ercim-news.ercim.eu

Number 126 July 2021

ERCIM NEWS

Special theme:

PRIVACY PRESERVING COMPUTATION

Also in this issue

Joint ERCIM Actions:

TRAPEZE – Transparency, Privacy and Security for European Citizens

Editorial Information

ERCIM News is the magazine of ERCIM. Published quarterly, it reports on joint actions of the ERCIM partners, and aims to reflect the contribution made by ERCIM to the European Community in Information Technology and Applied Mathematics. Through short articles and news items, it provides a forum for the exchange of information between the institutes and also with the wider scientific community. This issue has a circulation of about 6,000 printed copies and is also available online ,at https://ercim-news@ercim.eu.

ERCIM News is published by ERCIM EEIG
BP 93, F-06902 Sophia Antipolis Cedex, France
+33 4 9238 5010, contact@ercim.eu
Director: Philipp Hoschka, ISSN 0926-4981

Contributions
Contributions should be submitted to the local editor of your country

Copyright notice

Advertising
For current advertising rates and conditions, see https://ercim-news.ercim.eu/ or contact peter.kunz@ercim.eu

ERCIM News online edition: *ercim-news.ercim.eu/*

Next issue:
October 2021: Smart and Circular Cities

Subscription
Subscribe to ERCIM News by sending an email to en-subscriptions@ercim.eu

JOINT ERCIM ACTIONS

SPECIAL THEME

The special theme “Privacy Preserving Computation” has been coordinated by the guest editors Rudolf Mayer (SBA Research) and Thijs Veugen (TNO and CWI)

Introduction to the Special Theme

Privacy by design

Platforms

Collaborative Learning

Risk Estimation and Anonymisation

RESEARCH AND INNOVATION

ANNOUNCEMENTS

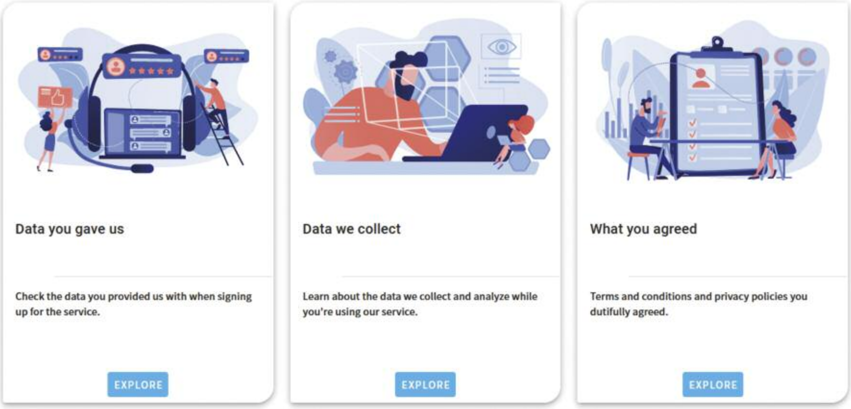
TRAPEZE – Transparency, Privacy and Security for European Citizens

by Peter Kunz

ERCIM is a partner in the H2020 project TRAPEZE – Transparency, Privacy and Security for European Citizens – a European Innovation Action with the ambitious goal of driving a cultural shift in the protection of the European data economy. It aims to achieve this by reconstructing the concepts of control, transparency and compliance through technical and methodological, citizen-first, innovations. The project will lead the way in putting often-misplaced cutting-edge technologies to practical use for the citizens.

As we witness the rise of the digital age and reap the benefits of a data-driven society, our activities, industrial processes, and research amass an unimaginable amount of data. Moreover, data from previously isolated sources are, be it intentionally or accidentally, combined and interlinked and used by companies and public bodies, big and small alike, often behind the corporate/government firewall. This "Deep Web of Data" holds huge potential for the European Digital Single Market and for business, science and society. However, its growth comes at a cost to the very society that created it – it has become immensely difficult, if not impossible, to manage and, hence, keep the data safe. In other words, this struggle for traditional businesses is both impeding progress in the EU economy and has also opened the door for cybercrime; an increasing concern for the European economy and society.

With the ever-increasing pace of data production, citizens in Europe find themselves at the mercy of those controlling the data. By May 2019, data protection authorities in the EU had received 144,376 GDPR-related queries and complaints from the European public. This is an important indicator that citizens are becoming increasingly aware of the data protection regulation, and risks relating to security and privacy. With the increasing awareness, people are taking a more active role in the protection of their own data. While awareness-raising is key in engaging all participants in the protection of citizens' fundamental rights, a foundation of trust is essential for strengthening society's overall cyber-resilience. The right tools and guidelines can help to support the will of the citizens and turn the fight against data misuse and cybercrime into a joint effort.



Data you gave us

Check the data you provided us with when signing up for the service.

Data we collect

Learn about the data we collect and analyze while you're using our service.

What you agreed

Terms and conditions and privacy policies you dutifully agreed.

Figure 1: The Privacy Dashboard demonstrates the data privacy management capabilities of the TRAPEZE platform. With the TRAPEZE Privacy Dashboard, users can review collected and processed data by a certain controller and configure permissions for processing of their personal data.

TRAPEZE is aiming to become a lighthouse for European and global initiatives that aspire to deliver citizen-first, cyber-resilient, innovation.

To make this goal a reality, TRAPEZE aims to put citizens' security and privacy into their own hands by providing them, first of all, with innovative dashboards that will enable fine-grained and dynamic control of their data protection preferences across all relevant controllers. These will be accompanied by transparency and feedback mechanisms that will allow data subjects to comprehend the complex flows of their data and actively participate in the prevention, detection, and reporting of legal noncompliance or incidents, and in exercising their legal rights. Furthermore, to ensure citizens of all groups, skills, and physical abilities can manage and monitor their data flows, TRAPEZE will place a special emphasis on usability, but also privacy preferences and sociological aspects across different member states, seeking to establish a feedback loop with its end-users internationally. This collaboration (or co-production) will enable direct involvement of the EU citizen in the development of privacy-enhancing technologies. Additionally, to contribute to the resilience of European society, we aim to increase awareness and competence through open knowledge, gamification, and micro-learning.

TRAPEZE is significantly different from existing approaches in that it does not attempt to protect the citizen by abruptly reshaping the European digital economy. Instead, it seeks to empower the data subject, while enabling a realistic, steady, transition to a more trustworthy data ecosystem that extends beyond online services and deep into the controllers' data silos. TRAPEZE aims to enable privacy-aware and privacy-preserving data value chains by leveraging the concepts of linked data graphs and distributed ledgers (blockchain). Linked data will be used to control the handling of the payload data (actual personal data relating to the citizen) stored and processed by controllers', or processors' systems, even downstream (re-sharing from controller to controller/processor) in the data value chain. Blockchain technology will ensure compliance and decentralisation of records of processing activities, as well as immutability and non-repudiation of said records (with GDPR compliance in mind). In addition, TRAPEZE aims to secure citizens' smart terminals and online communication through a software development kit for mobile security.

TRAPEZE's proposed architecture and tools will be developed and evaluated under real-world conditions in three pilot scenarios in government, telecommunication and IT services, and banking. All three pilots involve the processing and aggregation of large amounts of personal data from various data sources, with policies specified at different levels of granularity.

TRAPEZE is not starting from scratch, but builds on a decade of EU-funded research in security and privacy, as well as on proprietary solutions and know-how, towards marketable innovations.

Trapeze aims to:
- bring all stakeholders together under a common resilience framework;
- empower citizens with the necessary tools and know-how to manage their security and privacy;
- support the acquisition of citizens' consent at collection time and the recording of both the data and the metadata with scalable automated compliance checking in mind;
- restore citizens' trust in the digital economy by enforcing log integrity and non-repudiation;
- reconstruct data lineage and implement transparency by design;
- demonstrate its applicability in three different operating environments of the public, telecom and financial sectors.

The project includes 13 partners from seven European countries: TENFORCE (BE), ERCIM – The European Research Consortium for Informatics and Mathematics (FR), TU Berlin (DE), Informatie Vlaanderen (BE), Deutsche Telekom (DE), CaixaBank (ES), CINI – Consorzio Interuniversitario Nazionale per l'Informatica (IT), Unabhängiges Landeszentrum für Datenschutz, Schleswig-Hostein (DE), Kaspersky Lab Italia (IT), Institute Mihajlo Pupin (RS), IPSOS (BE), Athens Technology Centre (GR) and E-Seniors Association (FR).

Please contact:
Alexander Vasylchenko, TENFORCE , Belgium
alexander.vasylchenko@tenforce.com

Metadata Interoperability Workshop at the EBDV Data Week 2021

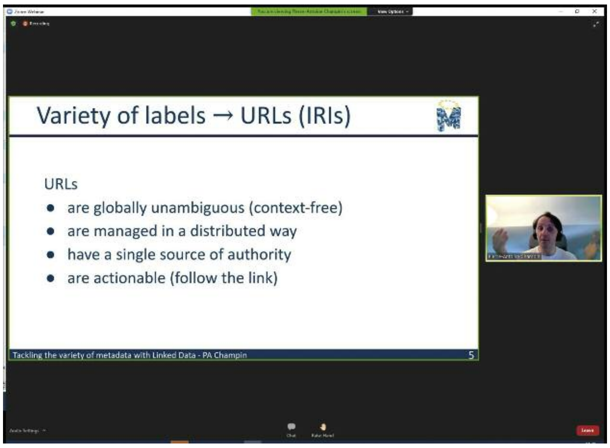
by Peter Kunz

In the frame of the European Big Data Value Data Week, 32 metadata experts from academia and industry attended the Workshop on Metadata Interoperability on 27 May 2021. The workshop was organised by Rigo Wenning, supported by the European H2020 projects MOSAICrOWN (Multi-Owner data Sharing for Analytics and Integration respecting Confidentiality and OWNer control) and TRAPEZE (Transparency, Privacy and Security for European Citizens). ERCIM is a partner in both projects.

The EBDV Data Week is the spring gathering of the European Big Data Value and Industrial AI research and innovation community. The 2021 Data Week was held online over three days. The well-established event continued in the tradition of promoting opportunities, sharing knowledge and fostering ecosystem development.

The Metadata Interoperability workshop aimed at exploring ways to make metadata interoperable while ensuring appropriate data protection. Interoperable metadata is crucial to enable data value chains that build up the data economy. The protection of data is key to increase the sharing and processing of data without privacy risks. The workshop chair Rigo Wenning (W3C/ERCIM) introduced a panel of five speakers who presented current research and developments tackling the metadata interoperability challenge.

Pierre-Antoine Champin from Univerisity of Lyon and W3C/ERCIM introduced "Linked Data: principles and perspectives". He explained how heterogeneous data can be captured into graphs, and why URLs (or IRIs) are a good solution for the disambiguation of labelled graphs. He further explained that Linked Data, as a layer providing interoperability, does not require a change in the underlying metadata production chain. He also briefly presented work in progress at the World Wide Web Consortium – W3C, which



Variety of labels → URLs (IRIs)

URLs
- are globally unambiguous (context-free)
- are managed in a distributed way
- have a single source of authority
- are actionable (follow the link)

Tackling the variety of metadata with Linked Data - PA Champin 5

Pierre-Antoine Champin from Univerisity of Lyon and W3C/ERCIM introduced "Linked Data: principles and perspectives".

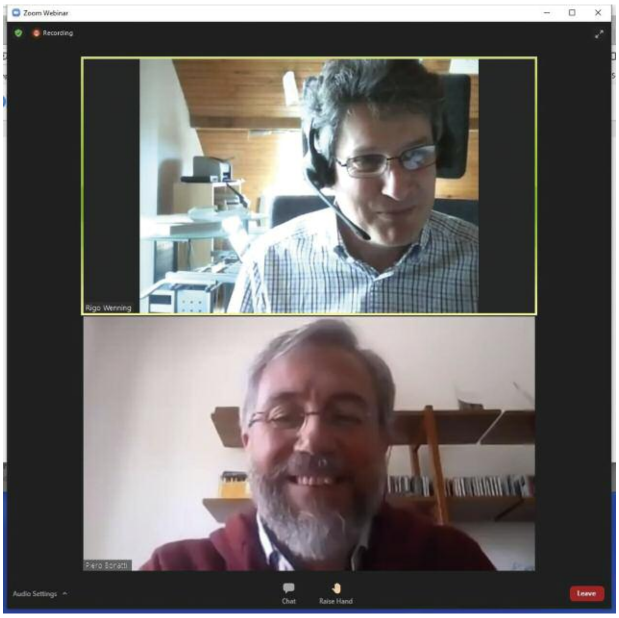
includes Decentralized Identifiers (DIDs), content negotiation by profile, and RDF-star (an extension of RDF to make RDF more flexible by allowing metadata of edges).

Víctor Rodríguez Doncel from Universidad Politécnica de Madrid presented “Metadata operations in Lynx”. Lynx is a European H2020 project that has built a service platform for ontologies applied to different use cases, such as labour law (https://www.lynx-project.eu/). This was achieved by developing a multilingual legal knowledge graph built on an RDF Data model, enriched with annotations, and compliant with the NLP Interchange Format NIF. As a lesson learned, he mentioned the huge effort invested to build the data model. In the future, he will be concentrating on methods for import and export of data and applying a more pragmatic approach for internal operations. This raised the question about how to make data models reusable and to whom public data models should be reported.

Albert Zilverberg from ATB Bremen GmbH gave an example from the automotive industry with his talk on “Standardization challenges in cross-sectorial data streams”. The European CROSS-CPP project developed an ecosystem for services based on integrated cross-sectorial data streams (https://www.cross-cpp.eu/). The goal was to give data customers access to cyber-physical products (CPP) data streams to build sectorial and cross-sectorial services. This allows data owners to exploit their CPP CPS data, which is their most valuable asset. In a brand-specific data format environment, data customers need one single access point to get access to CPP data with one interface. A solution is the common industrial data model (CIDM) providing one common standard for all kind of CPP data. Albert then presented in detail the CIDM specifications, designed in a layered structure taking into account different types of sensor signals, CIDM measurement channels, etc. CIDM Data packages contain complex metadata and he discussed the question of what level of harmonization is achievable by CIDM.

Svetla Boytcheva from Sirma AI (Ontotext) spoke about “Metadata in the health care sector”. The EU project EXAMODE – Extreme scale analytics via multimodal ontology discovery and enhancement (https://www.examode.eu) develops prediction and analysis tools for clinical settings and research. Clinical data is highly heterogeneous. The project investigates a digital workflow for a hospital information system using the health interoperability standard HL7 Int, semantic data interoperability standards such as RDF, RDF Star, OWL and SKOS, and technical interoperable standards like JSON and JSON-LD. Ontologies standard classifications are the key challenges for combining heterogeneous data. The development of new ontologies was needed to integrate these ontologies in a portal. New ontologies have been developed for four different diseases.

Piero Bonatti from Università di Napoli Federico II, gave a presentation entitled “Metadata, Policy and Reasoning” summarising the work carried out in the European TRAPEZE project (https://trapeze-project.eu/). The goal of the project is to give the users control over their data by assuring transparency while legal compliance is automatically checked. He presented the architecture of the TRAPEZE method where privacy policies and consent are considered as metadata. He explained the many requirements for data usage policies and how these policies are being developed satisfying all requirements, leveraging OWL2 and JSON.



Workshop chair Rigo Wenning and Piero Bonatti, Università di Napoli Federico II) during the workshop discussion. Screenshot.

The presentations were followed by a lively discussion. The panellists pointed out that the considerable and impressive efforts put into each project clearly show that there is a need for exchanging methods and practices and sharing results on metadata work. The panellists and workshop participants were invited to contact the speakers to discuss and exchange current and future challenges and solutions of metadata interoperability, best practices and developments.

Links:
The workshop was recorded and is available at
https://www.youtube.com/watch?v=SFHUyfgQEPI
on BDVA’s YouTube channel at https://kwz.me/h7T
as well as on the Data Week’s web site
https://www.big-data-value.eu/dw21-agenda/

Please contact:
Rigo Wenning, ERCIM/W3C
rigo@w3.org

ERCIM “Alain Bensoussan” Fellowship Programme

The ERCIM PhD Fellowship Programme has been established as one of the premier activities of ERCIM. The programme is open to young researchers from all over the world. It focuses on a broad range of fields in Computer Science and Applied Mathematics.

The fellowship scheme also helps young scientists to improve their knowledge of European research structures and networks and to gain more insight into the working conditions of leading European research institutions. The fellowships are of 12 months duration (with a possible extension), spent in one of the ERCIM member institutes. Fellows can apply for second year in a different institute.

> “ ERCIM, a superb platform for building up my research career! I am extremely happy that ERCIM provided me the opportunity to work at NTNU, Norway. Overall, several scientific and other training programs during the fellowship helped me in various aspects of my life and also helped me in obtaining a Marie Curie Individual Fellowship. I have also established a couple of new research collaborations. A great start of my research career after my PhD.
>
> **Shounak Chakraborty**
> Former ERCIM Fellow

Why to apply for an ERCIM Fellowship?

The Fellowship Programme enables bright young scientists to work on a challenging problem as fellows of leading European research centers. ERCIM fellowship helps widen and intensify the network of personal relations among scientists.

The programme offers the opportunity to ERCIM fellows:

- to work with internationally recognized experts;
- to improve knowledge about European research structures and networks;
- to become familiarized with working conditions in European research centres;
- to promote cross-fertilization and cooperation, through the fellowships, between research groups working in similar areas in different laboratories.

Conditions

Candidates must:

- have obtained a PhD degree during the last eight years (prior to the year of the application deadline) or be in the last year of the thesis work;
- be fluent in English;
- have completed their PhD before starting the grant.

The fellows are appointed either by a stipend (an agreement for a research training programme) or a working contract. The type of contract and the monthly allowance/salary depends on the hosting institute.

Application deadlines

Deadlines for applications are currently 30 April and 30 September each year.

Since its inception in 1991, over 700 fellows have passed through the programme. In 2020, 21 young scientists commenced an ERCIM PhD fellowship and 77 fellows have been hosted during the year. Since 2005, the Fellowship Programme is named in honour of Alain Bensoussan, former president of Inria, one of the three ERCIM founding institutes.

http://fellowship.ercim.eu

ERCIM
European Research Consortium
for Informatics and Mathematics

Horizon Europe Project Management

A European project can be a richly rewarding tool for pushing your research or innovation activities to the state-of-the-art and beyond. Through ERCIM, our member institutes have participated in more than 90 projects funded by the European Commission in the ICT domain, by carrying out joint research activities while the ERCIM Office successfully manages the complexity of the project administration, finances and outreach.

Horizon Europe: How can you get involved?

The ERCIM Office has recognized expertise in a full range of services,including:

- Identification of funding opportunities
- Recruitment of project partners (within ERCIM and through ournetworks)
- Proposal writing and project negotiation
- Contractual and consortium management
- Communications and systems support
- Organization of attractive events, from team meetings to large-scale workshops and conferences
- Support for the dissemination of results.

How does it work in practice?

Contact the ERCIM Office to present your project idea and a panelof experts within the ERCIM Science Task Group will review youridea and provide recommendations. Based on this feedback, theERCIM Office will decide whether to commit to help producing yourproposal. Note that having at least one ERCIM member involvedis mandatory for the ERCIM Office to engage in a project.If the ERCIM Office expresses its interest to participate, it willassist the project consortium as described above, either as projectcoordinator or project partner.

Please contact:
Peter Kunz, ERCIM Office
peter.kunz@ercim.eu

Introduction to the Special Theme

Privacy Preserving Computation

by the guest editors Rudolf Mayer (SBA Research) and Thijs Veugen (TNO and CWI)

Many branches of the economy and society are increasingly dependent on data-driven predictions, decision support and autonomous decision-making by systems. These systems often depend on the availability of large amounts of data to learn from, which may include details about individuals, or otherwise sensitive information. Disclosure of the individuals represented by this data must be avoided for ethical reasons or regulatory requirements, which have been tightened in recent years, e.g. by the introduction of the EU's General Data Protection Regulation (GDPR). This means that the use of data is restricted, making sharing, combining, and analysing data problematic. Privacy-preserving computation tries to bridge this gap: to find a way to leverage data while preserving the privacy of individuals.

As diverse as data collection, analysis scenarios, and workflows are, so are the approaches for privacy-preserving data analysis. These range from settings where data is collected centrally, or analysed by third parties, to settings where data is locally collected at many individual locations, and jointly analysed in a secure way; sharing and centralising the data in one location is often not a feasible option in this case.

Cryptographic approaches aim to keep data confidential during computation. Secure multi-party computation (SMPC) allows a joint result to be computed from data distributed over multiple sources, while keeping the data inputs private. The efficiency of SMPC techniques has improved considerably in recent decades, enabling more complex computation, such as sophisticated machine learning algorithms. A related technique is homomorphic encryption, suitable for outsourcing computations on sensitive data.

Novel paradigms, such as federated learning, offer an alternative for analysing distributed data at low computational overhead.

In terms of anonymisation, implementations of differential privacy can help mitigate privacy risks for dynamic database queries and beyond. Methods to measure privacy or leakage are a cornerstone of evaluating the success of privacy-preserving computation.

Within Europe, considerable research is being conducted into privacy-preserving machine learning. This is, in part, because Europe is a pioneer in data protection, with the GDPR being one of the world's strongest and most comprehensive regulations. This naturally puts a strong research focus on data privacy, and this is reflected in the research funding schemes of the EU – either in the form of project funding, dealing directly with novel approaches to protecting individuals' data, or indirectly, as strong privacy assessment and management are required in many research endeavours, e.g. in most research projects dealing with medical and health data.

Privacy by design

Even as early as the data collection stage, regulations need to be considered. Bianchini et al. (page 10) define a framework that evolves the usual approach of the DevSecOps paradigm by introducing the analysis and validation of privacy and data protection, and security dimensions at the point of conception of the technology, enforcing a holistic assessment. Chrysakis et al. (page 11) discuss socio-technical tools to promote collective awareness and informed consent.

Platforms

Miksa et al. (page 13) describe a platform that allows non-disclosive data analysis on sensitive data complemented by a detailed auditing mechanism. A consent management system and linkage between different data sources allows data across different sources to be integrated and analysed.

Gremaud et al. (page 15) present, for the use case of smart home IoT devices, a system for storing data in a centralised manner; they eliminate the need to entrust a system operator by utilising an enclave where data is always encrypted; this also enables collaboration between different data owners.

Abraham et al. (page 16) propose a marketplace for brokering personal data; the planned exchange of information between participants is via an SMPC framework.

Rocha et al. (page 18) discuss how to collaborate among distributed immunological datasets. To this end, a system is provided for managing consent and to provide adequate permission levels according to the sensitivity of the data to be shared.

Delsate et al. (page 20) describe a platform that manages data access to multiple sources, utilising pseudonymisation and data aggregation to reduce risks for identification of individuals in the database.

Collaborative Learning

Lorünser et al. (page 21) show how collaboration and optimisation of processes across company boundaries can be facilitated by SMPC, without disclosing actual business secrets to competitors.

Abspoel et al. (page 23) examine ways to improve the efficiency of SMPC protocols; their specific focus is on computation domains such as integers modulo powers of two. Pennekamp et al. (page 24) discuss how non-disclosive computation, e.g. in the form of homomorphic encryption, can enable industrial collaboration, especially in settings where a strong emphasis is put on confidentiality of the data exchanged and shared in the collaboration.

Kamphorst et al. (page 26) discuss two solutions to collaboratively mine distributed data for clinical research in the oncology domain. The solutions perform privacy-preserving survival analysis in different scenarios; particularly, depending on the type of patient data distribution, e.g. whether the (hypothetically) combined data results in information on more individuals or in more information per individual, the solution based on federated learning or SMPC applies.

Van Egmond et al. (page 27) address the issue of information exchange between banks to detect money laundering. As data sharing is generally not an option, they investigate the feasibility of SMPC to enable this collaboration.

Spini et al. (page 29) propose a workflow to exchange information between multiple stakeholders that need to collaborate to identify individuals eligible for certain social welfare programmes, without revealing their data to each other. This is achieved through homomorphic encryption to maintain confidentiality.

Grimm et al. (page 30) utilise federated learning to detect fraud in accounting and auditing, and thus enable anomaly detection and classification without the need to exchange data.

Basile (page 32) focuses on formal verification of SMPC settings, to create a contract-based design methodology to enforce security accountability and reputation of distributed digital entities.

Risk Estimation/Anonymisation

Nitz et al. (page 33) analyse requirements for data anonymisation in the domain of cyber security with the aim of helping small and medium enterprises share their cyber threat intelligence data with others, to fast-track and improve the process of detecting attacks.

Pejó et al. (page 35) investigate the question of how important the contributions of individual parties are to a model collaboratively learned via a federated learning approach. This can be the basis to identify both participants that just want to benefit from the collaborative model without adequately contributing, and those that want to exaggerate their impact on the model when trying to tamper with (poison) the result.

Hittmeir et al. (page 36) address the domain of the human micro-biome, which has attracted the interest of researchers because of its links with a number of medical conditions. The authors investigate and assess the privacy risks stemming from identification of individuals participating in a database of micro-biome samples taken from multiple parts of the human body, and discuss countermeasures such as anonymisation and data synthetisation.

Campbell et al. (page 38) address the domain of voice-based interaction with computing devices, which is heavily dependent on user-created data to adapt to the multitude of languages and dialects individuals use to communicate with these devices. To reduce the risk of identification of specific users in the aggregated training data, methods to anonymise the voice and text representation are proposed, e.g. to make the recorded speech less identifiable.

Šarčević and Mayer (page 40) investigate multiple utility measures, which are employed to estimate the impact of anonymisation techniques on the information remaining within the data. They conclude that in many cases, simple and generic measures are not able to correctly predict which anonymised version is best for specific tasks, such as learning a machine learning model.

This issue of ERCIM news focuses on current research on privacy-preserving machine learning. As the scope, nature and goals of machine learning activities are very broad, so is the need for solutions that can best fit a specific setting. While there is a wealth of approaches, new data collection and analysis settings emerge frequently, with the introduction of new devices and services, and the widespread adoption of those by many users. Thus, further research in this area will have to address these novel, yet unknown settings, and at the same time aim to improve the current solutions, to increase privacy but at the same time aim for a maximum possible utility. While strong data protection guidelines such as the GDPR might, at first glance, seem to contradict the latter goal of highest utility, such challenges can often be the catalyst for novel and enhanced solutions.

Please contact:
Rudolf Mayer
SBA Research, Austria
rmayer@sba-research.org

Thijs Veugen
TNO and CWI, The Netherlands
thijs.veugen@tno.nl

Applying Privacy-by-Conception in Cybersecurity

by Alessio Bianchini, Elena Sartini and Luigi Briguglio (CyberEthics Lab.)

Security is a mandatory requirement for critical infrastructures that are increasingly threatened by cyber-attacks. However, when designing cyber-shield systems to protect assets and networks we must also consider other fundamental dimensions. This article presents the experience of CyberEthics Lab. defining and applying a holistic approach based on privacy, ethics, security and social dimensions.

Normalcy in daily life relies on vital systems (also known as critical infrastructures) such as transportation, communication, industry, finance, disaster response, water and energy. These infrastructures are continuously monitored and maintained to guarantee that their day-to-day operations can continue uninterrupted by failures, as well as to mitigate potential physical and cyber threats. The Electrical Power and Energy System (EPES) is one of the most complex infrastructures, and its disruption may have huge cascading impacts on other critical infrastructures. The EPES is evolving towards the integration and potential convergence of physical operational technology and cyber information technology through the adoption of industrial internet and internet of things (IOT) [1]. In this context, the PHOENIX project [L1] aims to offer a cyber-shield armour to European EPES infrastructure, enabling cooperative detection of large-scale, cyber-human security and privacy incidents and attacks, guaranteeing the continuity of operations and minimising cascading effects in the infrastructure itself, the environment, the citizens and the end-users at reasonable cost. To be effective, such cyber-shield armour has to be applied to organisational, communication, technological and process frameworks. Indeed, EPES process data from a huge number of edge network nodes (e.g., smart meters, gateways, primary and secondary stations, SCADA and control rooms). As a consequence, traditional EPES development and operation process, which is mainly driven by functional and security requirements (also known as DevSecOps process), is not applicable, and it is vital to pay attention to a wider set of perspectives, including privacy and data protection, ethics and social concerns.

The PHOENIX project aims to reconcile technology development activities with privacy, ethics, security and societal concerns, and to this end an ad hoc methodology has been developed and implemented: the PRESS framework. To enable a harmonic dialogue between technical components and legal/ethical issues, we have drafted a comprehensive tool for all the companies involved in the project, which follows four steps (see Figure 1):

1) definition of the conceptual framework in which the technological solution was intended to be placed and with which the desired solution should find a way to dialogue in harmony;
2) identification (i.e. logical deduction from the conceptual framework) of the compliance requirements for the final design of the technological solution;
3) juxtaposition of the requirements identified with potential concerns/threats which might have originated from their non-compliance, alongside guidelines and policies that aim to avoid (or at least mitigate) the occurrence of threats/concerns;
4) definition of a checklist with the translation in technical language of the "conceptual" requirements, relevant concerns/threats and policies, alongside the most apt technical components. The latter is a valuable tool, to be shared between technical teams and auditors, for monitoring the appropriate evolution of the technology implementation, enacting the compliance assessment, and reporting tests and evidence for qualifying the delivered artefact.

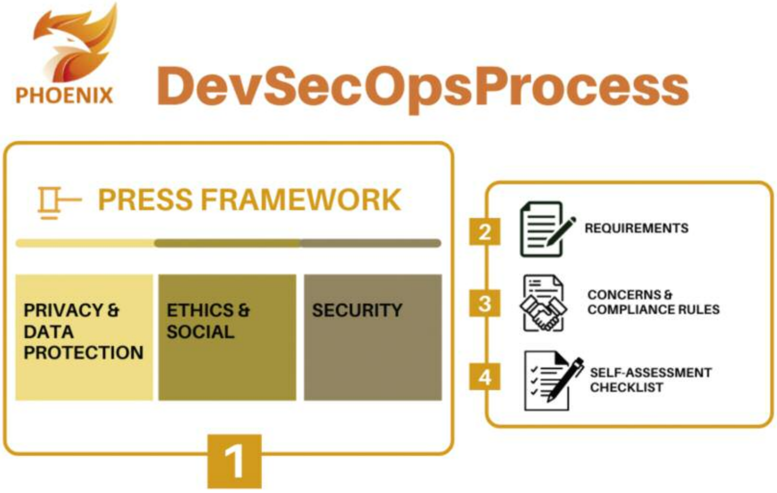

PHOENIX
DevSecOpsProcess
PRESS FRAMEWORK
PRIVACY & DATA PROTECTION
ETHICS & SOCIAL
SECURITY
1
2
REQUIREMENTS
3
CONCERNS & COMPLIANCE RULES
4
SELF-ASSESSMENT CHECKLIST

Figure 1: Privacy-by-Conception in PHOENIX DevSecOps process.

Although this approach was defined within the context of the PHOENIX project, it can easily be applied in other contexts. Indeed, the ultimate goal of this methodology is to reconcile legal and ethical requirements with the necessities connected to the deployment of technology.

The PRESS Framework established in PHOENIX evolves the usual approach of the DevSecOps paradigm by introducing the analysis and validation of privacy and data protection, ethics and social, and security dimensions at the point of conception of the technology, ushering in a holistic assessment. Specifically, the "PRESS Checklist" (step 4 of PRESS Framework) has been defined with an 18-go/no-go steps checklist for self-assessment of DevSecOps tasks. All the actors involved in the PRESS-based assessment will use and adapt this checklist for performing the specific checks, in order to satisfy both specifications and PRESS recommendations. This checklist provides developers with flexibility to adapt acceptance constraints and rules based on their specific component specification and development, as well as the possibility to refine template during the life-cycle of components.

To this end, the PRESS Checklist is an effective tool for driving the specification of the components by taking care of the PRESS recommendations and the suggested mechanisms and techniques to address them, as well as to trigger warnings during the development process and flag where support is required from the ethics team and committee.

As mentioned above, EPES deals with a huge amount of data from different sources. PHOENIX ensures that those data are organised and managed in such a way that organisations can meet enterprise business needs along with legal and governmental regulations. A blockchain-based privacy protection enforcement (PPE) mechanism guarantees better protection for personal data in compliance with the GDPR [2] by providing the following features (see Figure 2):

1) express consent required to process data;

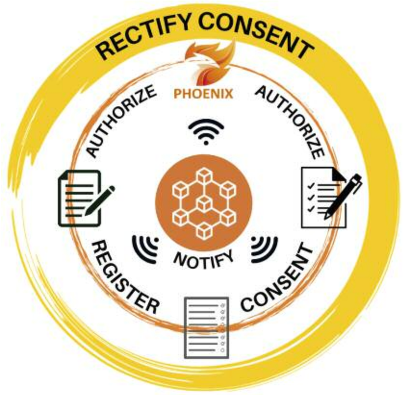


Figure 2: Blockchain-based Privacy Protection Enforcement features.

2) the right to rectify given consent;
3) more and clearer information about processing;
4) the right to notification if data is processed/compromised;
5) immutable data access log.

In PHOENIX, the concept of "Advanced Permission" has been introduced. It comprises two concepts: Consent and Permission.

Consent represents, as stated in Art.4(11) of the GDPR, the data subject's agreement to the processing of personal data relating to him or her, whereas Permission is an abstract concept that represents the system's agreement (or disagreement) to the processing of that specific data based on the Consent status. The combination of that concept of "Advanced Permission", together with blockchain technology and the PRESS framework represents one of the biggest challenges that the PHOENIX project is addressing.

The PHOENIX project received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No.832989.

Links:
[L1] https://phoenix-h2020.eu/
[L2] https://www.cyberethicslab.com

References:

[1] Bailey, et al.: "The energy-sector threat: How to address cybersecurity vulnerabilities", 2020, https://kwz.me/h6V
[2] Regulation (EU) 2016/679 General Data Protection Regulation (GDPR), https://eur-lex.europa.eu/eli/reg/2016/679/oj

Please contact:

Luigi Briguglio
CyberEthics Lab., Italy
l.briguglio@cyberethicslab.com

CAP-A – Raising Privacy Awareness Depends on Us!

by Ioannis Chrysakis (FORTH-ICS and Ghent University), Giorgos Flouris (FORTH-ICS), Theodore Patkos (FORTH-ICS) and George Ioannidis (IN2 Digital Innovations GmbH)

CAP-A is offering socio-technical tools to promote collective awareness and informed consent, whereby data collection and use by digital products are driven by the expectations and needs of the consumers themselves.

Consumers are currently generating vast amounts of data, mostly through applications installed in smart devices, such as mobile phones and smart TVs. Since much of this data is personal, it is important for users to know everything about the use of their data, including whether apps are compliant with the recently established GDPR legislation, or which device permissions are mandatory and why.

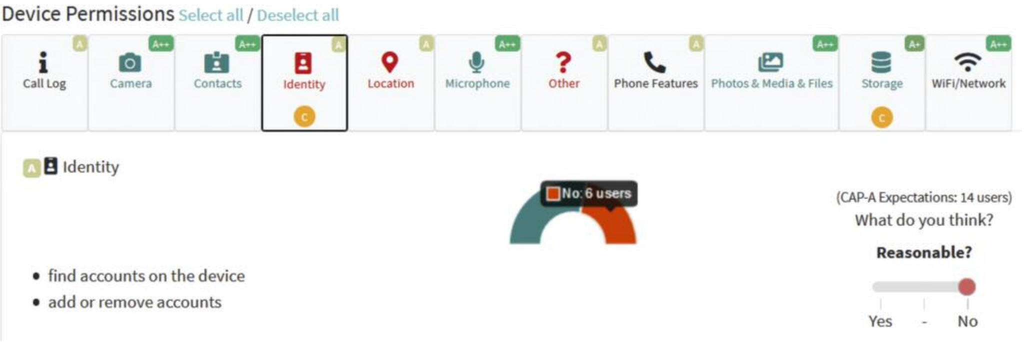
However, this is practically impossible, since the utilisation of such data by apps is usually hidden behind vague privacy policy documents, which are often lengthy, difficult to read (due to the legal terms and definitions they contain) and frequently changing.

At the heart of the CAP-A project [L1] is the hypothesis that data protection can also be powered by society itself. By mobilising consumers to become active players in digital marketplaces and by developing tools to harness our collective power, the adoption of technical and regulatory frameworks can become more effective and ubiquitous, and the market will respond, largely because it is profit-maximising.

To this end, CAP-A is offering socio-technical tools to promote collective awareness and informed consent, whereby data collection and use by digital products are driven by the expectations and needs of the consumers themselves.

The CAP-A tools

In the CAP-A project, we have developed a set of tools that employ crowdsourcing techniques to support consumers in expressing their privacy concerns and expectations (Figure 1), annotating PrP documents (Figure 2), and



Device Permissions Select all / Deselect all

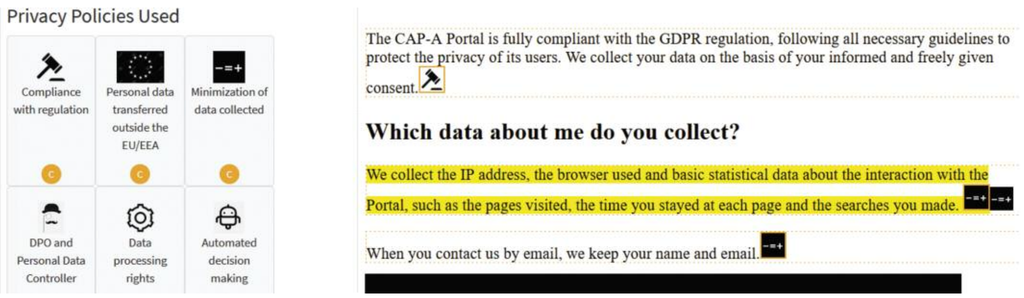
A Identity

- find accounts on the device
- add or remove accounts

(CAP-A Expectations: 14 users)
What do you think?

Reasonable?

Figure 1: Expressing privacy expectations in CAP-A.



Privacy Policies Used

Compliance with regulation
C
Personal data transferred outside the EU/EEA
C
Minimization of data collected
C
DPO and Personal Data Controller
Data processing rights
Automated decision making

The CAP-A Portal is fully compliant with the GDPR regulation, following all necessary guidelines to protect the privacy of its users. We collect your data on the basis of your informed and freely given consent.

Which data about me do you collect?

We collect the IP address, the browser used and basic statistical data about the interaction with the Portal, such as the pages visited, the time you stayed at each page and the searches you made.

When you contact us by email, we keep your name and email.

Figure 2: Annotating the PrP document of an app with CAP-A.

better understanding privacy-related information regarding the used apps [1].

The CAP-A tools are freely available online for anyone to use [L2]. They include a CAP-A portal and an accompanying native Android CAP-A app. The CAP-A project is part of the CAPrice initiative [L3], a grassroots community that exists to apply crowdsourcing solutions to raise awareness about and provide solutions to privacy-related matters.

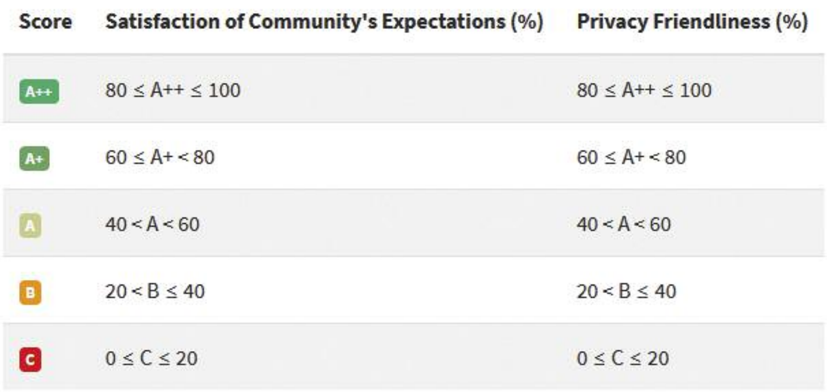
The CAP-A approach assesses mobile apps along two different metrics (Figure 3), which quantify their privacy-related behaviour as assessed by consumers. To enhance participation and provide motivation for active contribution to the platform, we apply a unified rewarding strategy [2] that includes gamification features for active consumers and developers such as points and tiers for users (Figure 4).

Results

The CAP-A portal has digested privacy-related information about more than 19,000 Android apps, which is available for users to explore. During the project, 164 users registered and used the CAP-A portal, whereas 51 users installed the mobile app. Their contributions resulted in the expression of personal expectations for about 567 apps and in 1181 annotations on different Privacy Policy documents.

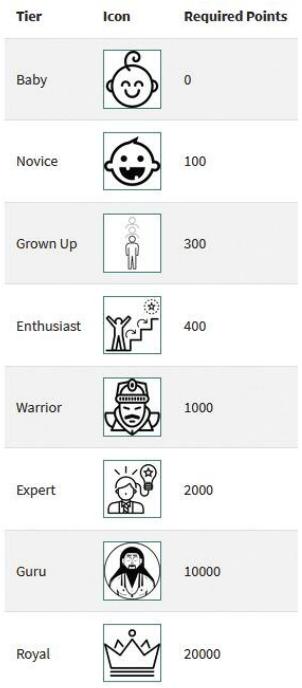
Beyond the portal and the project website, our communication and dissemination activity has reached hundreds of users in social media, helped grow the CAPrice Community, namely the mailing list by 240% (455 users, as of April 2021) and the total community size, including social media followers, by 143% (1563 users/followers/subscribers, as of April 2021). The CAP-A project appeared in 7 scientific venues and 12 wide public events.

One of the main objectives set at the beginning of the project, i.e., to attract the interest of a considerable number of users to start generating informative privacy norms, has thus been achieved. The CAP-A dashboard, which is encap-



Score	Satisfaction of Community's Expectations (%)	Privacy Friendliness (%)
A++	80 ≤ A++ ≤ 100	80 ≤ A++ ≤ 100
A+	60 ≤ A+ < 80	60 ≤ A+ < 80
A	40 < A < 60	40 < A < 60
B	20 < B ≤ 40	20 < B ≤ 40
C	0 ≤ C ≤ 20	0 ≤ C ≤ 20

Figure 3: Visual Cues of CAP-A: Community metrics.



Tier	Icon	Required Points
Baby		0
Novice		100
Grown Up		300
Enthusiast		400
Warrior		1000
Expert		2000
Guru		10000
Royal		20000

Figure 4: Visual Cues of CAP-A: Rewarding Tiers.

sulated in the CAP-A portal, provides a wealth of statistics, such as the percentage of consumers who considered it reasonable to allow access to a certain type of data, such as camera or contacts, for a given app category [L4]. This information can be used by stakeholders (e.g., developers, social scientists, policy makers) to conduct analyses and interpret the behaviour and mind-set of various user groups, according to age or other demographic characteristics.

None of this would be possible without consumer participation. So, in order to increase the number of user contributions in the CAP-A tools, it is critical for the formulated CAPrice community to become self-sustainable and grow. Our aim is for consumers to realise that we are all responsible for raising privacy awareness.

Project details

The CAP-A project received funding from the EU Horizon 2020 research and innovation programme under the NGI TRUST grant agreement no 825618. The project began in August 2019 and was planned to run for one year; however, due to the COVID-19 pandemic, an extension until the end of 2020 was granted. The project consortium consisted of FORTH and IN2 Digital Innovations. FORTH is the largest research institute in Greece; FORTH coordinated the project and participated with the Institute of Computer Science (ICS) and the PRAXI Network. IN2 Digital Innovations, is a software development company offering web-based solutions. Through CAPrice, the outcomes of the project will be maintained in the future.

Links:
[L1] https://www.cap-a.eu
[L2] https://www.cap-a.eu/tools/
[L3] https://www.caprice-community.net/
[L4] https://cap-a.eu/portal/#stats

References:

[1] I. Chrysakis et al.: “Evaluating the data privacy of mobile applications through crowdsourcing,” in Legal knowledge and information systems, virtual event, 2020, vol. 334, pp. 219–222.
[2] I. Chrysakis, et al: “REWARD : ontology for reward schemes,” in Proc. of ESWC 2020, Heraklion, Crete, Greece, 2020.

Please contact:

Ioannis Chrysakis, FORTH -ICS,
Tel: +30 2811 391635
hrysakis@ics.forth.gr

WellFort: A Platform for Privacy-Preserving Data Analysis

by Tomasz Miksa, Tanja Šarčević, Rudolf Mayer (SBA Research) and Laura Waltersdorfer (Vienna University of Technology)

Data has become deeply ingrained in all phases and aspects of industrial and scientific research. The potential for new discoveries based on data-driven research is growing fast, due to the high volume and granularity of personal data collected by individuals, e.g., by means of ubiquitous sensors and IoT devices. However, small and medium-sized organisations typically face challenges in acquiring and storing personal data, particularly in sensitive data categories.

To enable organisations to leverage the full potential of the personal data they collect, two main technical challenges need to be addressed: (i) organisations must preserve the privacy of individual users and honour their consent, while (ii) being able to provide data and algorithmic governance, e.g., in the form of audit trails, to increase trust in the result and support reproducibility of the data analysis tasks performed on the collected data.

Organisations could further improve their analysis by integrating data from different, complementary sources and users, but there is no established way to request such data – and individuals often refrain from sharing data due to lack of trust. We believe that individuals would contribute their data to research and welcome services that enhance their experience, for example, in the fitness or medical domain, if security and privacy were guaranteed and users could maintain control by giving explicit consent.

On the other hand, organisations must be able to provide evidence that the data is used according to the consent given, and to collect information on how the analysis was performed. This information must encompass the traditional provenance, such as who and when data was accessed, but also information on software libraries and scripts used to analyse the data. This is especially important in litigation cases and scientific peer review when new claims are scrupulously evaluated. Privacy-preservation cannot be the reason for not making the data analysis auditable.

To address these problems, we are developing a platform called WellFort, which provides secure storage for users’ sensitive data, while delivering a trusted analysis environment for executing data analytics processes in a controlled privacy-preserving environment. A novelty of our approach is that organisations do not have direct access to data, but only allow this in aggregated or anonymised form. Organisations can benefit from a large group of individuals that are potentially willing to share their data for research. Users benefit from a privacy-preserving and secure platform for their data, and can contribute to research projects in a secure manner. Finally, scientific researchers have a detailed source of microdata, if data subjects give consent to their research proposals.

The conceptual architecture of the platform is depicted in Figure 1. There are three distinct actors:

- Users store their data in the platform, give consent to analyse it, etc. They use an application provided by the organisation and interact with the

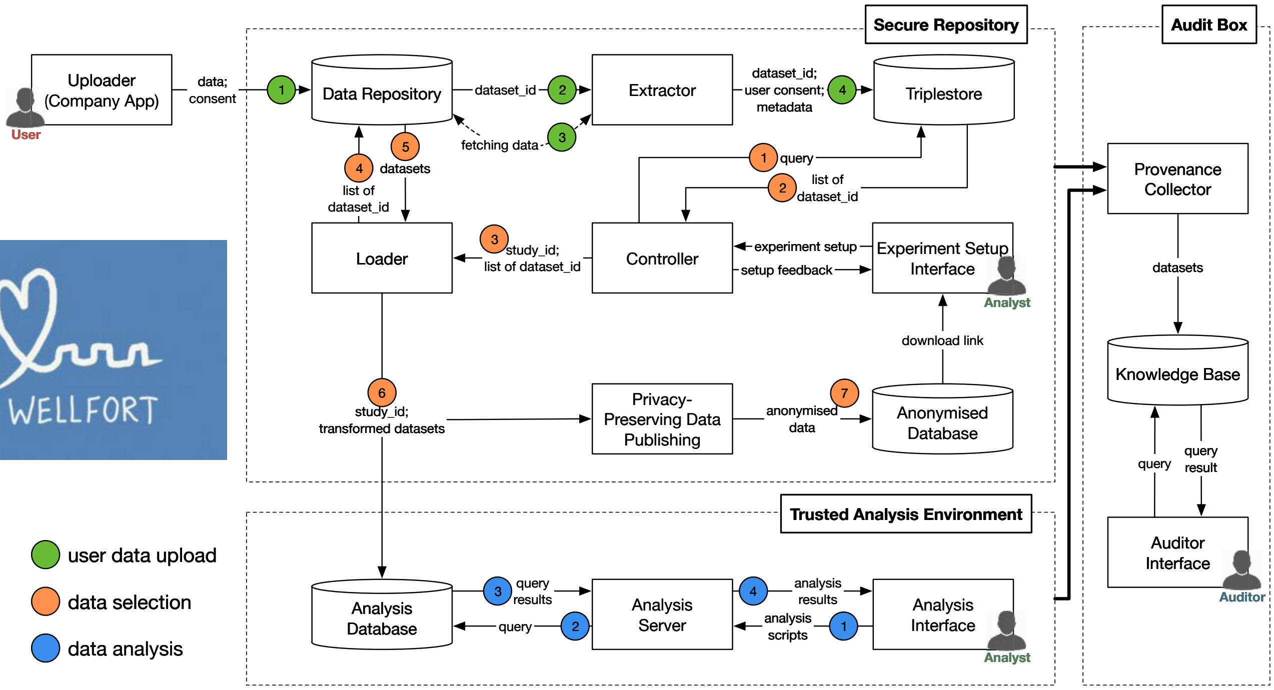


Figure 1: The WellFort architecture, comprising the Secure Repository, Trusted Analysis Environment and the Audit Component.

platform using a dedicated user interface.

- Analysts can run experiments on the platform. They define which types of data will be used and perform the actual analysis.
- Auditors can analyse evidence collected to answer specific audit questions that depend on the purpose of the audit, e.g., a litigation case. A special form of auditor is a user wanting to know when and by whom their data was used.

The architecture consists of three component groups (each marked with dashed lines in Figure 1), each serving a different purpose:

- Secure Repository – stores data uploaded by a user, together with a fine-grain consent [1], and allows the selection of data to be used in experiments by the analyst.
- Trusted Analysis Environment – selected data that fulfils experiment criteria, e.g., consent, fit for purpose, etc. is duplicated to this component for further analysis. This component provides mechanisms to conduct data analysis in a privacy-preserving manner, e.g. using DataShield [2]. Data selection is usually expressed via queries.
- Audit box – collects and manages provenance data to support auditability [3]; it can be accessed to answer audit-related questions on personal data access and usage.

Figure 1 further depicts three processes that may be executed in the platform:

- User data upload – starts when a user's application sends data to the platform. It extracts metadata from the data, and stores it together with the data and the consent indicated during the upload in the platform. Thus, every dataset uploaded to the platform is linked to a minimal set of information that allows for its retrieval.
- Data selection – analysts define the search criteria for data they want to use in their experiments. If the platform has enough data fulfilling their criteria (and consent for usage), then the process loads the actual data into the Trusted Analysis Environment. Analysts do not have access to individual datasets. The search for data relies only on high-level information provided in the metadata.
- Data analysis – analysts process the data and produce results by submitting code to the platform. The platform will ensure that the analysts will not be able to identify or infer data subjects from the analysis.

The platform is currently evaluated in the medical domain, with two start-ups providing and analysing medical and wellbeing data. These two data sources are analysed individually, and are also integrated to provide a more holistic view on patients. In the future, we plan to focus on use cases in other domains, to evaluate whether our approach extends well to other types of data and analysis processes.

The WellFort project receives funding from the Austrian Research Promotion Agency FFG under grant 871267 (WellFort).

Link:
[L1] https://kwz.me/h6X

References:

[1] J.D. Fernández et al.: "User consent modeling for ensuring transparency and compliance in smart cities", Personal and Ubiquitous Computing (2020), 1–22.
[2] A. Gaye, Y. Marcon, J. Isaeva, et al.: "DataSHIELD: taking the analysis to the data, not the data to the analysis." International journal of epidemiology 43.6 (2014): 1929-1944.
[3] R. Mayer, T. Miksa, and A. Rauber: "Ontologies for describing the context of scientific experiment processes"; in Proc. of the 10th Int. Conf. on e-Science, Guarujá, SP, Brazil, 2014.

Please contact:

Tomasz Miksa
SBA Research, Austria
tmiksa@sba-research.org

Using TEEs to Build a Privacy-Preserving Internet of Things Ecosystem

by Pascal Gremaud, Arnaud Durand and Jacques Pasquier (University of Fribourg, Switzerland)

Cloud-based Internet of Things commercial solutions offer an ever-growing set of possibilities. However, these come at the cost of entrusting data to the platforms running these systems. We explain how Trusted Execution Environments can be used to enforce device and user data confidentiality for an entire ecosystem.

The Internet of Things (IoT) is an ever-growing field, with multiple applications aimed at different types of users. Cloud-based solutions allow users to connect their devices, enabling them to easily set up a rich ecosystem. However, these systems may not only suffer from external attacks, but they are also susceptible to being compromised by internal parties. Indeed, cloud platforms as well as providers of the services running on these platforms have access to all data contained in them. In order to function, these systems rely on their users entrusting data to these companies, simply because so far there is no alternative to this security model.

Our project is centred around a simple idea: at no point in time should data be accessible by any party other than its owners, unless specified by the owners themselves. Based on this principle, we are aiming to create a complete IoT ecosystem designed for smart home applications and connected appliances in general. Such a security requirement can easily be met by services such as messaging or data storage, since data is not processed by non-trusted parties. However, the strength of a typical IoT ecosystem is precisely the ability to enable complex interactions between multiple devices and users, which requires data processing. Because we target non-expert users, an easily deployable, cloud-based solution is a must for achieving our goal.

Our ecosystem, shown in Figure 1, relies on Intel's Software Guard Extensions (SGX) to protect data on a cloud platform. This set of instructions allows the creation of a memory-protected region, called an enclave. In our project, this enclave is responsible for client registration and authentication, as well as data processing. In order to ensure privacy in this cloud environment, all data passing to and from the enclave are encrypted. A web server is responsible for passing client messages to the enclave, and for sending responses. We use application-layer encryption to guarantee that transiting data cannot be accessed either by an external attacker, or by the cloud platform provider (including when being treated by the web server). We designed a simple protocol on top of HTTP in order to easily communicate with web clients. Our system is also capable of using the Object Security for Constrained RESTful Environments (OSCORE) protocol, the use of which we evaluated in the context of secure IoT [1]. Both these protocols use a RESTful API exposed by the middleware platform to interact with it.

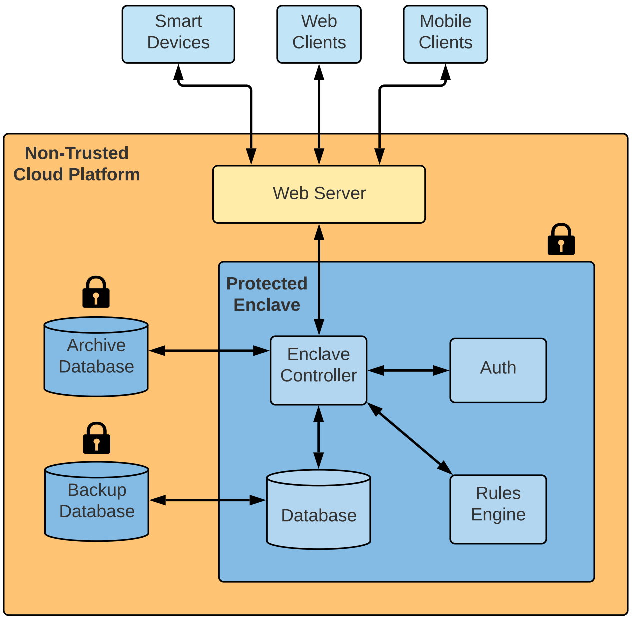


Figure 1: The architecture of the ecosystem. Components in shades of blue are considered trusted.

We store data in two different ways, depending on the type of data. An in-memory database running inside the enclave is used to store data related to the middleware model, such as clients, event types, rules, etc. An encrypted backup of this database is saved outside the enclave in case of a system reboot. A second database running outside the enclave is responsible for archiving encrypted past messages and can be used to get the history of the system's events. Our system uses a simple Event-Condition-Action (ECA) engine adapted from the iFLUX middleware model [2] as its rules engine. An ECMAScript engine running inside the enclave allows middleware rules to be defined as scripts, enabling rich interactions between devices and complex scenarios. For instance, a user can set smart radiator valves to stop heating their home when it is assumed that the house is vacant. A combination of the user's phone not being connected to their home WiFi network and deductions based on their online planner can be used as a condition for this scenario.

Client registration and authentication is performed using a simple Public Key Infrastructure (PKI). The owner of the system (one of its users) creates a self-signed certificate that is distributed to each client, including the enclave. This special user acts as the root of trust for the entire system. The enclave acts as a Certification Authority (CA), and is able to issue new certificates to clients and verify them when authenticating. The creation and modification of middleware logic resources (clients, rules, event types, etc.) are performed via web or mobile clients. Complex IoT scenarios can be proposed by third parties in the form of predefined configuration files, and then instantiated using a dedicated web client. Because all the interaction with the enclave are done using this client, there is no need to grant any data access to these third parties.

One key point of the system is the ability to attest that the enclave code corresponds to the users' expectations. Intel proposes a remote attestation mechanism to comply with this requirement. Before the verification, the public certificate of the system owner is placed in the enclave, which ensures that this particular enclave instance is linked with that specific user.

Using the architecture we described, our ecosystem is able to achieve both a high level of data security and an ease of use and deployment for non-experienced users. We plan on extending the system features and creating real-life scenarios by deploying devices using a dedicated firmware to interact with our system. We believe that such systems will become a suitable response to security concerns that arise with the vast amount of data used in the IoT. We hope to see a growing interest in similar projects in the near future. Updates on the project can be found at [L1].

Links:
[L1] https://kwz.me/h6z

References:

[1] A. Durand et al.: "Trusted lightweight communication for IoT systems using hardware security", in: Proc. of the 9th Int.Conference on the Internet of Things, 2019.

[2] O. Liechti et al.: "Enabling reactive cities with the iFLUX middleware", in: Proc. of the 6th Int. Workshop on the Web of Things,2015.

Please contact:

Pascal Gremaud
University of Fribourg, Switzerland
+41 79 454 41 20
pascal.gremaud@unifr.ch

KRAKEN - Brokerage and Market Platform for Personal Data

by Andreas Abraham (Graz University of Technology), Juan Carlos Perez Braun (Atos Spain S.A.), and Sebastian Ramacher (AIT Austrian Institute of Technology)

The EU Horizon 2020 KRAKEN project is dedicated to building a trusted and secure personal data platform enabling exchange and analytics of personal data.

Data sharing platforms are facing several challenges in terms of security, privacy, trust, and regulatory compliance. To address these challenges, the KRAKEN (brokerage and market platform for personal data) project [L1,L3] aims to develop a trusted and secure personal data platform, with the state-of-the-art privacy aware analytics methods, which guarantees metadata privacy and query privacy, empowering citizens to control their personal data, including sensitive data, and motivate users to share this kind of data.

KRAKEN provides a highly trusted, secure, scalable and efficient personal data sharing and analysis platform that relies on self-sovereign identity services and cryptographic tools to cover the security, privacy and user control of data. As part of the project, we are also investigating data processing mechanisms within the encrypted domain with the aim of increasing security, privacy, functionality and scalability for boosting trust.

KRAKEN is based on three main pillars:

- The self-sovereign identity paradigm providing a decentralised user-centric approach to personal data sharing. KRAKEN is returning control of personal data back into the hands of data subjects and data providers. Its subsequent use is controlled by explicit user consent.
- KRAKEN will develop a set of analytics techniques based on advanced cryptographic tools that will permit privacy-preserving data analysis, end-to-end secure data sharing and confidentiality of privacy-sensitive data.
- A data marketplace will allow personal data to be shared in a preserving-privacy manner when artificial intelligence/machine learning analysis is performed. Additionally, to motivate the user to share their data, the developing of fair-trading protocols and incentive models is envisaged, establishing economic value and innovative business models for 'personal data spaces'.

As personal and sensitive data are managed and shared, KRAKEN provides an ethical and legal framework to accomplish the General Data Protection Regulation [L2] and eIDAS compliance, following standards for compatibility and interoperability, and promoting best practices.

The health and education domains were selected to demonstrate how SSI and cryptographic technologies can improve the security and privacy of personal data, including sensitive data, when shared in a marketplace. The health scenario involves sensitive data such as biomedical and well-being data, which implies the use of powerful privacy-preserving techniques assuring the data are always protected. The education scenario involves personal data such as grades, courses or diplomas, which can be provided to a third party in a privacy-preserving way. In both cases, the use of SSI and cryptographic technologies ease the shared use of these data assuring the data are protected and the owner has the control over the use of the data. Finally, the aim is to generalise the KRAKEN experience to other economic domains (Figure 1).

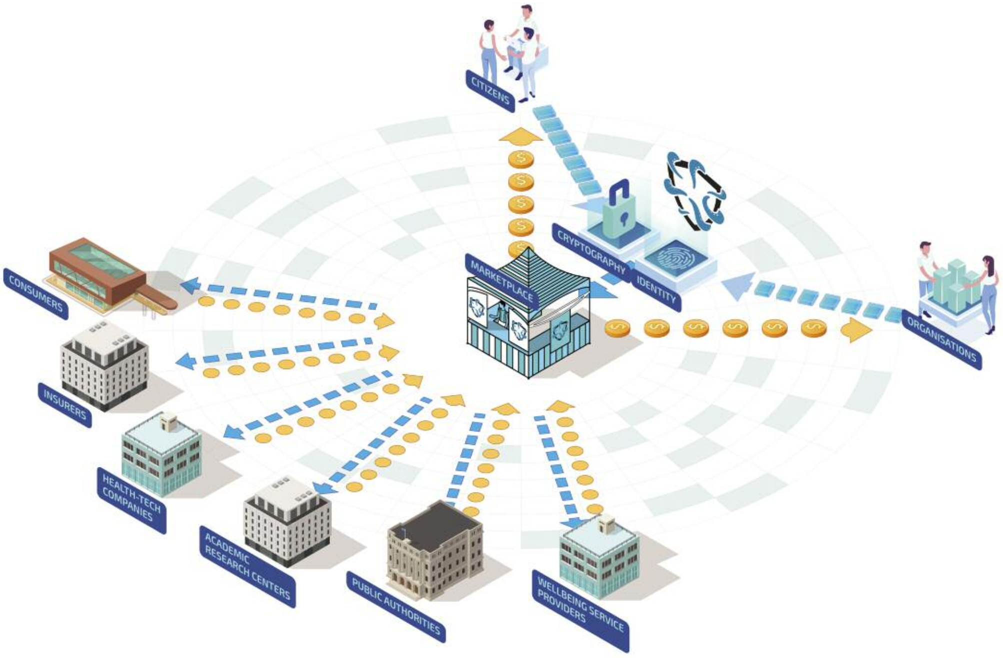


Figure 1: The KRAKEN data marketplace provides opportunities for various data owners and stakeholders to exchange data and analytics for monetary compensation.

Computation platform

The core primitive leveraged by the platform is secure multi-party computation [1], which allows nodes to jointly perform a computation without each node learning the input data of the others. Data providers can decompose their data into fragments such that no single fragment contains any information about the original data. For each data item, each node is then granted access to one of the shares, and the nodes can jointly perform analytics, compute statistics, or answer queries from consumers, without learning the individual data provider's data, as long as a single node behaves honestly. In addition to secure multi-party computation, KRAKEN deploys further privacy-enhancing technologies, such as group signatures and zero-knowledge proofs to ensure that data consumers receive strong and undeniable cryptographic evidence about the correctness of the received results.

KRAKEN's design also allows data providers to apply fine-grained policies to their data that specify which computations may and may not be performed on their data. These policies are checked by the nodes before participating in any further computation, thereby avoiding potential misuse through unauthorised consumer requests. The result is a cryptographically secured and feature-rich market platform that achieves an unprecedented level of privacy for personal input data.

Self-sovereign identity

KRAKEN further utilises the recent self-sovereign identity technology to address the digital identity aspect of the project. Digital identities are required for users to identify and authenticate towards service providers. Digital identities are often based on central authorities where users do not have full control of their data. Self-sovereign identity systems tackle these issues by utilising technologies such as the distributed ledger technology to address the central authority.

KRAKEN will enhance the state-of-the-art of the self-sovereign identity technology for different aspects. One of these aspects is that KRAKEN will enable the privacy-preserving identity attribute showing [2]. This is especially relevant if a user wants to reveal only a subset of their identity attributes to service providers. Additionally, self-sovereign identity systems lack identity data with legal background, i.e., qualified identity data issued by trust service providers operating in traditional identity systems which do not support self-sovereign identity paradigms. Thus, KRAKEN will develop an efficient and privacy-preserving way to derive existing identity data into a self-sovereign identity-based system. Zero-knowledge proofs are utilised to achieve this and further elevate the level-of-assurance in the identity data used within the identity system.

The KRAKEN project has been running since December 2019 and is a 36-month project that receives funding from the European Union’s Horizon 2020 Research and Innovation programme under grant agreement No 871479. The project is coordinated by Atos and its consortium consists of ten partners from academia and industry from six different countries.

Links:
[L1] https://krakenh2020.eu/
[L2] https://kwz.me/h6v
[L3] https://kwz.me/h6w

References:
[1] K. Karl, et al.: “Privacy-preserving Analytics for Data Markets using MPC2, in: Privacy and Identity Management 2020, Springer IFIP AICT 619 (to appear).
[2] A. Abraham, et al: “Privacy-Preserving eID Derivation for Self-Sovereign Identity Systems”, ICICS 2019.

Please contact:
Sebastian Ramacher
AIT Austrian Institute of Technology, Vienna, Austria
sebastian.ramacher@ait.ac.at

Handling Privacy Preservation in a Software Ecosystem for the Querying and Processing of Deep Sequencing Data

by Artur Rocha, Alexandre Costa, Marco Amaro Oliveira (INESC TEC) and Ademar Aguiar (University of Porto and INESC TEC)

iReceptor Plus will enable researchers around the world to share and analyse huge immunological distributed datasets, from multiple countries, containing sequencing data pertaining to both healthy and sick individuals. Most of the Adaptive Immune Receptor Repertoire sequencing (AIRR-seq) data is currently stored and curated by individual labs, using a variety of tools and technologies.

iReceptor Plus aims to lower the barrier to accessing and analysing large AIRR-seq datasets, which will make this important data more available to academia, industry and clinical partners.

The project will stimulate the public sharing of AIRR-seq data, while providing a mechanism for users to protect private data when required. To this end, we are developing a layered security framework across a distributed (federated) software ecosystem.

The international iReceptor Plus [L1] (iR+) consortium aims to promote human immunological data storage, integration and controlled sharing for a wide range of clinical and scientific purposes. iR+ is an ongoing four-year project, started in 2019, and co-funded by the EU and Canadian government, that aims to develop an innovative platform to integrate distributed repositories of Adaptive Immune Receptor Repertoire sequencing (AIRR-seq) data [1] that will enable improved personalised medicine and immunotherapy in cancer, inflammatory and autoimmune diseases, allergies and infectious diseases.

This platform will empower researchers around the world to share and analyse huge immunological distributed datasets, from multiple countries, that contain sequencing data pertaining to both healthy and sick individuals. Currently, most of these data banks are stored and curated by individual labs, using a variety of tools and technologies. iR+ software ecosystem will lower the barriers to accessing and analysing large AIRR-seq datasets, which will make these important data more available to academia, industry and clinical partners.

Layered security framework

AIRR sequencing [L2] technology has made it possible to sample the immune repertoire in exquisite detail but also poses substantial challenges, such as the preservation of the privacy of data subjects.

The issue of privacy is a topic of continuous discussion within the health informatics community, especially when it comes to genetic datasets, which are subject to constraints of confidentiality, security, rights and ownership. While analyses performed on these datasets may provide crucial research evidence, both data access and their processing must be conducted in a way that does not compromise privacy.

The role of iR+ layered security framework is to enable secure access between the components of the software ecosystem, following the current standards of security, to provide multiple levels of authentication and authorisation to AIRR Data Commons (ADC) [2] compliant software.

The layered security framework delivers to iR+ a working Authentication and Authorisation Infrastructure enabling the following features [L3]:

- federated authentication for data consumers, compatible with multiple third-party identity providers (and identity brokers);
- secure ADC repository endpoints according to the permissions set by data stewards;
- a dashboard for data stewards to manage data consumer's permissions for each end-point and resource they own.

Due to the distributed nature of the data providers and to the technological heterogeneity of the various repository services, the security framework was implemented following a technology-agnostic approach. It was vital to determine an interoperable mechanism for managing resources, independent of the underlying repository implementation.

Authorisation component

The main standard for managing authorisation is user-managed access (UMA 2.0). UMA is an OAuth-based access management protocol for managing authorisation to resources. It grants data stewards the ability to manage permissions and accessibility to their resources, and control who can access their resources (data consumers). The basic workflow follows an exchange of permission tickets between the security framework and the requesting user. The process is used to identify the user, determine which dataset the user is trying to access, and finally to resolve which sets of data should be returned to the user.

The UMA 2.0 authorisation standard was designed specifically for protected data. However, in iR+, protected data may live side by side with public data in the same repositories. Therefore the security framework had to deal with this limitation and extend regular UMA implementations by acknowledging both authenticated and unauthenticated access to publicly available data:

By default, any requests made to a secured repository will return data defined by the data steward as publicly accessible. This means the requesting user will not need to be registered and will not need to explicitly request access to the data steward to view public data. On the other hand, we leveraged on the HTTP protocol by

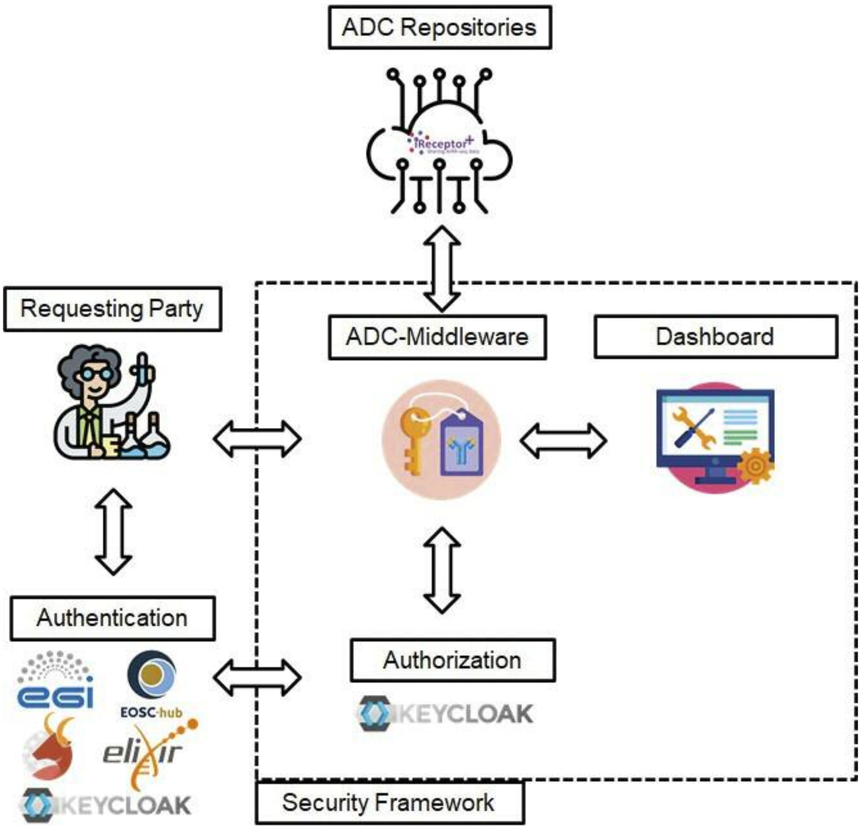


Figure 1: Overview of the Security Framework and interaction among its main components.

appending a custom HTTP header that should be sent along with the request, to trigger the default UMA authorisation workflow to access protected data.

Dashboard component

The security dashboard is an interface that allows data stewards to control access using different levels of granularity through an interface modelled after the ADC data standards. It enables fine-grained customisation over what is exposed by the security framework.

Accessibility levels may be customised using arbitrary permission scopes. For example, a data steward may enable an intermediary permission level for exploratory data analysis, where only aggregated, non-identifying information is delivered to the requesting user, by defining a specific scope for such purpose.

It provides flexible settings through security templates that allow data stewards to quickly set up recurring accessibility levels for different datasets.

ADC-Middleware

The ADC-Middleware [L4], is the central component of the security framework and the main service responsible for providing a control layer between the requesting users and the ADC repositories. It takes into account all the security configurations, data ownership, who the data was shared with, fine-grained customisations, and uses this information to control which sets of data should be exposed to users.

It effectively acts as a barrier between the ADC Repository, only making it possible to request contents the user has access to, and filters out any data the user does not have access to. This filtering process builds on the UMA 2.0 authorisation service to determine permissions, along with the ADC-Middleware internal filtering engine to determine more fine-grained access control.

The ADC-Middleware provides programmatic access to AIRR-seq data sets following the same querying and filtering formats that a normal ADC API would, and is fully interoperable with ADC API implementations.

Conclusions

The layered security framework builds on the privacy by design and data minimisation principles to attain privacy preservation in a federated software ecosystem for the querying and processing of AIRR-seq data. If data has been previously made public, it can be accessed via standard APIs without triggering the default UMA workflow. Should access restrictions apply, data stewards can use the security framework to configure adequate permission levels according to the sensitivity of the data to be shared.

As an example, summary statistics, non-disclosive features derived from genetic data, or other forms of aggregated data can be set to an intermediary level of permissions. A registered user could then access these features in an exploratory data analysis stage, before deciding to activate the necessary legal instruments for the sharing of potential sensitive data.

Links:

[L1] https://www.ireceptor-plus.com/
[L2] https://kwz.me/h67
[L3] https://kwz.me/h65
[L4] https://kwz.me/h66

References:

[1] F. Rubelt, et al.: “Adaptive immune receptor repertoire community recommendations for sharing immune-repertoire sequencing data", Nature immunology 18.12 (2017): 1274-1278.

[2] S. Christley et al.: “The ADC API: a web API for the programmatic query of the AIRR Data Commons”, Front, Big Data 3: 22. doi: 10.3389/fdata (2020).

Please contact:

Artur Rocha
Institute for Systems and Computer Engineering, Technology and Science, Portugal
artur.rocha@inesctec.pt

INAH: The Ethical & Secure Platform for Medical Data Analysis

by Terence Delsate, Xavier Lessage, Mohamed Boukhebouze and Christophe Ponsard (CETIC)

INAH (The Institute of Analytics for Health) platform is created to enable ethical and secure use of medical data in statistical and medical research. This platform could benefit society and improve both patient life quality and public health while ensuring medical data privacy.

Like all domain, healthcare is revolutionized by the access and analysis of (big)data to create social and economic value. Several health players such as universities, life science companies and authorities are interested in accessing and analyzing medical data to accelerate medical research and move to personalized, predictive and preventive medicine, which enables improving the patient life quality and helps to implement health policies accordingly. However, the use of these medical data has to deal with several technical, juridical, and ethical challenges to preserve privacy of patients and ensure the quality and security of medical data.

To deal with these challenges, the Walloon government launches the development of the INAH platform that allows secure and ethical access to medical data. This platform, which is led by our research center and the FRATEM (Regional Federation of Medical Telematics Associations [L1]), enables multicentric analysis of medical data as part of medical and statistical research projects by respecting following five key principles:

- Sovereignty of data providers who remain free to participate in the submitted projects as well as have control and governance over their data.
- Trust, based on ethical and secure access, forbidding both direct and indirect identification of patients.
- Partnership though collaboration between data users, data providers and practicians around research projects.
- Velocity ensuring fast, efficient access, and freshness of data.
- Conformity to medical standards (e.g., SNOMED) and legislation (e.g., GDPR).

Figure 1 depicts the technical architecture of INAH platform. To ensure the data sovereignty principle, the medical data do not leave data providers infrastructure. Consequently, INAH platform relies on distributed data warehouses (virtual data lake), hosted at the data providers premises (infrastructure). We refer these data warehouses, together with the data access control component that is implemented as INAH Remote. These remote data warehouses follow the same data model and contain the extraction of the key medical concepts. To preserve privacy, no clear patient identifiers are encoded inside the remote data warehouse. For each ingested data, the patient identifier is pseudonymized with a secret key, each key being different for each remote instance [1]. These keys are hosted in a Trusted Third Party (TTP), which exposes a pseudonymization service. Therefore, two remote instances are not compatible with each other, since not a single patient will be represented in the same way. The remaining suite of the remote instance is used to manage the communication between the data sources and the central platform, implementing all the necessary security checks, such as the fact that a specific request has been authorized by the data source manager, and to perform the actual analytical tasks.

In INAH platform, the medical data access is requested by submitting a project. This latter is evaluated by an approbation committee, which preapproves or not the project from an ethical and a scientifical point of view. Once the first validation is passed, the project will be sent to each data providers (ethical committee), who can

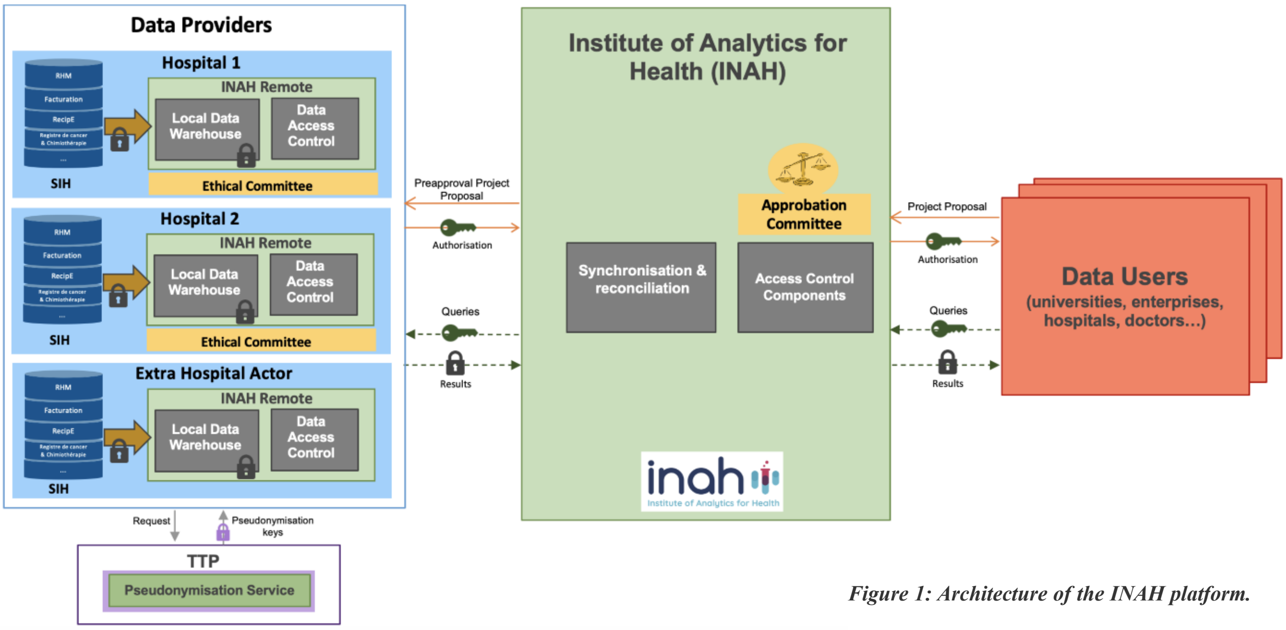


Figure 1: Architecture of the INAH platform.

decide to participate or not to the project, and further choose which part of its data could be used for the project. After the approval of a project, the access authorization token is generated. Based on this token, the data users can express their queries from the INAH to define a statistical population [2]. The expressed queries are sent to the data providers in order to locally identify the patient forming this population. A multisite synchronization procedure can then be applied to merge the result. In this procedure, a project specific pseudonymisation is applied using a secret key in the TTP. This second pseudonymisation helps to prevent inter-project data crossing for the same data user. INAH platform enables to exploit the defined statistical population in different ways: the population could be monitored in real time (for instance for an epidemic survey), a specific dataset can be requested (such as comorbidity of a newly vaccinated population), specific statistical quantities could be extracted (to provide a non-exhaustive list of examples of possible use cases).

The INAH platform is currently deployed as pilot project within three major Walloon hospitals and also involves local life science companies. It is raising the interest of health actors (e.g., public authorities, universities, pharmaceutical companies). The next step is to launch the exploitation of the platform with the collaboration of the hospital federations.

Acknowledgement:
We thank Dr. A. Vandenberghe for his fruitful contribution. We also thank all the INAH project partners as well as our internal technical team, R. Michel, O. Dridi, A. Nuttinck for their great job. This work is supported by AVIQ and SPW-EER and funded by the Walloon government.

Link:
[L1] https://www.reseausantewallon.be

References:

[1] D. Darquennes: “Privacy models in healthcare data processing”, CETIC Lecture, November 2019.
[2] T. Delsate and M. Boukhebouze: “Anonymous multi-source counting statistics New methodology applied to the health sector”, ICTS4HEALTH workshop, Barcelona, 2019.

Please contact:

Mohamed Boukhebouze
CETIC, Belgium
+32 497 78 59 51
mohamed.boukhebouze@cetic.be

SlotMachine – A Privacy-preserving Marketplace for Slot Management

by Thomas Lorünser (AIT), Christoph Schütz (JKU) and Eduard Gringinger (Frequentis)

To enable more efficient management of airport departure and landing slots, SlotMachine envisions a new kind of marketplace in air traffic management. The platform will enable a more flexible, fast and scalable semi-automated flight prioritisation process for airlines in a fair and trustworthy way. Built with a privacy-first approach it will protect sensitive airline data from competitors and airport operators but fully unleash the potential of inter-airline slot swapping.

In times of growing air traffic and limited capacity, it is crucial to improve the utilisation of resources (airports, airlines and air navigation service providers) and to mitigate the economic impact of disruptions. When airports operate at the limit of their capacity, a small disruption, e.g., bad weather, may cause delays to many flights. Delays result in additional costs for airlines, such as compensation for passengers and costs associated with crew changes. To minimise the overall costs caused by delays, airlines want to be able to dynamically rearrange and prioritise certain flights. This is already possible within a fleet [1] but to minimise costs, airlines need to be able to prioritise delayed flights across airline boundaries and would like to do so without prolonged negotiations. This is inherently difficult because airlines as competitors are very careful not to disclose any business secrets such as the flight-specific estimated costs associated with delays of different severities.

SlotMachine [L1] tackles this challenge by combining tools for privacy preserving computation on data based on multiparty computation (MPC) with evolutionary algorithms and blockchain technology to build a decentralised system that enables collaboration for optimal flight sequencing in challenging conditions. It introduces a new approach to cooperative slot management and establishes a platform for on-demand automated operation. The platform serves as a marketplace for airlines with the overall aim of developing a novel flight prioritisation platform – the SlotMachine architecture – to improve the use of available resources at airports and reduce costs for airlines.

To achieve this, secure and trustworthy modules for optimisation of flight lists based on evolutionary algorithms are combined with privacy preserving methods based on cryptography to protect sensitive input data from individual participants while optimising operation at airports. Finally, a proof-of-concept implementation offering privacy-preservation will also demonstrate how fairness and equity will be guaranteed in the long run by managing delay associated tokens in a blockchain.

In general, the following phases must be supported in hotspot situations when demand by airlines exceeds the airport capacity, typically because of unplanned events rendering the original flight plan unfeasible.

(1) When identifying a hotspot, the air traffic manager (ATFM) needs to reschedule flights to later slots, imposing delays. With SlotMachine in place, ATFM then initiates a flight pri-

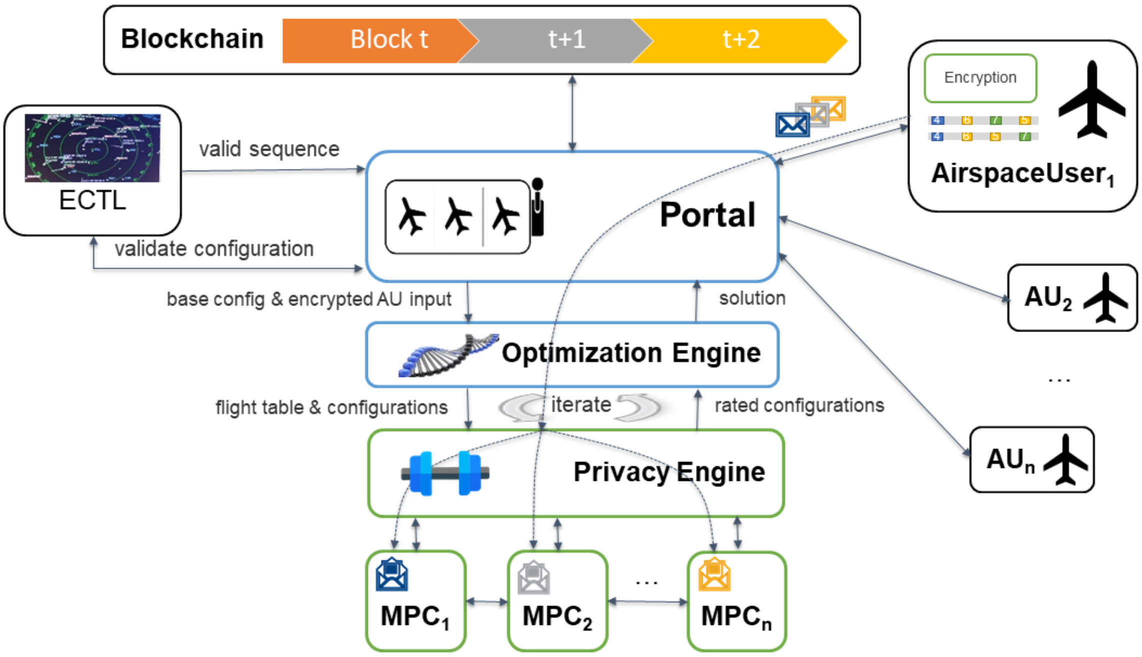


Figure 1: SlotMachine architecture with main components. Inputs provided by airspace users are processed within the privacy engine, used by the optimisation engine and served over the portal. Final results are approved by the network manager (Eurocontrol) and recorded in a blockchain.

oritisation process – with the goal of finding a better reconfiguration.

(2) During the flight prioritisation process airlines submit preferences for their flights (i.e., margins: time-not-before/time-not-after). Preference values may represent cost savings or additional costs. SlotMachine guarantees to process preference values in a privacy-preserving manner in order not to disclose a flight's cost structure to any party, not even to the SlotMachine platform provider. In fact, all sensitive data reside within the privacy engine (PE) which is based on MPC and guarantees that sensitive information is never used in plaintext within the system, which still allows for reasonable performance in the optimisation [2]. The PE assists the optimisation process and assures that input data is well-formed according to the rules for fairness and equity.

(3) The goal of a flight prioritisation process is to find a near optimum reconfiguration by considering airlines' constraints and private preference values as well as ATFM/ATC's constraints and appropriateness criteria. The combinatorial size of the problem means that it is not feasible to find an optimum reconfiguration. Evolutionary algorithms make it possible to find near optimum solutions for such complex problems. In evolutionary configuration optimisation, the constraints of airlines and ATFM/ATCs, including possible slots for flights, guide the generation and recombination of reconfigurations.

(4) SlotMachine will also keep track – in a privacy-preserving manner – of positive and negative benefits for each airline in a way that guarantees equity in the long run [3]. This will be realised by giving credit to each airline and by updating this credit after each flight prioritisation process (increasing the credit for a flight allocated to a slot with a negative preference value and decreasing the credit for a flight allocated to a slot with a positive preference value). By extending MPC with verifiability and maintaining all public data in a Blockchain accessible to all airlines, the trustworthiness of the system will be increased. Additionally, transparency can be increased by managing metadata about auctions and transactions in the blockchain in privacy preserving form using zero-knowledge proof techniques.

In summary, SlotMachine will enable a completely new form of collaboration among competing airlines to optimise air traffic by introducing more flexibility for all participants. The project is a joint effort between industry and academia, comprising all relevant stakeholders. It will contribute to a more flexible and efficient management of air traffic based on increased collaboration between airlines and lead to better usage of existing resources thus also contributing to the European Green Deal.

Link:
[L1] https://kwz.me/h68

References:

[1] S. Pilon,S., et al.: "Improved Flexibility and Equity for Airspace Users during Demand- Capacity Imbalance - An Introduction to The User-Driven Prioritisation Process", Sixth SESARInnovationDays, Delft, Netherlands, 2016.
[2] T. Lorünser, F. Wohner: "Performance Comparison of two Generic MPC-frameworks with Symmetric Ciphers", in Proc. of the 17th Int. Joint Conference on E-Business and Telecommunications, 587–594, 2020. https://doi.org/10.5220/0009831705870594
[3] S. Ruiz, et al.: "A New Air Traffic Flow Management User-Driven Prioritisation Process for Low Volume Operator in Constraint: Simulations and Results", Journal of Advanced Transportation, 2019. https://doi.org/10.1155/2019/1208279

Please contact:

Thomas Lorünser, AIT Austrian Institute of Technology GmbH
Thomas.Loruenser@ait.ac.at

Secure Computation over Integers Modulo Powers of Two

by Mark Abspoel (CWI), Ronald Cramer (CWI and Leiden University) and Daniel Escudero (Aarhus University)

Secure computation with integers modulo powers of two has immense practical impact due to the use of these types in modern hardware. Unfortunately, the lack of a good algebraic structure makes the task of designing secure computation protocols over these domains a complex endeavour, which we approach in this project.

The goal of this project is to design protocols that enable a set of mutually distrustful parties to securely compute a function that is described using standard operations on integers modulo powers of two, while keeping the inputs to the function private and revealing only the output.

Traditional approaches to this problem do not support integers modulo powers of two, but rather focus on integers modulo a prime number. This is because of the nice algebraic structure that results in this case: every non-zero element admits a multiplicative inverse, and this helps immensely in the task of designing secure computation protocols. However, modern hardware and modern computations do not tend to make use of this type of arithmetic. Instead, it is more common to find arithmetic modulo powers of two, as is the case with the standard datatypes int32 and int64 found in most programming languages.

It is motivated by these issues that, as the first outcome of this project, the protocol SPDZ2k for power-of-two computation, the first one of its kind to tolerate active corruptions of all-but-one of the participants, was developed [1]. This protocol is built by adapting the message authentication codes from other protocols, like the SPDZ and MASCOT, to the power-of-two setting, a non-trivial task that was able to find many applications beyond this particular protocol.

The SPDZ2k protocol was implemented as part of the follow-up work [2]. There it is shown that, as expected, computation modulo powers of two via the SPDZ2k protocol has the potential to provide noticeable speedups with respect to other types of computation. This is particularly relevant for computations that require operations at the "bit level", such as secure comparisons, bit decompositions, or arithmetic over the reals (emulated via fixed point arithmetic). Furthermore, SPDZ2k was found to be particularly suitable for machine learning applications, such as SVM or decision trees evaluation. Finally, SPDZ2k is already implemented in one of the most popular secure multiparty computation frameworks: MP-SPDZ. This software enables the programmer to securely evaluate a function by simply writing high level Python-like code.

The SPDZ2k protocol tolerates a dishonest majority, that is, even if all but one parties are maliciously corrupted, the privacy of the remaining honest party is maintained. However, there are some settings in which it is reasonable to assume that not all parties are corrupted. If only the minority of the parties is corrupted, protocol design is highly simplified because the set of cryptographic techniques that can be used are much more efficient and simple. Unfortunately, like the dishonest majority setting, most protocols have been designed to operate over highly restrictive algebraic structures. As an outcome of this project [3], a set of protocols that tolerate fewer corruptions but achieve higher notions of security –such as perfect or statistical security – were devised. These are rooted in standard techniques to distribute a secret among several participants using Shamir secret sharing but extending them to work even if the underlying algebraic structure is not a field, as is typically assumed.

Improving the efficiency of secure computation protocols is still one of the biggest open problems in the area and considering computation domains such as integers modulo powers of two seems to be a promising way to move forward. This project will continue to expand this knowledge barrier in several directions, including more practical protocols, as well as theoretical results that illustrate how far can computation with powers-of-two moduli can be pushed.

References:

[1] R. Cramer, I. Damgård, D. Escudero, P. Scholl, and C. Xing. “SPDZ2k: Efficient MPC mod 2^k for Dishonest Majority.” CRYPTO 2018. Springer, 2018.

[2] I. Damgård, D. Escudero, T. K. Frederiksen, M. Keller, P. Scholl, and N. Volgushev. “New primitives for actively-secure MPC over rings with applications to private machine learning.” 2019 IEEE Symposium on Security and Privacy (S&P). IEEE, 2019.

[3] M. Abspoel, R. Cramer, I. Damgård, D. Escudero, and C. Yuan. “Efficient Information-Theoretic Secure Multiparty Computation over Z/p^k Z via Galois Rings.” Theory of Cryptography Conference (TCC 2019). Springer, 2019.

[4] R. Cramer, I. Damgård, and J. Nielsen. Secure Multiparty Computation and Secret Sharing. Cambridge University Press, 2015

Please contact:

Mark Abspoel
CWI, The Netherlands
M.A.Abspoel@cwi.nl

Ronald Cramer
CWI and Leiden University, The Netherlands
Ronald.Cramer@cwi.nl

Daniel Escudero
Aarhus University, Denmark
escudero@cs.au.dk

Unlocking Secure Industrial Collaborations through Privacy-Preserving Computation

by Jan Pennekamp (RWTH Aachen University), Martin Henze (Fraunhofer FKIE) and Klaus Wehrle (RWTH Aachen University and Fraunhofer FKIE)

In industrial settings, significant process improvements can be achieved when utilising and sharing information across stakeholders. However, traditionally conservative companies impose significant confidentiality requirements for any (external) data processing. We discuss how privacy-preserving computation can unlock secure and private collaborations even in such competitive environments.

Recent developments demonstrate the value data science can have for industries. A prime example is the research cluster “Internet of Production” [L1], which aims to turn data into value throughout the entire product lifecycle, i.e., production, development, and usage. The cluster, which was established in 2019, brings together more than 200 engineers and computer scientists from more than 35 institutes at RWTH Aachen University and the Fraunhofer Society. Its key vision is to interconnect companies with the aim of exchanging knowledge and know-how globally (Figure 1), i.e., advancing use cases within and across domains to establish reliable, cost-efficient, sustainable, and accountable production. Not surprisingly, the involved industrial stakeholders mandate strict confidentiality concerning their data as they fear a loss of control [1]. To address these concerns, privacy-preserving computation with its diverse building blocks, such as homomorphic encryption (HE), private set intersection (PSI), or oblivious transfers (OTs), can act as a key enabler. Here, industrial settings provide unique challenges and opportunities compared to traditional privacy-preserving computation: While demanding strict confidentiality and scalability around data volumes and data rates, industrial settings can benefit from publicly known stakeholders, which depend on their reputation to conduct business, easing the identification and sanctioning of misbehaviour.

A research roadmap to unlock secure industrial collaborations

In this work, we report on our research roadmap for realising secure industrial collaborations, consisting of three research directions (Figure 2), sorted by increasing complexity. First, privacy-preserving comparisons allow companies to identify unrealised potential without an immediate feedback loop into existing processes. Extending on this idea, privacy-preserving matching provides a mechanism to retrieve information to directly improve local production, while still requiring manual interaction. Finally, privacy-preserving machine learning promises to feed newly derived knowledge directly into running production processes without manual interaction.

Privacy-preserving comparisons

A prominent application of privacy-preserving comparisons is company benchmarking, i.e., comparing business performance among companies. Studying real-world requirements for such benchmarks in industrial settings, we identified two key challenges [2]: First, meaningful benchmarks require complex and hierarchical computations of key performance indicators, imposing a significant burden for privacy-preserving computation. For example, in a benchmark for the injection moulding sector, one performance indicator, measuring the overall effectiveness of manufacturing equipment, covers 23 inputs and 83 calculations (23x addition/subtraction, 27x multiplication, 25x division, 8x minimum). Second, given these complex calculations, the benchmark algorithm itself becomes a valuable asset that warrants protection.

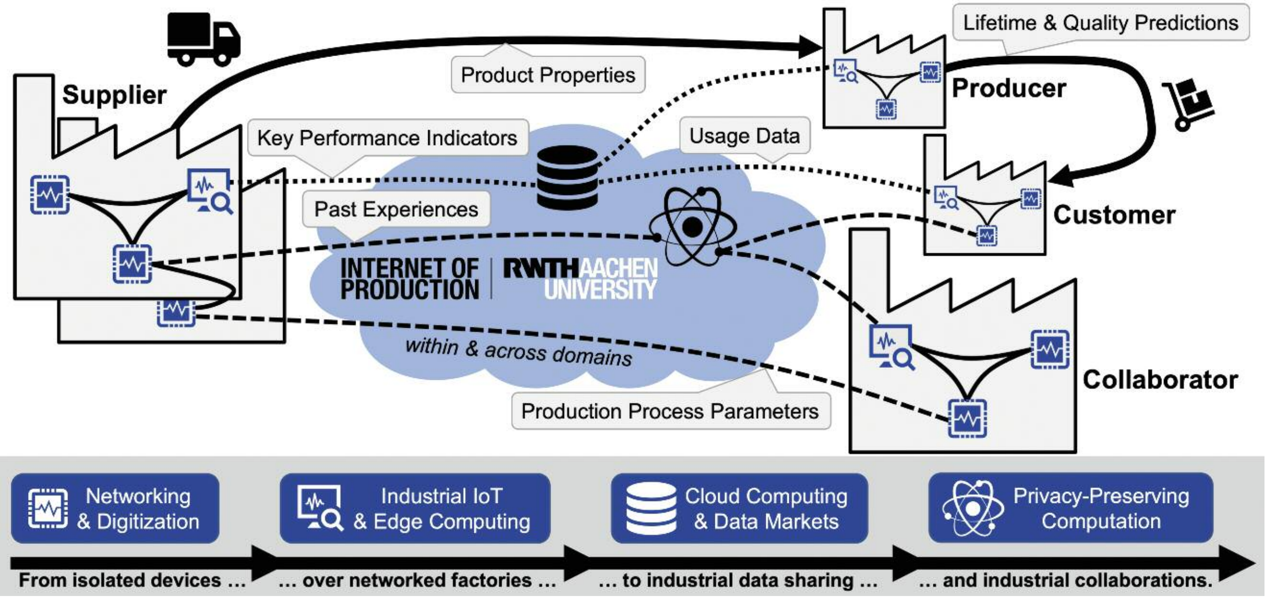

Lifetime & Quality Predictions
Product Properties
Supplier
Producer
Key Performance Indicators
Usage Data
Past Experiences
Customer
INTERNET OF PRODUCTION
RWTH AACHEN UNIVERSITY
within & across domains
Collaborator
Production Process Parameters
Networking & Digitization
Industrial IoT & Edge Computing
Cloud Computing & Data Markets
Privacy-Preserving Computation
From isolated devices …
… over networked factories …
… to industrial data sharing …
… and industrial collaborations.

Figure 1: Privacy-preserving computation is a promising technology to unlock secure industrial collaborations, i.e., an exchange of knowledge that goes beyond simple data sharing, while still considering the confidentiality needs of companies.

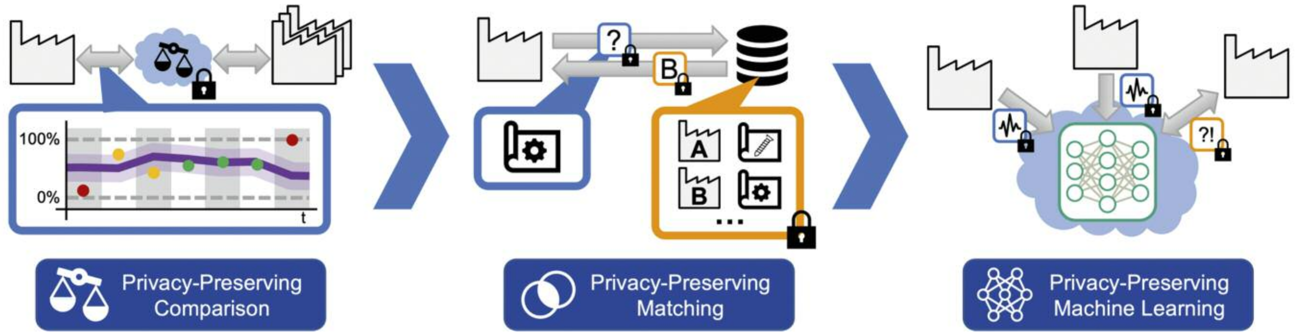

100%
0%
t
A
B
...
?
B
?!
Privacy-Preserving Comparison
Privacy-Preserving Matching
Privacy-Preserving Machine Learning

Figure 2: The increasing complexity of comparisons, matching, and machine learning also challenges the development of suitable privacy-preserving computation solutions, especially in industrial settings.

Addressing these challenges, we developed a secure solution for company benchmarking using HE that preserves not only the privacy of participating companies but also protects the benchmarking algorithm. We evaluate our approach by repeating a real-world benchmarking in the injection moulding industry, covering 48 distinct performance indicators calculated out of hundreds of input values. A runtime of 8.7 minutes per company and an average deviation of 0.16% compared to plaintext calculations underline the real-world applicability of our approach.

Privacy-preserving matching

Moving one step further in secure industrial collaboration, privacy-preserving matching directly impacts production processes, e.g., when commissioning and configuring new production lines. Traditionally, companies use empirical testing to identify machine parameters, which is costly and time-consuming. As others might already operate similar production lines, re-using this knowledge is a sensible and sustainable approach, if realised securely. To achieve this goal and thus allow companies to securely exchange information that can, e.g., be used to configure production sites, we developed two approaches with different privacy trade-offs [3]. By combining established building blocks (OTs, PSIs, and Bloom filters), we show the potential of industry-tailored privacy-preserving computation. To evaluate our approach, we (i) realise a process parameter retrieval for injection moulding to reduce ramp-up phases and (ii) exchange machine tool parameters to improve the machine settings for individual workpieces. Our evaluation shows that our approach meets today's real-world privacy and processing requirements. Thus, privacy-preserving computation can enable the secure exchange of sensitive industrial information, even in competitive environments.

Privacy-preserving machine learning

Finally, privacy-preserving machine learning provides a more tightly integrated knowledge sharing, directly feeding new (and improved) information into local industrial processes. For example, in high-pressure die casting, machine learning-based quality prediction allows defects to be discovered even when in-situ methods are not applicable. Here, technical advances promise to utilise a larger set of input data across stakeholders, i.e., using federated learning, and thus improve predictions. However, thoughtless decisions can result in unfounded high scrap rates, while in other settings, feedback loops can even result in physical harm, e.g., when coordinating line-less mobile assembly systems. Likewise, privacy-preserving computation must ensure that no sensitive information is leaked (indirectly), e.g., through dataset inference or reconstruction attacks. Our ongoing work aims to enhance the industry's decision-making and feedback loops by securely utilising external knowledge and data.

Conclusion

Privacy-preserving computation indeed promises to unlock sophisticated secure industrial collaborations. In the future, the relevance of such collaboration will further increase, as the goals of confidentiality and sustainability will complement today's dominant factors of costs and product quality. Until then, we need to address several research challenges [L2] to reliably and securely realise the vision of globally-interconnected production. These challenges are not limited to privacy-preserving knowledge exchange, but also include device and network security, among others.

The work is funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC-2023 Internet of Production – 390621612.

Links:

[L1] https://www.iop.rwth-aachen.de

[L2] https://www.comsys.rwth-aachen.de/research/industrial-internet-of-things

References:

[1] J. Pennekamp et al.: "Dataflow Challenges in an Internet of Production: A Security & Privacy Perspective", ACM CPS-SPC, p. 27-38, 2019.

[2] J. Pennekamp et al.: "Revisiting the Privacy Needs of Real-World Applicable Company Benchmarking", WAHC, p. 31-44, 2020.

[3] J. Pennekamp et al.: "Privacy-Preserving Production Process Parameter Exchange", ACSAC, p. 510-525, 2020.

Please contact:

Jan Pennekamp
RWTH Aachen University, Germany
jan.pennekamp@comsys.rwth-aachen.de

Martin Henze
Fraunhofer FKIE, Germany
martin.henze@fkie.fraunhofer.de

Oncological Research on Distributed Patient Data: Privacy can be Preserved!

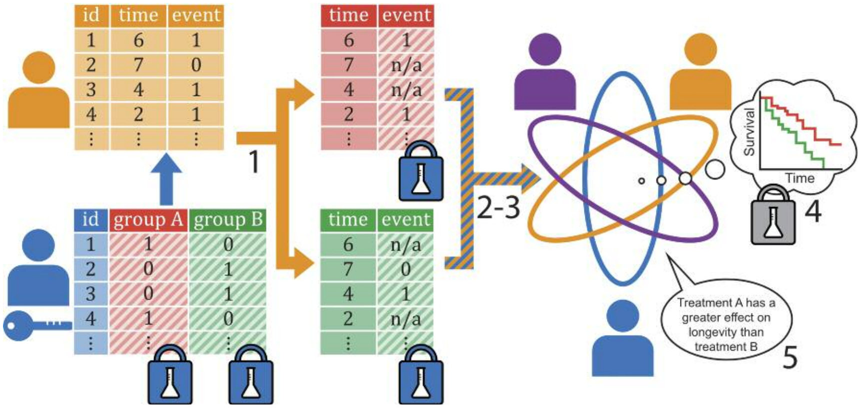
by Bart Kamphorst (TNO), Daan Knoors (IKNL) and Thomas Rooijakkers (TNO)

Researchers in oncology require comprehensive patient data to reflect on cancer care and prevention. However, given the complexity of cancer, some research questions require patient data that is distributed over multiple registries, and it can be challenging to access or exchange such highly sensitive health data. To get around this problem, the Netherlands Comprehensive Cancer Organisation (IKNL) and the Netherlands Organisation for Applied Scientific Research (TNO) have collaboratively developed algorithms that enable survival analyses on distributed data with rigorous privacy guarantees.

The Netherlands Comprehensive Cancer Organisation (IKNL) maintains the Netherlands Cancer Registry (NCR) to enable healthcare professionals, researchers and policymakers to reflect on cancer care and prevention. Even though the NCR is one of the largest disease-specific registries in the world, given the complexity of cancer, some research questions require additional information that is collected by other organisations. For instance, studies that aim to understand which factors influence a patient's chance of survival could reveal new patterns when additional information is considered, like drug usage, hereditary conditions, or comorbidities.

Clinical studies benefit from having as much relevant data as possible. However, organisations are prevented from combining data due to privacy concerns, regulations, and other factors. Particularly, sensitive patient-level data must always be treated with great care. On the other hand, population-level insights that can be obtained from analysing patient-level data might be less sensitive. As a result, over recent decades, new methods have been investigated that obtain population-level insights while providing strong guarantees that the private information of patients is protected. IKNL and the Netherlands Organisation for Applied Scientific Research (TNO) have designed and implemented such privacy-preserving methods in the domain of survival analysis.

Survival analysis – analysing the expected time it takes for an event, such as death, hospitalisation, or tumour recurrence, to occur – is an important aspect of oncological research. Survival analysis can be used to indicate the likelihood of someone being alive a few years after diagnosis. Additionally, it can give insights into which characteristics might relate to the chances of survival, e.g., the patient's fitness, the treatment method, and hospital of diagnosis.



id	time	event
1	6	1
2	7	0
3	4	1
4	2	1
⋮	⋮	⋮

id	group A	group B
1	1	0
2	0	1
3	0	1
4	1	0
⋮	⋮	⋮

time	event
6	1
7	n/a
4	n/a
2	1
⋮	⋮

time	event
6	n/a
7	0
4	1
2	n/a
⋮	⋮

1
2-3
Survival
Time
4
Treatment A has a greater effect on longevity than treatment B
5

Figure 1: The protocol to securely compute the log-rank statistic for vertically-partitioned data. One party (Blue) owns data on patient groups, the other party (Orange) owns data on event times (did the patient experience an event '1' or not '0', and when did this occur). Protocol outline: Blue encrypts its data using additive homomorphic encryption and the encrypted data is sent to Orange. Orange can securely, without decryption, split its data in the patient groups specified by Blue (1) using the additive homomorphic properties of the encryptions. Orange performs some preparatory, local, computations (2) and with the help of Blue secret-shares the data (3) between Blue, Orange and Purple, where Purple is introduced for efficiency purposes. All parties together securely compute the log-rank statistic associated with the (never revealed) Kaplan-Meier curves (4) and only reveal the final statistical result (5).

An often-used survival analysis technique is the Kaplan–Meier estimator, a non-parametric statistic used to estimate the survival function of a lifetime table. To compare survival between groups, we can use the log-rank test associated with the Kaplan-Meier estimator. The log-rank test is a statistical procedure that compares two or more survival distributions. A direct application is to test whether one treatment has a greater effect on the longevity of a patient compared to another. Advances in machine learning and cryptography allow us to compute this log-rank statistic without disclosing any underlying patient-level information.

IKNL is leading the development of an infrastructure called vantage6 [L1], which enables organisations to jointly perform analyses without needing to share their respective data. This federated-learning based approach works well if the data is horizontally distributed, e.g., the participating organisations maintain the same type of data of different patients. In the Kaplan-Meier setting, this translates to organisations that all record the patient group, the outcome of the experiment and the time of that outcome for separate patients. Vantage6 facilitates privacy-preserving analyses on the combined sets of patients, leveraging the fact that every organisation can perform the analysis on the data of its own patients.

An alternative scenario is that data is vertically distributed, e.g., participating organisations maintain different, complementary types of information about the same patient. In our setting this translates to one organisation recording the patient group (e.g., based on comorbidities), and another organisation recording the survival data. Computing the log-rank statistic, however, requires knowledge of both the patient group information and the survival data. Lacking either type of data makes it impossible to deduce any meaningful insights. Using the cryptographic concepts of Secure Multi-Party Computation (MPC), it is possible to perform the analysis in this scenario while preserving the patients' privacy.

MPC is a set of techniques that enables multiple entities to jointly evaluate a function on their data, without revealing that data to one another. Some techniques achieve this property by supporting computations on encrypted data (e.g., homomorphic encryption), which particularly enables computations that involve the sensitive but encrypted data of another entity, whereas some other techniques (e.g., secret sharing) split the sensitive data in multiple pieces in such a way that computations can be performed on the separate pieces. Most importantly, within some specified security model, every MPC technique guarantees to preserve privacy throughout the entire computation.

In our joint 2020 research project, we have developed and implemented new MPC solutions to compute the log-rank statistic of the Kaplan-Meier estimator on vertically-distributed data. These privacy-preserving solutions do not reveal the group information and the survival data to anyone. Experiments show that the solutions are sufficiently fast and scalable to be used in real-world settings. The protocol is visualised in Figure 1. An open-source implementation is provided on GitHub [L2]. Our protocol does not reveal the Kaplan-Meier estimators themselves since patient-level information can be deduced from them. Presenting the Kaplan-Meier estimators in a more privacy-friendly way is described in Vogelsang et al. [1].

Motivated by these promising results, TNO and IKNL developed other relevant algorithms to enable privacy-preserving survival analyses, including Cox Proportional Hazard. Future activities include the extension of the toolkit to other relevant privacy-preserving machine learning algorithms for medical analyses in the cancer domain.

Links:
[L1] https://vantage6.ai/
[L2] https://kwz.me/h6S

References:

[1] Vogelsang et al.: "A Secure Multi-Party Computation Protocol for Time-To-Event Analyses", in Studies in health technology and informatics, 270, 2020, doi: 10.3233/SHTI200112.

Please contact:

Bart Kamphorst
TNO, the Netherlands
bart.kamphorst@tno.nl

Privacy-Preserving Collaborative Money Laundering Detection

by Marie Beth van Egmond, Thomas Rooijakkers and Alex Sangers (TNO)

Criminal transaction flows can be obfuscated by spreading transactions over multiple banks. Collaboration between banks is key to tackling this; however, data sharing between banks is often undesirable for privacy reasons or is restricted by legislation. In the MPC4AML project, research institute TNO and Dutch banks ABN AMRO and Rabobank are researching the feasibility of using Secure Multi-Party Computation (MPC) to detect money laundering.

Financial crime is a huge, world-wide problem. In 2018, an estimated 5.8 trillion dollars (6.7% of global GDP) worth of financial crime was perpetrated. Banks have a gatekeeper role in the financial system and a legal obligation to identify unusual transactions. However, criminal transaction flows will hardly ever stay confined to the network of one bank and thus often remain undetected. Therefore, collaboration and data sharing is key in detecting financial crime. On the other hand, legislation such as GDPR and competition law, as well as privacy concerns, can restrict data sharing.

Privacy-enhancing technologies are promising to enable collaboration without sharing sensitive data. This is also recognised by the recently published Future in Financial Intelligence Sharing (FFIS) paper [1] that describes ten case studies on this topic. One of these is the MPC4AML project, a collaboration between research institute TNO and Dutch banks ABN AMRO and Rabobank, where the technical feasibility of using Secure Multi-Party Computation (MPC) for detecting money-laundering is being researched. The possibility of performing calculations on the entire transaction network while keeping data private creates a lot of opportunities. In 2017, TNO published an article on secure PageRank for detecting transactional fraud [2]. In the current project, the research is focused on both the secure use of graph embeddings for finding malicious communities in the network, and on secure risk propagation for identifying exposure to high-risk cash or cryptocurrency deposits. We elaborate on the latter in this article.

Risk propagation

Currently, many banks attribute risk scores associated with money laundering to their customers, for example, based on transactions involving large amounts of cash or cryptocurrencies, or being from or to certain high-risk countries. These risk scores are of limited value as long as they are based on only the local network of a single bank. However, by propagating this risk through the transaction network of multiple banks, a lot more information on criminal flows could be identified. An example of such a criminal flow can be found in Figure 1.

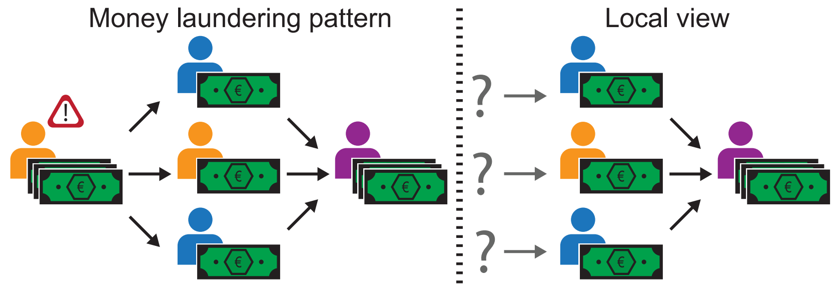


Figure 1: We consider a three-bank scenario (Orange, Blue, and Purple). In this scenario the first (left) account at bank Orange is classified as high risk (due to e.g., large cash deposits) by bank Orange. This account wishes to launder its resources. To stay under the radar, the resources are funnelled through multiple accounts, at various banks, before arriving at their eventual destination, e.g., the account at bank Purple (right). To detect money laundering, we wish to follow (propagate) the risky money and classify the endpoint as high risk too. Full (global) knowledge of the network enables us to propagate the risk. However, how can we achieve something similar when there is only partial (local) knowledge of the entire network available? This is where MPC comes into play.

$$r_k^j = (1-\delta) r_{k-1}^j + \frac{\delta}{T_j} \cdot \sum_{i \in S(j)} r_{k-1}^i \cdot A_{i,j}$$

- r_k^j is the risk score of node j at iteration k,
- δ is a public parameter between 0 and 1,
- $S(j)$ is set of nodes linking to node j ,
- $A_{i,j}$ is the transaction amount that node i sends to node j,
- T_j is the total amount that node j receives.

Figure 2: Formula for risk propagation. Because of the properties of Additive Homomorphic Encryption, this can be performed on homomorphically encrypted risk scores as well.

The goal of risk propagation is to identify nodes that are involved in such a money-laundering pattern. The risk propagation algorithm requires as input a transaction network (containing clients and transactions) of a certain time period. Every client (a node in the network) has an initial risk score, which was assigned by the client's bank. In one iteration of the algorithm, risk scores are updated using the weighted incoming risk score, i.e. the risk scores of incoming nodes weighted by the transaction amounts. In other words, if a client receives a lot of money from a client with a higher (or lower) risk score, its risk score will increase (or decrease). The formula for risk propagation can be found in Figure 2.

Secure risk propagation

Criminals often obfuscate money laundering patterns, such as in Figure 1, by performing transactions out of sight of any single bank. However, the risk scores that we need for the risk propagation are sensitive information that cannot freely be shared with other banks. Fortunately, using MPC techniques, the risk propagation algorithm can be performed securely on the entire transaction network of the participating banks. Risk scores are encrypted using Additive Homomorphic Encryption (AHE); a form of encryption that enables computations on encrypted data. To be precise, if we denote *[x]* to be the encryption of a value x, additive homomorphic encryption has the property *[a] • [b] = [a + b]* and therefore *[a]ᶜ = [c • a]*.

To perform a secure risk propagation iteration, banks that participate in the protocol need to share the (relevant) encrypted risk scores with each other. Thanks to the properties of AHE, all banks can perform the required computations for risk propagation (in the formula in Figure 2) on these encrypted risk scores. Next to that, every bank can also use locally known information for each of its own clients, which enables a very efficient protocol. The result of the secure computation is an encrypted updated risk score for every client. With these updated scores, either a new iteration can take place, or a bank can decrypt the resulting risk score of some of its own clients. The latter can only happen with consent of the other banks, using “threshold decryption”.

Results

In collaboration with ABN AMRO and Rabobank, TNO built a first proof-of-concept of the secure risk propagation [L1] using synthetic data [L2] that includes money laundering patterns. This shows that it is possible to securely perform the risk propagation algorithm among different banks and demonstrates the value of collaborative transaction analysis.

Future challenges

Two technical challenges have been identified for the near future. First, the computational scalability of the solution will need to be evaluated and compared with the theoretical hypothesis. Second, MPC protects the confidentiality of the input data and any intermediate data during the computation. However, for application on real transaction data, it is important to investigate how much information can be deduced from the resulting risk scores after running the protocol.

The next step is to apply the secure risk propagation on real transaction data in a pilot. Many other challenges will no doubt arise from a pilot on real data. This will bring us one step closer to catching criminals involved in sophisticated interbank money laundering patterns.

Links:

[L1] https://kwz.me/h6q
[L2] https://github.com/IBM/AMLSim

References:

[1] N. Maxwell: “Innovation and discussion paper: Case studies of the use of privacy preserving analysis to tackle financial crime”, Future of Financial Intelligence Sharing (FFIS) research programme, 2020.

[2] A. Sangers, et al.: “Secure multiparty PageRank algorithm for collaborative fraud detection", Int. Conf. on Financial Cryptography and Data Security, Springer, 2019.

Please contact:

Marie Beth van Egmond,
TNO, The Netherlands
marie_beth.vanegmond@tno.nl

Alex Sangers
TNO, The Netherlands
alex.sangers@tno.nl

Increasing Access to Social Welfare Programmes with Proportional Data Usage

by Gabriele Spini and Alex Sangers (TNO)

Social welfare programmes are complex, and individuals who might be entitled to a form of social assistance are sometimes unaware of it. Identifying these individuals is a difficult task potentially requiring large amounts of sensitive personal data; access to these data is regulated by law and typically limited. Cryptographic techniques, however, can help in identifying eligible welfare beneficiaries while minimising the amount of data that is revealed in the process.

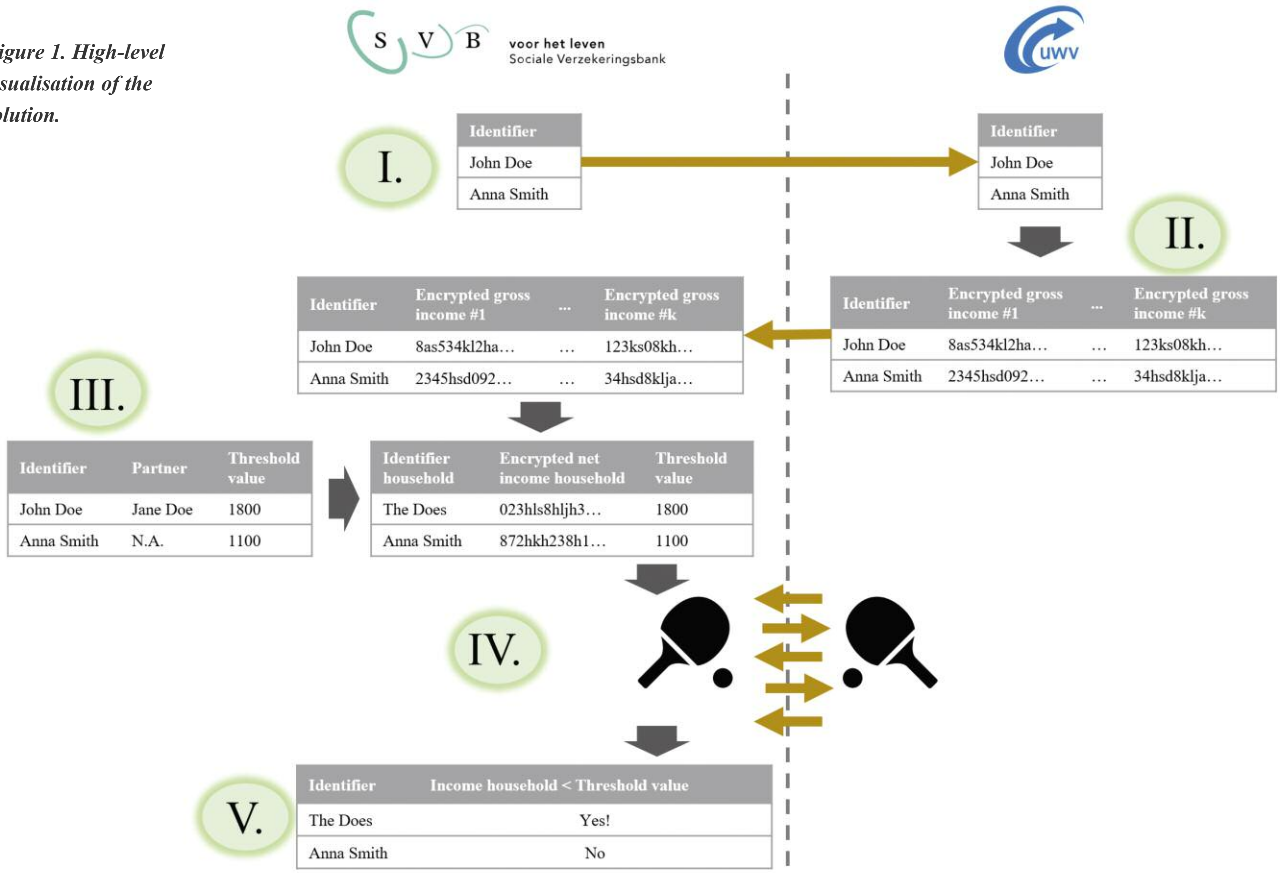
The Netherlands has various forms of social welfare programmes. An institution named SVB (Sociale Verzekeringsbank) is responsible for some of these programmes, including the AIO scheme, a supplementary income provision for retired people. Low income retirees who meet certain criteria are entitled to this provision; however, a survey by the Dutch court of audit [1] estimated that approximately half of the AIO-entitled individuals do not receive it, presumably because they are unaware that they are eligible for it.

The SVB would like to inform the individuals that are potentially eligible for the AIO about this supplementary income provision, but it needs to safeguard the privacy of involved citizens. This safeguard is complicated by the fact that two types of data are essential to identify potential AIO-beneficiaries: household composition and income. While the SVB does know household composition of retirees, income data are known to another institution, UWV (Dutch Employee Insurance Agency). If the income of a relevant household is below a certain threshold, then it is reasonable to assume that the corresponding individual is entitled to the AIO. However, these are personal data and cannot simply be linked. A Privacy Impact Assessment (PIA) has been used to investigate the privacy risks and potential benefits, and simply sharing data between UWV and SVB on this scale has been deemed non-proportional with respect to the European General Data Protection Regulation (GDPR).

Therefore, TNO (the Dutch Organisation for Applied Scientific Research), Novum (the innovation lab of the SVB), the SVB itself and UWV have started a research project to investigate whether advanced cryptographic techniques can enable the SVB to identify potential beneficiaries of the AIO in a privacy-preserving manner.

Using cryptographic techniques for privacy-preèserving data analysis

Cryptographic techniques, and in particular, Secure Multi-Party Computation (MPC), can provide a solution to this problem. Such a solution should allow the SVB to identify which



Identifier
John Doe
Anna Smith

Identifier	Encrypted gross income #1	...	Encrypted gross income #k
John Doe	8as534kl2ha…	…	123ks08kh…
Anna Smith	2345hsd092…	…	34hsd8klja…

Identifier	Partner	Threshold value
John Doe	Jane Doe	1800
Anna Smith	N.A.	1100

Identifier household	Encrypted net income household	Threshold value
The Does	023hls8hljh3…	1800
Anna Smith	872hkh238h1…	1100

Identifier	Income household < Threshold value
The Does	Yes!
Anna Smith	No

Figure 1. High-level visualisation of the solution.

households in their database have a cumulative income that is below the relevant AIO-threshold, but without revealing any extra information about this income. Similarly, UWV should not obtain any information about household composition or on which individuals may be entitled to the AIO.

Several approaches and techniques are possible within MPC; for this project, Homomorphic Encryption (HE) was selected. Intuitively, HE is a form of encryption that enables computations to be done on encrypted data; decrypting these modified ciphertexts yields the result of the computation on the original data. HE was selected for two main reasons: first, it is inherently “asymmetric” (compared to other popular MPC techniques such as Secret Sharing), which means that one organisation takes a lead role and needs to perform most computations; this is important for the AIO-problem, as the primary responsibility lies with one party: the SVB. The second advantage of HE is that it can be more readily connected with the existing IT infrastructure of the SVB and UWV.

Secure solution with homomorphic encryption

The developed solution works in five steps (see Figure 1). In the first step (I), the SVB sends to UWV a list of identifiers of individuals in their database and, if applicable, of their partner. UWV then gathers the gross income data of these individuals, encrypts them with an HE scheme and sends the encrypted values back to the SVB (II). At this point, the SVB computes encryption of (approximated) net income data per individual, and then per household (III). The fourth step (IV) is to compare these encrypted income values with the relevant threshold; due to the type of encryption scheme used, this step requires some interaction with UWV, which will nevertheless learn no information as a result of this step; the reader can refer to [2] for more details and to [L1] for an open source publication. Eventually, the SVB thus obtains a list of individuals whose cumulative household income lies below the relevant threshold (V).

Results

A Proof-of-Concept was developed within this project, simulating the two data parties SVB and UWV with servers in two different Dutch cities. Experiments were run on synthetic data, showing how the solution scales linearly in the number of involved individuals; preliminary results on non-optimised code yield a run-time of roughly 10 hours for 8000 households: more than non-private computation, but in line with requirements of the SVB and UWV, and with plenty of room to improve efficiency.

Aside from these technical results, a PIA has been written to argue that the data usage is, in this case, proportional to the expected benefit, and is under scrutiny by the relevant stakeholders.

Future work

Given the promising results obtained in this first phase, a follow-up pilot has been started to assess the impact of the solution on real data. The pilot will identify a first batch of 1000 potential AIO-beneficiaries and evaluate the effectivity of this proactive policy.

Link:

[L1] https://kwz.me/h69

References:

[1] Algemene Rekenkamer. (2019). Ouderdomsregelingen ontleed, https://kwz.me/h6f

[2] T. Veugen: “Correction to “Improving the DGK comparison protocol”, IACR Cryptology ePrint Archive, 2018” https://eprint.iacr.org/2018/1100.pdf

Please contact:

Gabriele Spini
TNO, the Netherlands
gabriele.spini@tno.nl

Alex Sangers
TNO, the Netherlands
alex.sangers@tno.nl

Federated Learning for Fraud Detection in Accounting and Auditing

by Stefanie Grimm, Stefanie Schwaar and Patrick Holzer (Fraunhofer ITWM)

During the course of process digitalisation, new possibilities arise to efficiently check billing transactions. Our previous research has led to the development of auditing methodology using machine learning for several industries. To take this approach to the next level, we are helping organisations to collaborate through federated learning that complies with all aspects of confidentiality and security restrictions.

Federated learning can be used to train models across multiple clients individually without exchanging training data but utilising those trained models to contribute to a joint model. In the Department of Financial Mathematics at Fraunhofer Institute for Industrial Mathematics, we employ centralised federated learning in a cross-silo setting, i.e., models are sent and aggregated via a central server, and we assume a small number of clients, most of whom have large datasets. The basic procedure is to transmit a model, e.g. the architecture of a neural net, to all clients, train the model on each client separately using well known algorithms, send the training results, e.g. weights of a neural net, back to a central server and aggregate them to a global model as visualised in Figure 1. This process is repeated until some stopping criterion steps in. Obviously, there are many ways of performing this procedure. Our aim is to find the most appropriate variants for use cases arising in fraud detection for accounting audits.

Account auditing is required in various areas: fraudulent claims affect both pri-

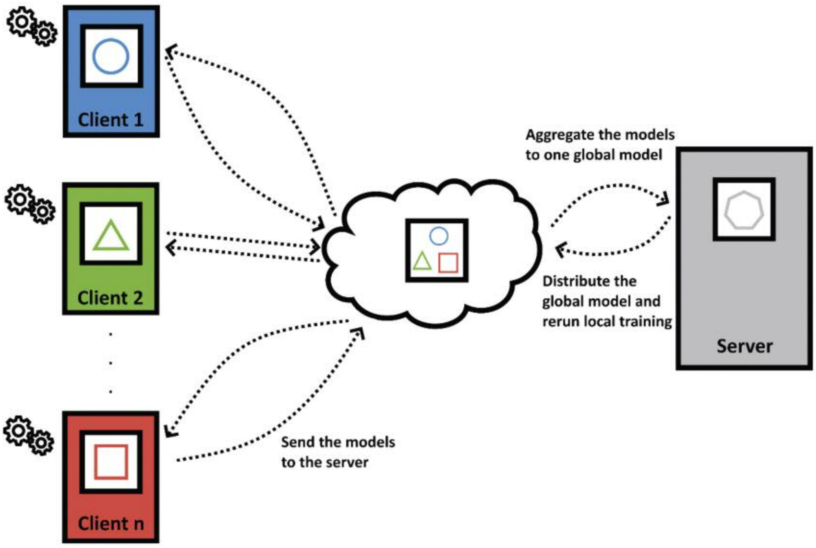

Client 1
Client 2
Client n
Aggregate the models to one global model
Distribute the global model and rerun local training
Server
Send the models to the server

Figure 1: Basic centralised federated learning procedure.

vate sector companies and public entities, and the consequences of detected fraud range from minor accounts receivable to criminal prosecution. Thus, the requirements and objectives can differ substantially between applications. Nevertheless, most cases share one feature in common: the growing amount of data makes it impossible to audit all claims and billings individually. At this point, machine learning algorithms come into the picture. Depending on variables such as data structure and the aim of the investigation, data scientists can apply algorithms to address different objectives – e.g., outlier detection, change detection or classification.

This brings us to the question: how can federated learning help with fraud detection in accounting audits? Even though most individual organisations would possess enough data to meet the requirements of common machine learning algorithms, there can still be significant benefits to collaborating with others. In particular, organisations with a diverse range of data can benefit from collaborating with others with the same type of data. Yet, sharing data is often not an option due to data security and confidentiality obligations. By sharing training results, it is not only possible to increase the data basis but also to spot undetected fraudulent structures. Additionally, although federated learning itself is still a young research area, it promises to overcome privacy, organisational and technical obstacles to artificial intelligence methods in application domains with advanced data integrity requirements, and to make collaboration possible.

In one of the first studies in this area to date, Yang et al. [1] investigated the application of federated learning–based methods in credit card fraud detection. Employing a real-world credit card transaction dataset, they experimentally demonstrated that federated learning methods can be used to implement a working fraud detection system that does not require financial institutions to share private data with each other. Further, a study by Suzumura et al. [2] (not yet peer-reviewed) show improved results when employing a centralised cross silo fraud detection setting.

We are investigating research questions that arise in fraud-detection applications. We are using our own framework for federated learning, which is designed for highly diverse models – e.g., random forests, neural networks or linear regression – and was jointly developed by our Departments of High Performance Computing and Financial Mathematics. We have integrated methods based on horizontal as well as vertical splits. Horizontal federated learning, i.e., datasets that share the same feature base, can improve results by increasing the amount of training data and thus improving goodness of the fitted models. While horizontal federated learning is sometimes dismissed as being unrealistic when pairing models across organisations, accounting data often has to follow certain forms, especially in highly regulated areas. For applications that don’t fulfil these consistency assumptions, we use domain knowledge and break down the datasets into categories of features. Beyond the horizontal approach, which aims for enlargement of data basis and sharing of labelling cost, vertical federated learning, i.e., datasets that share the same sample spaces, also gives us interesting insights into fraudulent structures. For example, claims of a suspect at a single organisation might be unsuspicious, but the vertical combination over organisations is worth reporting. Therefore, we are combining our knowledge in anomaly detection and classification, the domain knowledge of our partners, and the aforementioned federated techniques to provide a decision support system for fraud detection in accounting audits as a first result.

References:

[1] W. Yang et al.: “FFD: a federated learning based method for credit card fraud detection”, IEEE BigData 2019. Springer, Cham.

[2] T. Suzumura et al.: “Towards federated graph learning for collaborative financial crimes detection”, arXiv:1909.12946, 2019.

Please contact:

Stefanie Grimm
Fraunhofer Institute for Industrial Mathematics (ITWM), Germany
stefanie.grimm@itwm.fraunhofer.de

Secure Multi-Party Computation with Service Contract Automata

by Davide Basile (ISTI-CNR)

By combining research from model-based software engineering, dependable computing, and formal methods, it is possible to create a contract-based design methodology to enforce security accountability and reputation of distributed digital entities provided by potentially mutually distrusted organisations.

Our society is increasingly dependent on heterogeneous digital infrastructures, for example in the healthcare, financial and transport domains. These infrastructures are examples of systems of systems, i.e., they are realised through the composition of several sub-systems provided by potentially mutually distrusted or competing organisations. An example is the ERTMS/ETCS Level 3, a new railway signalling system where virtual positioning is replacing legacy physical systems, and the geolocation sub-system is provided by a third party (e.g., European GNSS service). Moreover, emerging computing paradigms (e.g., fog, mobile-edge or cloud computing, to mention a few) rely on components discovered and accessed over the internet. The composed behaviour needs to be validated to guarantee overall security, as well as safety and interoperability requirements.

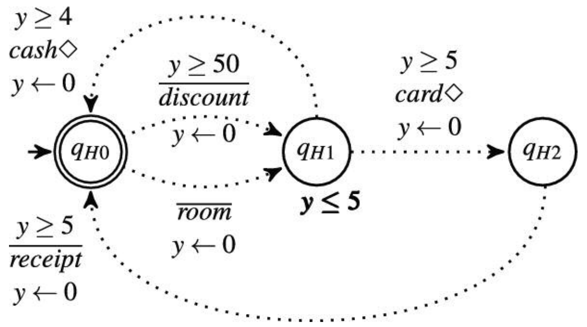


Figure 1: An example of a real-time service contract automaton.

In these emerging multi-party paradigms, no assumption shall be made about third-party systems, which are accessed as a black box. Thus, standard monolithic verification techniques used for validating digital entities cannot be applied to ensure the overall security of these digital infrastructures. Indeed, novel formal verification techniques must cope with the unwanted scenario where a verified system does not comply with its expected behaviour (called contract), either unintentionally or maliciously, or when the necessary security measures are not in place. For cyber-physical systems, we also cannot make assumptions about the open physical environment in which these systems are operating, whose behaviour (e.g., delays of radio communications, geo-positioning uncertainty) could be tampered with by attackers to drive an unprepared system to unsafe configurations to carry out the attack.

Service contracts [1] have been introduced in the literature as a methodology for designing systems where the requirements and obligations of each party are rigorously specified and rendered as formal specifications, e.g., automata (see Figure 1). The security threats are thus considered from the early design phases of a system. This can reduce costs by detecting design flaws as early as possible, for example, unsecure assumptions on other components or the environment (e.g., stochastic distribution on delays or positioning errors). Contracts are digital entities that must be composable to predicate over their aggregate multi-party behaviour. Firstly, it is necessary to check whether the requirements of each contract are satisfied in the composition by some other contract. Traces leading to violation of the requirements must be pruned to obtain a composition where all involved parties adhere to the shared behaviour. Starting from a raw composition of contracts, this contract agreement can be synthesised automatically [2]. The contract agreement is then proposed to each involved party for validation or further formal verification, before starting their interactions, to ensure the correctness and security of their composed behaviour. Due to the stochastic, physical nature of phenomena involved in a cyber-physical infrastructure, a challenge is to investigate novel formalisms and verification techniques for specifying and verifying contracts expressing both the discrete and continuous aspects under analysis, as well as the stochastic physical phenomena involved.

During the computation, the agreement is realised through coordination of distributed software entities, to allow them to fulfil both their specified requirements and declared obligations. The coordination is generally achieved using a choreographic or orchestrated approach [3], and the requirements for realising a choreography are more stringent because each party must be able to fulfil its requirements and duties independently of the other entities involved in the overall computation. This amounts to project the global agreement to each local component, and if the proper conditions are satisfied, using the local contract agreement instead of the global one to check that each component fulfils its agreed behaviour. On the other hand, an orchestration drives the involved parties to realise their agreed computation, at the cost of extra coordination interactions. In the orchestrated approach, the orchestration is responsible for guaranteeing that the contract agreement is realisable. Thus, the orchestration needs to be a trusted software component.

The key aspect is that the multi-party computation can be monitored at run-time by exploiting the contract agreement each party has signed beforehand, to detect possible contract breaches in case obligations are not fulfilled, providing log information for post-mortem analyses. Indeed, it is assumed that each party can fulfil its contract and is responsible for violations. In this scenario, it becomes possible to identify the organisations liable for providing services breaching the contract they have agreed upon. This is at the basis of a methodology for formally specifying systems able to guarantee the necessary security accountability and reputation mechanisms for digital organisations.

An open-source API available at [L1] has been produced by the author for developing contract-based applications using a model-driven state-based design approach for software applications built around their specified contract. An open-source graphical application for designing contract specifications, composing them and synthesising a coordination policy in agreement is available at [L2], which has been developed using the API in [L1].

This research activity is partially funded by the PRIN 2017 project "IT MaTTerS: Methods and Tools for Trustworthy Smart systems", funded by the Italian Ministry of Education, University and Research, where the synthesis of run-time monitors is addressed, and by the 4SECURail project "FORmal Methods and CSIRT for the RAILway sector", targeting the construction of railway infrastructures whose sub-systems are provided by different railway companies. 4SECURail received funding from the Shift2Rail Joint Undertaking (JU) under the European Union's Horizon 2020 research and innovation programme under grant agreement No. 881775.

Links:

[L1] https://kwz.me/h6E
[L2] https://kwz.me/h6K

References:

[1] D. Basile: "Specification and Verification of Contract-Based Applications" (Ph.D. thesis, Department of Computer Science, University of Pisa), 2016. hhttps://kwz.me/h7i

[2] D. Basile, et al.: "Controller synthesis of service contracts with variability", Science of Computer Programming, 187; 2020. https://kwz.me/h7h

[3] D. Basile, M. H. ter Beek, R. Pugliese: "Synthesis of Orchestrations and Choreographies: Bridging the Gap between Supervisory Control and Coordination of Services", Logical Methods in Computer Science, 16, 2020. https://lmcs.episciences.org/6527

Please contact:

Davide Basile, ISTI-CNR Pisa, Italy
davide.basile@isti.cnr.it

Towards Privacy-Preserving Sharing of Cyber Threat Intelligence for Effective Response and Recovery

by Lasse Nitz, Mehdi Akbari Gurabi, Avikarsha Mandal and Benjamin Heitmann (Fraunhofer FIT)

Many European organisations suffer from a lack of sufficient resources to provide satisfactory and timely response and recovery (R&R) actions when targeted by cyber-attacks. R&R capabilities can be significantly improved through sharing of information related to incident detection and handling. In this context, privacy-preserving technologies can enable data sharing, while protecting privacy- and security-critical information. The technologies to achieve this are being developed and evaluated in the SAPPAN project.

The computer security incident response team (CSIRT) plays a crucial role in an organisation's digital infrastructure. One of the responsibilities of a CSIRT is to detect, investigate, and mitigate potentially security-critical incidents. To help with the vast number of potential threats, many CSIRTs rely on partly automated systems, especially for the detection of incidents. Since the quality of these detection systems has a direct impact on the manual workload of incident handlers, who have to investigate the detected incidents, the false-positive rate of the incident detection should be as low as possible. The same applies to the false-negative rate, as every undetected incident might pose a serious security risk to an organisation. There is hence a need for high-quality detection system components, which detect incidents reliably without unnecessarily increasing the investigative workload of human operators. But since considerable effort is required to create such high-quality components, it is unfeasible for many small and medium-sized enterprises (SMEs) to create them on their own.

This problem could be overcome by the sharing of cyber-threat intelligence that helps detect, assess and handle incidents, for example as trained classifiers or cybersecurity playbooks. An abstract overview of a sharing system is shown in Figure 1. For security providers, this could constitute a meaningful way of extending their services, and for academic organisations it would allow research results to be made usable in practice. The main problem in sharing resources, however, is that they are usually based on privacy- and security-critical data, so it is vital that no sensitive information can be extracted from the shared resources.

While anonymisation and sanitisation solutions exist for various kinds of data within the cybersecurity domain (e.g., for IP addresses), other kinds of data – for example, uniform resource locators (URLs) – have not received the same level of attention. While URLs have been used in research, e.g., for the identification of phishing websites [1], methods for sanitising URLs are not yet mature. In particular, URLs collected as benign samples do not only reveal information about the browsing behaviour of individuals but can also provide access to restricted web resources via access tokens, and leak organisation-internal information via directory and file names, e.g., for URLs pointing to resources in a company's intranet. Hence, measures must be taken to prevent shared URLs and detection system components trained on URLs from leaking sensitive information. To avoid such leakage, URLs could be transformed into pseudo-URLs, which do not include any feasibly retrievable sensitive information, but still contain enough properties of the original URLs to be suitable for various tasks, such as machine learning. Compared to techniques like differentially private machine learning, such an approach based on pre-processing has the advantage of allowing not only trained models but also training data to be shared. We are evaluating different pre-processing approaches in regard to privacy guarantees and their suitability for various use cases.

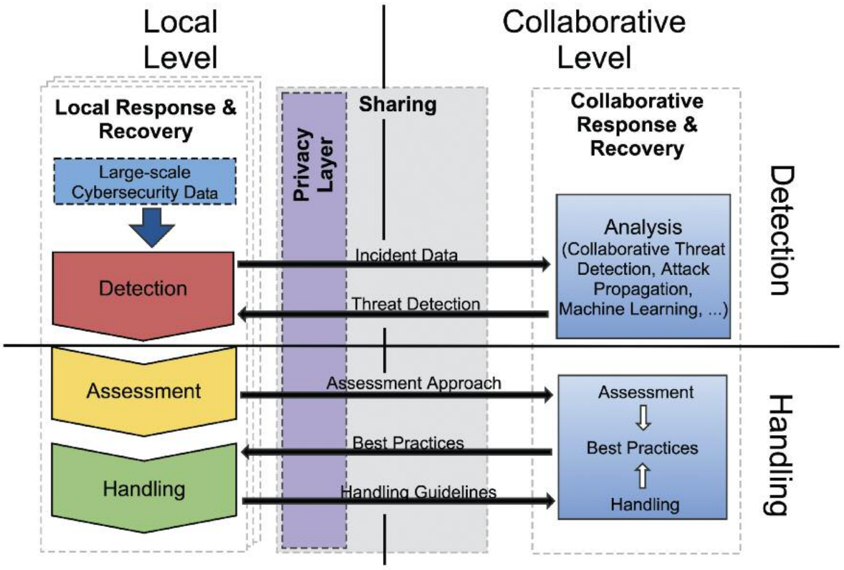


Figure 1: Privacy-preserving data sharing approach for response and recovery. The process is split into four phases: local detection, local handling, collaborative detection, and collaborative handling. The local detection and handling address the detection, assessment and handling phases of the incident response lifecycle at the local level. On the collaborative level, information from the local level is shared to achieve a mutual perspective on attack detection, incident assessment and incident handling. Privacy issues are handled before or during the sharing of information.

Sharing of response and recovery (R&R) recommendations via machine-readable cybersecurity playbooks between organisations can facilitate security orchestration, automation and response (SOAR) [2]. A cybersecurity playbook is a guideline to build an action plan to follow before, during and after a cyber-attack. It includes the important and common steps to prepare, assess, and handle the incidents and provides best practices for combating similar threats. Many of the steps in playbooks are organisation- and resource-specific, and in sharing this confidential information with external parties, an organisation risks opening itself up to threats from attackers and aggressive business competitors. One of the main privacy requirements of playbook sharing is to identify crucial sensitive data, such as personally identifiable information (PII), tools, and infrastructure elements, which should not be revealed in the shared playbooks. Another requirement is to define resources to indicate the confidentiality level of any specific element of shared playbooks. In this case, if an element is marked 'confidential' by the producer, it must be masked even with no predefined sensitive or private information.

The aim of our project is to work out how to offer simple solutions such as access control on the shared data, as well as advanced anonymisation techniques to mask or remove confidential data. Making a playbook more generally applicable could be seen as one step in a sanitisation process, since playbooks that are less organisation-specific are more widely applicable. We are also considering how to enable consumers of the playbook to map abstract identifiers onto their organisation-specific identifiers. Increasing the abstraction level of playbooks may hamper automation and reduce its ability to identify a proper response, thus we will also evaluate the abstraction level with respect to the trade-off between data protection and usability of shared playbooks.

This work is being done within the EU H2020 project SAPPAN: Sharing and Automation for Privacy Preserving Attack Neutralization [L1]. SAPPAN has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833418. The SAPPAN consortium consists of eight partners from five countries: Germany (Fraunhofer FIT as project coordinator [L2], RWTH Aachen University, University of Stuttgart), Czech Republic (CESNET, Masaryk University), Ireland (HPE), Finland (F-Secure), and Switzerland (Dreamlab). The project scope is not limited to privacy aspects of data sharing. Other topics include federated machine learning, automation of incident response, and suitable visualization methods for work within CSIRTs.

Links:
[L1] https://sappan-project.eu/
[L2] https://kwz.me/h6j

References:

[1] O. K. Sahingoz, E. Buber, O. Demir, B. Diri: "Machine learning based phishing detection from URLs", Expert Systems with Applications, vol. 117, pp. 345-357, 2019.
[2] C. Islam, M. A. Baer, S. Nepal: "A Multi-Vocal Review of Security Orchestration", ACM Computing Surveys, 2019.

Please contact:

Avikarsha Mandal
Fraunhofer Institute for Applied Information Technology (FIT), Germany
+49 241 80 21510
avikarsha.mandal@fit.fraunhofer.de

Measuring Contributions in Privacy-Preserving Federated Learning

by Balázs Pejó, Gergely Biczók and Gergely Ács (Budapest University of Technology and Economics)

How vital is each participant's contribution to a collaboratively trained machine learning model? This is a challenging question to answer, especially if the learning is carried out in a privacy-preserving manner with the aim of concealing individual actions.

Federated learning

Federated learning [1] enables parties to collaboratively build a machine learning model without explicitly sharing the underlying, potentially confidential training data. For example, millions of mobile devices can build an accurate input prediction system together without sharing the sensitive texts typed by the device owners [L1], or several pharmaceutical companies can train a single model to predict the bioactivity of different chemical compounds and proteins for the purpose of drug development without revealing which exact biological targets and chemical compounds they are experimenting with [L2]. Unlike traditional centralised learning, where training data from every participant are pooled to build a single model via a trusted entity, in federated learning, clients exchange only model parameter updates (e.g., gradients). Therefore, these model updates represent all the public knowledge about the private training data of different participants.

Although federated learning inherently mitigates some privacy attacks to an extent, it also introduces additional vulnerabilities stemming from its distributed nature. Some participants, called free-riders, may benefit from the joint model without contributing anything valuable in the training phase. Moreover, malicious (byzantine) participants may intentionally degrade model performance by contributing false data or model parameters, referred to as data/model poisoning. In another scenario, some parties may do so unintentionally by incorrectly pre-processing their own training data.

Contribution scores

Contribution scoring allows parties to measure each other's usefulness when training collaboratively. If implemented carefully, such an approach can detect free-riders and malicious attackers, which intentionally or by chance would degrade model performance. The Shapley value [2], the only provably fair reward allocation scheme, is a candidate for such a contribution metric. Despite being the only reasonable scoring mechanism, the Shapley value is not broadly implemented: it works by computing on every possible subset of the participants and is therefore too demanding for real use-cases. In a machine learning context, this would render the training process impractical: instead of a single joint model trained by all the participants, every possible subset of participants should train a separate model. This is clearly not feasible when even training a single model requires non-negligible time and computational resources.

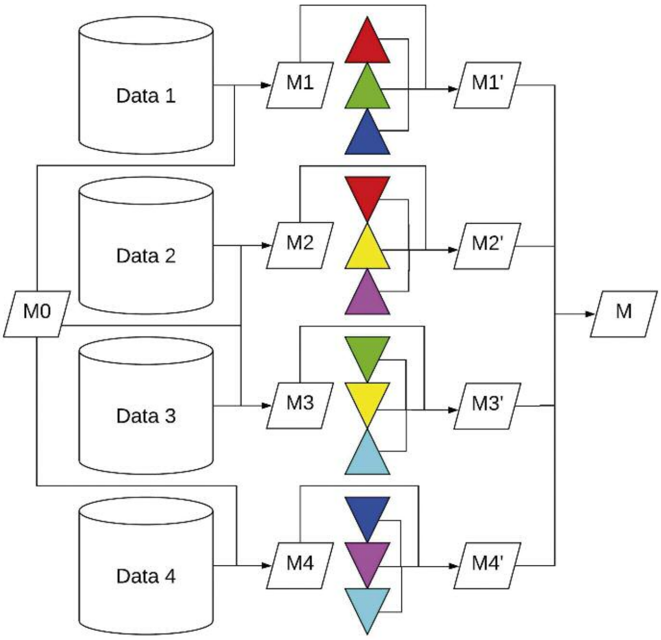
Many approximation techniques exist to facilitate Shapley value computation, e.g., via the use of gradients, influence functions, reinforcement learning, and sampling. Despite the wide range of available methods, unfortunately, none of them are compatible with privacy-preserving technologies. Indeed, the goal of privacy protection is quite the opposite of any contribution scoring mechanism: the former aims to hide an individual's contribution while the latter aims to measure it.

Our approach

Secure aggregation [3] (see Figure 1) is a frequently used privacy preservation mechanism within federated learning. It is a lightweight cryptographic protocol that allows anybody to glean the sum of the model updates without the individual contributions, i.e., M1, M2, M3, and M4 are concealed with pairwise noises. Therefore, we can only access the models corresponding to the smallest and largest coalitions, i.e., either no-one or everybody updates the model (corresponding to M0 and M respectively). This is clearly not enough information to compute the contribution of the participants as it contains no individual-level information.

On the other hand, participants do know their own updates as well, hence we can utilise two more coalitions: the one in which they are the only member (i.e., M1, M2, M3, and M4) and the one

Figure 1: Illustration of Secure Aggregation with 4 parties. M0 is updated by the participants (M1, M2, M3, M4) which are concealed with pairwise noises (M1', M2', M3', M4') and aggregated into M.



where they are the only one out (i.e., M-M1, M-M2, M-M3, and M-M4). These latter coalitions form the basis of the Leave-One-Out scoring methods, such as LOO-Stability and LOO-unfairness (e.g., M and M-M1 for participant 1). However, we can obtain a more accurate approximation of a participant's Shapley value based on four coalitions (e.g., M0, M1, M-M1 and M for participant 1) even if Secure Aggregation is employed (see Figure 1).

Furthermore, since the participants' data might come from different distributions, they might disagree on contribution scores: a model update assessed as 'good' for someone might be 'bad' for another.

Consequently, based on the participants' evaluations, we might not be able to differentiate between a malicious update and a correct one from a different distribution. Hence, an update originating from a specific distribution should be evaluated on the same distribution, meaning only the participants themselves should evaluate their own updates: this would clearly introduce bias. We can handle this issue in a variety of ways, e.g., consistency can be guaranteed by utilising a smart weighting scheme, or using a public or joint representative dataset for contribution score evaluation on which all participants agree.

Our preliminary results show that our proposed approach is clearly superior to the LOO-based methods, the only other currently existing contribution scoring technique suitable for Secure Aggregation. As future work we plan to tackle problematic self-reported contributions: the participants might cheat and manipulate their scores. We foresee several solutions to handle this, such as verifiable computation, zero-knowledge proofs, and commitments.

Links:
[L1] https://kwz.me/h6H
[L2] https://www.melloddy.eu/

References:

[1] Q. Yang, et al.: “Federated machine learning: Concept and applications”, ACM Transactions on Intelligent Systems and Technology (TIST) 10.2 (2019): 1-19.
[2] E. Winter: “The shapley value”, Handbook of game theory with economic applications 3 (2002): 2025-2054.
[3] K. Bonawitz, et al.: “Practical secure aggregation for privacy-preserving machine learning”, in proc. of the 2017 ACM SIGSAC Conference on Computer and Communications Security,2017.

Please contact:

Balázs Pejó
CrySyS Lab, HIT, VIK, BME, Hungary
pejo@crysys.hu

Privacy Risks and Anonymization of Microbiome Data

by Markus Hittmeir, Rudolf Mayer and Andreas Ekelhart (SBA Research)

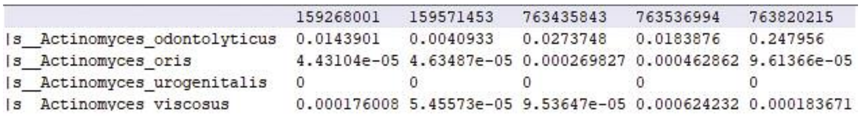
The microbial communities on the human body are subject to extensive research. While individual variations in the microbiome reveal valuable information about health and diseases, they also allow for the identification of individuals among populations of hundreds. The resulting demand for solutions to protect the privacy of participants in microbiome studies can be met by adapting well-known anonymisation techniques.

The bacteria, fungi and protists living on various sites of the human body have a substantial influence on our wellbeing. Studies of the human microbiome can help us with the prediction, diagnosis and treatment of diseases, and new findings are published on a regular basis. For instance, changes in the gut microbiome may be related to gastrointestinal diseases, obesity, diabetes, and depression [1]. As more data on the microbiome is gathered and stored, investigations into the temporal and individual stability of microbiome readings and the ensuing privacy risks have gained importance.

In 2015, Franzosa et al. presented a method for the unique characterization of hundreds of individuals via short codes constructed from their microbiome samples [2]. Using follow-up samples collected between 30 and 300 days later, about 30% of the individuals could still be matched correctly by comparing the samples' codes. While this result is the average of several body sites, the gastrointestinal microbiome appeared to be exceptionally stable and allowed the researchers to match up to 80% of individuals. The authors concluded that their work demonstrates the feasibility of microbiome-based identifiability, which poses ethical implications for the design of microbiome studies and a need for privacy-enhancing solutions for microbiome data. Recently, this demand has been strengthened by an improvement of Franzosa et al.'s technique [3], leading to an increased number of individuals that can be re-identified based on their microbiome.

In order to give an overview of the new method in [3] and its differences to [2], let us start by taking a closer look at the microbiome data. In addition to the aforementioned gastrointestinal microbiome, samples may be taken from several other body sites, such as saliva, throat, anterior nares (the external portion of the nose), supragingival plaque (at the teeth) or buccal mucosa (at the inside of the cheek). Starting with large volumes of raw data containing the genetic sequences of microbes found in the sample, there are several possibilities for the subsequent feature extraction. One method is to measure the abundance of bacterial and archaeal species found in the sample, leading to a table similar to the excerpt shown in Figure 1. The rows refer to the various species, and the columns (the “sample vectors”) contain the abundance counts for the individual samples. The relative counts in Figure 1 are proportions, meaning that the sum of all values in each column equals 1. Full examples for such datasets can be found under [L1], together with an implementation of the method in [2].

While there are publicly available techniques [L2] for microbiome-based identification on the raw genetic data, both [2] and [3] focus on privacy risks that arise from datasets containing sample vectors as discussed above. For each such sample, Franzosa et al. consider the features as either present or absent, based on a threshold (e.g., 0.0001) for the abundance. The code of each sample is then a unique combination of its present features, and the experiments in [2] demonstrate their temporal stability. The improvement in [3] is based on considering not just a subset of the present features, but comparing complete sample vectors. In order to match a single sample against a whole dataset, the method computes its distance to all the columns and finds the closest one (the “nearest-neighbour”). Compared to [2], this leads to an improved identification on most of the considered datasets. In particular, we see an increase in the average percentage of true-positive matches of 28% on the widely studied gut microbiome. In addition, the introduction of a criterion for accepting neighbouring pairs of samples as possible matches prevents a large number of false positives (i.e., incorrect matches). Figure 2 shows the results on six different body sites.



	159268001	159571453	763435843	763536994	763820215
|s__Actinomyces_odontolyticus	0.0143901	0.0040933	0.0273748	0.0183876	0.247956
|s__Actinomyces_oris	4.43104e-05	4.63487e-05	0.000269827	0.000462862	9.61366e-05
|s__Actinomyces_urogenitalis	0	0	0	0	0
|s Actinomyces viscosus	0.000176008	5.45573e-05	9.53647e-05	0.000624232	0.000183671

Figure 1: Excerpt from a microbiome table with features based on relative species abundance. The nine-digit number in the first row is the identifier of the individuals of the study.

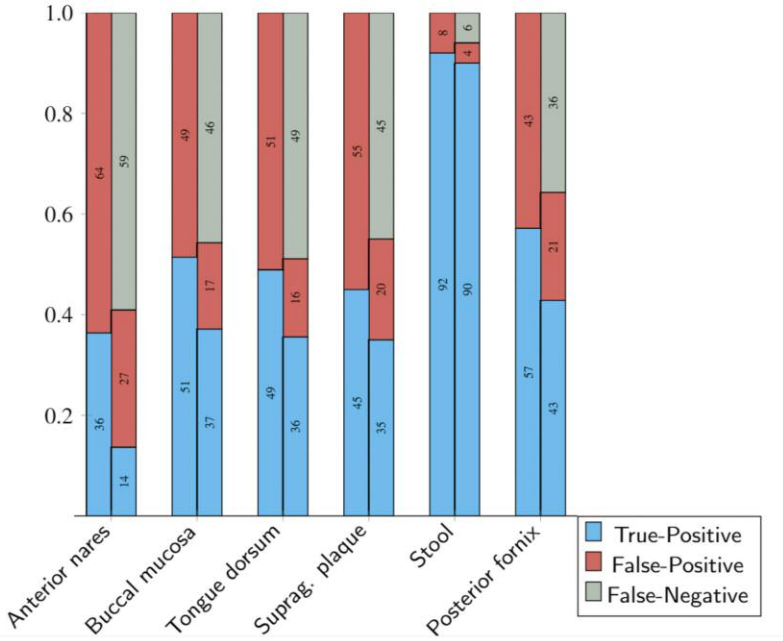


Figure 2: Re-identification results in % of the approach in [3] on six different body sites. On each body site, the left bar displays the results without acceptance criterion. After applying the criterion, we can see that most false positives turn into false negatives, improving the accuracy of the technique.

The threat analysis conducted in [2] and [3] demonstrates that the extent of the privacy risk depends on factors such as feature types and body sites. In this context, an adversary is any party in possession of unidentified microbiome samples with the intention to link them to other samples for accumulating information about the underlying individual, such as the participation in a specific study, or metadata linked to the identified record. There are multiple avenues by which an adversary could obtain microbiome samples, including public databases, cyberattacks against healthcare facilities and research organisations, data exfiltration via insiders, and potentially, directly from the victim (e.g., saliva).

One solution for protecting a microbiome database D is to establish k-anonymity, meaning that groups of at least k samples in D are indistinguishable to the discussed identification techniques. It is then impossible to find unique matches, and an adversary has to guess the correct individual from at least k different choices. This goal may be achieved by adapting a variety of classical techniques for k-anonymity on relational data. Let us briefly consider one such idea for establishing 2-anonymity. One first computes the pairwise distances between all the samples in D and finds pairs of samples that are most similar. Next, each pair is generalised by computing the mean of all the abundance counts of the two samples. Finally, each original sample in D is replaced by the generalisation of its corresponding pair, leading to 2-anonymity. Note that k-anonymity may be achieved by considering clusters instead of pairs. Moreover, there are several possibilities to optimise the procedure and minimise the information loss. In this sense, future work will focus on the refinement of techniques for mitigating the capabilities of an adversary and, thus, the related risks.

This work was partially funded by the Austrian Research Promotion Agency FFG under grant 877173 (GASTRIC).

Links:

[L1] https://kwz.me/h6W
[L2] https://github.com/princello/GePMI

References:

[1] G. Rogers, et al.: “From gut dysbiosis to altered brain function and mental illness: mechanism and pathways”, Mol Psychiatry 21, 738-748, 2016.

[2] E. Franzosa, et al.: “Identifying personal microbiomes using metagenomic codes”, PNAS 112, E2930-E2938, 2015.

[3] M. Hittmeir, et al.: Distance-based techniques for personal microbiome identification, 2021, under review.

Please contact:

Markus Hittmeir, Rudolf Mayer and Andreas Ekelhart
SBA Research gGmbH, Austria
{mhittmeir, rmayer, aekelhart}@sba-research.org

Enabling Voice-Based Apps with European Values

by Akira Campbell (Inria), Thomas Kleinbauer (Saarland University), Marc Tommasi (Inria) and Emmanuel Vincent (Inria)

'Cost-effective, Multilingual, Privacy-driven voice-enabled Services' (COMPRISE) is a Horizon 2020 project that provides tools to facilitate the deployment of conversational AI while maintaining the European values of privacy, accountability and inclusiveness. A major aim of the project is to provide the means for app developers to not only add voice-based interaction to their apps but also to facilitate the improvement of the underlying AI models in various European dialects and languages while maintaining a high level of data privacy.

In the past 10 years a shift has occurred in how average users interact with software/services. Rather than monitors, keyboards and mice, the public now often uses smaller interfaces such as smartphones, home appliances and smart speakers that include a voice interaction method. Once limited to writers, translators, pilots or the physically handicapped, voice interaction is used by the general public with little to no training. In many cases, the average consumer thinks that the 'effort-reward' ratio is better than traditional interfaces. This is thanks to hardware and communication infrastructure improvements, but also to improved Speech-to-Text (STT) and Natural Language Understanding (NLU) models that result in improved understanding of the user's query and, as a result, better replies from the dialogue manager.

This improvement has a cost: the amount of annotated data needed to train STT and NLU models has increased by up to 10,000 hours or more for STT. Data is not only required in one language, but preferably each language and each dialect or accent. Furthermore, domain-specific expressions and task-specific language details need to be understood. To create and improve voice-based systems, it is essential to obtain a broad range of in-domain data and include all categories of the population to minimise the digital gap. This is typically achieved by storing all user queries, manually annotating some of them, and using them as training data.

This requirement raises two major concerns: cost and privacy. Hiring annotators to annotate the collected data leads to huge costs. Protecting the privacy of

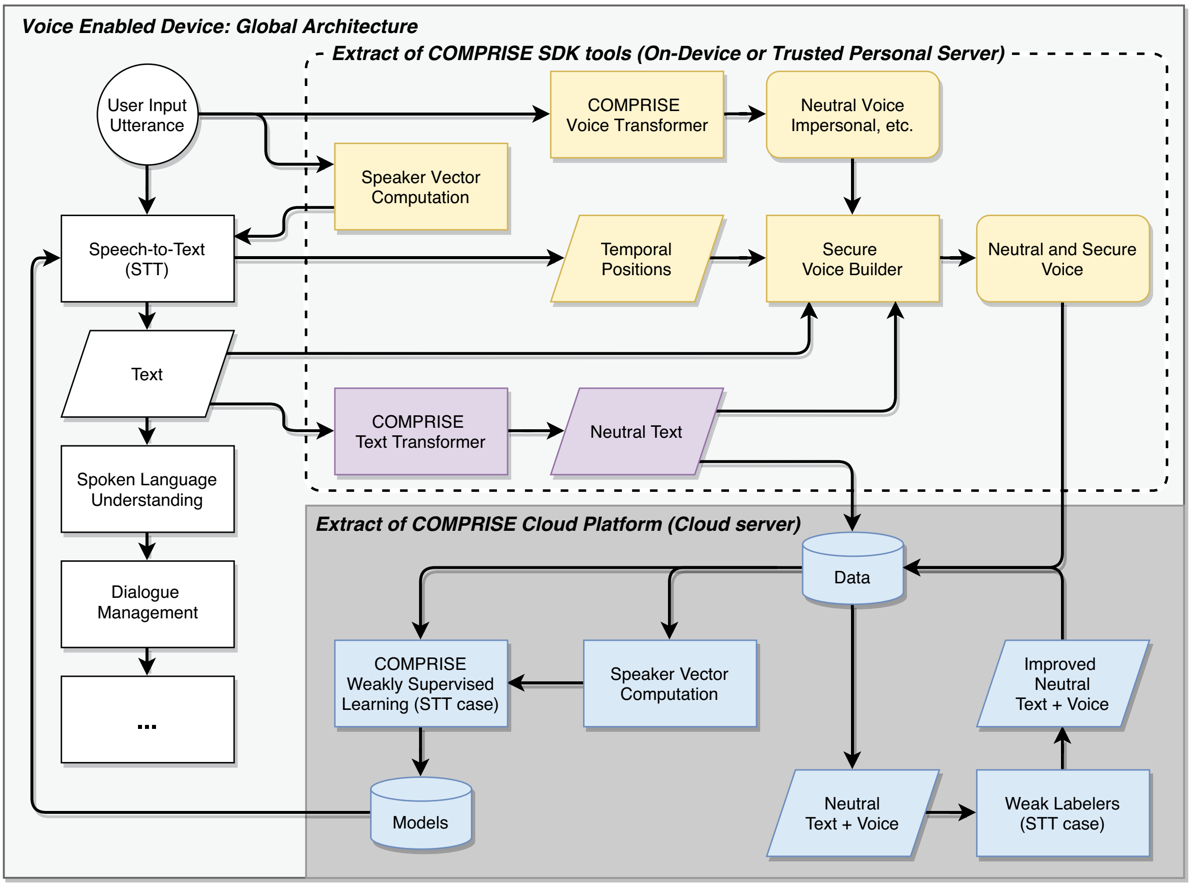

Voice Enabled Device: Global Architecture
Extract of COMPRISE SDK tools (On-Device or Trusted Personal Server)
User Input Utterance
COMPRISE Voice Transformer
Neutral Voice Impersonal, etc.
Speaker Vector Computation
Speech-to-Text (STT)
Temporal Positions
Secure Voice Builder
Neutral and Secure Voice
Text
COMPRISE Text Transformer
Neutral Text
Spoken Language Understanding
Dialogue Management
...
Extract of COMPRISE Cloud Platform (Cloud server)
Data
COMPRISE Weakly Supervised Learning (STT case)
Speaker Vector Computation
Improved Neutral Text + Voice
Models
Neutral Text + Voice
Weak Labelers (STT case)

Figure 1: Overview of the global architecture. Privacy is ensured by running all computations on the user's device or a trusted personal server, with only the anonymised data uploaded to the COMPRISE Cloud Platform.

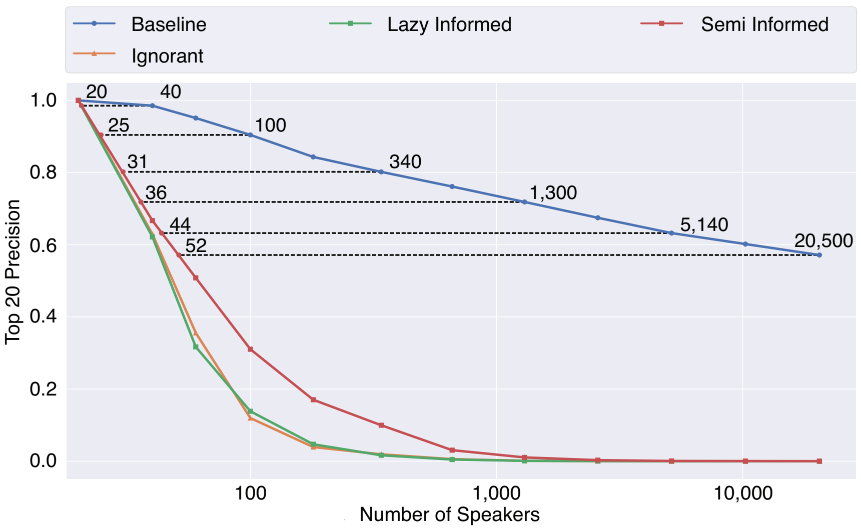


Figure 2: Top-20 precision of speaker identification for different attackers as a function of the number of speakers in the population. The numbers of speakers needed before anonymisation (N on blue curve) and after anonymisation (n on red curve) to achieve an equivalent drop in precision are highlighted.

users is also a major concern. To counter this, the COMPRISE [L1] solution is designed to reduce cost and preserve privacy by design (Figure 1).

Privacy and utility are a fine balance. There is no point in creating an anonymisation framework if the resulting data is unusable. Voice data not only requires to be transcribed and annotated, but it also needs to maintain its acoustic and linguistic characteristics to use it for training STT and NLU models. Furthermore, voice interaction uses data that is not only biometric but also contains details that can be used to profile the user, such as gender, profession, religion, race, place of origin, sexual orientation, medical details, mental health, etc. These details should be kept for the language model training but altered to guard user privacy, for example, by mapping the voice to another pseudo speaker to keep the speaker traits but disconnect them from the real identity of the speaker. Hence the creation of the COMPRISE Voice Transformer and the COMPRISE Text Transformer.

The Voice Transformer replaces the characteristics that make the user's voice identifiable with a different, random speaker while keeping the original words and prosody.[1] It uses a method called x-vector based voice conversion [2], which preserves the diversity of speech and provides comparable results to the original non-transformed data when used to train STT models. Importantly, it reduces the precision of user identification among a population of 100 users by approximately 60–80% when compared to non-transformed data. Increase the population size to 1,000 user voices and the precision is reduced to almost zero (Figure 2).

The Text Transformer replaces sensitive words, such as names, places and organisations with benign alternatives to de-identify text [3]. It offers different replacement strategies, which users can select. For instance, the replacement could be an abstract symbol akin to the blackening of words as seen in official documents. A more sophisticated strategy is to replace problematic contents with randomly chosen words of the same type, say, a person's name with another person's name. A number of NLU tasks have shown to perform on par with untransformed data even when trained on data privacy-enhanced by the Text Transformer [3].

Using these open-source tools, with privacy at their core, we are able to better align with the core European principles while providing a means to localise voice-enabled technology. On top of that, the COMPRISE Cloud Platform provides the means to annotate, manage, and train models from the anonymised data collected. The COMPRISE Weakly Supervised STT and Weakly Supervised NLU tools help automate some of the annotation, and train STT or NLU models by learning the difference between the manual and automatic labels. This lowers the cost, and the potential risk of data breaches by reducing the amount of data that need human intervention.

COMPRISE has had the privilege of contributing to the scientific community through scientific publications, and providing an open-source platform and a software development kit that can continue to be developed as a whole, and also as individual tools. Furthermore, the above-mentioned Voice Transformer and Text Transformer can be found within the European Language Grid (ELG) platform. [L2] We believe that the tools created have provided a means to be accountable towards the privacy of voice-enabled devices, and prevent a new digital gap occurring from our voice that is unique and natural to us.

Links:

[L1] https://www.compriseh2020.eu
[L2] https://kwz.me/h64

References:

[1] B. M. L. Srivastava, et al.: "Evaluating Voice Conversion-based Privacy Protection against Informed Attackers", ICASSP 2020, IEEE Signal Processing Society, hal-02355115v2.
[2] B. M. L. Srivastava, et al.: "Design Choices for X-vector Based Speaker Anonymization", INTERSPEECH 2020, ISCA. hal-02610447v2
[3] D. Adelani, et al.: "Privacy guarantees for de-identifying text transformations", INTERSPEECH 2020, ISCA. hal-02907939

Please contact:

Emmanuel Vincent
Inria Nancy – Grand Est, France
emmanuel.vincent@inria.fr

Measuring the Effectiveness of Anonymised Data

Tanja Šarčević and Rudolf Mayer (SBA Research)

Anonymising data has become increasingly important due to the legal constraints imposed by authorities such as the EU's GDPR and for ethical reasons relating to privacy. One large drawback of anonymised data is its reduced quality (utility). Therefore it is crucial to quantify and minimise the utility loss prior to data sharing. We take a closer look at the question of how well this utility loss can be estimated for a specific task, in terms of effectiveness and efficiency of the resulting dataset. Our evaluation shows that the most valuable utility metrics are also the most expensive to measure, and thus often, a suboptimal solution must be chosen.

With the rise of data-intensive computing applications, data is collected and used across different domains, such as healthcare, biomedicine, or for commercial purposes. One of the most valuable types of data in all these domains is personal data, which often comes in the form of 'micro-data', where each individual is represented with their own data record. However, the privacy of individuals in micro-data can be compromised even if direct personally identifiable information is removed (de-identification). The Netflix Prize from 2007[L1] is a famous example of how customer privacy can be threatened even if data without direct identifiers are shared, by linking based on other remaining attributes. Distributing personal data is highly regulated by law, especially within the European Union

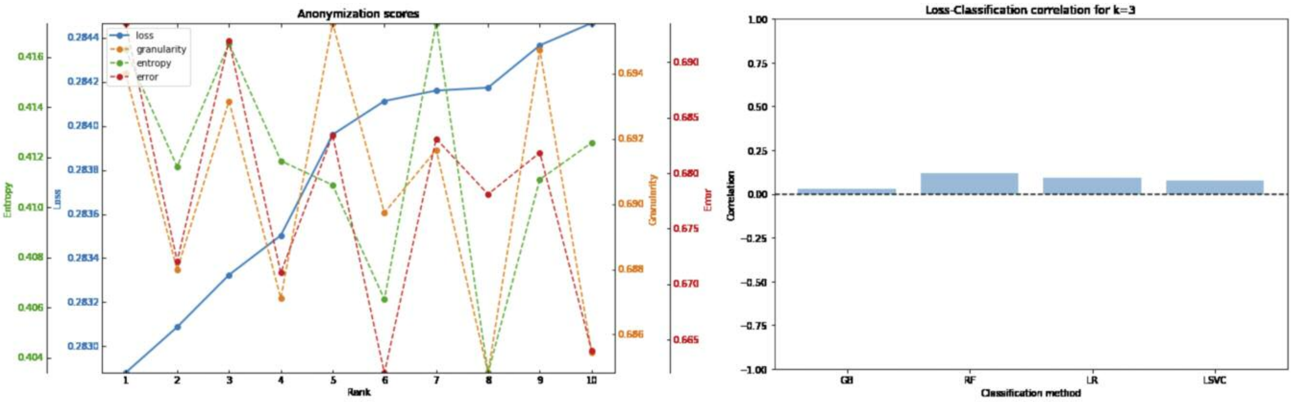


Figure 1: Utility results using different metrics, namely: loss, granularity, entropy and error (left) and the correlation between utility metric loss and machine learning performance metric F1 score (right). The comparison presented is among the anonymised datasets satisfying 3-anonymity.

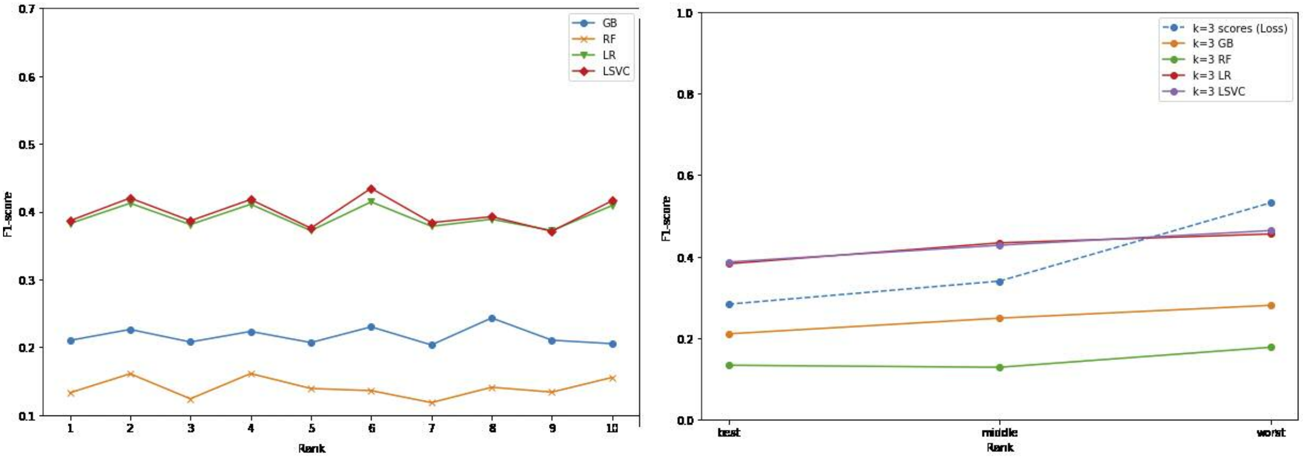


Figure 2: Utility in the notion of machine learning performance (F1 score) of optimal and suboptimal solutions satisfying 3-anonymity of k-anonymity algorithm (ARX [L2]) based on information loss metric on Adult Census Income dataset [L3]. Four classifiers are compared: gradient boosting (GB), random forest (RF), logistic regression (LR) and linear support vector classifier (LSVC). The difference in utility is shown for the top 10 k-anonymous solutions (left) and 3 solutions from different parts of the optimality spectrum: the best, middle and the worst solution (right).

with the General Data Protection Regulation (GDPR). For many purposes, datasets must be therefore anonymised before distribution.

K-anonymity is a privacy model that can be applied to sensitive datasets by obfuscating information that can be utilised to re-identify individual records in a dataset from which direct identifiers have been removed [1]. K-anonymity has certain privacy weaknesses, for which extensions have been proposed, such as l-diversity and t-closeness and other privacy models, such as differential privacy and synthetic data generation. However, k-anonymity as a model that facilitates easy data sharing is still considered in several settings.

In addition to privacy, another aspect to consider for datasets that have been sanitised is the utility of the resulting data. While anonymisation techniques provide a GDPR-compliant anonymity for the individuals in a dataset, they at the same time affect the utility of the data. This is because when sanitising a dataset via anonymisation or other approaches, some information at the level of individual records is invariably altered or removed.

Data utility can be evaluated by several approaches. One is to utilise quantitative measures of information loss [2]. Another is to measure the effectiveness of the final statistical analysis to be carried out on the data, such as the accuracy of a predictive machine learning model, compared to an analysis that would have been using the original, unabridged data. The latter is a very task-specific approach and is less efficient, as it is generally more resource-consuming (time, computing power) than the quantitative measures on the data itself. However, in many settings it provides a more useful insight into the utility of the data, given that such tasks are often carried out on the data. Without an exact knowledge of the final task, and with limited resources, it is therefore crucial to understand to what extent information loss can be used as a proxy measure for the other. In our analysis we estimated this in an experimental evaluation [3]. We utilised different machine learning models on different classification tasks and benchmark datasets and investigated how the performance of these classifiers correlate to the other utility loss metrics. The analysis has shown little correlation between the two types of utility evaluation, as shown in Figure 1, leading us to the conclusion that the estimation of the performance on a specific task cannot be replaced by more generic and faster utility metrics.

Another aspect of data utility is that there is generally not only one solution for achieving a sanitised version of a dataset that fulfils the desired level of privacy. Often a large number of candidate solutions exists, and finding the optimal solution is generally solved via heuristic approaches where implicitly one utility metric is used for finding an optimal solution. Our analysis showed that there is actually very little difference between optimal and suboptimal solutions (Figure 2), even between the optimal and worst solutions. In addition, depending on which utility metric is used in the heuristics, the optimal solution will also differ. This entails that the utility of resulting anonymised datasets are rather stable and not influenced by potentially minute aspects in the heuristic. This suggests that the data owner has a large solution space when deciding on anonymised data release. Relying on one, subjectively most appropriate utility metric will therefore not necessarily mean that the utility will be compromised based on other metrics.

The analysis showed that there is a large variety of estimates of the utility of an anonymised dataset, and no single anonymised version of a dataset that will score best across all investigated measures. Many possibly good solutions exist, assuming that the predefined level of privacy is achieved for all of them. Therefore, the choice of utility metric heavily depends on the actual use case for the data. The performance of a machine learning task is an example of such a specialised utility metric and can be used in scenarios when the usage of data can be foreseen. Using a variety of metrics can be advantageous for estimating the utility in the more general scenarios, but also needs to be put in relation to the cost of estimating these utility scores.

This work was partially funded from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826078 (project "FeatureCloud").

Links:
[L1] https://kwz.me/h6Z
[L2] https://arx.deidentifier.org/
[L3] https://kwz.me/h0C

References:

[1] L. Sweeney: "k-anonymity: a model for protecting privacy", Int. Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2002, https://doi.org/10.1142/S0218488502001648

[2] J. Eicher, K.A. Kuhn, F. Prasser: "An experimental comparison of quality models for health data de-identification", MEDINFO 2017: Precision Healthcare through Informatics, https://doi.org/10.3233/978-1-61499-830-3-704

[3] T. Šarčević, R. Mayer, D. Molnar: "An analysis of different notions of effectiveness in k-anonymity", Privacy in Statistical Databases (PSD) 2020 Proc., Tarragona, Spain. https://doi.org/10.1007/978-3-030-57521-2_9

Please contact:

Tanja Šarčević, Rudolf Mayer
SBA Research, Austria
tsarcevic@sba-research.org,
rmayer@sba-research.org

Standardisation for Security Applications and Technologies

by Hui Han (Fraunhofer IESE)

Standardisation can help ensure proper contractual procedures for protecting digital information and systems, guaranteeing security and privacy in the dynamic digital environment. With standardisation, companies can effectively collaborate with their partners, thus strengthening trust among organisations. As a result, various standards have been established for security applications and technologies.

Security

When identifying a system's deficiencies, and potential threats from internal and external sources, it is important to consider the characteristics of the security applications and technologies that are being used by an organisation. Security issues can be classified into three types [1]:

- Physical security: preventing unauthorised crew or even occasional interlopers from accessing internal software components and hardware.
- Network security: preventing malware (malicious software) or cyber-attacks on underlying networking infrastructures and communication systems.
- Data security: protecting data from the actions of unauthorised users, including data encryption, tokenisation, and key management.

Physical security standardisation

Three typical standards used to define physical security are the IEC 62443, the ISO 27033 series and ISO/IEC 29180:2012, which represent the security standards for the control systems, information system networks and sensor networks, respectively. The IEC 62443 series addresses the security required for business IT applications by industrial automation and control systems (IACSs). The ISO/IEC 27033 series addresses security facets of the design, implementation, and management of information system networks. The ISO/IEC 29180:2012 addresses the security requirements of the ubiquitous sensor network (USN). Furthermore, it classifies the security technologies based on the security functions that meet the above-mentioned security requirements and where the security technologies are to be used for constructing the security model of USN.

The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard for computer security certification. It provides assurance for the process of designation, execution and assessment of a computer security product.

Trusted Platform Module (TPM, also known as ISO/IEC 11889) is an international standard for a computer chip (microcontroller) that is designed to provide hardware-based, security-related functions through integrated cryptographic keys.

Protection and privacy for data science. Source: Fraunhofer IESE.

eIDAS (electronic IDentification, Authentication and trust Services) creates a standard framework on electronic identification and trust services for electronic transactions that applies as law within the whole of the EU.

OAuth 2.0 is a security standard which gives one application permission to access data in another application.

Network security standardisation

The Organisation for the Advancement of Structured Information Standards (OASIS) is a non-profit consortium that develops web services standards along with security standards. OASIS security standards relevant to cloud computing are: SAML, XACML, SPML, WS-Security Policy, and WS-Trust. In addition, Cloud Data Management Interface (CDMI) are cloud-computing standards for customer interactions with cloud-based storage, cloud data management, and cloud-to-cloud storage interactions.

The Transport Layer Security (TLS) protocol is the de facto standard when it comes to securing communications on the World Wide Web.

PKCS (Public Key Cryptography Standards) are a set of public-key cryptography standard protocols that enable secure information exchange on the internet. GOST 28147-89 is a well-known 256-bit block cipher that submitted to ISO 18033 to become a worldwide industrial encryption standard.

QUIC (Quick UDP Internet Connections) is a new encrypted-by-default internet transport protocol that contributes many improvements designed to speed up HTTP traffic and make it more secure, with the purpose of eventually replacing TCP and TLS on the web.

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a widely accepted protocol for sending digitally signed and encrypted messages.

Data security standardisation

Privacy is an important aspect of security. Government policies and protocols in this domain are receiving more attention because of the growing concern of citizens about the abuse of personal data and violations of privacy. In this area, the General Data Protection Regulation (GDPR) that entered into force in the EU in May 2018 provides for governments to establish standardisation on data protection and privacy.

The World Wide Web Consortium (W3C) forms the XML-Encryption standard, which specifies a process for encrypting data and displaying the result in XML.

Secure Channel Protocol (SCP) is a way of transferring data that is resistant to overhearing and tampering.

ISO/IEC 29176 is a consumer privacy-protection protocol for mobile RFID services. ISO/IEC 29134:2017 are guidelines for privacy impact assessment (e.g. assessing operating data processing systems). ISO 29190:2015 provides guidance about how to assess their capability to manage privacy-related processes.

The project: Software Engineering for AI (SE4AI) in the context of small and medium-sized enterprises (SME)

SMEs face different challenges to large enterprises when it comes to digitisation and the application of AI and data-driven methods. The Data Science department at Fraunhofer IESE has developed and has been applying several methods to help companies in their digital transition [2], but these are not dedicated to SMEs. Our new project focusses on how current SE4AI methods apply to SMEs and will propose solutions for the implementation and evaluation of these methods. Security standardisation is a main challenge faced by SMEs when applying SE4AI methods.

References:

[1] P. Leitao, J. Barbosa, M. E. C. Papadopoulou, and I. S. Venieris, “Standardization in cyber-physical systems: the ARUM case,” in Proceedings of the IEEE International Conference on Industrial Technology, 2015, pp. 2988–2993, doi: 10.1109/ICIT.2015.7125539.

[2] J. Heidrich, A. Trendowicz, and C. Ebert, “Exploiting Big Data’s Benefits,” IEEE Software, vol. 33, no. 4, pp. 111–116, 2016.

Please contact:

Hui Han, Fraunhofer Institute for Experimental Software Engineering (IESE), Germany
hui.han@alumnos.upm.es

Brain Segmentation Using Active Contours Models

by Stelios Zimeras (University of the Aegean)

Medical image segmentation is needed for diagnosis and treatment in healthcare. The detection of organs and organic structures in 2D images is an important task during diagnosis. Manual segmentation is very expensive as it requires expertise and is very time consuming. Methods for applying segmentation vary widely depending on the specific application, imaging modality and other factors like treatment (e.g., cancer treatment, image-guided surgery, and invasive techniques) or diagnostic imaging. Therefore, automatic segmentation algorithms are needed [1].

During brain imaging, the segmentation of the organ structure as well as the shape of the tumour is essential for diagnosis and cancer treatment. Figure 1 illustrates a 2D CT brain image where the position of the tumour appears as a shadow.

Image segmentation techniques include methods of regional area identification based on splitting techniques to extract images of structures and provide images that closely represent the real data (2D regions or 3D voxels). Several contour and region approaches to segmentation have been proposed. Contour techniques are often less robust than region techniques and more sensitive to noise and variability of data.

There are three main ways to perform image segmentation: (i) manual: an expert with training draws the required boundaries manually. Manual drawing of boundaries is difficult and time consuming; (ii) fully automatic: the available techniques, such as thresholding or region growing can be applied and they are quite robust for big data medical images; (iii) semiautomated: this method uses boundary finding results generated by sophisticated automatic algorithms as an initial guess.

To reduce the user interaction required for the segmentation, active contour models (ACM) could be introduced, where contours and homogeneous regions are integrated into image structures. ACMs are adaptive contour representations, also known as snakes or deformable models. ACMs are 2D image curves, which are adjusted from an initial approximation to image features by a movement of the curve caused by simulated forces [2]. The idea behind these models is to represent the contours as parts of elasticity and rigidity. The general concept of active contours is autonomous adaptation of the shape and location of objects, finding the important contour points to reconstruct the image. An internal tension of the curve resists against highly angled curvatures, which makes the ACM movement robust against noise. After a starting position is given, it is adapted to an image by relaxation to equilibrium of the external force and internal tension. The method performs a fitting process based on the elasticity of the contour lines. To calculate the forces, an external energy has to be defined. The gradient of this energy is proportional to the external force. ACM models are a class of energy minimising spline curves or surfaces. These models are very important in a number of inverse visual problems such as the segmentation and reconstruction of objects from images in mathematically ill-posed problems [3].

Implementation of the active contour models (ACM) is performed in Figure 2 based on the work of [2]. Based on the resulting images, the tumour's contour is well defined, with sharp boundaries around the investigating region. The algorithm converges in 100 iterations, performing the optimal results. The performance times are 1.15 seconds for 20 iterations, 1.28 seconds for 50 iterations and 2.32 seconds for 100 iterations.

References:

[1] S. Zimeras: "Brain segmentation tools under uncertain conditions for radiotherapy treatment planning", Biomedical Research and Clinical Practice, Vol 4, 1-5, 2019

[2] L. Wang, L. He, A. Mishra, C. Li: "Active contours driven by local Gaussian distribution fitting energy". Signal Processing, 89 (2009) 2435–2447.

[4] S. Zimeras, G. Karangelis: "Segmentation of anatomical structures using volume definition tools", Lecture Notes in Computer Sciences 27, Computer Application in Modern Medicine, M., Springer-Verlag, 825-836, 2008.

Please contact:

Stelios Zimeras, University of the Aegean, Greece
zimste@aegean.gr

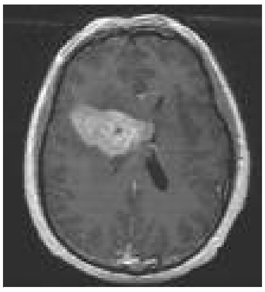


Figure 1: 2D CT brain image: position of the tumour is visible as a shadow.

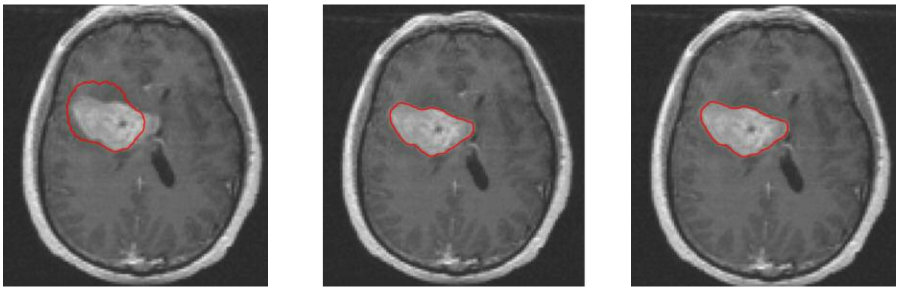


Figure 2: Contour representation of the tumour based on active contour models. From left to right: 20 iterations, 50 iterations, 100 iterations.

Security and Resilience Issues in Supply Chains – A Research Perspective

by Peter Kieseberg (St. Pölten UAS), Michael Herburger (UAS Upper Austria) and Alexandra Anderluh (St. Pölten UAS)

Supply chains can be considered the backbone of modern industry. Although supply chains may be highly integrated, security practices are often focussed around single companies and do not incorporate issues that arise from the integration of other partners within the chain. Thus, to make supply chains resilient against cyber-attacks, we need to adopt a holistic view of supply chain security.

Networked, highly integrated supply chains (SC) are an essential characteristic of modern business. Complex supply chains can already be found behind relatively simple-seeming products, owing largely to the increasing specialisation of companies. In addition, complexity has significantly increased in recent years due to three trends: (i) the trend towards customised products, such as in the automotive industry, where a car can only be completed after an order has been placed, based on individual wishes; (ii) the trend towards just-in-time production (JIT) and lean management in order to keep storage costs low; and (iii) globalisation, resulting in worldwide branched SCs.

These trends have led to a massive increase in time pressure, even in non-critical industries. Redundancies have been reduced as far as possible, and accordingly supply chains must function as smoothly as possible to avoid incurring considerable losses, e.g. due to waiting times and idle machines. The vulnerability of SCs and entire industries has been demonstrated not only by the disruptions caused by the COVID-19 pandemic, but also during the recent blocking of the Suez Canal [L1].

Different degrees of integration exist in SCs, depending on the size and structure of the partners involved, and the level of collaboration. Among equal partners, or within very open structures with many different customers, often no dedicated integrated SC-platforms are created. This can lead to very low levels of organisation, which are correspondingly susceptible to social engineering techniques [1], but also to a proliferation of different tools, which are correspondingly difficult to maintain. This can easily lead to attacks on partners, e.g. by changing payment modalities, or by stealing know-how or tender and bid documents. Such information is often used merely to obtain information for subsequent social engineering.

Large companies, having recognised the problems of low-integration SCs, have integrated their suppliers into their backbone systems and require them to perform any communication and information exchange within this platform (see Figure 1). This integration is particularly important in terms of cyber security: while large enterprises spend vast sums of money to make their IT and OT (operations technology) systems secure, many of their specialised suppliers are SMEs, often competing in a very aggressive market and therefore unable to focus on IT security issues. Due to the deep integration of their systems with the big players' platforms, they provide a perfect vector to attack large enterprises, enforcing several different attack strategies: (i) the attacker might try to leverage a vendor's corrupted system to attack the platform; (ii) vendors can often access a variety of information from the platform, so information exfiltration may be an issue; and (iii) it can be used as a means of reconnaissance to launch other forms of attack, such as social engineering. Finally, (iv) the corrupted system could be used to inflict damage by disrupting the SC through attacks such as Denial of Service (DOS), command manipulation, or other acts of vandalism.

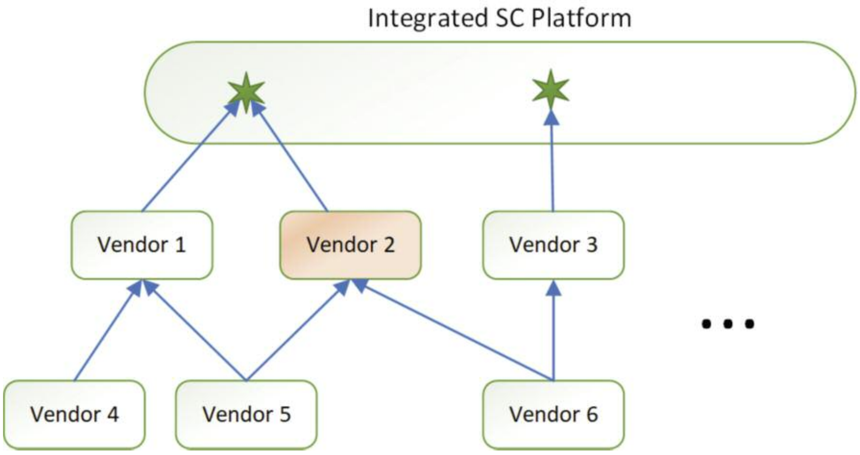


Figure 1: Schematic of highly integrated SCs.

Securing SCs against cyber risks is not a new idea [2]. Nevertheless, essential aspects have so far only been researched in a rudimentary way and dealt with on an academic level:

- *Holistic analysis of attacks and attack targets:* Currently available literature on securing SCs essentially focuses on specific use cases and application areas, typically looking at only a small section of an SC, usually one or two companies. In addition, security literature typically focusses on single entities (companies) and do not consider the SC [3].
- *SCs with different degrees of organisation:* SCs differ significantly in their degree of integration, which must be taken into account accordingly in the security architecture and in the choice of countermeasures.
- *Real-world use cases:* Most of the literature does not focus on model cases, which are useful for developing and

demonstrating specific technologies, but make it very difficult to translate the lessons learned into reality.
- Situational awareness for SCs: Situational awareness is currently typically associated with governments and related agencies, though many large companies also use similar technologies. The aim is to continuously monitor all entities in a system, regardless of whether they are technical assets or resources. However, classical security approaches are not suitable for SCs, as the focus is currently put mainly on relatively static computer networks, which means that the strong dynamics in complex adaptive systems such as SCs cannot be considered accordingly.

Within the SSCCS project [L2], methods for solving these challenges will be researched, with the general aim of defining problems as close to real life as possible, i.e. the problems to be solved are defined from real use cases. For this purpose, the project consortium can draw on a great deal of comprehensive know-how from many areas of supply chain management and logistics, especially in the field of multimodal logistics. From an academic point of view, the targeted research results are not only interesting from the point of view of SCM and logistics, as well as IT security, but also relevant to the topic of resilience, a theme that has moved into the focus of research, and also of relevant societal and governmental actors.

Links:
[L1] https://kwz.me/h6Q
[L2] https://projekte.ffg.at/projekt/3984614

References:

[1] S. Nasralla, A. Croft, Adrian: “Austria’s FACC, hit by cyber fraud, fires CEO”, 2016. Reuters. URL:https://www.reuters.com/article/us-facc-ceo-idUSKCN0YG0ZF
[2] V. Hassija, et al.: “A survey on supply chain security: Application areas, security threats, and solution architectures”, IEEE Internet of Things Journal, 8 (8), 6222-6246, 2021
[3] C. Colicchia, A. Creazza, D. A. Menachof: “Managing cyber and information risks in supply chains: insights from an exploratory analysis”, Supply Chain Management: An International Journal, 24(2), 215-240, 2019.

Please contact:

Peter Kieseberg
St. Pölten UAS, Austria
peter.kieseberg@fhstp.ac.at

Michael Herburger
Steyr UAS, Austria
Michael.Herburger@fh-steyr.at

CHARITY: Cloud for Holography and Cross Reality

by Patrizio Dazzi and Massimiliano Corsini (ISTI-CNR)

ISTI-CNR is involved in the H2020 CHARITY project (Cloud for HologrAphy and Cross RealITY), which started in January 2021. The project aims to leverage the benefits of intelligent, autonomous orchestration of a heterogeneous set of cloud, edge, and network resources, to create a symbiotic relationship between low and high latency infrastructures that will facilitate the needs of emerging applications.

This goal is accompanied by the extra challenge of easing the transition from traditional hosting environments to the novel environment proposed by CHARITY. To address this issue, the project will equip application providers with adaptive, end-to-end lifecycle management tools and continuous integration and delivery techniques. At the same time, automation at the network level will be facilitated by zero-touch network slice life-cycle management. The project will further enable and foster the development of a Virtual Network Function (VNF) repository to assist applications to benefit from the compute and network continuum management environment.

The key value proposition is CHARITY’s work on infusing intelligence at the resource management strategies level that does not rely solely on utility functions, as has been done so far. Instead, it relies on cognitive decision-making, based on an overall understanding of the resource, application and context characteristics. To this end it will be of paramount importance to provide solutions and approaches enabling the efficient and seamless management of heterogeneous computing and network resources.

CHARITY has the potential to tackle any kind of highly interactive class of services and applications and it will be validated against a wide class of highly anticipated applications characterised by extreme levels of interaction and data exchange between the end users and application components, i.e., AR, VR and Holography applications.

In summary, the main outcome of CHARITY will be a community-driven, open-source framework consisting of:

- A system for the autonomous orchestration, life-cycle management and efficient exploitation of a wide range of

compute and network resources and infrastructures that is not dependent on a single large vendor yet remains compatible with all.
- A collection of tools, mechanisms and algorithms enabling the efficient, contextualised and network-aware exploitation of edge resources and application reconfiguration.
- A set of VNFs along with a VNF repository that will support highly interactive application leveraging tools, technologies and platforms stemming from fields such as big data.
- Tools for the application providers to simplify the deployment and management of application components, mainly targeting the needs of SMEs (DevOps automations, specifications, APIs and best practices).

CHARITY runs from 1 January 2021 to 31 December 2023. It is coordinated by Uwe Herzog (EURESCOM) while Tarik Taleb (ICTFICIAL) is serving as technical manager for the project. ISTI-CNR is leading WP3 energy, data and computationally efficient mechanisms supporting dynamically adaptive and network-aware services.

Link:
https://cordis.europa.eu/project/id/101016509

Please contact:
Patrizio Dazzi and Massimiliano Corsini
ISTI-CNR, Pisa, Italy
patrizio.dazzi@isti.cnr.it, massimiliano.corsini@isti.cnr.it

Academic Positions at the Department of Computer Science – University of Cyprus

The University of Cyprus was founded in 1989 and admitted its first students in 1992. Today, it is ranked as the 84th young university (under 50 years) and #501-600 worldwide by the Times Higher Education

Rankings.
These distinctions are the result of dedication to continuous development. The pursuit of research excellence constitutes a key strategic objective of the University of Cyprus. Moreover, the University continually extends and upgrades its programs of undergraduate and graduate studies.

To best serve its research and educational aims, the University recruits high-caliber academic staff who can make significant contributions to the development of internationally competitive research projects and to the design and delivery of new curricula. The University of Cyprus invites applications for two tenure-track academic positions at the rank of Lecturer or Assistant Professor in the Department of Computer Science, as follows:

- **one position in the field of "Software Engineering"**
- **one position in the fields of "Networks or Cybersecurity"**

For all academic ranks, an earned Doctorate from a recognised university is required.

Requirements for appointment depend on academic rank and include: prior academic experience, research record and notable scientific contributions, involvement in the development and teaching of high quality undergraduate and graduate curricula. The minimum requirements for each academic rank are listed at:

https://www.ucy.ac.cy/acad.staff.procedures.

Candidates need not be citizens of the Republic of Cyprus.

The official languages of instruction are Greek and Turkish. For the above positions, fluency in the Greek language is necessary.

In case the selected candidate does not have sufficient knowledge of the Greek language, it is the candidate's and the Department's responsibility to ensure that the candidate acquires sufficient knowledge of the Greek language within three years from appointment. Each Department sets its own criteria for the required level of fluency in the Greek language.

The annual gross salary for full time employment, according to the current legislation, is:
- Assistant Professor: €58,428.91-€78,798.61
- Lecturer: €44,410.28-€72,265.43

Candidates are invited to submit their application at the following link:

https://applications.ucy.ac.cy/recruitment.

Application deadline
The deadline for applications is Monday 27 September 2021.

For more information, candidates may contact the Human Resources Service:
+357 22 89 4146/4155, applications@ucy.ac.cy

or the Department of Computer Science:
+357 22 892669).

CWI: 75 Years of Pioneering Research

This year, CWI is celebrating! 75 years ago, the institute opened its doors, under the name Mathematisch Centrum. Its aim was to promote the use of pure and applied mathematics in the reconstruction of the Netherlands after the Second World War, to improve prosperity in the Netherlands, and to enhance the Dutch contribution to international scientific culture. Computer Science was later added to the mix, and the centre was duly renamed Centrum Wiskunde & Informatica, or in short CWI.

Talented researchers in mathematics and computer science work at CWI, conducting fundamental, ground-breaking research that lays the foundation for future breakthroughs. CWI strives to share the knowledge it acquires with society, and its research therefore always has a social relevance.

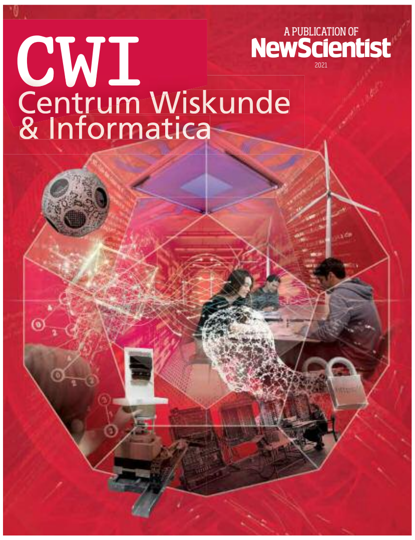
First computers

In 1952 the Mathematical Center developed the first Dutch computer, the Automatische Relais Rekenmachine Amsterdam (ARRA). After the North Sea flood disaster in 1953, ARRA was used to create models and perform calculations for the Delta Works. Today, the Delta Works still protect the Netherlands against high water.

Spin-offs and partnerships

Cooperation is central to how CWI works, both on a national and international level, with companies and with individual researchers who themselves go on to launch spin-offs. The first CWI spin-off was in 1956: Electrologica, the first Dutch computer manufacturer. To date, CWI has launched 28 spin-offs. Modern examples are Stokhos, which makes software that predicts how ambulances can be efficiently distributed within a region, and MonetDB, founded by database scientists at CWI.

In 1989 CWI co-founded ERCIM together with Inria in France and GMD in Germany.



Together with the Dutch edition of New Scientist, CWI published an anniversary magazine featuring a wide variety of CWI research.

Shortest path algorithm and navigation

In 1959 one of the world's top computer scientists, Edsger Dijkstra, developed the shortest path algorithm, also known as Dijkstra's algorithm. This is the basis of all route planners used today. In 2007, CWI researcher Lex Schrijver, with others, created an algorithm that was used to redesign and optimize the timetable of the Dutch Railways.

Programming languages

For most of its 75 years, CWI has been a hotbed of programming language design and development, starting with the algorithmic languages ALGOL 60 and ALGOL 68, and continuing with Python, developed in 1989 by Guido van Rossum.

Internet

CWI has also been a leader in the development of the internet. In April 1986 CWI registered ".nl" as one of the first country domains worldwide, and in November 1988, CWI set up the first node on the open internet in Europe. CWI also had one of the world's first websites. CWI researchers have contributed to the design of many web standards including CSS, HTML, XHTML, RDF and many others.

Security and privacy

For security and privacy on the web and the internet, data is usually encrypted. CWI is on the forefront of research in encryption, both in creating encryption methods, and in testing them by attempting to break them. In 1999 CWI coordinated the breaking of the encryption standard RSA-512, by factoring large numbers into their prime factors. In 2008 a group of CWI researchers and international colleagues exposed weaknesses in the MD5 security standard (‘cracking https’), which was widely used on the Internet. In 2017, the same happened again with the security standard SHA-1 which was used to protect credit card transactions and digital signatures.

Quantum software

In the near future quantum computers will surpass ordinary computers in performance: In 2015, CWI and the University of Amsterdam launched QuSoft, the research center for quantum software to explore the possibilities and limitations of software that can be used on quantum computers once they are available.

Imaging, energy, and AI

In 2017, CWI opened the unparalleled X-ray scanner that provides real-time 3D images. With the FleX-ray Lab, mathematics and 3D scanning are brought together, so the new calculation methods can immediately prove themselves in practice. Patients now are treated following optimal radiation plans created by AI. CWI also works on energy research, with main questions like: How do you achieve the most with artificial intelligence and calculation models from available energy sources? And how do you distribute energy fairly and efficiently?

Future possibilities

Throughout its history, CWI has been an innovator, connector, and driver in mathematics and computer science. By joining forces with the best and most motivated scientists in the field, we will increase our efforts to collaborate with universities and knowledge institutions to create the best opportunities for the future.

On the occasion of the 75th anniversary, CWI and New Scientist published a one-off anniversary magazine, featuring a wide variety of CWI research (a free paper copy can be ordered online). CWI has also produced a podcast series, where scientists share their thoughts on the influence of computer science and mathematics on tomorrow’s world.

More information:
https://kwz.me/h7s

SCHLOSS DAGSTUHL
Leibniz-Zentrum für Informatik

Call for Proposals

Dagstuhl Seminars and Perspectives Workshops

Schloss Dagstuhl – Leibniz-Zentrum für Informatik is accepting proposals for scientific seminars/workshops in all areas of computer science, in particular also in connection with other fields.

If accepted the event will be hosted in the seclusion of Dagstuhl's well known, own, dedicated facilities in Wadern on the western fringe of Germany. Moreover, the Dagstuhl office will assume most of the organisational/ administrative work, and the Dagstuhl scientific staff will support the organizers in preparing, running, and documenting the event. Thanks to subsidies the costs are very low for participants.

Dagstuhl events are typically proposed by a group of three to four outstanding researchers of different affiliations. This organizer team should represent a range of research communities and reflect Dagstuhl's international orientation. More information, in particular, details about event form and setup as well as the proposal form and the proposing process can be found on

https://www.dagstuhl.de/dsproposal

Schloss Dagstuhl – Leibniz-Zentrum für Informatik is funded by the German federal and state government. It pursues a mission of furthering world class research in computer science by facilitating communication and interaction between researchers.

Important Dates
- Proposal Submissions:
  October 15 to November 1, 2021
- Seminar dates: In 2023.

Call for Participation

CWI in Business 2021 on Secure Multiparty Computation

13 September 2021, online

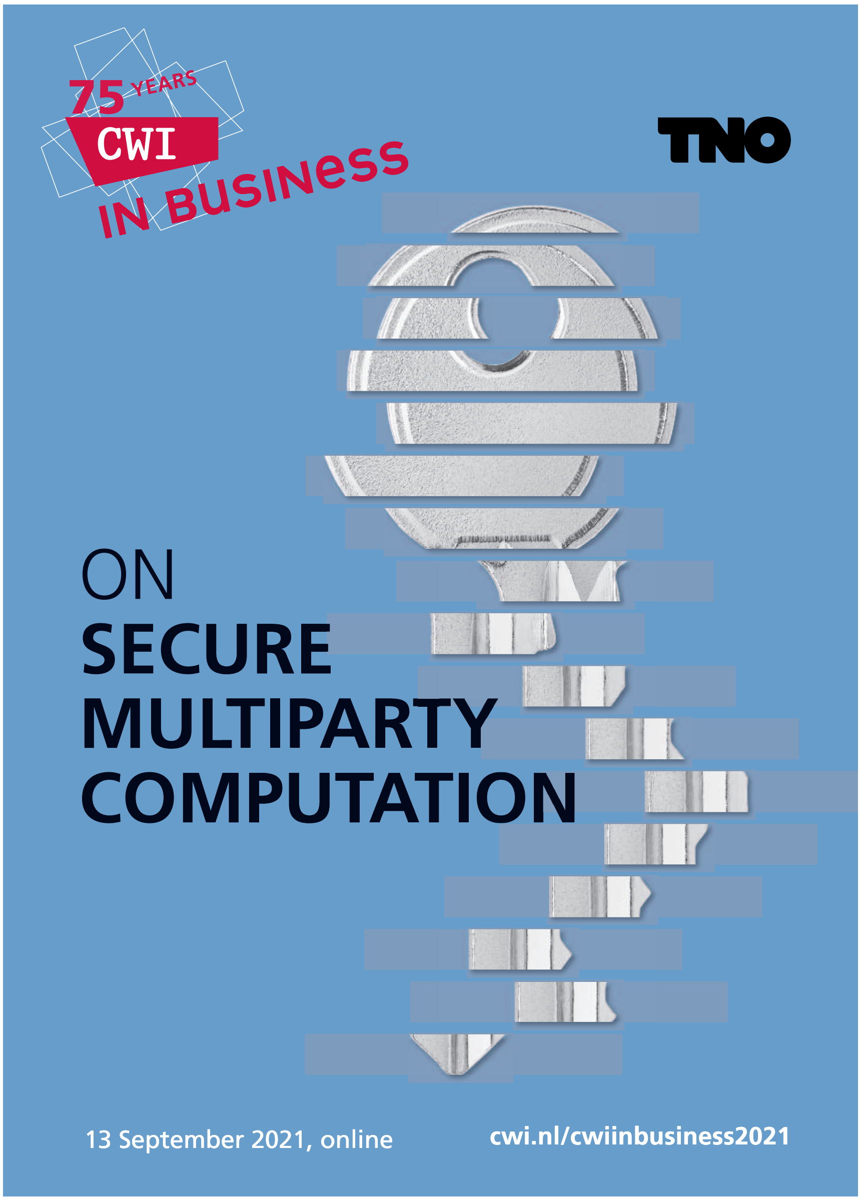
CWI and TNO are jointly organising the 2021 edition of the CWI in Business event revolving around Secure Multi-Party Computation (MPC).

MPC offers a cryptographic approach for privacy-protecting secure data sharing and -processing. This area is gaining worldwide recognition as a potential solution to an increasing number of applications, for instance in health and finance.

During the last decade, many scientific results contributed to significant improvements of the efficiency of these techniques, thereby bringing MPC further towards maturity. On the other hand, the development of big data and artificial intelligence has established a growing need for secure data analysis mechanisms on distributed sensitive data. A further incentive is given by the requirements of the European privacy laws (GDPR). This event will give a scientific overview of the field, and present a number of use cases that were solved by means of MPC.

CWI in Business will take place online and is freely accessible after registration (registration open in August). For more information, including the preliminary programme, see:

https://www.cwi.nl/cwiinbusiness2021



Europe Needs Strong Software Research

"Software is eating the world." Like oxygen is an essential element for all life forms, software is the invisible yet crucial fabric of our society. There is no aspect of society that is not facilitated or mediated by software, and industry leaders have proclaimed that "every company is now a software company". Furthermore, software presents an enormous boost to scientific progress, and underlies many of our critical infrastructure (like power, telecom, etc.).

However, the complexity of software continues to increase. The total volume of software is growing at an exponential rate. Software is omnipresent, but it remains extremely difficult to efficiently construct and maintain software, and to guarantee its correctness, reliability, and performance. Europe has been at the forefront with many innovations in software, but is now risking to get behind the curve. The ever growing size and complexity of software urgently requires new techniques and principles to address the software challenges of the future, to safeguard Europe's autonomy and sovereignty, and protect core values such as privacy, safety, fairness, and inclusiveness.

These problems won't solve themselves, but require fundamental research. Now is the time for increased funding of software research. To start a conversation and to raise awareness of the importance of software research, we (researchers from France, Finland, and the Netherlands) have written a call-to-arms document, and published it as an online petition. It has already gathered more than 800 signatures from researchers across Europe. If you think Europe needs strong software research too, please sign the petition here:

http://tiny.cc/strong-software.

Paris Avgeriou, Marieke Huisman, Jean-Marc Jezequel, Tomi Männistö, Tommi Mikonen, Romain Rouvoy, Alexander Serebrenik, Kari Smolander, Tijs van der Storm, on behalf of the national software engineering associations VERSEN, GDR GPL, and TIVIA.

Call for Participation

FMICS Conference at QONFEST 2021

Paris Online 24 to 27 August

The aim of the Formal Methods for Industrial Critical Systems (FMICS) conference series is to provide a forum for researchers who are interested in the development and application of formal methods in industry.

FMICS brings together scientists and engineers who are active in the area of formal methods and interested in exchanging their experiences in the industrial usage of these methods. The FMICS conference series also strives to promote research and development for the improvement of formal methods and tools for industrial applications.

FMICS is the ERCIM Working Group conference on Formal Methods for Industrial Critical Systems, and it is the key conference in the intersection of industrial applications and formal methods.

Topics include:

- Case studies and experience reports;
- Methods, techniques and tools;
- Verification and validation methods;
- Impact of the adoption of formal methods.

Keynote Speaker: Joe Kiniry (Galois Inc. and Free & Fair, US): "Haunting Tales of Applied Formal Methods from Academia and Industry"

The conference is held under the umbrella of QONFEST 2021 which also includes the conferences CONCUR, FORMATS and QEST

More information:
https://qonfest2021.lacl.fr/fmics21.php

ERCIM – the European Research Consortium for Informatics and Mathematics is an organisation dedicated to the advancement of European research and development in information technology and applied mathematics. Its member institutions aim to foster collaborative work within the European research community and to increase co-operation with European industry.

ERCIM is the European Host of the World Wide Web Consortium.

Consiglio Nazionale delle Ricerche
Area della Ricerca CNR di Pisa
Via G. Moruzzi 1, 56124 Pisa, Italy
www.iit.cnr.it

Centrum Wiskunde & Informatica
Science Park 123,
NL-1098 XG Amsterdam, The Netherlands
www.cwi.nl

Fonds National de la Recherche
6, rue Antoine de Saint-Exupéry, B.P. 1777
L-1017 Luxembourg-Kirchberg
www.fnr.lu

Foundation for Research and Technology – Hellas
Institute of Computer Science
P.O. Box 1385, GR-71110 Heraklion, Crete, Greece
www.ics.forth.gr

Fraunhofer ICT Group
Anna-Louisa-Karsch-Str. 2
10178 Berlin, Germany
www.iuk.fraunhofer.de

INESC
c/o INESC Porto, Campus da FEUP,
Rua Dr. Roberto Frias, nº 378,
4200-465 Porto, Portugal
www.inesc.pt

Institut National de Recherche en Informatique
et en Automatique
B.P. 105, F-78153 Le Chesnay, France
www.inria.fr

I.S.I. – Industrial Systems Institute
Patras Science Park building
Platani, Patras, Greece, GR-26504
www.isi.gr

Norwegian University of Science and Technology
Faculty of Information Technology, Mathematics and Electrical Engineering, N 7491 Trondheim, Norway
http://www.ntnu.no/

RISE SICS
Box 1263,
SE-164 29 Kista, Sweden
http://www.sics.se/

SBA Research gGmbH
Floragasse 7, 1040 Wien, Austria
www.sba-research.org/

SIMULA
PO Box 134
1325 Lysaker, Norway
www.simula.no

Magyar Tudományos Akadémia
Számítástechnikai és Automatizálási Kutató Intézet
P.O. Box 63, H-1518 Budapest, Hungary
www.sztaki.hu/

University of Cyprus
P.O. Box 20537
1678 Nicosia, Cyprus
www.cs.ucy.ac.cy/

Universty of Warsaw
Faculty of Mathematics, Informatics and Mechanics
Banacha 2, 02-097 Warsaw, Poland
www.mimuw.edu.pl/

VTT Technical Research Centre of Finland Ltd
PO Box 1000
FIN-02044 VTT, Finland
www.vttresearch.com

The second GATEKEEPER Open Call is out!
Join the GK community!

GATE
KEE
PER

The GATEKEEPER 2nd Open Call has been launched!

The main objective of the 2nd Gatekeeper Open Call is to extend the benefits of Gatekeeper platform beyond the boundaries of current pilots, expanding the Gatekeeper ecosystem. It aims to attract entities leading the landscape of digital data-driven technologies, such as Artificial Intelligence, Big Data, Data Analytics, etc. It also aims to attract new use cases, additional platforms, new pilot sites, patient organisations, with the objective of providing more robust, highly autonomous, personalised and collaborative quality and cost-efficient healthcare.

Key information:

Target:

- start-ups, SMEs, Midcaps, Industries and Research technology organisations
- Consortia of public and private entities
- Healthcare provider, regional healthcare authorities, private hospital groups, patient associations

Budget: 600,000€, with a maximum of 8 projects funded

Deadline: September 28th, 2021, at 5 pm CEST

Project duration: 12 months starting from November 2021

The GATEKEEPER project is an EU-funded initiative under the Horizon 2020 Framework Programme. Its main objective is to create a GATEKEEPER that connects healthcare providers, businesses, entrepreneurs, elderly citizens and the communities they live in. This connection between stakeholders will promote an open, trust-based arena for matching ideas, technologies, user needs and processes, aimed at ensuring healthier independent lives for older adults.

For more information:
https://www.gatekeeper-project.eu/open-call