MARCO SCHREYER
DAMIAN BORTH
T. FLEMMING RUUD
MIKLOS A. VASARHELYI

A SUM GREATER THAN ITS PARTS: COLLECTIVE ARTIFICIAL INTELLIGENCE IN AUDITING

Advancing Audit Models through Federated Learning Without Sharing Proprietary Data

Artificial intelligence exhibits the potential to transform auditing by extracting insights from large volumes of audit-relevant data. This article introduces federated learning, an emerging artificial intelligence learning setting. It outlines the integration of federated learning into practical audit procedures to gather collective intelligence from various audit-relevant data sources while ensuring data privacy.

1. INTRODUCTION

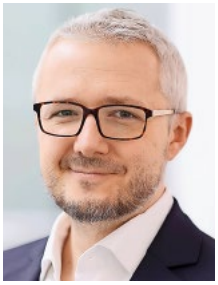
Advances in information technology, such as modern database technologies, cloud computing, and the Internet of Things (IoT), have spurred organisations to digitise their business processes [1]. Consequently, the digital ecosystems of enterprises experienced significant growth [2]. This trend is often referred to as digital transformation and has resulted in a fundamental shift in how organisations manage and utilise information [3]. Modern Enterprise Resource Planning (ERP) systems record vast quantities of audit-relevant information across business processes, accounting ledgers and journal entries [4]. This digital transformation has fundamentally altered, and will continue to influence, the nature of digital audit evidence [5].

The unprecedented availability of data presents an opportunity for auditors to extract valuable insights from internal organisational data and external sources [6]. Audit firms are increasingly adopting artificial intelligence (AI) capable of learning sophisticated deep-learning-enabled audit models [7]. Essentially, such models serve as a structured repository of knowledge acquired through learning from large volumes of audit-relevant data. Once an audit model is learned, it can enhance the auditors'decision-making processes concerning new and previously unseen data [8]. Recently, these models have been proposed for various audit tasks, including journal entry testing (ISA 240, ISA 315 [9]), audit sampling (ISA 530 [10]) and the analysis of disclosures (ISA 700, ISA 720 [11]). *Figure 1* illustrates, for example, the application of a deep autoencoder neural network model [12] to identify anomalies within journal entry data [13].

At the same time, large audit firms often audit multiple clients operating in the same sector or industry [15]. Such "peer clients" are affected by similar economic and market effects, e. g. supply chains, policies or energy costs [16]. The accumulation of specialised knowledge across clients offers considerable benefits regarding audit quality and efficiency. It enables audit firms to learn industry-specific deep-learning audit models, for instance models tailored towards the financial, automotive, or pharmaceutical industry [17].

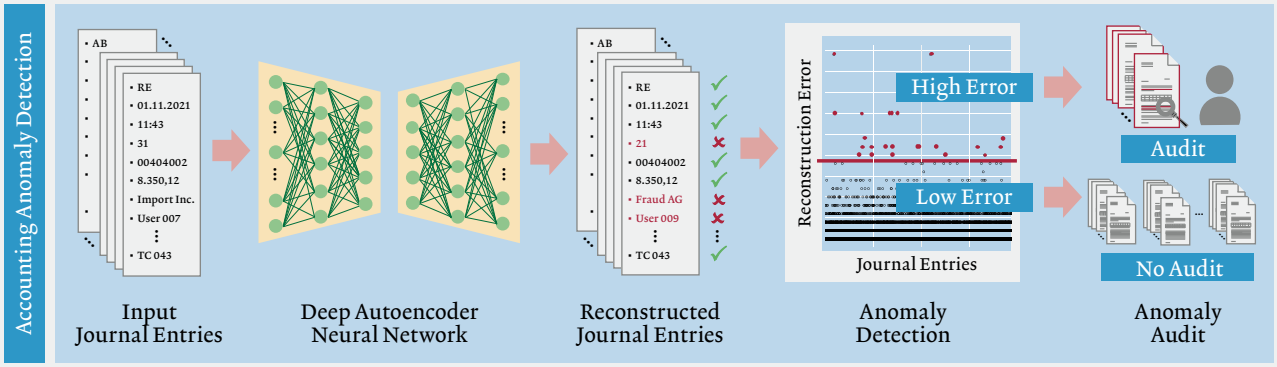
Professional practice principles and regulatory frameworks mandate that auditors must preserve the confidentiality of clients' data [18]. Nevertheless, auditors are generally not prevented from using proprietary client information to improve the quality of their collective assurance services [19]. Learning specialised audit models would require centralising sensitive data from various clients. However, such a centralisation increases the risk of substantial data breaches and unauthorised data access. Recently, it has been demonstrated that deep-learning models are vulnerable to "data leakage attacks," e. g. attacks that extract sensitive or personally identifiable information [20]. In addition, audit firms have experienced significant data breaches or data confidentiality

MARCO SCHREYER, POSTDOCTORAL DAAD IFI RESEARCH FELLOW,* INTERNATIONAL COMPUTER SCIENCE INSTITUTE (ICSI), UNIVERSITY OF CALIFORNIA BERKELEY



DAMIAN BORTH, PROF. DR., CHAIR OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING DIRECTOR AT THE INSTITUTE OF COMPUTER SCIENCE (ICS), UNIVERSITY ST. GALLEN

Figure 1: **ARTIFICIAL INTELLIGENCE-BASED ANOMALY DETECTION IN ACCOUNTING JOURNAL ENTRIES USING DEEP AUTOENCODER NEURAL NETWORKS** [14]



incidents [21]. As a result, developing deep-learning models in auditing presents unique data privacy, confidentiality and security challenges [22]. The concept of federated learning [23] has emerged to mitigate these challenges while still seizing the advantages of ongoing technological transformation. Federated learning facilitates:

→ The collaborative learning of audit models across different entities, thereby leveraging the collective intelligence evident in various data sources.

→ The preservation of the confidentiality of proprietary client data as it negates the need for direct data sharing among participating entities.

Section 1 of this article introduces federated learning. Section 2 promotes the idea of accumulating collective AI in auditing. Section 3 introduces the fundamental concepts underlying federated learning. Section 4 delves into challenges related to data privacy, confidentiality and security in auditing. The results of an empirical study are presented in section 5. Finally, section 6 concludes the article with a summary and outlook.

2. COLLECTIVE ARTIFICIAL INTELLIGENCE IN AUDITING

Auditors gain knowledge and expertise through exposure to diverse business scenarios and clients. This accumulation of experience allows to improve their skills. For example, an auditor in the pharmaceutical sector gains a deep understanding of industry-specific financial irregularities, enabling her to improve audit effectiveness. A compelling justification exists for implementing analogous knowledge accumulation in deep-learning-enabled audit models. This methodology embodies the fundamental concept of collective intelligence in internal and external auditing, where various entities, including business units or companies, collaborate to create more effective audit models.

Recently, there has been a growing interest in harnessing diverse knowledge when learning audit models [24]. Hoitash et al. [25] demonstrated that audit models incorporating peer client data yield better predictive results [26]. Similarly, the performance of deep-learning audit models improves when learned across various data sources. It exposes models to multiple scenarios and complexities, enhancing their accuracy and robustness.

→ In *internal auditing*, auditors engage with multiple business lines, segments or regional offices in the same organisation(s). Internal auditors could leverage deep-learning to learn across the organisation and derive a holistic perspective of the organisational nuances, e. g. to mitigate risks and improve audit effectiveness.

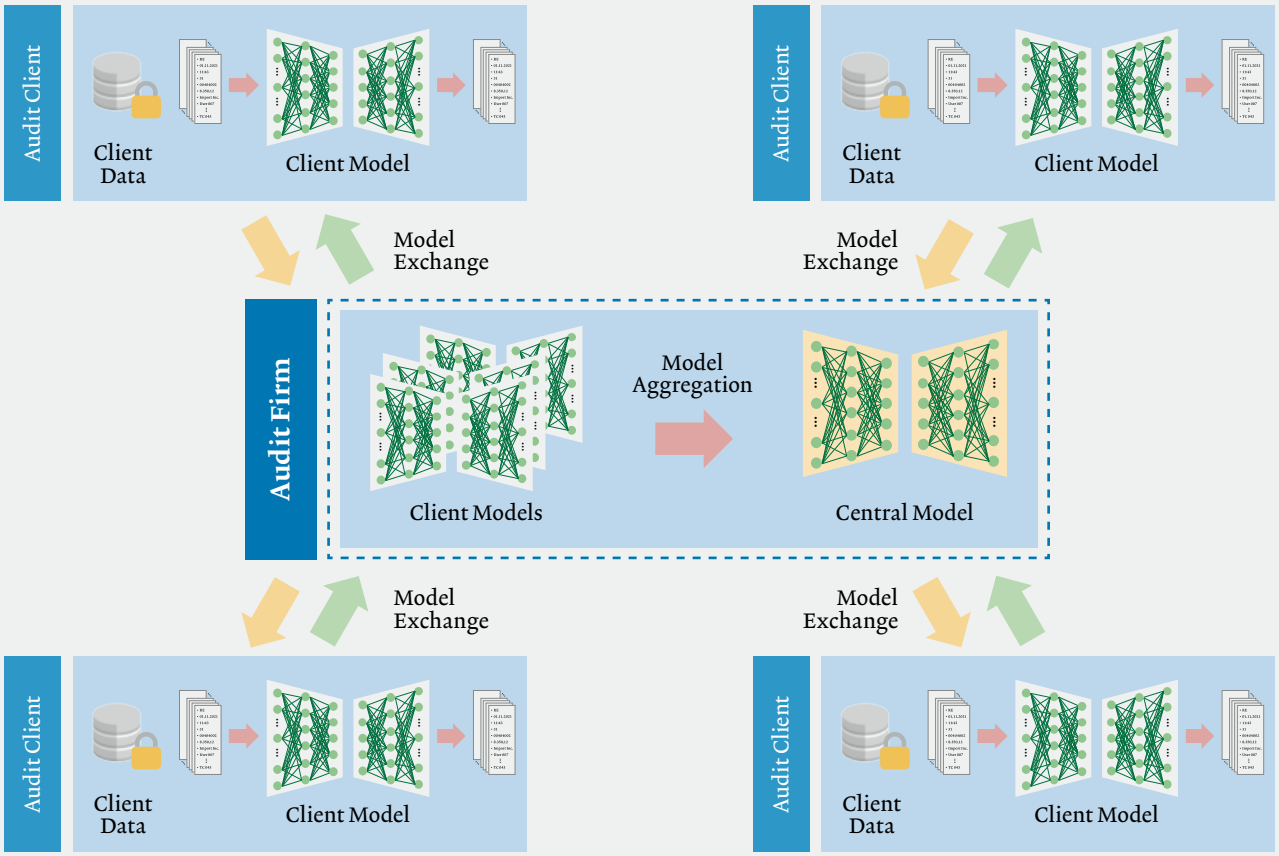
→ In *external auditing*, auditors engage with multiple companies in similar industries, jurisdictions or business environments. Audit firms could establish a deep-learning setup to learn across several audit engagements or groups of accounts, harnessing collective intelligence, e. g. to improve audit quality and efficiency.

In summary, the transition towards deep-learning augmented auditing calls for accumulating knowledge and expertise across multiple companies or business lines. The idea of fe-

T. FLEMMING RUUD, PHD, CERTIFIED PUBLIC ACCOUNTANT (NORWAY), PROF. OF INTERNAL & EXTERNAL AUDITING, BI NORWEGIAN BUSINESS SCHOOL (OSLO), PROF. EM UNIVERSITY ST. GALLEN

MIKLOS A. VASARHELYI, PHD., KPMG DISTINGUISHED PROF. OF ACCOUNTING INFORMATION SYSTEMS, RUTGERS BUSINESS SCHOOL, DIRECTOR RUTGERS ACCOUNTING RESEARCH CENTRE

Figure 2: **FEDERATED LEARNING OF DEEP AUTOENCODER NEURAL NETWORK MODELS FROM PROPRIETARY JOURNAL ENTRY DATA OF MULTIPLE AUDIT CLIENTS** [30]



derated learning provides a pathway in this direction, aggregating a vast range of audit experiences and promising more robust and reliable audit outcomes.

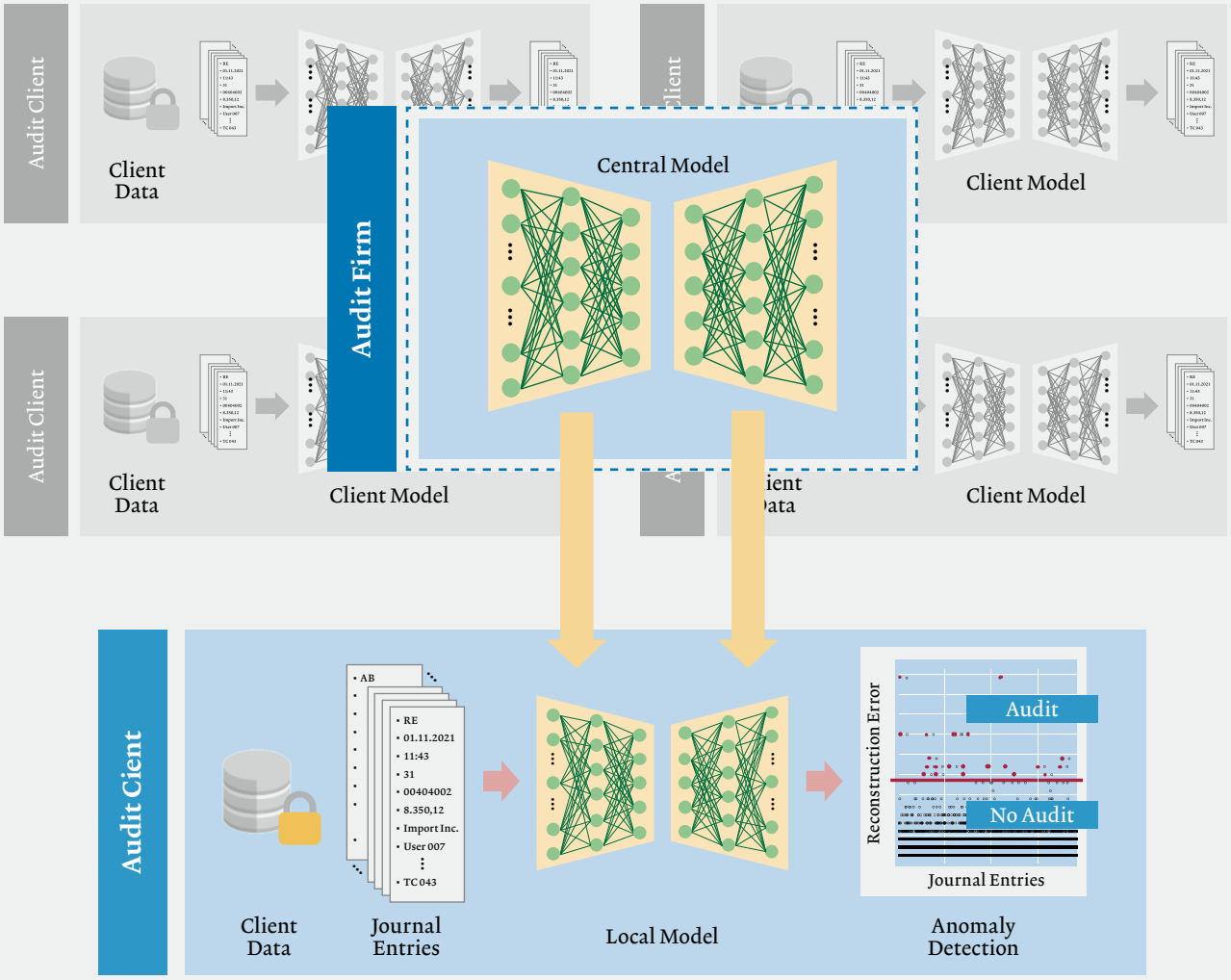
3. FEDERATED LEARNING IN AUDITING

The idea of federated learning, introduced initially in 2017 by McMahan et al. [27], enables multiple entities to collaboratively learn a collective deep-learning model under the orchestration of a central trusted entity [28]. To implement federated learning in auditing, a distinction is made between central and decentral audit models [29]. The central audit model, maintained by a trusted entity such as an audit firm, is learned collaboratively by several decentral and collaborating entities, e. g. a population of audit clients. Each client maintains and learns a decentral audit model without sharing its proprietary data. Upon successful decentral model learning, the audit firm aggregates the knowledge of the decentral client models into a central audit model. *Figure 2* illustrates an example in which federated learning is used to learn a collective audit model based on the proprietary data of multiple audit clients.

A federated learning process commonly unfolds through six consecutive steps, ensuring both learning efficiency and data privacy [31]:

1. *Central initialisation:* The first step involves initialising a central audit model by the audit firm that forms the foundation for further learning. Though not trained, this model establishes a starting point for the FL process, ensuring all participants begin with a uniform model structure and parameters.
2. *Selection:* The audit firm identifies a set of clients to participate in federated learning. This selection is based on criteria including, for example, the industry sector, company size, business characteristics or specific journal entry types, thereby ensuring the availability of a relevant and diverse data pool for model learning.
3. *Broadcast:* The selected audit clients receive the central audit model and a training program outlining the model parameter adjustment procedures. This step is fundamental for synchronising the model's starting point across all participants.
4. *Local training:* Each participating audit client computes their local data using the training program. This involves adjusting the client audit model parameters to fit the client's data accurately. The critical aspect is that all computations must be local to ensure no data is transferred off the client's premises.
5. *Collection:* The central audit firm collects the updated client models upon training. These client models reflect the knowledge learned from each client's unique data set. Audit clients unable to provide timely updates may be excluded to maintain process efficiency.

Figure 3: **FEDERATED AUDITING OF A CLIENTS' PROPRIETARY JOURNAL ENTRIES USING A COLLECTIVELY LEARNED DEEP AUTOENCODER NEURAL NETWORK MODEL** [32]



6. *Central aggregation:* The final step involves the audit firm integrating the aggregated client audit models into the central audit model. This integration enriches the model's accuracy and adaptability by incorporating diverse client data insights. The enhanced central model reflects the collective knowledge across the participants.

The federated learning process is inherently iterative, with steps 2–5 repeated multiple times to refine the central audit model and progressively accumulate knowledge. As learning progresses, the central model embodies the collective intelligence of the participating clients. The individual clients can then audit their proprietary data using the central model. *Figure 3* depicts the audit firm's central model used by an individual audit client to audit its data.

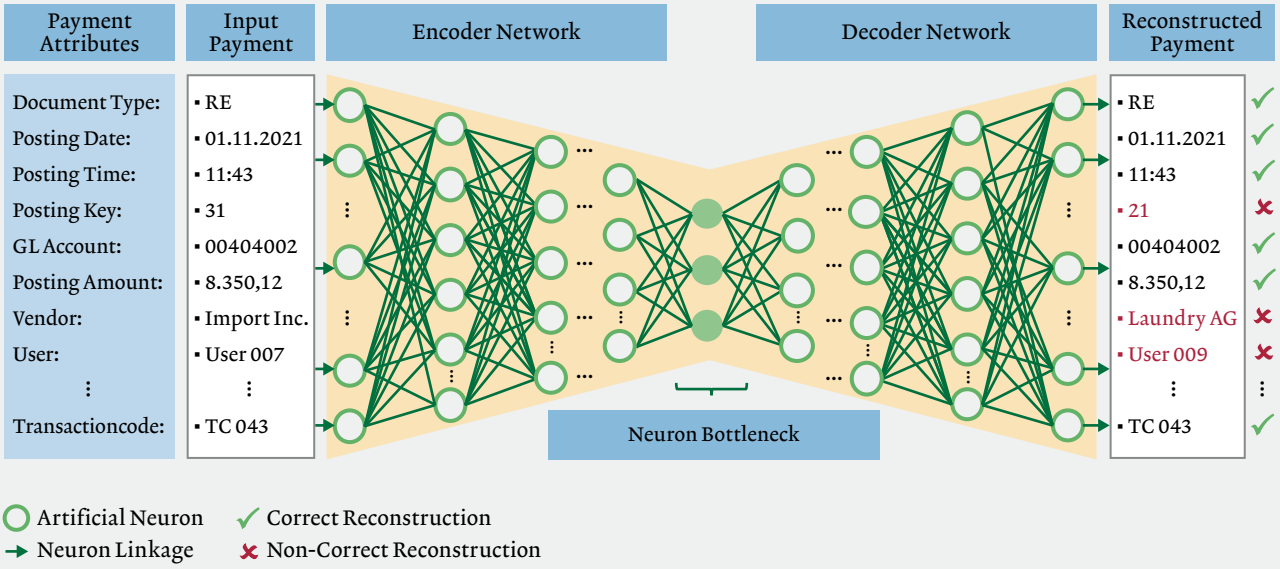
4. PRIVACY-PRESERVING ARTIFICIAL INTELLIGENCE IN AUDITING

The shift towards deep-learning augmented auditing poses risks of violating existing regulations [33]. Especially with the integration of advanced deep-learning-enabled models in auditing, adhering to data privacy, confidentiality and security regulations is imperative:

→ *Data privacy considerations:* Audit firms often handle data classified as "personal data". This includes but is not limited to, employee identifiers visible in journal entries or geographic details in customer master data. In certain jurisdictions, individuals are afforded the right to privacy and protection against the improper use of their data [34]. In this context, auditors examining their clients' records are bound by specific legal obligations regarding data privacy [35]. Consequently, audit firms must comply with relevant data protection regulations, particularly when handling client data.

→ *Data confidentiality considerations:* Audit firms are mandated to uphold the confidentiality of information obtained through professional client relationships [36]. This obligation of confidentiality for external auditors is articulated in specific legal provisions, which state that the external auditor must protect the business secrets of the audited company in their assessments [37]. The auditor's commitment to data confidentiality is often also reinforced under specific legal

Figure 4: **SCHEMATIC STRUCTURE OF A DEEP NEURAL AUTOENCODER NETWORK AND EXEMPLARY PAYMENT RECONSTRUCTION** [44]



clauses [38]. Any breach of this obligation could result in a custodial sentence or a monetary fine.

→ *Data security considerations:* Audit firms store sensitive client data when conducting detailed analytical audit procedures. This setup positions them as primary targets for cybercriminal activity [39]. Data protection legislation exhibits specific regulations specifying data security requirements of legal entities [40]. Audit firms have to implement adequate technical and organisational safeguards to ensure data security. Non-compliance with data security regulations is subject to significant penalties.

In summary, auditors must protect the confidentiality of their client's data and be mindful of the data shared and processed during an audit [41]. A desirable objective would be to establish a federated learning setting that enables the accumulation of audit-relevant knowledge from a diverse set of data sources without the need for data sharing or centralisation [42].

5. CASE STUDY: JOURNAL ENTRY TESTING

An empirical study evaluated the federated learning setting to detect unusual city payments [43]. Throughout the study, an audit firm served as central coordinating entity, directing the learning process among a network of city departments. Each client iteratively learned an anomaly detection model on its proprietary data. The federated learning was simulated by the exchange of model parameters between the audit firm and the city departments rather than the actual data, thereby safeguarding data privacy.

The study utilised publicly available datasets resembling real-world journal entry line items. The datasets, sourced from the City of Philadelphia (USA [45]), the City of Chicago (USA [46]) and the City of York (UK [47]), provided varied contexts for the empirical evaluation. The three city payments datasets were randomly partitioned into city department subsets to participate in federated learning.

Deep autoencoder neural network [48] audit models were learned to detect city payment anomalies [49]. An autoencoder neural network generally defines a deep-learning model that learns to reconstruct its input. The model consists of an encoder and a decoder network featuring multiple layers of artificial neurons. *Figure 4* illustrates a schematic representation of an autoencoder network. The autoencoder neural network model learns characteristic patterns in the payments of each city, enabling efficient reconstruction of regular payments with minimal error. In contrast, anomalous payments exhibiting uncommon payment attributes or attribute correlations will correspond to high reconstruction errors that flag deviations from standard patterns [50]. Eventually, the learned autoencoder audit model assists auditors in differentiating between regular and anomalous payments.

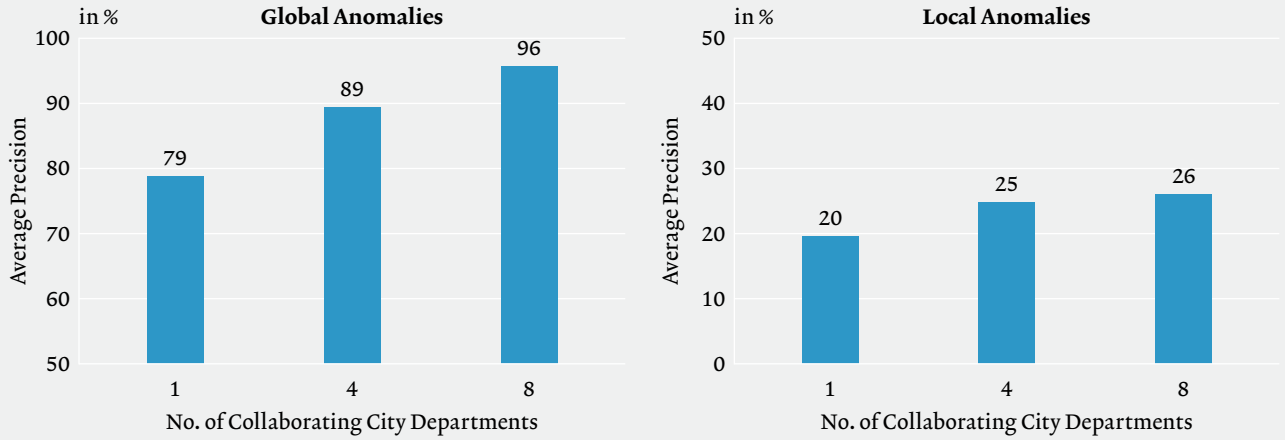
In the study's federated learning setting, experiments were conducted with one, four and eight collaborating city departments. The departments' common learning objective was to identify two classes of payment anomalies:

→ *Global payment anomalies* that correspond to payments exhibiting unusual or rare individual attribute values, e. g. rarely used vendors, contracts or posting times. Such anomalies are often more industry-specific and possess a higher error risk.

→ *Local payment anomalies* that correspond to payments exhibiting unusual attribute value correlations, e. g. rare co-occurrences of departments, amounts and vendors. Such anomalies are often more client-specific and possess a higher fraud risk.

The federated learning setting demonstrated significant benefits for both anomaly classes. With more city departments participating, an increase in global payment anomaly

Figure 5: **GLOBAL AND LOCAL ANOMALY DETECTION RESULTS ACROSS CITY PAYMENTS WITH VARIOUS NUMBERS OF COLLABORATING DEPARTMENTS**



detection precision was observed. Specifically, the average detection precision across all datasets improved from 79% with a single audit client contributing to the central model's learning to 96% when participation increased to eight city departments (refer to *Fig. 5*, left). At the same time, the study found a similar improvement in local payment anomaly detection with a growing number of departments. The average detection precision across all datasets improved from 20% with the involvement of only one audit client in the central model's learning process to 26% when participation increased to eight city departments (refer to *Fig. 5*, right). In summary, the study underscored the practical benefits of federated learning in auditing, particularly learning from multiple data sources. As more city departments collaborate and contribute their model parameters (without sharing their proprietary data), the anomaly detection performance was noticeably enhanced.

6. SUMMARY AND OUTLOOK

This article outlined the idea of federated learning in auditing, an emerging learning setting that represents an initial step into an era of collective audit intelligence. Envisioning a future where auditors are equipped with advanced audit models, federated learning enables learning from a wide range of clients while complying with data privacy, confidentiality and security regulations. These audit models, which are continuously evolving and enhancing their capabilities [51], exhibit the potential to substantially advance the emerging paradigm of artificial intelligence "co-piloted auditing [52]". ■

Notes: *Disclosure of funding: The research conducted by Marco Schreyer at Rutgers University was funded by the University of St. Gallen under the Mobi.Doc fellowship, grant number 1031606. Presently, his research at UC Berkeley is supported by a fellowship in the IFI program, funded by the German Academic Exchange Service (DAAD), with grant number 57515245.
1) Brown-Liburd, H. and Miklos A. Vasarhelyi. "Big Data and Audit Evidence." Journal of Emerging Technologies in Accounting 12, no. 1 (2015): 1–16. **2)** Alles, Michael G. "Drivers of the Use and Facilitators and Obstacles of the Evolution of Big Data by the Audit Profession." Accounting Horizons, vol. 29, no. 2, 2015, pp. 439–449; Cho, Soohyun, Miklos A. Vasarhelyi, and Chanyuan Zhang. "The Forthcoming Data Ecosystem for Business Measurement and Assurance." Journal of Emerging Technologies in Accounting 16, no. 2 (2019): 1–21. **3)** Mayer-Schönberger, V. and Kenneth Cukier. Big Data: A Revolution That Will Transform How We Live, Work, and Think. Houghton Mifflin Harcourt, 2013. **4)** Dai, Jun and Miklos A. Vasarhelyi. "Imagineering Audit 4.0." Journal of Emerging Technologies in Accounting 13, no. 1 (2016): 1–15; Rausenberger, René and Kristina Prenrecaj. "Audit 4.0 – Digitale Wirtschaftsprüfung: Der Einsatz von innovativen Technologien verändert Abschlussprüfung und -prüfer." Expert Focus 2017/11, pp. 779–783. **5)** Appelbaum, D. "Securing Big Data Provenance for Auditors: The Big Data Provenance Black Box as Reliable Evidence." Journal of Emerging Technologies in Accounting, vol. 13, no. 1, 2016, pp. 17–36; Yoon, Kyunghee, Lucas Hoogduin and Li Zhang. "Big Data as Complementary Audit Evidence." Accounting Horizons 29, no. 2 (2015): 431–438. **6)** Alles, Michael G. "Drivers of the Use and Facilitators and Obstacles of the Evolution of Big Data by the Audit Profession." Accounting Horizons, vol. 29, no. 2, 2015, pp. 439–449; Gu, Yu, Jun Dai and Miklos A. Vasarhelyi. "Audit 4.0-based ESG assurance: An example of using satellite images on GHG emissions." International Journal of Accounting Information Systems 50 (2023): 100625. **7)** LeCun, Yann, Bengio, Yoshua and Hinton, Geoffrey. "Deep Learning." Nature, vol. 521, no. 7553, 2015; Sun, Ting. "Applying Deep Learning to Audit Procedures: An Illustrative Framework." Accounting Horizons, vol. 33, no. 3, 2019, pp. 89–109. **8)** Cho, Soohyun, Miklos A. Vasarhelyi and Chanyuan Zhang. "The Forthcoming Data Ecosystem for Business Measurement and Assurance." Journal of Emerging Technologies in Accounting 16, no. 2 (2019): 1–21. **9)** Nonnenmacher, Jakob, et al. "Using Autoencoders for Data-Driven Analysis in Internal Auditing." HICSS Proceedings of the 54th Hawaii International Conference on System Sciences, 2021, p. 5748; Schultz, M. and Tropmann-Frick, M. "Autoencoder Neural Networks Versus External Auditors: Detecting Unusual Journal Entries in Financial Statement Audits." HICSS Proceedings of the 53rd Hawaii International Conference on System Sciences, 2020; Zupan, Mario, Budimir, Verica and Letinic, Svjetlana. "Journal Entry Anomaly Detection Model." Intelligent Systems in Accounting, Finance, and Management, vol. 27, no. 4, 2020, pp. 197–209. **10)** Schreyer, M. et al. "Learning Sampling in Financial Statement Audits Using Vector Quantised Variational Autoencoder Neural Networks." International Conference on Artificial Intelligence, 2020; Schreyer, M., Sattarov, T. and Borth, D. "Multi-View Contrastive Self-Supervised Learning of Accounting Data Representations for Downstream Audit Tasks." International Conference on Artificial Intelligence, 2021. **11)** Ramamurthy, Rajkumar, et al. "ALiBERT: Improved Automated List Inspection (ALI) with BERT." 21st ACM Symposium on Document Engineering, 2021; Sifa, Rafet, et al. "Towards Automated Auditing with Machine Learning." In ACM Symposium on Document Engineering 2019. **12)** Hinton, G.E. and Salakhutdinov, R.R. "Reducing the Dimensionality of Data with Neural Networks." Science, vol. 313, no. 5786, 2006, pp. 504–507. **13)** Schreyer, M., et al. "Artificial Intelligence in Internal Audit as a Contribution to Effective Governance." Expert Focus 2022 / January, pp. 45–50; Schreyer, Marco, et al. "Detection of Anomalies in Large Scale Accounting Data Using Deep Autoencoder Networks."

arXiv:1709.05254, 2017. **14)** For details, please refer to Schreyer, M., Baumgartner, M., Ruud, T.F. and Borth, D. "Artificial Intelligence in Internal Audit as a Contribution to Effective Governance-Deep-learning Enabled Detection of Anomalies in Financial Accounting Data." Expert Focus 2022/ January: 39–44. **15)** Hoitash, Rani, Kogan, Alexander and Vasarhelyi, Miklos A. "Peer-Based Approach for Analytical Procedures." Auditing: A Journal of Practice & Theory, vol. 25, no. 2, 2006, pp. 53–84. **16)** Hogan, Chris E. and Jeter, Debra C. "Industry Specialization by Auditors." Auditing: A Journal of Practice & Theory, vol. 18, no. 1, 1999, pp. 1–17; Chan, D., et al. "A Spatial Analysis and Test of Oligopolistic Competition in the Market for Audit Services." Technical Report. Working paper, University of British Columbia, 2004. **17)** Kogan, Alexander and Yin, Cheng. "Privacy-Preserving Information Sharing Within an Audit Firm." Journal of Information Systems, vol. 35, no. 2, 2021, pp. 243–268. **18)** For example, 1.700.001.01 of the AICPA Code of Professional Conduct states that "a member in a public practice shall not disclose any confidential client information without specific consent of the client". **19)** Interpretations of the Statements of Auditing Standard (SAS) no. 56 indicate that "in circumstances where the auditor specialises in a specific industry, the auditor may use client data" to develop reasonable expectations (cf. Guy, Dan M., Carmichael, Douglas R. and Lach, Linda A. "Wiley Practitioner's Guide to GAAS 2003: Covering all SASs, SSAEs, SSARSs, and Interpretations." Wiley, 2002). **20)** Carlini, Nicholas, et al. "Extracting Training Data from Large Language Models." arXiv:2012.07805, 2020; Yin, Hongxu, et al. "See Through Gradients: Image Batch Recovery Via Gradinversion." Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2021. **21)** Cheng, Christine, Flasher, Renee and Higgins, James P. "Accounting Firm Data Breaches: One State's Records." Journal of Accountancy, vol. 227, no. 5, 2019, pp. 40–45. **22)** Shokri, Reza and Vitaly Shmatikov. "Privacy-Preserving Deep Learning." Proceedings of the 22nd ACM SIGSAC conference on computer and communications security, 2015. **23)** McMahan, Brendan, et al. "Communication-Efficient Learning of Deep Networks from Decentralized Data." Artificial Intelligence and Statistics. PMLR, 2017, pp. 1273–1282. **24)** Kogan, Alexander and Yin, Cheng. "Privacy-Preserving Information Sharing Within an Audit Firm." Journal of Information Systems, vol. 35, no. 2, 2021, pp. 243–268. **25)** Hoitash, Rani, Kogan, Alexander and Vasarhelyi, Miklos A. "Peer-Based Approach for Analytical Procedures." Auditing: A Journal of Practice & Theory, vol. 25, no. 2, 2006, pp. 53–84. **26)** Hoitash, Rani, Kogan, Alexander and Vasarhelyi, Miklos A. "Peer-Based Approach for Analytical Procedures." Auditing: A Journal of Practice & Theory, vol. 25, no. 2, 2006, pp. 53–84. **27)** Shokri, Reza and Vitaly Shmatikov. "Privacy-Preserving Deep Learning." Proceedings of the 22nd ACM SIGSAC conference on computer and communications security, 2015. **28)** Kairouz, Peter, et al. "Advances and Open Problems in Federated Learning." arXiv:1912.04977, 2019; Marfoq, Othmane, et al. "Throughput-Optimal Topology Design for Cross-Silo Federated Learning." In Advances in Neural Information Processing Systems, vol. 33, 2020. **29)** Schreyer, Marco, Sattarov, Timur and Borth, Damian. "Federated and Privacy-Preserving Learning of Accounting Data in Financial Statement Audits." Proceedings of the Third ACM International Conference on AI in Finance, 2022, pp. 105–113. **30)** Schreyer, Marco, Sattarov, Timur and Borth, Damian. "Federated and Privacy-Preserving Learning of Accounting Data in Financial Statement Audits." Proceedings of the Third ACM International Conference on AI in Finance, 2022, pp. 105–113. **31)** Kairouz, Peter, et al. "Advances and Open Problems in Federated Learning." arXiv:1912.04977, 2019. **32)** Schreyer, Marco, Sattarov, Timur and Borth, Damian. "Federated and Privacy-Preserving Learning of Accounting Data in Financial Statement Audits." Proceedings of the Third ACM International Conference on AI in Finance, 2022, pp. 105–113. **33)** AICPA. "Code of Professional Conduct." American Institute of Certified Public Accountants, 2014; Appelbaum, Deniz. "Securing Big Data Provenance for Auditors: The Big Data Provenance Black Box as Reliable Evidence." Journal of Emerging Technologies in Accounting, vol. 13, no. 1, 2016, pp. 17–36. **34)** Cf. Swiss Federal Act on Data Protection (effective from 1 September 2023). **35)** Cf. Art. 727 of the Swiss Code of Obligations. **36)** IFA. "Handbook of the International Code of Ethics for Professional Accountants." International Federation of Accountants, 2018; Kogan, Alexander and Yin, Cheng. "Privacy-Preserving Information Sharing Within an Audit Firm." Journal of Information Systems, vol. 35, no. 2, 2021, pp. 243–268. **37)** Cf. Art. 730*b* of the Swiss Code of Obligations. **38)** cf. Art. 321 of the Swiss Criminal Code. **39)** Cheng, Christine, Flasher, Renee and Higgins, James P. "Accounting Firm Data Breaches: One State's Records." Journal of Accountancy, vol. 227, no. 5, 2019, pp. 40–45; Politzer, Malia. "Top Cyberthreats Targeting Accounting Firms." Journal of Accountancy, 2020. **40)** Cf. Swiss Federal Act on Data Protection (effective from 1 September 2023). **41)** Hofmann, Susanne and Meyer, Michael Adrian. "Datenschutz in der Schweiz, Eine Darstellung Aktueller Entwicklungen." Expert Focus, 2017/6–7, pp. 422–425; Munoko, Ivy, Brown-Liburd, Helen L. and Vasarhelyi, Miklos. "The Ethical Implications of Using Artificial Intelligence in Auditing." Journal of Business Ethics, vol. 167, no. 2, 2020. **42)** Konecny, Jakub, et al. "Federated Optimization: Distributed Machine Learning for On-Device Intelligence." arXiv preprint arXiv:1610.02527, 2016; Mathews, Sherin Mary and Assefa, Samuel. "Federated Learning: Balancing the Thin Line Between Data Intelligence and Privacy." In AAAI Workshop on AI in Financial Services: Adaptiveness, Resilience & Governance, 2022; Yunis, Manal M., El-Khalil, Raed and Ghanem, Miray. "Towards a Conceptual Framework on the Importance of Privacy and Security Concerns in Audit Data Analytics." 2021. **43)** The comprehensive study results are published and discussed in Schreyer, M., Sattarov, T. and Borth, D.; "Federated and Privacy-Preserving Learning of Accounting Data in Financial Statement Audits." In Proceedings of the Third ACM International Conference on AI in Finance, USA, 2022. **44)** Schreyer, M., et al. "Artificial Intelligence in Internal Audit as a Contribution to Effective Governance." Expert Focus 2022/January, pp. 45–50. **45)** https://www.phila.gov/2019-03-29-philadelphias-initial-release-of-city-payments-data/. **46)** https://data.cityofchicago.org/Administration-Finance/Payments/s4vu-giwb/. **47)** https://data.yorkopendata.org/dataset/all-payments-to-suppliers/. **48)** Hinton, G.E. and Salakhutdinov, R.R. "Reducing the Dimensionality of Data with Neural Networks." Science, vol. 313, no. 5786, 2006, pp. 504–507. **49)** Schreyer, M., et al. "Detection of Anomalies in Large Scale Accounting Data Using Deep Autoencoder Networks." arXiv:1709.05254, 2017. **50)** Schultz, Martin and Tropmann-Frick, Marina. "Autoencoder Neural Networks Versus External Auditors: Detecting Unusual Journal Entries in Financial Statement Audits." HICSS Proceedings of the 53rd Hawaii International Conference on System Sciences, 2020. **51)** Schreyer, Marco, et al. "Federated Continual Learning to Detect Accounting Anomalies in Financial Auditing." arXiv preprint arXiv:2210.15051, 2022; Schreyer, Marco; Sattarov, Timur; and Borth, Damian. "Federated and Privacy-Preserving Learning of Accounting Data in Financial Statement Audits." Proceedings of the Third ACM International Conference on AI in Finance, 2022, pp. 105–113. **52)** Gu, Hanchi, Marco Schreyer, Kevin Moffitt and Miklos A. Vasarhelyi. "Artificial Intelligence Co-Piloted Auditing." Available at SSRN 4444763, 2023.