cross entropy loss and the final learning objective on each client is:

$$\theta_g^*, \theta_h^* = \arg\min_{\theta_g,\theta_h} \mathbb{E}_{q_{\theta_h}(\mathbf{z})} CE(\hat{y}_{\theta_h}(\mathbf{z}), y) + \alpha \cdot D_{KL}(q_{\theta_g}(\mathbf{z})||p(\mathbf{z})), \tag{3.7}$$

where CE is the cross entropy loss and α is the weight for the KL term, we empirically set it to 0.5 in our work.

The workflow of pFedV is illustrated in Figure 3.4. During each communication round, the server sends the global model to the

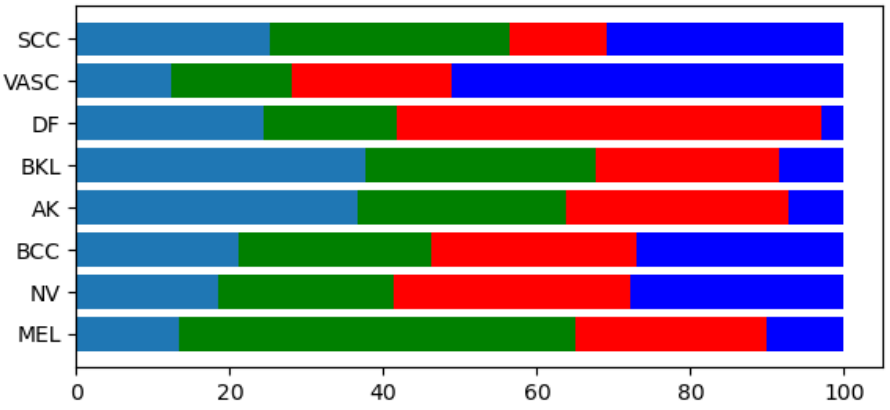


Figure 3.3: Label distributions of ISIC-2019 on each client

participating clients for local training. Then the local model is trained using the loss function defined in Equation 3.7. After several local training epochs, the model updates are transferred back to the server for aggregation, and the classifier on each client is reserved for personalization.

2 Security and Privacy in Federated Learning

Ensuring the security and privacy of data in federated learning is critical as it involves multiple parties contributing their local private data to train a machine learning model.

2.1 Research Problem

Gradient inversion attack is a privacy threat that can occur in federated learning. In federated learning, a central server can collect model updates from different clients. However, a malicious server or any attacker who can access the shared information can exploit the gradients to infer the privacy from other clients' data. Hence, it is crucial to investigate the extent of potential damage caused by such attack on federated learning and identify effective defense strategies against them.

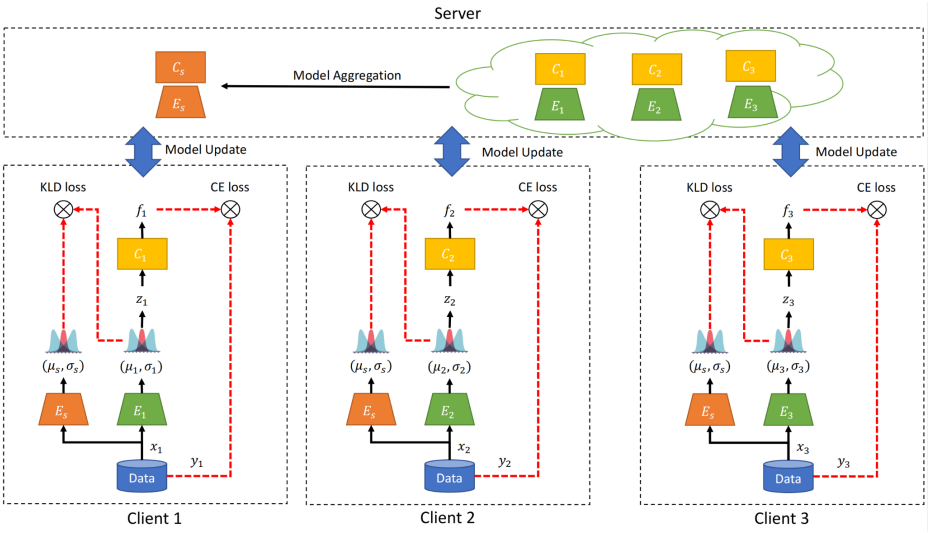


Figure 3.4: Overview of pFedV approach

Figure 3.5 depicts the gradient inversion attack concept. In federated learning, a client performs local training with input image x and corresponding label y, while the model weight is represented as W. The client calculates the model update ∇W via back-propagation. If an attacker gains access to the client's model update, they can attempt to deduce training samples from the model weights and updates. The attacker initializes a dummy image x' and label y' randomly, then computes the dummy gradient $\nabla W'$, leveraging known model parameters and hyperparameters. The aim is to align the dummy and true gradients by optimizing the dummy image and label. As the dummy image and label approach the actual sample, the gradient difference significantly decreases. Ultimately, continuous optimization allows for the restoration of training samples.

2.2 Our Contributions

In Paper II, we have identified several limitations that impede their practical effectiveness. These limitations include: (1) previous works have only been tested under ideal conditions with unique labels, while real-world scenarios often encounter batched data with duplicated

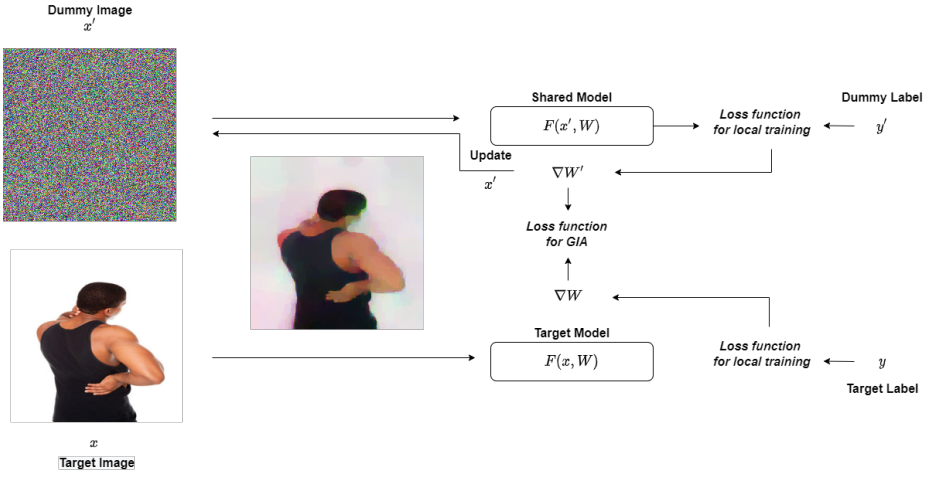


Figure 3.5: Illustration of Gradient Inversion Attack

labels; (2) most frameworks can only attack the gradient sharing schema (FedSGD), while FedAVG, which is more commonly used due to its higher efficiency; (3) existing defenses rely on privacy-preserving techniques such as differential privacy and cryptographic methods, which can increase the computational load of federated learning or negatively impact the model's utility.

Our study provides significant contributions to the federated learning privacy. Specifically, we demonstrate the critical importance of label inference and enhance the zero-shot batch label inference method to overcome existing limitations. We propose a versatile attack framework that can target both FedSGD and FedAVG, and present novel techniques to improve image restoration, such as proper initialization and regularization tricks, and utilizing multiple updates as a group consistency. Our observations on the confusion caused by duplicated labels motivate future research directions. Finally, we propose several ways to mitigate this attack, including increasing the number of epochs for local training, and ensuring that samples of certain classes appear multiple times in each batch.

3 Dataset Distillation

Large-scale training datasets are critical to deep learning applications, and recent studies show that the dataset scale used in deep learning is exponentially increasing. While this growth improves the model's generalization ability, it also leads to higher training costs, including storage and computation. To mitigate this pressure, dataset distillation employs smaller datasets with higher information density. Unlike traditional sampling methods, dataset distillation generates previously unseen samples that possess stronger representational power than sampled ones.

3.1 Research Problem

Dataset distillation is a process that involves compressing a large dataset into a smaller, more manageable dataset while retaining its key properties. The idea behind dataset distillation is to create a compact representation of the original dataset that can be used for training machine learning models without sacrificing performance. Assuming in machine learning, $\mathcal{D}$ is the dataset, f_θ is a neural network parameterized by θ. $f_\theta(x)$ is the model prediction on the data point $x \in \mathcal{D}$. The expected loss for model f_θ evaluated on $\mathcal{D}$ is formulated as:

$$\mathcal{L}_{\mathcal{D}}(\theta) = \mathbb{E}_{(x,y)\sim P_{\mathcal{D}}}[\ell(f_\theta(x), y)], \tag{3.8}$$

where x and y are the input data and label pair from $\mathcal{D}$, $\ell(f_\theta(x), y)$ is the loss value between the prediction and ground truth.

Dataset distillation aims to learn a much smaller synthetic dataset $\mathcal{S} = \{(\hat{x}_j, \hat{y}_j)\}_{j=1}^{|\mathcal{S}|}$ from the origin training set $\mathcal{T} = \{(x_j, y_j)\}_{j=1}^{|\mathcal{T}|}$, so that the model performances trained on two dataset are similar. The objective is formulated as:

$$\mathcal{L}_{\mathcal{T}}(\theta^{\mathcal{S}}) \simeq \mathcal{L}_{\mathcal{T}}(\theta^{\mathcal{T}}), \tag{3.9}$$

where $\theta^{\mathcal{S}}$ and $\theta^{\mathcal{T}}$ are the parameters of the models trained on $\mathcal{S}$ and $\mathcal{T}$ respectively.

3.2 Our Contributions

Holistic Survey

Despite recent advancements, a holistic understanding of the approaches and applications is currently lacking. To bridge this gap, we present a novel taxonomy of dataset distillation, providing a comprehensive overview of existing approaches and techniques. It also discusses critical challenges in this domain and highlights promising research directions.

We propose a unique classification system that sorts current research from multiple angles. In our survey, we category the existing dataset distillation methods into to groups, the meta-learning-based approaches and the surrogate objective-based approaches.

Meta-Learning Based Methods Meta-learning based dataset distillation methods involve using a meta-learner to learn how to distill a dataset that is more effective for a given task. The meta-learner is trained on a set of tasks and learns to adapt to the specific characteristics of each task and the model being trained.
Pros

- Meta-learning based methods can be more flexible than other methods, as they can be applied to a wide range of tasks and models.

Cons

- Meta-learning based methods can be more sensitive to the choice of hyperparameters, as they require tuning the hyperparameters of both the meta-learner and the model being trained.
- Meta-learning based methods can be more computationally expensive than other methods, as they require training the meta-learner on a large number of tasks.

Surrogate Objective-Based Methods Surrogate objective based dataset distillation methods involve using a simplified surrogate objective to select the most informative samples from the original dataset.

The surrogate objective can be based on parameter matching or distribution matching. Parameter matching surrogate objectives aim to create a distilled dataset that can produce similar model parameters to those obtained from the original dataset. Distribution matching surrogate objectives aim to create a distilled dataset that can capture the statistical properties of the original dataset.
Pros

- Surrogate objective-based methods can be more computationally efficient than other methods, as they do not require unrolled optimization.

Cons

- Surrogate objective-based methods can suffer from truncation bias, which can lead to a loss of information in the distilled dataset.
- Surrogate objective-based methods may not always be able to capture the full complexity of the original dataset, as they rely on a simplified surrogate objective.

We also point out hat while the majority of these efforts focus on image datasets, the processing of discrete text and graph data poses considerable difficulties. The area of robustness has seen minimal exploration, and as the technology becomes more widespread, additional research will be imperative. Our analysis offers insight into the current state of this domain and points out potential avenues for future investigations.

Security Study

The existing research on dataset distillation mainly concentrates on the transferability and computational efficiency of dataset generation. Unfortunately, there is limited work on the privacy and robustness of this method. Moreover, most studies only focus on a single attack method, which may not provide a comprehensive evaluation of the method's security. In contrast, our paper [1] aims to expand the connotation of security to include privacy, robustness, and fairness.

We recognize that these are essential factors that must be considered in evaluating the effectiveness of dataset distillation. By considering a broader range of security metrics, our work contributes to a more comprehensive understanding of the strengths and limitations of this technique. In Paper III, we propose a benchmark to evaluate the security of dataset distillation. The research question of the work is:

(i) Is the synthetic dataset sufficient enough to protect data privacy?

(ii) How will the models trained on distilled dataset perform in the face of adversarial attacks?

(iii) Is dataset distillation fair for all classes in classification tasks?

We conduct a large-scale analysis of state-of-the-art distillation methods, based on the proposed research questions. We utilize four representative distillation techniques: Differentiable Siamese Augmentation (DSA), Distribution Matching (DM), Training Trajectory Matching (MTT), and Information-Intensive Dataset Condensation (IDC). Subsequently, we design numerous experiments to assess the effect of data distillation on the model's privacy, fairness, and robustness. By conducting extensive comparative experiments, we identify the key factors that influence these metrics.

Our experimental results on dataset distillation provide several insightful findings. Firstly, we observed that dataset distillation amplifies the unfairness of the model's predictions between different classes, and this effect increases with the distillation rate. Secondly, we discovered that dataset distillation does not inherently possess privacy-preserving capabilities. The success of membership inference attacks is dependent on several factors, including the distillation rate, initialization, and number of classes. Finally, we found that the robustness of the model is impacted to varying degrees, but the distillation rate has only a minor influence. Notably, the distillation rate denotes the ratio of the number of images per class after distillation to before distillation. This study is the first to systematically evaluate dataset distillation techniques and their security risks.

4 Blockchain-supported Distributed Information System

4.1 Research Problem

Blockchain's non-tamperable characteristics make it an ideal tool for ensuring the security of digital assets, enabling decentralized transactions and storage, and improving data transparency and traceability. For instance, blockchain can facilitate secure transactions, ensuring that transaction records cannot be tampered with. Additionally, blockchain can create decentralized applications and smart contracts for automated transactions and contract execution. It can also protect intellectual property and ensure the traceability of supply chains.

My research focuses on utilizing blockchain technology to ensure the security of distributed information systems, particularly in open systems where users and data are diverse and require sufficient interactivity. By leveraging the unique properties of blockchain, such as its immutability and decentralized nature, we aim to develop innovative solutions for improving the security and privacy of distributed systems, while ensuring the seamless interaction between various stakeholders.

4.2 Our Contribution

In Paper I [7], we introduce the concept of Open Infrastructure as Code (OpenIaC) which reimagines the creation, deployment, protection, operation, and retirement of information systems. Our OpenIaC approach aims to provide services based on Zero Trust Architecture (ZTA) principles in a decentralized identity (DID)-based federation of connected resources. Our goal is to create an open-source hub with fine-grained access control for shared resources (such as sensing, storage, computing, and 3D printing) managed by consortium. This approach could pave the way for developing new platforms, business models, and modern information ecosystems required for 5G networks.

We highlight several challenges that need careful consideration and

resolution when developing a comprehensive architecture, including service orchestration, service level agreements (focusing on billing, metering, and capacity planning), more secure networks, shared edge computing nodes, and service provisioning accountability and reliability of suppliers. Figure 3.6 provides an overview of the Computing Management Services layer and a summary of the underlying services and resources required to support the OpenIaC layer for 5G networks.

In paper [2], we propose a scheme to integrate decentralized identifiers (DID) into a federated learning system. Specifically, we describe a scenario where our DID-enhanced federated learning system (DID-eFed) enables Federated Learning-as-a-Service (FLaaS) between hospitals and research institutions. By leveraging DID, we can achieve more flexible and reliable decentralized access management, which is crucial for maintaining privacy and security in federated learning. In traditional federated learning systems, access management can be a challenging task, particularly in scenarios where multiple parties with different roles and responsibilities are involved. DID offers a solution to this problem by providing a decentralized approach to identity management. By assigning unique and persistent identifiers to each participant, DID can help establish trust and accountability among the various stakeholders involved in the FLaaS process. Moreover, the use of DID can also enhance privacy and security in federated learning by enabling fine-grained access control. With DID, participants can control the information they disclose, thereby reducing the risk of data breaches and unauthorized access. Additionally, DID can facilitate secure data sharing and collaboration, enabling healthcare institutions and research organizations to work together more effectively while maintaining the confidentiality and privacy of patient data.

Paper IV focuses on designing and developing a flexible decentralized access control system for inter-enterprise data sharing. Our goal is to allow organizations to set different access policies for the resources they share in the network. Since sensitive data is shared between interested parties, preventing misuse of data is critical. We must also ensure data privacy and avoid disclosing personal information. To meet these criteria, our system requires dynamic access control,

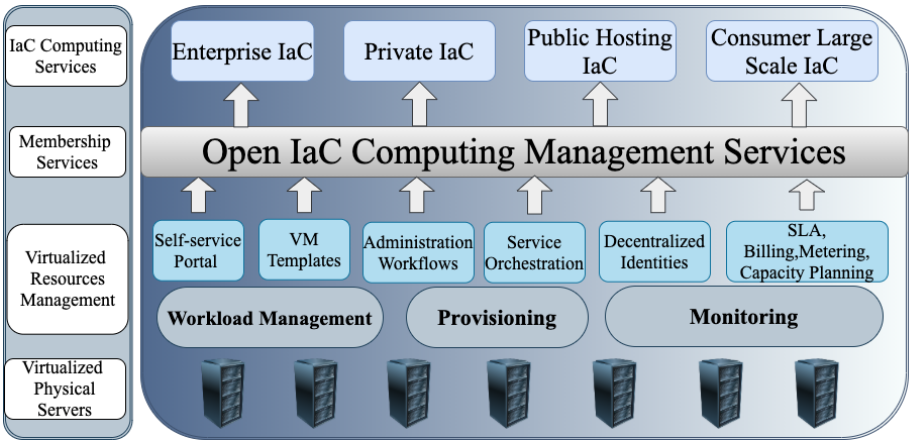


Figure 3.6: The overview of open infrastructure as code.

accountability and transparency, self-sovereignty, and audience.

To achieve these goals, we combine the Hyperledger Indy/Aries decentralized identity scheme for traceability and mutual authentication of identities within the system [9]. To enable flexible access control, we adopted the XACML architecture. We design different smart contracts to decouple the attributed-based access system.

An ideal cross-organizational workflow management system must fulfill two primary requirements. First, it must keep data local and bring computation to the data to avoid the risks associated with data migration. Second, it must ensure transparency in the collaborative process and reduce mistrust between organizations. Blockchain technology is gaining attention from academia and industry due to its transparent and immutable nature. The distributed storage and consensus algorithms on which blockchain is based make it nearly impossible for data to be tampered with. Smart contracts can ensure that specific protocols are carried out fairly and without interference. In paper V [3], We have developed a cross-organizational data and computing cooperation platform that is based on blockchain technologies, JupyterFlow, and JupyterHub. Participants who share the same purpose can contribute data and computation scripts separately and use the workflow management tool to execute tasks automatically. The private data used for computation is kept locally at its

origin, while metadata and access control protocols are recorded in the distributed ledger.

We also proposes a novel NFT-like scheme [8] that utilizes metadata to convert digital assets into digital object identifiers. By doing so, we can convert digital objects that require clear sovereignty into NFTs, thereby ensuring the authenticity and uniqueness of ownership. In our scheme, we leverage metadata to create a decentralized and secure method for managing digital assets. By embedding metadata into digital assets, we can establish a clear ownership history and enable more flexible and dynamic management of these assets. Moreover, by converting digital objects into NFTs, we can ensure that they remain unique and irreplaceable, even when they are duplicated or shared across various platforms. Our scheme also utilizes smart contracts to facilitate the dynamic management of digital objects. By deploying smart contracts, we can automate the management of ownership and access rights, as well as the enforcement of rules and regulations governing the use of digital objects. This approach ensures that digital objects are managed securely and transparently, without the need for intermediaries or centralized authorities.

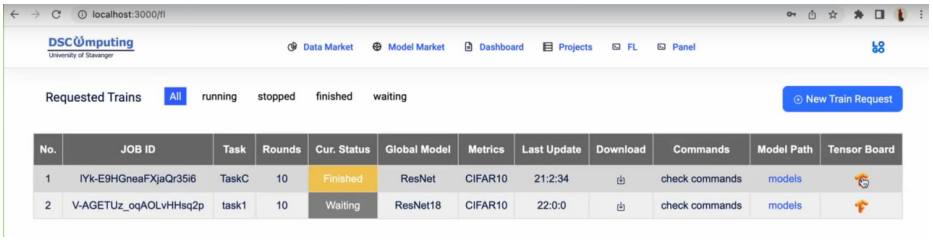


Figure 3.7: Overview of our federated learning platform.

5 Open-Source Implementation

5.1 Federated Learning Platform

We first demonstrate our federated learning platform. The overview interface is shown in Figure 3.7. Users can click "New Train Request" to create a new federated learning task. The table below shows

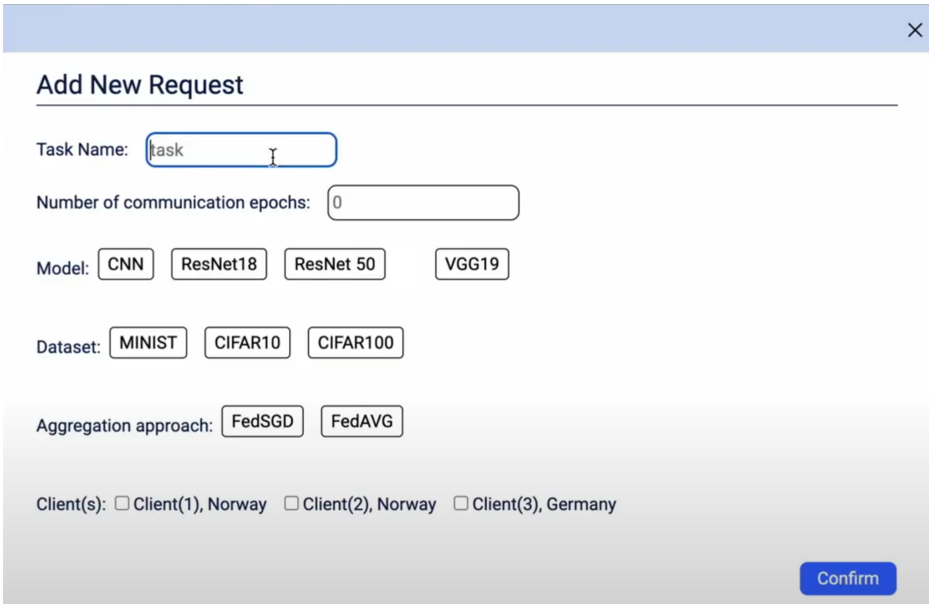


Figure 3.8: The interface for adding new training request, users can define the configuration of federated learning system.

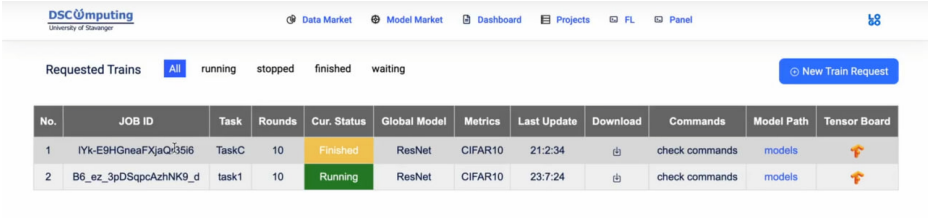


Figure 3.9: The process of creating a workflow.

all federated learning tasks, including running tasks, stopped tasks, finished tasks and waiting tasks.

When a new federated learning task is initiated, a tab for configuring the federated learning task will pop up, as shown in Figure 3.8, where the user can configure the federated learning algorithm, including the algorithm used, the nodes participating in the training, and so on. After clicking the "Confirm" button, the training task will enter the waiting stage. During this period, the back-end will generate corresponding script files according to the configuration information

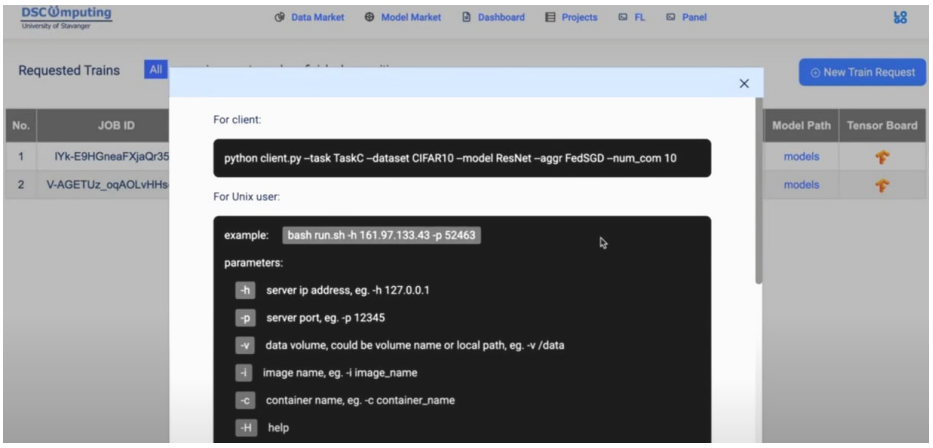


Figure 3.10: We have the command line ready, respectively for UNIX users and Windows users.

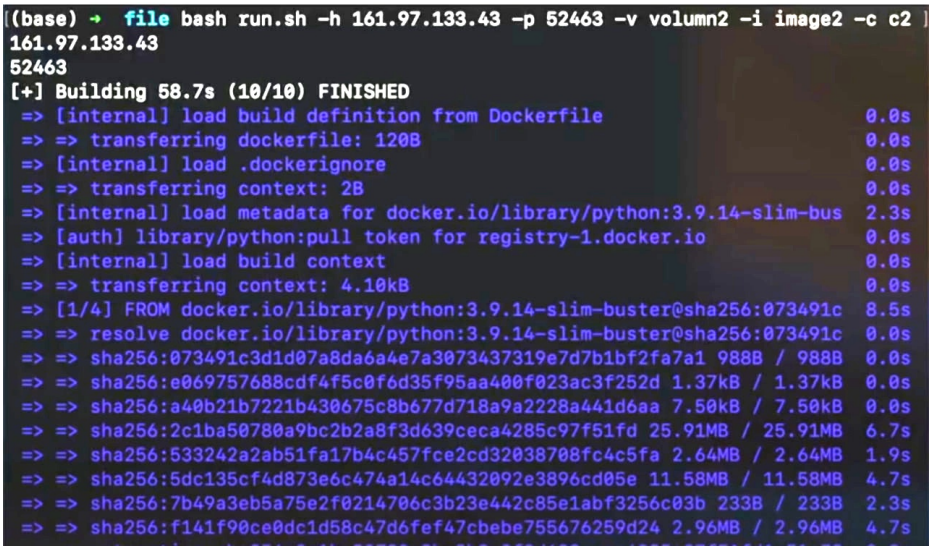


Figure 3.11: Users can quickly build a federated learning runtime environment with provided bash script.

for local client execution, create a running environment on the server side and initiate an aggregation algorithm for monitoring clients. At this time, users of different nodes can click ”Downloads” to download the scripts they need to run locally. The script will use Docker to

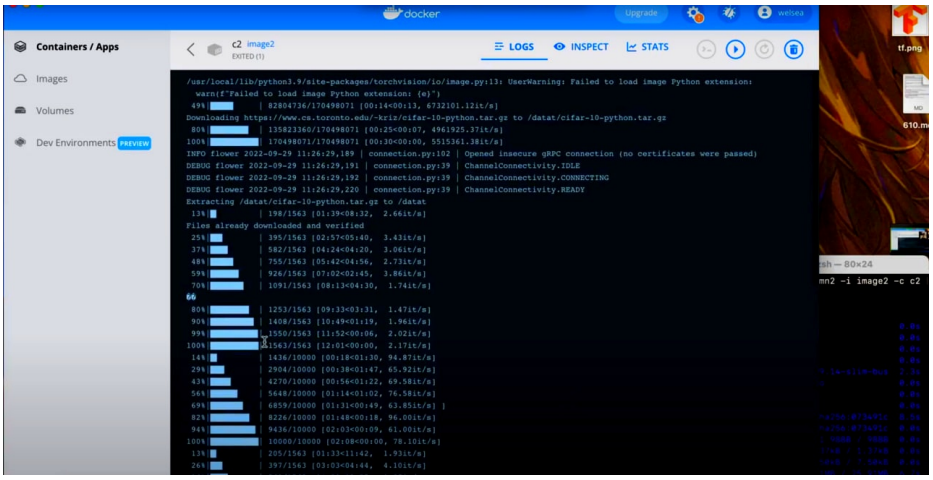


Figure 3.12: Users can view the training logs in the local Docker container.

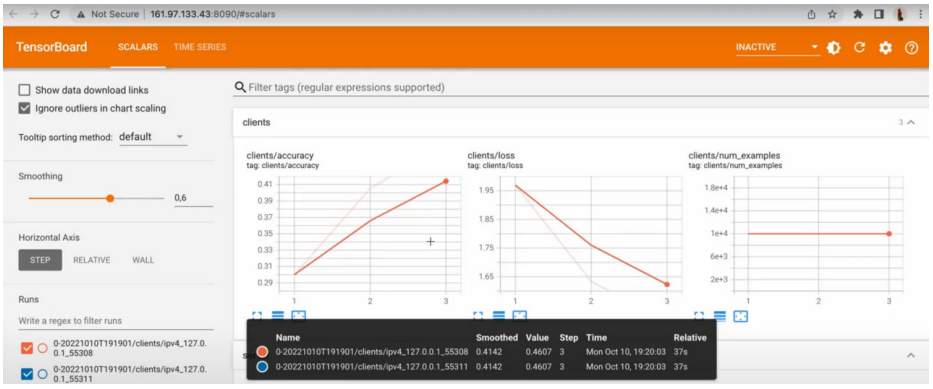


Figure 3.13: Users can view the training curve and different metrics of the current model in TensorBoard.

Figure 3.14: Global models for downloading.

create a local running environment. Clicking "Commands" button, the user can get the current response and train the federated learning

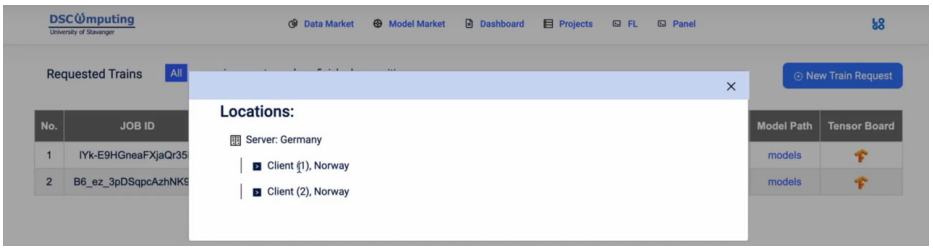


Figure 3.15: Users can check the connection status in the federated learning system.

training script as shown in Figure 3.10. When the preparation is completed, the "Current Status" will turn green and display "Running", as shown in Figure 3.9. At this point, the user can run the training script locally, as shown in Figure 3.11. The user can view the local training log, as shown in Figure 3.12, or use TensorBoard to view the pre-defined metrics during the training process, as shown in Figure 3.13. In "Model Path", the user can view the global model as shown in Figure 3.14, click on the Job ID, and the user can also view the connection status of the current federated learning system, as shown in Figure 3.15.

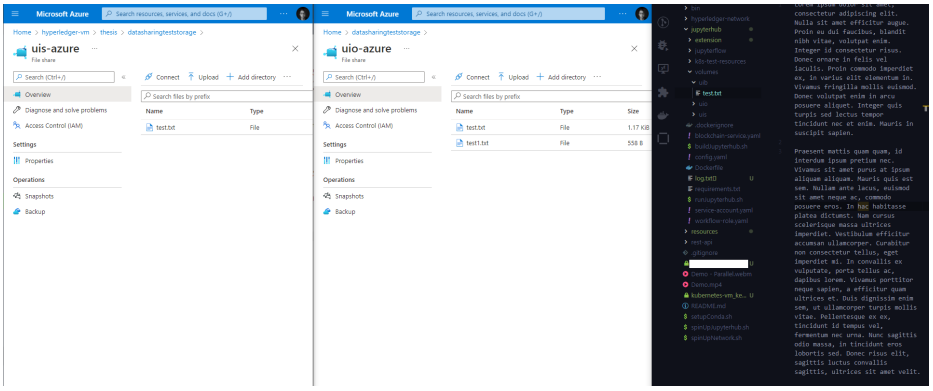


Figure 3.16: The process of creating a workflow.

```
Policies:
    Readers:
        Type: Signature
        Rule: "OR('UiSMSP.admin', 'UiSMSP.peer', 'UiSMSP.client')"
    Writers:
        Type: Signature
        Rule: "OR('UiSMSP.admin', 'UiSMSP.client')"
    Admins:
        Type: Signature
        Rule: "OR('UiSMSP.admin')"
    Endorsement:
        Type: Signature
        Rule: "OR('UiSMSP.peer')"
```

Figure 3.17: Dataset access control definition.

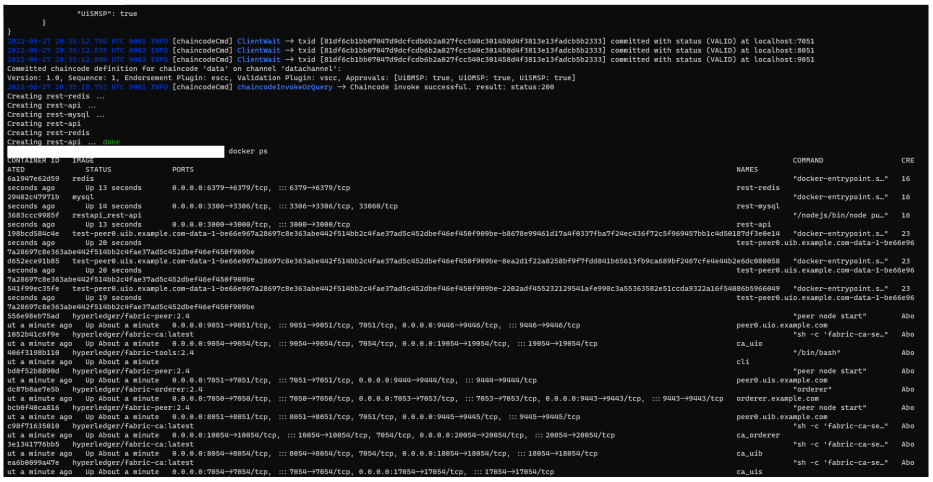


Figure 3.18: The process of creating a workflow.

5.2 Decentralized Workflow Platform

We demonstrate our decentralized workflow platform, combined with Hyperledger Fabric blockchain for access control, JupyterFlow for workflow creation and execution, and JupyterHub Extension as a distributed data creation and management interface. Due to limited storage capacity, our data will be stored on Microsoft Azure Fileshare, and only the hash value of the data will be stored in the decentralized ledger.

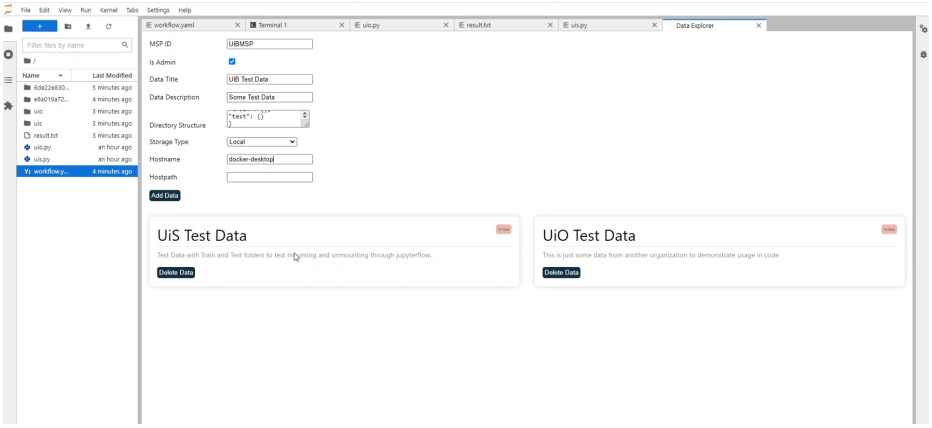


Figure 3.19: The process of creating a workflow.

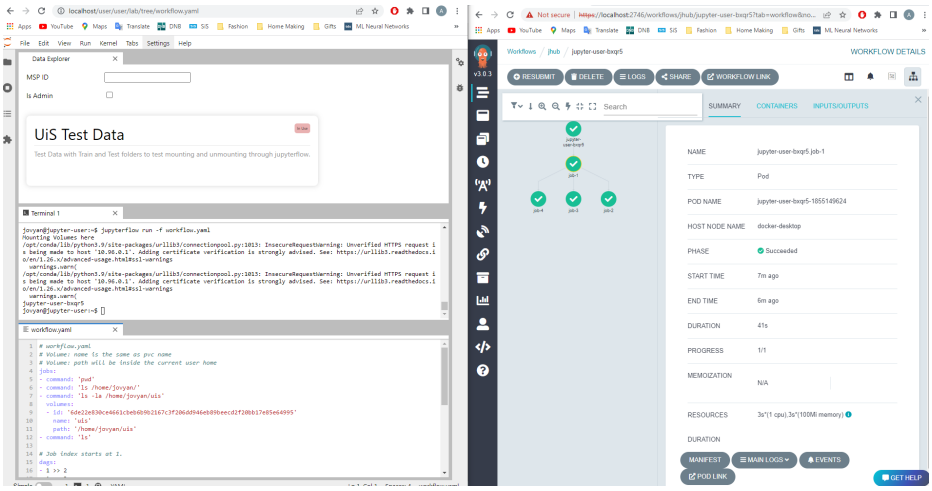


Figure 3.20: The process of creating a workflow.

The experimental task we show is to perform text-specific word statistics, and the data will be first stored in Microsoft Azure File-share as shown in the Figure 3.16. Suppose we have create two dataset named ”test.txt” under the organization name ”UiS” and ”UiO” respectively. Secondly, we need to define the access rights of different data sets through smart contracts, either based on the name of the organization or based on the attributes of the organization, a simple setup is shown in Figure 3.17. We successfully deploy the

smart contract to the blockchain system as shown in Figure 3.18.

Then we move to the configuration of the workflow to register data for our workflow, as shown in the Figure 3.19. Only organizations with access rights can find the corresponding data sets and configure them into our workflow. After after, we need to define the workflow and use the JupyterFlow feature to add the corresponding data volume and python script information to the workflow.yaml file, as shown in the left half of Figure 3.20. The result of the workflow execution is shown in the right half of Figure 3.20.

References

[1] Zongxiong Chen, Jiahui Geng, Herbert Woisetschlaeger, Sonja Schimmler, Ruben Mayer, and Chunming Rong. "A Comprehensive Study on Dataset Distillation: Performance, Privacy, Robustness and Fairness." In: *arXiv preprint arXiv:2305.03355* (2023).

[2] Jiahui Geng, Neel Kanwal, Martin Gilje Jaatun, and Chunming Rong. "DID-eFed: Facilitating Federated Learning as a Service with Decentralized Identities." In: *Evaluation and Assessment in Software Engineering*. 2021, pp. 329–335.

[3] Jiahui Geng, Ali Akbar Rehman, Yongli Mou, Stefan Decker, and Chunming Rong. "Blockchain-based Cross-organizational Workflow Platform." In: *2022 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*. IEEE. 2022, pp. 53–59.

[4] Qinbin Li, Yiqun Diao, Quan Chen, and Bingsheng He. "Federated learning on non-iid data silos: An experimental study." In: *2022 IEEE 38th International Conference on Data Engineering (ICDE)*. IEEE. 2022, pp. 965–978.

[5] Yongli Mou, Jiahui Geng, Sascha Welten, Chunming Rong, Stefan Decker, and Oya Beyan. "Optimized Federated Learning on Class-Biased Distributed Data Sources." In: *Machine Learning and Principles and Practice of Knowledge Discovery in Databases: International Workshops of ECML PKDD*

2021, Virtual Event, September 13-17, 2021, Proceedings, Part I. Springer. 2022, pp. 146–158.

[6] Yongli Mou, Jiahui Geng, Feng Zhou, Chunming Rong, Stefan Decker, and Oya Beyan. "pFedV : Mitigating Feature Distribution Skewness via Personalized Federated Learning with Variational Distribution Constraints." In: *Advances in Knowledge Discovery and Data Mining - 26th Pacific-Asia Conference, PAKDD 2023, Proceedings, Part I*. Springer. 2023.

[7] Chunming Rong, Jiahui Geng, Thomas J Hacker, Haakon Bryhni, and Martin Gilje Jaatun. "OpenIaC: open infrastructure as code – the network is my computer." In: *Journal of Cloud Computing* 11.1 (2022), pp. 1–13.

[8] Chunming Rong, Jiahui Geng, and Martin Gilje Jaatun. "Managing Digital Objects with Decentralised Identifiers based on NFT-like schema." In: *2022 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*. IEEE. 2022, pp. 246–251.

[9] Hanif Tadjik, Jiahui Geng, Martin Gilje Jaatun, and Chunming Rong. "Blockchain Empowered and Self-sovereign Access Control System." In: *2022 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*. IEEE. 2022, pp. 74–82.

Chapter 4

Conclusion and Future Work

This chapter presents the conclusions drawn from the current research. By answering the research questions formulated in chapter 1, we have arrived at several key findings. Additionally, this chapter discusses the future directions for further research.

1 Conclusion

(i) **RQ1: How to build machine learning systems that bring computation to data to preserve privacy?**
Currently, there are various machine learning methods available that enable calculations to be performed on data and allow for data analysis and mining.

Privacy-preserving techniques such as federated learning, secure multi-party computation (SMPC), and homomorphic encryption enable multiple parties to collaborate on machine learning tasks while maintaining the privacy of their data. These techniques keep data distributed among parties, preventing unauthorized access and maintaining privacy. Encryption is a common feature among them to ensure data privacy during the collaborative process. Federated learning encrypts data before it is sent for aggregation, SMPC uses encryption to compute a result without revealing inputs, and homomorphic encryption enables computation on encrypted data without decryption.

Another category of technologies includes differential private deep learning and dataset distillation, they both focus on protecting sensitive data privacy during machine learning and data analysis. Differential private deep learning combines differential privacy with deep learning techniques to create models that analyze sensitive data while preserving individual privacy. These models ensure that an individual's data does not significantly impact the overall outcome by adding noise to the data or model parameters to prevent re-identification of individuals. Dataset distillation involves creating a smaller, less complex dataset that still retains the essential features of the original data. The reduced dataset is then used to train models and perform analysis while protecting the privacy of individuals. Dataset distillation can be used with differential privacy for even more robust privacy protection in machine learning and data analysis. Our work mainly studies two technologies of federated learning and data set compression.

(ii) **RQ2: How to achieve the balance between data utility and data privacy?**
In our research, we aim to balance the utility and data privacy of data by exploring and implementing different technologies, including secure access control and federated learning without sharing data. Implementing access controls allows us to limit access to sensitive data to only authorized individuals, thereby maintaining data privacy while still making it available to those who need it. However, most access control systems are centralized, which means that users lose control over data when sharing resources. It is difficult to track how storage service providers and others operate their data, who has the right to access this data, and how this data is accessed. This loss of transparency and control will lead to wrong use of data, and the rights of users will not be guaranteed. This may lead to a single point of failure, makes these systems vulnerable to cyber-attacks and compromises the security of the data. Blockchain-based access control may be more secure because the blockchain system is decentralized, It can prevent single

point of failure. Secondly, the access control system based on blockchain is transparent, and all operations are endorsed by each node and recorded in the distributed ledger. This increases the transparency of operation. In this thesis, we propose the use of blockchain to control user access. For more detailed blockchain system design, see RQ3.

While federated learning prevents direct data sharing, research has shown that malicious attackers can still infer private information from shared parameters. We investigate the most severe privacy attack, training data reconstruction. Attackers can infer not only the labels corresponding to each batch, but also the complete original image using the gradient information and model weights shared by the model. Previous work limited this attack to sharing gradients and non-repeated labels per batch. However, we experimentally prove that this attack can surpass those limitations. To address this issue, we propose a zero-shot batch label inference method and a simple yet effective fidelity regularization. These findings remind us of the need to consider potential privacy risks during federated learning training. We also demonstrate that data confusion and selective category combinations can alleviate this risk. In addition, in order to solve the model performance degradation caused by data heterogeneity to federated learning, we propose two methods to alleviate this problem. One method is to use a balanced global validation set to alleviate class bias severity. We refine the model aggregation algorithm using the Balanced Global Validation Score (BGVS). In Publication (iv), we leverage a variational inference approach by incorporating a variational distribution into neural networks and adding a KL-divergence term to the loss function during training.

Dataset distillation is an emerging research direction that involves training a machine learning model on an original dataset and using it to generate a distilled dataset. The distilled dataset contains only the most relevant and non-sensitive information from the original dataset, while discarding sensitive information. This technique can be useful in situations where privacy

concerns prevent the sharing of raw data, such as in healthcare. By using dataset distillation, it is possible to create a distilled dataset that can be shared with researchers while preserving patient privacy. In Paper III, we analyze the privacy, robustness, and fairness of this technology and point out that it still has varying degrees of privacy risk, such as membership inference, which are related to the distillation rate and number of classification task classes. It may also amplify inequities across categories. We also conduct a systematic survey on dataset distillation techniques, including optimization approaches, data modalities, and downstream applications.

(iii) **RQ3: How to build blockchain system with flexible access control mechanism with trustworthy traceability?**

To build a blockchain system with flexible access control and trusted traceability, it is essential to implement several design principles and techniques. One approach involves developing robust access control mechanisms that limit data access based on user roles, attributes, or responsibilities, thereby minimizing the risk of unauthorized access and data leakage. Additionally, the system can incorporate smart contract-based access control and decentralized identity technology at the security boundary to enhance flexibility and ensure the immutability of validation. Finally, it is crucial to implement reliable and trustworthy traceability mechanisms capable of tracking and monitoring all transactions and data changes to enhance transparency and accountability.

In Paper I, we introduce the OpenIaC concept, highlighting the importance of decentralized identity and zero-trust architecture in creating an open and trustworthy infrastructure. Decentralized identity provides greater privacy than centralized systems as individuals have control over authentication information and access. Moreover, decentralized identity improves interoperability, enabling users to access multiple platforms with a single decentralized identity.

In Paper IV, we combine decentralized identity with smart contracts to achieve data access control. Our architecture is based on XACML, with a decoupled access policy infrastructure that manages the dynamicity of the SSIDD. We use Hyperledger Fabric and Hyperledger Indy/Aries to implement our approach and verify its performance relationship with block size and batch timeout.

Paper V presents our Proof of Concept (PoC), which enables sharing data between untrusted organizations while maintaining ownership. We implement our PoC using a Jupyter-based cross-organizational data and computing collaboration platform that utilizes blockchain technologies for secure and private cross-organizational workflow management. Our proposed solution empowers data owners with full control over their data. We evaluate our approach using a simple data processing use case.

In addition, using blockchain to protect the copyright of digital assets is also under our consideration.

2 Future Work

The future work of OpenIaC holds significant promise in revolutionizing the way organizations manage and operate their digital infrastructure. By addressing security, governance, community engagement, and interoperability challenges, we can create a more transparent, secure, and collaborative OpenIaC ecosystem that fosters innovation and trust among stakeholders. Continued research, development, and implementation of these advancements will be instrumental in realizing the full potential of trustworthy OpenIaC in the coming years.

In addition, artificial intelligence products like ChatGPT will have a more profound impact on OpenIaC.Language model systems like ChatGPT can be utilized to build automated customer service agents capable of handling user queries, issues, and needs. By connecting to open digital infrastructure and digital assets, the system can provide more accurate answers and guidance, facilitating efficient

user interactions. Automation systems connected to open digital infrastructure and digital assets can be integrated with ChatGPT-like systems to perform data analysis and provide decision support. This integration enables the system to handle large-scale data and offer real-time insights and recommendations. Integrating systems similar to ChatGPT with open digital infrastructure and digital assets promotes connectivity and collaborative work across different domains. This integration enables the system to interact with data and functionalities from multiple domains, providing comprehensive and integrated services.

Paper 1:
OpenIaC: open infrastructure as code-the network is my computer

OpenIaC: open infrastructure as code-the network is my computer

Chunming Rong[1], Jiahui Geng[1], Thomas J. Hacker[2], Haakon Bryhni[3], Martin Gilje Jaatun[1,4]

[1] Department of Electrical Engineering and Computer Science, University of Stavanger
4036 Stavanger, Norway

[2] Department of Computer and Information Technology, Purdue University
West Lafayette, Indiana, USA

[3] Simula Metropolitan Center for Digital Engineering
Oslo, Norway

Paper 1: OpenIaC: open infrastructure as code-the network is my computer

Abstract:
Modern information systems are built fron a complex composition of networks, infrastructure, devices, services, and applications, interconnected by data flows that are often private and financially sensitive. The 5G networks, which can create hyperlocalized services, have highlighted many of the deficiencies of current practices in use today to create and operate information systems. Emerging cloud computing techniques, such as Infrastructure-as-Code (IaC) and elastic computing, offer a path for a future re-imagining of how we create, deploy, secure, operate, and retire information systems. In this paper, we articulate the position that a comprehensive new approach is needed for all OSI layers from layer 2 up to applications that are built on underlying principles that include reproducibility, continuous integration/continuous delivery, auditability, and versioning. There are obvious needs to redesign and optimize the protocols from the network layer to the application layer. Our vision seeks to augment existing Cloud Computing and Networking solutions with support for multiple cloud infrastructures and seamless integration of cloud-based microservices. To address these issues, we propose an approach named *Open Infrastructure as Code* (OpenIaC), which is an attempt to provide a common open forum to integrate and build on advances in cloud computing and blockchain to address the needs of modern information architectures. The main mission of our OpenIaC approach is to provide services based on the principles of Zero Trust Architecture (ZTA) among the federation of connected resources based on Decentralized Identity (DID). Our objectives include the creation of an open-source hub with fine-grained access control for an open and connected infrastructure of shared resources (sensing, storage, computing, 3D printing, etc.) managed by blockchains and federations. Our proposed approach has the potential to provide a path for developing new platforms, business models, and a modernized information ecosystem necessary for 5G networks.

1 Introduction and Motivation

The ongoing adoption of the 5G networking technologies and applications poses a significant challenge to the infrastructure and networking community who will be tasked with deploying and operating a full stack of services that are a composition of hyperlocalized, municipal, regional, national, and international infrastructure and services [4, 45, 7]. A recent (2020) paper by Duan et al. [56] provides an overview of challenges and opportunities inherent in the convergence of networking and cloud computing that will be at the core of 5G. It is clear that this convergence will pose significant challenges to operators who seek to provide a secure, reliable, and sustainable infrastructure that can be compliant with the policy frameworks and laws of overlapping corporate and governmental entities. 5G, as a new type of infrastructure, will promote the deep penetration and mutual integration of innovative technologies, including artificial intelligence (AI), blockchain and the Internet of Things (IoT). On the one hand, large-scale communication and mission-critical communication put higher requirements on the network's rate, stability, and latency [55]. Blockchain consensus mechanism establishment and mobile-based machine learning services are equally dependent on communication networks. On the other hand, 5G and beyond are expected to connect more than 100 billion terminal devices and heterogeneous networks [54]. Therefore, there is a need to provide trusted interoperability for 5G service management as well as for heterogeneous networks of IoT devices [36, 53]. And AI will not only reduce network latency and improve efficiency [6] but also create more service scenarios and unlock data value on top of IoT and blockchain [39, 44].

Today, mobile roaming services are now embedded in our daily lives where identities such as the IMEI (International Mobile Equipment Identity) identifier and SIM (Subscriber Identity Module) cards are used to access the cellular network infrastructure. With new capabilities provided by emerging 5G networks (and beyond), the traditional need for network resource sharing is rapidly extended to computing and resource sharing across distributed nodes, where inseparability and orchestration among the participating resource providers will be needed.

Eduroam [51] is a current example within this problem space that provides a pathfinding example. For educational institutions, Eduroam has been operational worldwide under an agreement protocol, where users are authenticated by their home institution on an as-need basis as users roam across institutions. The problem is simplified by the reality that sharing of a public WiFi resource is a relatively static exchange of information that can be shared with minimal cost. However, challenges arise when sharing incurs economic costs, e.g., if a printing service becomes part of an Eduroam agreement. There is an obvious need for open and dynamic sharing for participating members in a federation that can be managed via a contract agreement. This will require a global identifier that is recognized across and within a federation.

With fiber-connected large scale data centers as well as smaller data centers at the edge of a 5G deployment, digital value-chain creation should look beyond simple data storage in data facilities. Business value has greater potential to be created by secure, data-centered computing in a federated manner, based on the exploitation of emerging technologies such as machine learning, big data, cloud, and edge computing, software-defined communications, blockchain, and post-quantum cryptography. The availability of a trustworthy decentralized identity is necessary to enable user-focused innovations in federated ecosystems with multiple service providers. This is needed to integrate digital technologies, knowledge, and data assets to create a distributed information ecosystem that could become more responsive to citizens as well as improve customized digital services. This new decentralized infrastructure approach has great potential to address many digital ethics issues and requirements by the GDPR (General Data Protection Regulation by the European Union), including data ownership and usage, data quality, data privacy, security and accountability. These protections must be in place for managing industry data, public sector data, and personal data to ensure compliance with GDPR today and other emerging legal requirements in the future. Noticeably, major stakeholders in IT and banking have endorsed such research and innovations.

Due to the complex legal climate surrounding data, businesses

are understandably reluctant to allow data to flow outside the legal boundaries they operate within into the cloud, especially when their core business value may suffer loss. Additionally, individuals have concerns over privacy and lack of control. Hence, the industry has increasingly focused on a separated and controlled "walled gardens" rather than a common good shared public infrastructure. What is needed is a framework of App Repository Services that is similar to Google Mobile Services (GMS) and Google Play under which federated framework agreements, rules, and regulations, dispute resolution mechanisms, payment and billing are organized.

We posit that in order to achieve the goals of 5G and to provide seamless access to hyperlocalized services and information in 5G networks, a comprehensive architectural framework is needed that can be used to guide efforts to integrate the myriad of capabilities, open-source and commercial software, and hardware components. This architectural framework must ensure the utmost level of security, privacy, compliance with local laws and polices, and facilitate a viable business model that would encourage innovation and the provisioning of local, national, and international services.

Existing infrastructure approaches in use today will require significant rethinking to accommodate highly mobile users, the ability to place an infrastructure at scale at the "edge" near 5G devices, provide rock-solid security and privacy for mobile devices as well as fixed Internet of Things devices with limited onboard computing capability; and to greatly simplify and ease the integration and access to a broad range of existing and new devices. Some examples of the potential uses include: creating a virtual factory with advanced manufacturing that securely integrates geographically distributed equipment; printing devices (3D and paper); door card reader devices and room scheduling systems; and automobile information systems. A recent article in Forbes summarizes some of the potential applications of 5G technology [40]. We are now at the threshold of a time when almost every item runs software and can be interconnected.

Although existing software components and technologies can be used on an individual basis, what is lacking today is a comprehensive and robust framework that can be used to fully and securely integrate

devices and computing capabilities and scale up and out infrastructure to meet the coming needs. Generally, the gaps that need to be addressed include trust, authentication, infrastructure deployment and integration, reliability, service discovery, and data control. Figure 4.1 provides an overview of the Computing Management Services layer and a summary of the underlying services and resources that will be needed to support the open OpenIaC layer for 5G networks.

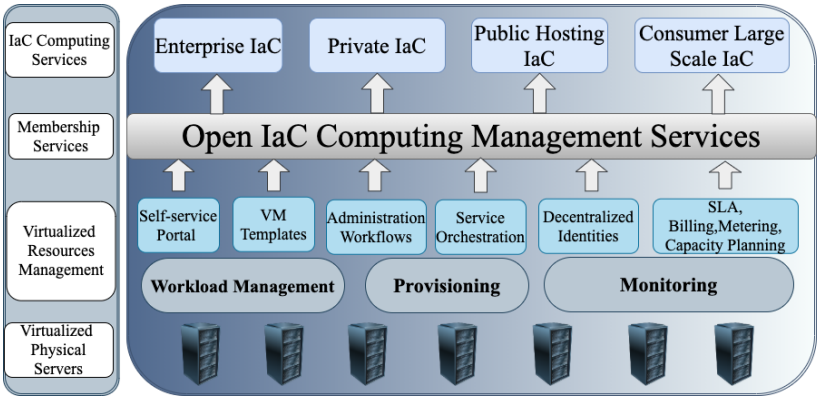


Figure 4.1: Computing Management Services and resource management in an IaC cloud

The next section of this paper summarizes some of the challenges that motivate our position. After this, we present our proposed framework.

2 Challenges to be Solved

A myriad of challenges must be solved to create a robust, secure, and reliable infrastructure platform upon which services based on technologies such as 5G and clouds need to operate. These challenges fall across many technology areas (such as networking, computing infrastructure, cloud computing, security) as well as socio-technical and legal environments.

Addressing these challenges will require the thoughtful application of existing and emerging technological components, and in many

cases require the revisiting of the underlying assumptions that were "baked into" the technologies at the time they were created.

In this section, we explore in detail some of these challenges that would need to be carefully considered and addressed to develop a comprehensive architecture. We discuss the following issues: service orchestration; service level agreements focused on billing, metering, and capacity planning; more secure networking; sharing edge computing nodes; and accountability and reliability of service providers.

2.1 Service Orchestration

The management and deployment of the infrastructure as well capabilities for 5G networks built on global and hyperlocalized services is likely to require extensive automation. Automation of management and creation of infrastructure to support 5G networks will require a common framework upon which a vast variety of service/application providers and hardware vendors can build on [56]. This is one of the motivations of our proposed OpenIaC effort. It will help break down silos between providers and inhibit the emergence of proprietary "walled gardens" that would discourage the adoption of 5G networks. Service Orchestration will be a significant challenge that will require highly reliable and scalable automated infrastructure and application environments built on Continuous Integration, Development, and Continuous Deployment pipelines.

Continuous Integration, Development, and Continuous Deployment (CI/CD) is a technique that has been developed to help automate the integration, testing, and transition into production software developed by individuals or teams that use a shared software repository, along with an automated pipeline for building and testing new and existing code, This functionality is at the heart of DevOps [34].

DevOps pipelines can include IaC capabilities as an integral part of operating the deployed infrastructure that provides the foundation for 5G services. Deploying CI/CD using IaC for a scaled-out hyperlocalized 5G installation is likely to be a formidable challenge without the presence of a widely adopted common framework.

Nemeth [34], a recent blog [50], and web article by Hisaka [21] describes some of the necessary services needed for basic CI/CD

system, which include the following components:

- Source Code Control. The heart of a continuous integration, delivery, and deployment system is represented by a stable and secure base of source code. The source code is not only for applications deployed, but also for Infrastructure-as-Code artifacts that are used to actually install and deploy the systems. GitHub [15] and GitLab [16] are popular software systems used for this today, and can provide a reasonable level of security as well as tracking the history of changes to the code base over time. Notably, Github is planning a transition to requiring tokens for access beginning in August 2021 [29].

- Automation of the process of building and testing code. As described by Nemeth [34], the CI/CD pipeline starts with a successful build operation of the code base, followed by automated testing and deployment. Tools such as Jenkins can be used to implement the workflow from build to deployment.

- Infrastructure. Computing infrastructure, provided by a cloud provider and/or organization owned resources, is needed for implementing the CI/CD pipeline. Infrastructure provisioning systems such as Kubernetes [28] or Terraform [46] as well as a container system (typically Docker [12]) is needed to create and tear down the required infrastructure for building and testing the code base.

- Images for testing and deployment. When using containers for implementing the CI/CD pipeline, as well as for application images for building, testing, and deploying, a container repository is needed for holding and disseminating the images. A docker repository is one example that can be used. Other examples include Helm [20] (for Kubernetes), JFrog Artifactory [3], and Nexus [35].

2.2 Infrastructure as Code (IaC)

Deploying and managing services within the OpenIaC framework requires capabilities to express the infrastructure using Infrastructure

as Code (IaC) [32] techniques. Implementing a production IaC system will need a consistent software and infrastructure support environment to reliably and securely function. Morris [31] describes some of the underlying principles motivating IaC that reflects the critical need for OpenIaC for 5G infrastructure. These principles include: building on the assumption that the underlying infrastructure and systems will not be dependable; avoiding specialization in individual systems (Morris calls these "snowflake systems"), in which every system is unique; and creating infrastructure that can be "disposable" as needs fluctuate to support efficient scaling. Overall, this approach is focused on exploiting software versioning, repeatability, and auditability of the infrastructure. These principles are all in service to the primary goal of seeking to fully automate the creation, deployment, and retirement of the complete top-to-bottom infrastructure.

As 5G infrastructure is created and deployed, there is a critical need to fully express the infrastructure "as code" rather than a jumbled collage of one-off systems that are overly complex that present users with a confused jumble of out-of-revision services with many vulnerabilities.

In the context of Infrastructure-as-code, there are several areas that represent challenges that will need to be addressed at the intersection of IaC and our envisioned OpenIaC framework.

- Integration of infrastructure IaC code into application and service CI/CD pipelines. If we assume that each application and/or service is managed using a CI/CD pipeline, then the CI/CD pipeline for the code for the infrastructure will need to be coordinated with the CI/CD pipelines for the applications and services. This will be especially important if the applications and services require specialized infrastructure components, or if there are conflicting requirements among the applications and services.

- IaC language basis. As described in Morris [31], the power of declarative (e.g., Puppet) vs. imperative (e.g., BASH scripts) languages used to express infrastructure requires a shift in thinking. Finding good balances between declarative and imperative

expressions of infrastructure is likely to be an ongoing challenge for IaC developers operating 5G network infrastructure.

- Managing the plethora of cloud infrastructure providers, provisioning and configuration management tools. There are many cloud vendors offering infrastructure, as well as options for owning and running infrastructure in-house. The challenge will be in managing the complexity of the combination of infrastructure, provisioning, and configuration management tools in an always-running production infrastructure scaled out geographically and scaled up in services and applications. For example, which tools (i.e., Kubernetes and Terraform) work best for infrastructure and provisioning? For configuration management, would Puppet or Ansible be best? How would the evolution across and among these tools be managed over time as needs and services change over time?

- Navigating the close vertical integration of networking, infrastructure, applications, and services, as well as the bootstrapping and management of these services as monolithic vs. micro stacks [31] that are expressed as IaC code will be an operational challenge.

- Managing the people side of this – who is authorized to make changes, is there an equivalent of a change control board, how are changes approved? can a change be backed out easily if it causes a problem?

2.3 Redesign Secure Networking

The layer 2 network architecture available today is based on Ethernet standards initially developed in the 1980s. Although these standards have evolved somewhat over time as we moved from coaxial cable to twisted pair and fiber optics, some of the fundamentals of how these networks operate and are used every day have not kept up with current needs and the increasingly hostile security environment. As a consequence, we rely today on outmoded capabilities that have serious inherent security drawbacks that represent a potential threat.

What is needed is to revisit and redesign the network architecture (hardware, software, and protocol) with an aim of updating the built-in assumptions in Ethernet from the past to increase performance, evolve networking for new application requirements, improve quality of service, improve energy efficiency and the environment (e.g., repairability and recyclability), increase security and resilience, and to evolve networking to inherently support a model of open technology frameworks that can easily integrate existing and new technologies and applications to provide a suite of services for other systems as well as for users.

Ethernet has served us well, and provided a reliable base for building applications and services over the global Internet for layer 3 and higher-layer services. Ethernet provided a stable platform that supported the development of significant capabilities and innovations in TCP/IP, ranging from the simple (such as ports and congestion avoidance) to the complex (such as IPSec and modern routing protocols). TCP/IP has evolved to facilitate the movement of packets across wide areas and many different administrative domains. In contrast to layer 3, Ethernet has been bound to provide services to only a limited geographic span – by practice and by necessity within a single administrative domain.

The lack of evolution of Ethernet has created significant capability gaps. The first gap is the assumption in Ethernet that a network operator can completely control where and when a system attaches to a network. This assumption needs to be revised to include an access control model that can be easily deployed. There have been many efforts to define standards for access control for wired networks (e.g. 802.1X, 802.1AE (MACsec)) over the past decade. In practice, however, these are not widely used to the same extent that access control is implemented for wireless networks. One example, Open1X [37], has been quiescent for over a decade. Moreover, if an end device is not 802.1X capable, or is attempting to PXE boot from the network port, 802.1X will not directly support this device without complex workarounds within the network and the system[8, 41].

With the need for enhanced network functionality grounded in layer 2, and the pervasively hostile networking environment, what

is needed for networking today and in the future is a fundamental shift to designing networks and applications based on a "zero trust" networking model based on an architectural approach described in the recent paper from NIST [42]. Any and all devices that attach to a wired or wireless network need a default "zero trust" mode that does not permit the device to attach to the network without meeting security standards to protect the device from attack or intrusion. The definition of a device ranges from simple IoT devices and sensors up to entire clusters of hardware nodes or VMs.

The second gap in Ethernet today is that it does not include a conceptual equivalent of ports in IP. IP ports allow a single host to provide access points for multiple services accessible at a single IP address. Ethernet features an EtherType field (represented in Linux in the */etc/ethertype* file) that is currently populated with defunct networking protocols (e.g., DECnet and AppleTalk) that could perhaps be re-purposed to represent Ethernet services using the equivalent of IP ports available at a single Ethernet address.

There are several consequences of this lack of evolution of Ethernet that have created security problems and capability gaps. First, we cannot easily control where and when services (such as DHCP and ARP) are offered within an Ethernet broadcast domain. This is the source of security vulnerabilities (such as ARP spoofing and multiple DHCP providers) arising from the multiple offering of the same service within a broadcast domain. There is no clear analog to ports or services for Ethernet that would allow the targeted inquiry and discovery of layer 2 services using a combination of Ethernet multicast and EtherType frames. There is also the possibility of the multiple overlapping offering of the same service within an Ethernet broadcast domain, and there are no comprehensive mechanisms (other than broadcast queries) to discover layer 2 services available in a broadcast domain.

These gaps in capabilities and problems lead to poor security and difficulties in controlling the publication and unpublication of layer 2 services. The workaround for these problems is to partition broadcast domains using VLANs or physical network separation (such as air gapping) that are complex and difficult to scale and manage, which

leads to inherent vulnerabilities. The overall consequence is that it is complicated and difficult to create new layer 3 protocols that can rely on large scale (geographic and number of stations) Ethernet broadcast domains.

It is clear that a comprehensive effort is needed to revisit and redesign the layer 2 network architecture (hardware, software, and protocols) with a focus on gaps existing today and with a view of anticipating future needs and vulnerabilities. Open challenges include performance, adaptability to application requirements, quality of service, resilience in the face of security threats, energy efficiency, environmental considerations (repairability and recyclability), and being increasingly supportive of open and decentralized technologies and services. A recent paper by Moubayed et al. [33] describes an architectural framework approach named *Software Defined Perimeter* that has the potential to address many of the gaps.

2.4 Sharing Edge Nodes

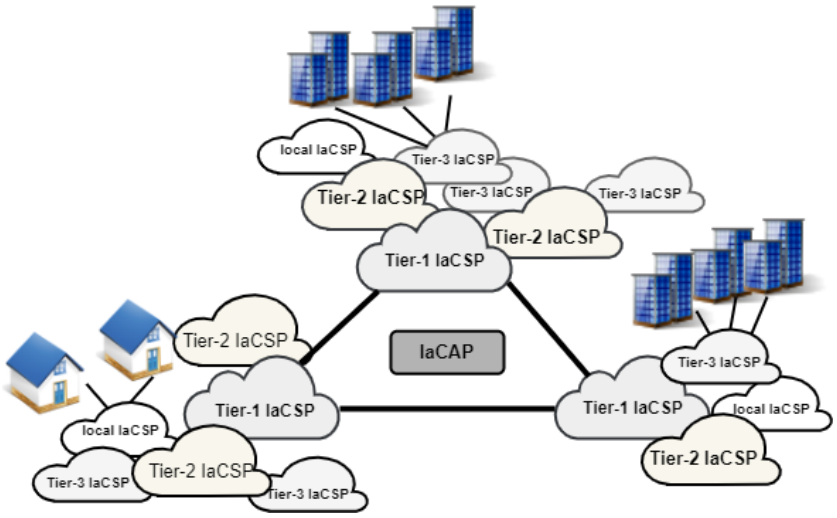


Figure 4.2: IaC nodes in a Network of networks.

Cloud computing has proved cost-effective compared to on-premises data centers and is now the de-facto choice for enterprise and public

use with some exceptions where very strict security and legislation for national control of storage location is required. However, cloud computing may not be used for an emerging class of applications with time-sensitive requirements due to the high and unconstrained latency from the application to the physical location of the processing capacity offered. In the cloud, the location may also change due to virtualization and load balancing. This is particularly important for the emerging Industry 4.0 applications and is a key feature of the 5G network structure. 5G provides 3 main service modes: Massive Machine Type Communications (mMTC); Ultra-reliable and Low-latency Communications (uRLLC); and Enhanced Mobile Broadband (eMBB). For the uRLLC service, it is necessary to place processing elements close to the subscribers. This computing facility is called Mobile Edge Computer (MEC) [19] and provides a means for time-sensitive computing, where processing can be guaranteed within a hard deadline.

In our near future, we will see a processing continuum from device, to edge processing in a MEC, to processing in a cloud. The cloud may belong to an organization, be within a national state, a larger area like EU, or be placed in any data center independent on location. Both application requirements to latency and bandwidth, cost of the different alternatives and the applicable legal frameworks like GDPR may mandate where processing is performed. The EU HORIZON program has recognized this challenge, and has called for large academic and industrial collaboration related to how AI can enable computing continuum from Cloud to Edge [52].

Figure 4.2 shows the OpenIaC network architecture. Similar to the Internet architecture, the different levels of service provider in OpenIaC (IaCSP) codify the distributed infrastructure as services to cover a wider range of consumers, enabling flexible and rapid remote deployment and proximity services, reducing the impact of spatial distance.

2.5 Accountability and reliability of service providers

One of the drawbacks of Eduroam is that when one roams to a different institution and cannot successfully connect to local services,

it is difficult to find support at the roaming institution or one's home institution to quickly resolve the problem. This is a dual problem of accountability and reliability. A described by prior work by co-author Jaatun [25], any service provider who wishes to be accountable must adhere to a set of principles that can be summarised as *define, monitor, remedy, and explain*. These have been set out in the context of personal and business confidential information [25], but can be applied to the provision of services in general. More explicitly, as described in [25], the necessary elements that need to be present are:

(i) **Obligation**: An organization willing to be obligated to accountability needs to accept responsibility for its actions and practices related to data.

(ii) **Policy Clarity**: Clear policy definitions regarding practices are necessary for organizational accountability.

(iii) **Compliance Monitoring**: Ongoing monitoring of compliance of data practices with policies.

(iv) **Amelioration**: Correction of identified violations of data polices.

(v) **Policy Auditing**: Beyond active monitoring, an essential element is the ability of an organization to show that it has complied with data polices over time.

Using the example of Eduroam, it is not clear who is responsible for ensuring that services work while roaming. Two parties are involved in ensuring that the service is available and reliable: the home institution of the person roaming, and the local provider of the service. Theoretically, every pair of institutions participating in Eduroam should be accountable for ensuring that the roaming network service is available and reliable. This is an $O(n^2)$ problem if n institutions participate in Eduroam. In 5G networks, with extensive roaming and potentially many hyperlocalized services, n will be much larger, and the problems will become much more difficult.

Potentially, willingness to be accountable could be used as a competitive advantage, if customers are sufficiently concerned to choose accountable providers over others [25].

2.6 Challenges from SLA, Billing, Metering and Capacity Planning

An essential aspect of providing a multilayered suite of services in a 5G service ecosystem will be the ability to offer, negotiate, invoice, and audit provider and consumer relationships. Service Level Agreements (SLAs) provide a means to define service providers' content (SPs) to consumers of those services. Gomez [17] provides a brief discussion of this problem in the context of cloud computing. SLAs can be among software service industries, between hardware infrastructure and software service providers, and between software service providers and general users.

When considering the problem of providing and billing services from a marketplace of local, regional, national, and global providers, the ability to verify and audit invoices and payments is necessary to establish and maintain trust in the system and overall growth in the marketplace.

One example today of this need is the reliability of cable TV services. If some of the subscribed channels become temporarily unavailable, then the contractual agreement to deliver the service of that channel to a customer is violated. Ideally, the cable company would actively monitor reliability and accordingly adjust monthly billing. However, in practice, customers are expected to contact the providers to seek credits when an outage occurs [13].

Alzubaidi [2] describes some of the issues related to SLAs related to IoT services, and describes their blockchain-based approach for monitoring and enforcing SLAs.

Hardware infrastructure providers offer parts or even complete IT infrastructure to virtual service providers. Due to the lack of transparency in the billing invalidating process, providers' compliance with service level agreements (SLAs) can be challenging to track. It can erode customers' trust in the service provider.

There are several advantages to moving to a blockchain-based mechanism for enforcing and monitoring SLAs. These advantages include:

- Blockchain supports an environment where both parties do not

need to trust each other, thus reducing market barriers, as trust is a priority when choosing a service provider.

- Participants will send process data directly from their system of record to the blockchain, helping to avoid errors during manual data entry, granting visibility to selected participants, and protecting privacy when multiple parties are involved.
- It brings transparency to service delivery, where all rules for SLA management are clearly defined in a public smart contract, minimizing the need for disputed cases and escalations.
- Improved incident management process. Reported incidents can be raised automatically and processed immediately in a non-repudiation manner.
- Better relationships are built with value chain partners, suppliers, and customers.

The challenges related to managing SLAs and smart contracts will be significant, and if not solved may pose a severe impediment to the adoption of 5G network based services.

3 Our position: the Network is My Computer

Sun Microsystems and Cloudflare created the concept that *"the network is the computer"* [47]. We posit that in reality the network is ***my*** computer. Eduroam is an early example of the direction that we posit needs to be pursued more generally and broadly with the emergence of 5G networks. Eduroam provides for sharing of access to institutional WiFi networks across higher education institutions internationally.

Another example is cell phone roaming. Roaming refers to the ability for a cellular customer to continue to use the communication and the Internet functions when traveling outside the coverage area of the operators. Roaming can be divided into "SIM-based" or "username/password-based" cases. A typical example of the former is the mobile international roaming service, and the latter is Eduroam.

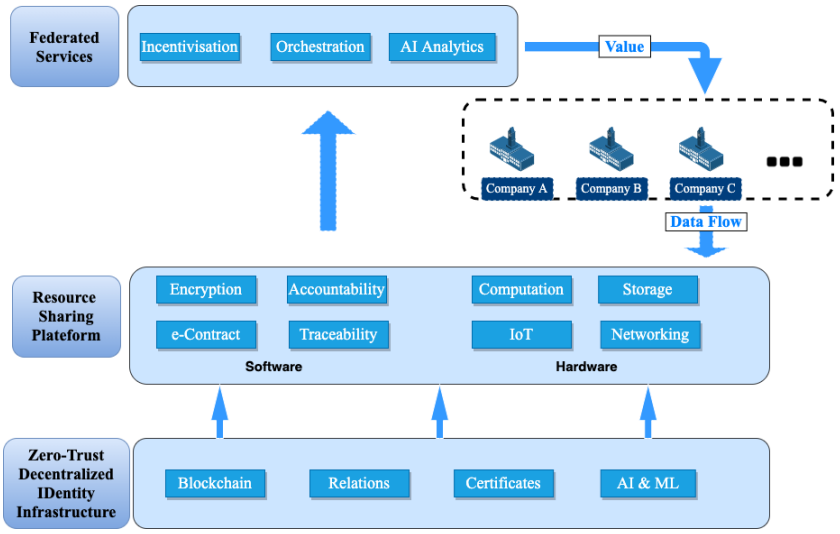


Figure 4.3: Services based on distributed membership in a federation

Roaming also includes the processes of mobility management, authentication, authorization and accounting billing.

In this section, we describe several emerging technological capabilities that we argue will be essential for operating the 5G infrastructure to realize the vision of *my network is the computer*. These technologies include blockchain-powered smart contracts, decentralized identity management and zero-trust information architecture. Figure 4.3 illustrates the provision of federated services in the OpenIaC system. Based on a zero-trust network and decentralized identity system, all services will need to be developed on shared resources, including software and hardware resources, ensuring cryptography, auditability, and traceability. And artificial intelligence, incentives, and service orchestration will accelerate the flow and interconversion of data and value.

IaC authorizes all computing resources, and the preparatory work can be done through code. Computing resources include computation, storage, network, security, etc. The IaC service platform, as illustrated in Figure 4.4 includes three cores: configuration, including templates, policies, etc., mapping infrastructure to programmable code; Orchestration engine, consisting of Terraform, Kubernetes, etc.,

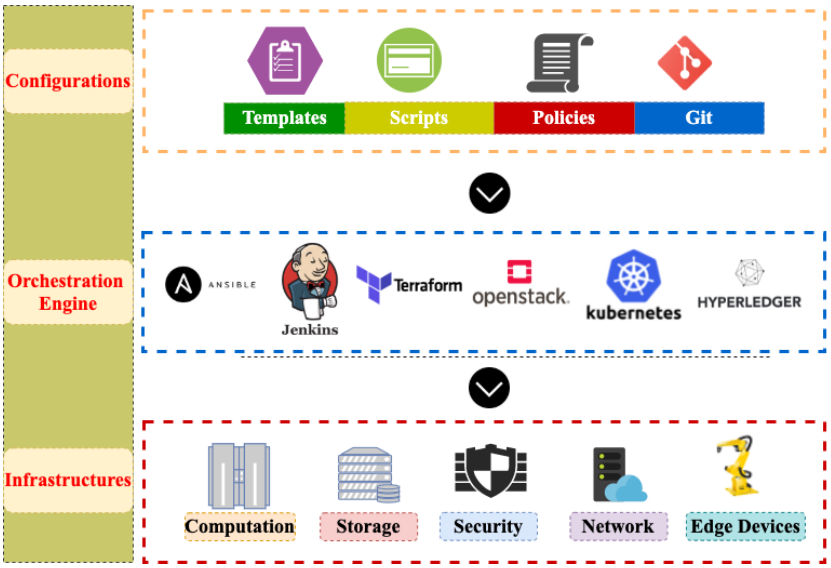


Figure 4.4: IaC Service Platform design: Membership and virtualized resources

creating resources based on configuration; and the bottom infrastructure. The whole orchestration is automated, starting with the system architecture design, considering load balancing and RDS resources. Then the designed architecture is converted into a configuration, which describes the relationships between resources. The created configuration is given to the orchestration engine, which manages the infrastructure according to the configuration, including allocation, updates, and upgrades.

3.1 Zero-Trust Architecture(ZTA)

The goal of our proposed OpenIaC approach is to provide borderless, mobile access to infrastructure services. Users can access services anytime and anywhere on any device, which increases convenience and productivity, but security risks inevitably increase.

The traditional network security model assumes that a network perimeter exists around intranet devices as a trust zone, where any operation inside is considered to be trusted after proper authentication. However, due to the mobility and heterogeneity of 5G and beyond,

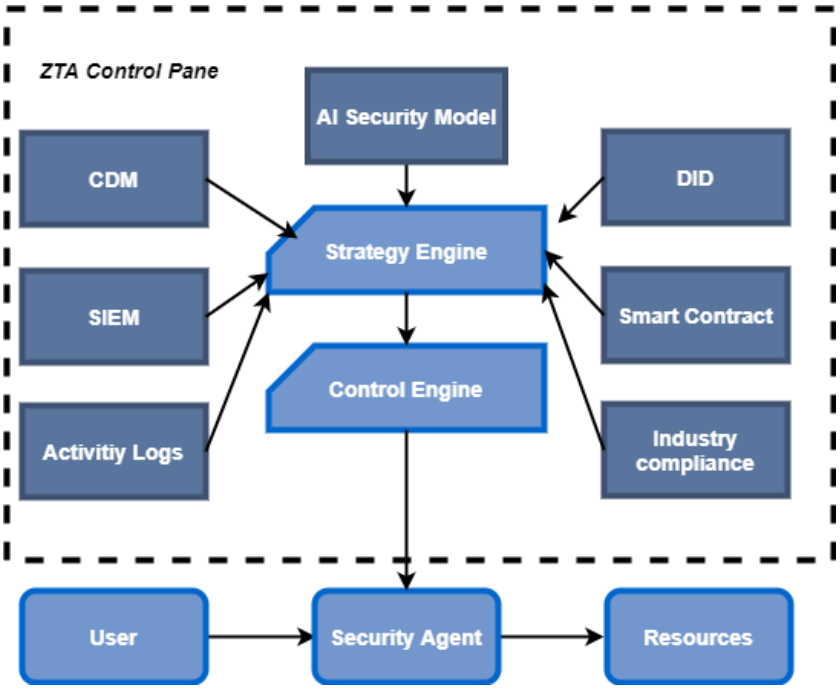


Figure 4.5: Security management in OpenIaC based on zero trust Principles

such an assumption has been broken. This has resulted in significant cybersecurity challenges, for example, the Colonial Pipeline cyber attack [9] and JBS S.A. cyberattack [26] in May 2021. Once inside the firewall or VPN, the control is minimal because of the default trust in the illusory network perimeter.

The concept of Zero Trust has been introduced and has evolved significantly over the past decade as perimeter-based network security architectures struggle to address today's cyber threats. The Zero Trust model was first proposed by Kindervag in 2010, who argued that any network traffic should not be trusted until it was verified [27]. Google has also focused on Zero Trust and published several papers related to BeyondCorp [49, 38, 5], providing a comprehensive overview of the BeyondCorp architecture and Google's practice from 2011 to the present. In 2013 Cloud Security Alliance (CSA) proposed Software-Defined Perimeter (SDP) [18], the core idea of which is to hide core network assets and facilities from exposure to the Internet.

In 2017 Gartner proposed the Continuous Adaptive Risk and Trust Assessment (CARTA) approach, in which continuous detection was implemented to assess risks, and access control was adaptively changing according to context. The National Institute of Standards and Technology (NIST) published a special publication [43] defining the zero trust architecture in detail in 2020, which has attracted much attention from research and industry.

OpenIaC proposes an innovative zero-trust security solution using smart contracts and decentralized identity(DID). As illustrated in Figure 4.5, the upper part is the control pane, and the lower part represents users, security agents, and resources, respectively. The security agent establishes a secure connection between the user and the resource mainly through a user-side plug-in and a resource-side gateway. The gateway forwards all traffic for monitoring traffic and evaluating access requests. Resources include computation, storage, and data assets, etc.

Control Pane consists of a policy engine, which integrates components including continuous diagnostics and mitigation (CDM), security information and event management(SIEM), activity logs, smart contract, DID (our identity management system described in the next section 3.2), industry compliance, and a control engine, which is responsible for responding to abnormal traffic at the gateway based on the policy engine's analysis. The unique AI security model provides situational awareness for overall system security, modeling user and user behavior and resources respectively by assessing in real time the user's confidence score, the risk of each operation request, and the vulnerability of specific devices within the system and possible attacks.

Figure 4.6 shows a usage scenario in OpenIaC, controllable remote computing. It is a secure computing paradigm for privacy protection. People have gradually realized the importance of data sovereignty and regulations like GDPR require that data access be verifiable and restrict data transmission without adequate protection. On the premise of not copying or uploading data, the user analyzes the data on the server of the data owner. A smart contract is a computer protocol that is self-executing and self-verifying without

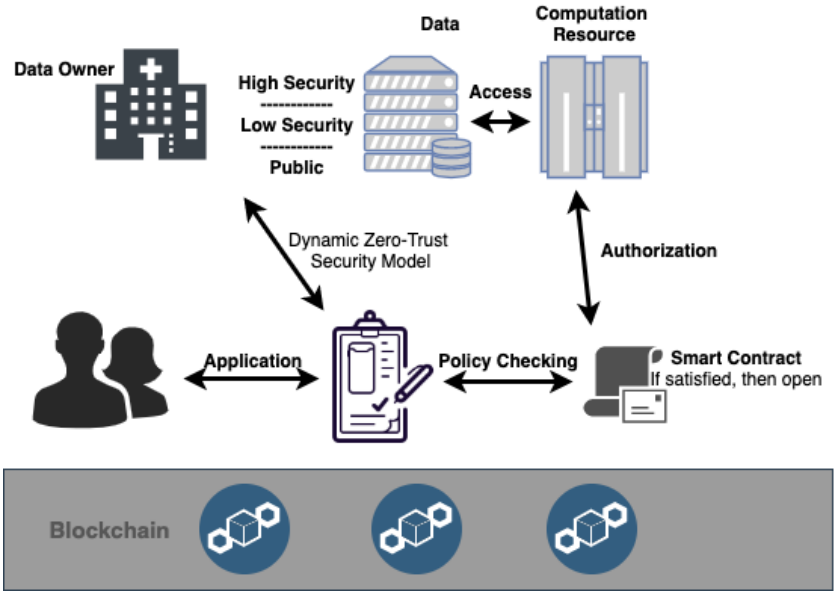


Figure 4.6: Virtual remote computing supported by OpenIaC

additional human intervention after the protocol has been developed and deployed. The decentralized and tamper-evident technology of blockchain makes the content of the contract and the record of each call tamper-evident. The data owner updates the data access policy, and the Zero Trust security model continuously assesses the risk of the system at the gateway, and the smart contract checks whether to grant the user access to remote computing.

3.2 Decentralized Identity (DID)

At the inception of the World Wide Web, no digital identity was designed into the underlying protocol. The TCP/IP protocol does not force users to provide proof of their identity, although the user's local Internet access point (e.g., some universities) may require users seeking Internet access to provide their real names. Despite this, the user's information is also held by the local Internet access point and is not used as part of the transmission of information over the Internet. In the traditional identity management(IdM) model, users

need to register separate accounts for each service, which complexity user account management. Mainstream websites now offer identity federation services. As an identity provider, they will send a statement to the service provider after verifying the user's identity with the information required by the service provider, including the username. The user can access the service more quickly, and the identity provider also increases user stickiness. Armed with vast amounts of user data, they can better analyze user behavior patterns and conduct commercial promotions to both users and service providers. Handing over personal identity information to a commercial organization poses a privacy risk. The British consultancy Cambridge Analytica accessed the personal data of millions of Facebook users without their consent and used the information for political advertising [1]. Governments and public organizations are trying to promote digital identity and identity federation. In the digital era, e-commerce, digital government, education, healthcare, and insurance will benefit from IdM. An impressive example of identity federation is eduGAIN (EDUcation Global Authentication INfrastructure) [22], co-funded by the European Union and Europe's NREN (National Research and Education Network), which aims to achieve an identity federation for national education and research networks across countries and to enable the sharing of global education and research resources. the sharing of global education and research resources.

Trust is the biggest challenge to achieving identity federation, and it occurs between individuals and organizations and among organizations. Users can be concerned about personal privacy, and reaching trust between organizations requires lengthy communication and negotiation. Now with cryptography and blockchain techniques, a trusted identity federation is considered to be feasible. Relying on the decentralized, traceable, and untamperable nature of blockchain, decentralized identity (DID) allows users to take back data sovereignty and the underlying decentralized public key infrastructure (DPKI) will help enable identity and statement verification. Working groups from the Decentralized Identity Foundation (DIF) [11] and the World Wide Web Consortium (W3C) [10] are defining and developing standards for DID. Several commercial companies are also promoting DID

technology solutions, such as Indy [23], Veramo [48] and civic [24]. Recent work by Maram [30] describes a DID system the authors developed (CanDID) that is a step towards a user-oriented DID system. Geng et al. propose to enhance the openness and security of federated learning system with the DID sytem[14].

OpenIaC regards identity federation as a critical aspect of open systems. Identity federation allows external users in one organization to access services provided by another organization with their own identities. Heterogeneous infrastructures, different security levels, SLAs, and billing systems require universal identity management for OpenIaC.

OpenIaC proposes a framework consisting of a DID resolution protocol, a DPKI-based DID ledger, and a challenge-claim authentication system. The new user will receive a DID Identifier and a DID Document after authentication. The DID document will be uploaded to the DPKI-based DID ledger and will be accessible to all. When the service provider (SP) wants to determine the quality of service based on the user's attributes, he will send a challenge to the user, and the user will provide the corresponding claim in response. The challenge-claim pair will be forwarded to the DID Resolver by the SP according to the DID resolution protocol, and the DID Identifiers of both parties contained in it will be resolved on the DID Ledger to verify the identity of both parties. The user's access record will be recorded in the distributed ledger for traceability. The challenge-claim authentication system is a protocol designed to protect user privacy.

The DID resolution process relies on the server: DID Resolver, which functions similarly to a DNS Server and translates DID Identifier into DID document addresses. Based on the DID Identifier provided by a user, a browser sends a request to a DID server, such as the local DID service provider, to send a DID resolution request. If this server has the DID address in its cache, it will then provide the correct information to the host sending the request. If the DID address is not found on this server, it will contact the root server. Usually, the root server will redirect this server to the correct top-level DID server.

A verifiable claim or credential is a statement issued by an issuer about specific attributes, and the digital signature is attached to prove the authenticity. Claims can be stacked, increasing the flexibility of identity verification. The general pre-issued claims containing user attributes can only handle simple scenarios. On the one hand, user data is enormous, Issuer may be a platform or enterprise, and it is impractical to transfer the vast data saved to the user device, and the user is concerned about the authorization of data access. On the other hand, complex attribute verification still requires interaction with the Issuer's database for confirmation based on the specific content of the challenge.

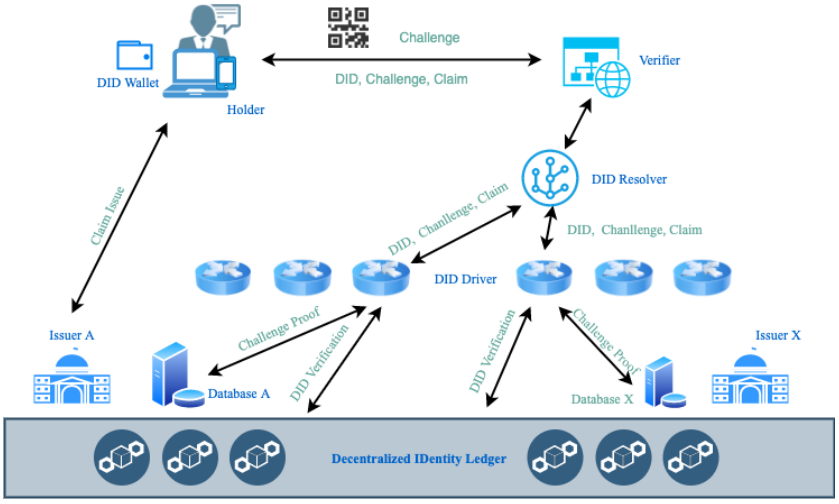


Figure 4.7: The DID system proposed by OpenIaC.

In Figure 4.7, we show the DID system with privacy protection proposed by OpenIaC. When faced with a complex Challenge request, the user selects the appropriate Claim from the DID wallet and signs it to send back to the service provider, the Verifier. The Claim contains the DID Identifiers of the user and Issuer. The service provider forwards the information to the DID Resolver. Through DID Resolver parsing, the appropriate DID Driver is selected to communicate with Issuer's database, and Issuer sends the challenge results to the DID Driver. DID Driver will confirm Challenge, Claim, and Proof digital signatures against the authentication material stored

in the DID distributed ledger to ensure data authenticity during this period. The hash results of the entire DID system log, including DID Resolver and DID Driver, will be recorded in the blockchain to ensure the trustworthiness of the results. Zero-Knowledge Proof and Privacy Set Intersection techniques can be used to protect user privacy and prevent leakage of Issuer and Verifier user distributions.

4 Conclusion

In this paper, we presented our position that an open and community adaptable framework is needed to form and operate the infrastructure needed to build out future 5G networks and services. We summarized some of the challenges that needed to be solved, service orchestration, infrastructure as code expression of infrastructure, the need for a significant security-oriented redesign of networking; and accountability and reliability. We presented a position that the network is *my* computer, which motivates the need for distributed identity, zero-trust architectures, and blockchain basis for metering, invoicing, and billing for the use of services. We sketched out a framework, OpenIaC, that will help establish a community-driven body of interoperability standards that will present an alternative path as a counterpoint to the motivation to develop ”walled garden” vendor locked-in 5G network and service ecosystems that would present impediments to sharing and mobility. In essence, future 5G networks should be globally interoperable, as WiFi networks are today, to avoid the development of non-interchangeable infrastructure - i.e., the way in which power systems globally use different voltages and plug standards.

Bibliography

[1] *"Cambridge Analytica and Facebook: The Scandal and the Fallout So Far"*. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. Accessed: 2021-08-16.

[2] Ali Alzubaidi, Karan Mitra, Pankesh Patel, and Ellis Solaiman. "A Blockchain-based Approach for Assessing Compliance with SLA-guaranteed IoT Services." In: *2020 IEEE International Conference on Smart Internet of Things (SmartIoT)*. 2020, pp. 213–220. DOI: 10.1109/SmartIoT49966.2020.00039.

[3] *Artifactory*. https://jfrog.com/artifactory/. Accessed: 2021-08-16.

[4] Murat Aydemir and Korhan Cengiz. "Emerging infrastructure and technology challenges in 5G wireless networks." In: *2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech)*. IEEE. 2017, pp. 1–5.

[5] Betsy (Adrienne Elizabeth) Beyer, Colin McCormick Beske, Jeff Peck, and Max Saltonstall. "Migrating to BeyondCorp: Maintaining Productivity While Improving Security." In: *Login* Summer 2017, VOl 42, No 2 (2017). ISSN 1044-6397.

[6] Manuel Eugenio Morocho Cayamcela and Wansu Lim. "Artificial Intelligence in 5G Technology: A Survey." In: *International Conference on Information and Communication Technology Convergence, ICTC 2018, Jeju Island, Korea (South), October 17-19, 2018*. IEEE, 2018, pp. 860–865. DOI: 10.1109/ICTC.2018.8539642. URL: https://doi.org/10.1109/ICTC.2018.8539642.

[7] Xing Chen, Shihong Chen, Xuee Zeng, Xianghan Zheng, Ying Zhang, and Chunming Rong. "Framework for context-aware computation offloading in mobile cloud computing." In: *Journal of Cloud Computing* 6.1 (2017), pp. 1–17.

[8] Cisco. *Wired*. Accessed: 2021-08-16. 2011. URL: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec%5C_1-99/Dot1X%5C_Deployment/Dot1x%5C_Dep%5C_Guide.html.

[9] *Colonial Pipeline attack made possible by compromised VPN password.* https://www.techradar.com/news/colonial-pipeline-attack-made-possible-by-compromised-vpn-password. Accessed: 2021-08-16.

[10] *Decentralized Identifiers (DIDs) v1.0 - Core architecture, data model, and representations, W3C Candidate Recommendation Draft, 2021.* https://www.w3.org/TR/did-core/. Accessed: 2021-08-16.

[11] *Decentralized Identity Foundation.* https://identity.foundation/. Accessed: 2021-08-16.

[12] *Docker.* https://www.docker.com/. Accessed: 2021-08-16.

[13] Taylor Gadsden. *Does your provider owe you money for their service outages?* allconnect.com/blog/get-bill-credits-for-service-outages. Accessed: 2021-09-07.

[14] Jiahui Geng, Neel Kanwal, Martin Gilje Jaatun, and Chunming Rong. "DID-eFed: Facilitating Federated Learning as a Service with Decentralized Identities." In: *Evaluation and Assessment in Software Engineering*. 2021, pp. 329–335.

[15] *GitHub.* https://github.com/. Accessed: 2021-08-16.

[16] *GitLab.* https://gitlab.com/. Accessed: 2021-08-16.

[17] Sergio García Gómez, Juan Lambea Rueda, and Augustín Escámez Chimeno. "Management of the Business SLAs for Services eContracting." In: *Service Level Agreements for Cloud Computing*. Ed. by Philipp Wieder, Joe M. Butler, Wolfgang Theilmann, and Ramin Yahyapour. New York, NY: Springer New York, 2011, pp. 209–224. ISBN: 978-1-4614-1614-2.

[18] Software Defined Perimeter Working Group et al. "Software defined perimeter." In: *Cloud Security Alliance, Toronto, Canada* (2013).

[19] Lav Gupta, Raj Jain, and H Anothony Chan. "Mobile edge computing—An important ingredient of 5G networks." In: *IEEE Software Defined Networks Newsletter* (2016).

[20] *Helm.* `https://helm.sh/`. Accessed: 2021-08-16.

[21] Alex Hisaka. *Service Orchestration: What It Is and Why You Need It.* `https://d2iq.com/blog/service-orchestration-what-it-is-and-why-you-need-it?`. Accessed: 2021-09-21.

[22] Josh Howlett, V Nordh, and W Singer. "Deliverable DS3. 3.1: eduGAIN service definition and policy Initial Draft." In: *Project Deliverable, May* (2010).

[23] *Hyperledger Indy.* `https://www.hyperledger.org/use/hyperledger-indy`. Accessed: 2021-08-16.

[24] *Identity Verification by Civic.* `https://www.civic.com/`. Accessed: 2021-08-16.

[25] Martin Gilje Jaatun, Siani Pearson, Frédéric Gittler, Ronald Leenes, and Maartje Niezen. "Enhancing Accountability in the Cloud." In: *International Journal of Information Management* 53 (2020). ISSN: 0268-4012. DOI: `http://dx.doi.org/10.1016/j.ijinfomgt.2016.03.004`. URL: `//www.sciencedirect.com/science/article/pii/S0268401216301475`.

[26] *JBS, world's largest meat producer, getting back online after cyberattack.* `https://www.cnbc.com/2021/06/02/jbs-worlds-largest-meat-producer-getting-back-online-after-cyberattack.html`.

[27] John Kindervag et al. "Build security into your network's dna: The zero trust network architecture." In: *Forrester Research Inc* (2010), pp. 1–26.

[28] *Kubernetes.* `https://kubernetes.io/`. Accessed: 2021-08-16.

[29] Matthew Langlois. *Token authentication requirements for Git operations*. Accessed: 2021-08-16. 2020. URL: https://github.blog/2020-12-15-token-authentication-requirements-for-git-operations/.

[30] Deepak Maram, Harjasleen Malvai, Fan Zhang, Nerla Jean-Louis, Alexander Frolov, Tyler Kell, Tyrone Lobban, Christine Moy, Ari Juels, and Andrew Miller. "CanDID: Can-Do Decentralized Identity with Legacy Compatibility, Sybil-Resistance, and Accountability." In: *2021 IEEE Symposium on Security and Privacy (SP)*. 2021, pp. 1348–1366. DOI: 10.1109/SP40001.2021.00038.

[31] Kief Morris. *Infrastructure as Code*. O'Reilly Media, 2020.

[32] Kief Morris. *Infrastructure as code: managing servers in the cloud*. " O'Reilly Media, Inc.", 2016.

[33] Abdallah Moubayed, Ahmed Refaey, and Abdallah Shami. "Software-defined perimeter (sdp): State of the art secure solution for modern networks." In: *IEEE network* 33.5 (2019), pp. 226–233. DOI: 10.1109/MNET.2019.1800324.

[34] Evi Nemeth, Garth Snyder, Trent R Hein, Ben Whaley, and Dan Mackin. "UNIX and Linux system administration handbook." In: *USENIX Open Access Policy* 59 (2018).

[35] *Nexus.* https://www.sonatype.com/products/container. Accessed: 2021-08-16.

[36] Dinh C Nguyen, Pubudu N Pathirana, Ming Ding, and Aruna Seneviratne. "Blockchain for 5G and beyond networks: A state of the art survey." In: *Journal of Network and Computer Applications* 166 (2020), p. 102693.

[37] *Open1X.* http://open1x.sourceforge.net/. Accessed: 2021-08-16.

[38] Barclay Osborn, Justin McWilliams, Betsy Beyer, and Max Saltonstall. "BeyondCorp: Design to Deployment at Google." In: *;login:* 41 (2016), pp. 28–34. URL: https://www.usenix.org/publications/login/spring2016/osborn.

[39] Kefa Rabah. "Convergence of AI, IoT, big data and blockchain: a review." In: *The lake institute Journal* 1.1 (2018), pp. 1–18.

[40] R. Scott Raynovich. *The Real Year of 5G: What it Means For Cloud Technology*. Forbes. Accessed: 2021-08-16. 2021. URL: https://www.forbes.com/sites/rscottraynovich/2021/03/31/the-real-year-of-5g-what-it-means-for-cloud-technology/.

[41] Bob Reny. *Ring the Bell, 802.1x is Dead*. Accessed: 2021-08-16. 2019. URL: https://www.forescout.com/company/blog/ring-the-bell-8021x-is-dead/.

[42] Scott Rose, Oliver Borchert, Stu Mitchell, and Sean Connelly. *Zero Trust Architecture*. NIST Special Publication 800-207. Accessed: 2021-08-16. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

[43] Scott Rose, Oliver Borchert, Stu Mitchell, and Sean Connelly. *Zero Trust Architecture (2nd Draft)*. Tech. rep. National Institute of Standards and Technology, 2020.

[44] Saurabh Singh, Pradip Kumar Sharma, Byungun Yoon, Mohammad Shojafar, Gi Hwan Cho, and In-Ho Ra. "Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city." In: *Sustainable Cities and Society* 63 (2020), p. 102364.

[45] Carlos Renato Storck and Fátima Duarte-Figueiredo. "A Survey of 5G Technology Evolution, Standards, and Infrastructure Associated With Vehicle-to-Everything Communications by Internet of Vehicles." In: *IEEE Access* 8 (2020), pp. 117593–117614. DOI: 10.1109/ACCESS.2020.3004779.

[46] *Terraform*. https://www.terraform.io/. Accessed: 2021-08-16.

[47] *The Network is the Computer*. https://blog.cloudflare.com/the-network-is-the-computer/. Accessed: 2021-08-16.

[48] *Veramo, A JavaScript Framework for Verifiable Data*. https://veramo.io/. Accessed: 2021-08-16.

[49] Rory Ward and Betsy Beyer. "BeyondCorp: A New Approach to Enterprise Security." In: *;login:* Vol. 39, No. 6 (2014), pp. 6–11.

[50] *What is CI/CD? Continuous integration and continuous delivery explained.* https://www.infoworld.com/article/3271126/what-is-cicd-continuous-integration-and-continuous-delivery-explained.html. Accessed: 2021-08-16.

[51] Klaas Wierenga and Licia Florio. "Eduroam: past, present and future." In: *Computational methods in science and technology* 11.2 (2005), pp. 169–173.

[52] *WORLD LEADING DATA AND COMPUTING TECHNOLOGIES 2022 (HORIZON-CL4-2022-DATA-01).* https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl4-2022-data-01-02. Accessed: 2021-08-30.

[53] Mingli Wu, Kun Wang, Xiaoqin Cai, Song Guo, Minyi Guo, and Chunming Rong. "A comprehensive survey of blockchain: From theory to IoT applications and beyond." In: *IEEE Internet of Things Journal* 6.5 (2019), pp. 8114–8154.

[54] Kaifeng Yue, Yuanyuan Zhang, Yanru Chen, Yang Li, Lian Zhao, Chunming Rong, and Liangyin Chen. "A Survey of Decentralizing Applications via Blockchain: The 5G and Beyond Perspective." In: *IEEE Communications Surveys Tutorials* (2021), pp. 1–1. DOI: 10.1109/COMST.2021.3115797.

[55] Qi Zhang and Frank HP Fitzek. "Mission critical IoT communication in 5G." In: *Future Access Enablers of Ubiquitous and Intelligent Infrastructures*. Springer, 2015, pp. 35–41.

[56] Zhiming Zhao, Chunming Rong, and Martin Gilje Jaatun. "A Trustworthy Blockchain-based Decentralised Resource Management System in the Cloud." In: *2020 IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS)*. 2020, pp. 617–624. DOI: 10.1109/ICPADS51040.2020.00086.

PLEASE NOTE:

Due to copyright restrictions, the next papers cannot be reproduced in the repository.
You will find the citations and the links to the published papers on the following pages.

Paper 2:
Improved Gradient Inversion Attacks and Defenses in Federated Learning

Improved Gradient Inversion Attacks and Defenses in Federated Learning

Jiahui Geng[1], Yongli Mou[2], Qing Li[1], Feifei Li[2], Oya Beyan[2], Stefan Decker[2], Chunming Rong[2]

[1] Department of Electrical Engineering and Computer Science, University of Stavanger
4036 Stavanger, Norway

[2] RWTH-Aachen University
Templergraben 55 52062 Aachen, Germany

DOI: 10.1109/TBDATA.2023.3239116

Paper 3:
A Survey on Dataset Distillation: Approaches, Applications and Future Directions

A Survey on Dataset Distillation: Approaches, Applications and Future Directions

Jiahui Geng[1], Zongxiong Chen[2], Yuandou Wang[3], Herbert Woisetschläger[4], Sonja Schimmler[2], Ruben Mayer[4], Zhiming Zhao[3], Chunming Rong[1]

[1] Department of Electrical Engineering and Computer Science, University of Stavanger
4036 Stavanger, Norway

[2] Fraunhofer FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin, Germany

[3] University of Amsterdam
Science Park904, 1098 XH Amsterdam, Netherlands

[4] Technical University of Munich
Boltzmannstraße 15, 85748 Garching bei München, Germany

https://www.ijcai.org/proceedings/2023/0741.pdf

Paper 4:
Blockchain Empowered and Self-sovereign Access Control System

Blockchain Empowered and Self-sovereign Access Control System

Jiahui Geng[1], Hanif Tadjik[1], Martin Gilje Jaatun[1,2], Chunming Rong[1]

[1] Department of Electrical Engineering and Computer Science, University of Stavanger
4036 Stavanger, Norway

[2] SINTEF Digital
Trondheim, Norway

DOI: 10.1109/CloudCom55334.2022.00021

Paper 5: Blockchain-based Cross-organizational Workflow Platform

Blockchain-based Cross-organizational Workflow Platform

Jiahui Geng[1], **Ali Akbar Rehman**[1], **Yongli Mou**[2], **Stefan Decker**[2], **Chunming Rong**[1]

[1] Department of Electrical Engineering and Computer Science, University of Stavanger
4036 Stavanger, Norway

[2] RWTH-Aachen University
Templergraben 55 52062 Aachen, Germany

DOI: 10.1109/CloudCom55334.2022.00018