eulisaroundtable.eu

Industry Roundtable
November 2021 - Report

Artificial Intelligence and Large-Scale IT Systems: Opportunities and Challenges

4 - 11 - 18 and 25 November 2021
Online Event

eulisaroundtable.eu

This report is public. Reproduction is authorised, except for commercial purposes, provided that the source is acknowledged.

eulisa.europa.eu

Catalogue number: EL-AN-21-002-EN-N
ISBN 978-92-95217-97-3
ISSN: 2600-2728
DOI:10.2857/870875

Table of Contents

Introduction 4

Session I - 4 November 2021. Artificial Intelligence for Advanced Data Analytics and Forecasting to Support Business Processes in the Area of Internal Security

Opening Remarks by Krum Garkov, Executive Director of eu-LISA 6
AI for Law Enforcement: The Slovenian Experience 7
Project Presentation: ITFLOWS – IT Tools and Methods for Managing Migration Flows 8
Q&A Session 9
Industry Presentations 10
- Fujitsu Technology Solution – ManageNow® Data Analytics 10
- Decisively Australia – Legislation to Execution. Automating Decision-making Processes 10
- Atos – Big Data Analytics for Risk Assessment in Border Management Context, Migration Analysis and Forecasting 11
- Almaviva Group – Artificial Intelligence Available Solutions for Justice and Home Affairs Challenges 11

Panel Discussion and Q&A 12

Session II - 11 November 2021. Privacy-preserving Approaches and Technologies for Data Analytics and AI

Keynote Presentation: Accountability for AI Use in the Area of Security 14
Industry Presentations 15
- Leonardo – Embedding Privacy in Data-driven Digital Transition Processes 15
- GMV – uTile PET 15
- secunet Security Networks – Privacy by Design 16

Panel Discussion and Q&A 17

Session III - 18 November 2021. Artificial Intelligence in IT Operations – AIOps

Industry Presentations 19
- NTT Data – AIOps as Autonomous IT Operations Facilitator 19
- PWC EU Services – Shared AI Platforms. Experience from European Piloting 19
- Sopra Steria Benelux – AI for IT Ops 20

Session IV - 25 November 2021. Artificial Intelligence in Biometric Recognition Technologies

Project Presentations 22
AI Supporting the Evaluation of Face Recognition Technology 22
Technology Foresight on Biometrics for the Future of Travel 23
Industry Presentations 25
- IDEMIA – AI & Biometrics 25
- Fujitsu – Palm Secure: Use Your Hand to Unlock the World 25
- Mobai – Industry Perspective on Face Morphing and Mobile ID Checks 26
- secunet Security Networks – Morphing Attack Detection in Practice 27

Panel Discussion and Q&A 28
Closing Remarks 30

Introduction

Throughout November 2021, eu-LISA, in collaboration with the Slovenian Presidency of the Council of the EU, hosted its 14th Industry Roundtable under the title “Artificial Intelligence and Large-Scale IT Systems: Opportunities and Challenges”. The event, conducted entirely online, brought together over 310 participants from 39 countries, representing international border management and security companies, EU Member State authorities, EU Institutions and JHA Agencies, as well as representatives of NGOs and academia.

The event took place in four sessions focusing on different applications of artificial intelligence and privacy-preserving technologies, including:

1) Artificial Intelligence for Advanced Data Analytics and Forecasting to Support Business Processes in the Area of Internal Security

2) Privacy-preserving Approaches and Technologies for Data Analytics and AI

3) Artificial Intelligence in IT Operations – AIOps

4) Artificial Intelligence in Biometric Recognition Technologies

This summary report provides an overview of the academic and industry presentations, as well as stimulating discussions that took place during the event.

Session I

Artificial Intelligence for Advanced Data Analytics and Forecasting to Support Business Processes in the Area of Internal Security

4 November 2021

Opening Remarks by Krum Garkov, Executive Director of eu-LISA

Mr Krum Garkov, Executive Director of eu-LISA, welcomed the participants of the Industry Roundtable emphasising that Artificial Intelligence (AI) is one of the key priorities for political decision-makers in the EU. In order to understand the importance of AI as a disruptive technology, it needs to be considered in the broader context of digital transformation. In recent years, and in particular since the onset of the pandemic, all areas of our lives have moved online and become increasingly digital. Mr Garkov illustrated this statement by mentioning that, for example, 90% of data available on the internet today, was created in the past three years; every minute more than 300 hours of video content is uploaded on YouTube; current prototypes of driverless cars that are heavily reliant on AI, generate 1 Gb of data per second; this year alone, 1.4 billion smartphones will be shipped worldwide; and in the next five years, there will be more than 50 billion connected devices. These are still rather conservative estimates, considering the exponential development of digital technologies.

Mr Garkov continued his introductory remarks stating that the implementation of AI is not a technical issue – the technology exists and it often works. However, in order to ensure that AI is implemented in a robust manner, we need to have a solid and flexible legislative framework in place, that is encouraging rather than restrictive when it comes to the implementation of AI solutions, while also providing balance between the capabilities of AI and the respect of fundamental rights, privacy, data protection, equality and non-discrimination, etc. Mr Garkov stressed that all technologies, and their implementation, are as successful as the level of trust in their capabilities in the society at large. Building on that, eu-LISA welcomes the proposed regulatory framework for AI presented by the European Commission in April 2021.

Focusing on the importance of AI for the domain of justice and home affairs, Mr Garkov mentioned a few important use cases for the implementation of AI, which include: automation of routine tasks and repetitive processes that need to handle large amounts of data; automated translation; advanced analytics; in-depth risk analysis, etc. Ultimately, AI has a great potential to increase the efficiency of border guards, law enforcement officers, migration officers and the judiciary across Europe.

Going forward, Mr Garkov emphasised that AI is not a threat in itself, as it will not replace border guards or police officers, but will help them to be more efficient and make better decisions. Therefore, when it comes to regulations, it is important to bear in mind that they focus on the specific application of technologies, not technologies themselves. eu-LISA is and will continue to be at the heart of these new and exciting developments, in particular by identifying AI application use cases and implementing relevant solutions in our domain of responsibilities. To that end, the Agency is committed to evolve as a centre of excellence for AI in the JHA domain, as recently proposed by the Commission, and will continue building the necessary capabilities. Undoubtedly, the Agency will not be able to do this alone, but only in close cooperation with the Member States, European Institutions and the industry.

In conclusion, Mr Garkov stated that now is the time to act, with a view to developing the EU's strategic independence in this domain. In order to do that, Mr Garkov suggested, we would need to tackle three issues that lie in the way to successful implementation of AI solutions. First, we need to ensure that the regulatory framework at the EU and MS level is in alignment with the capabilities of AI, and enables rather than prevents the adoption of AI solutions. Second, we need to invest substantial resources in training and capacity building of practitioners who will be applying AI in their daily work, because the benefits can only be reaped when users understand how AI works and what are its limitations. Finally, and most importantly, we need to build trust within society, that AI capabilities will bring added value, improve internal security and access to justice, make border management more efficient, while also ensuring that these capabilities are applied in an ethical and lawful manner. Failing to address these challenges will limit our ability to reap the benefits inherent in AI.

AI for Law Enforcement: The Slovenian Experience

Mr Aleksander Pur, Senior Police Superintendent, IT and Telecommunications Office, Slovenian Ministry of the Interior

Mr Aleksander Pur, Senior Police Superintendent from the Slovenian Ministry of Interior, welcomed the participants on behalf of the Slovenian Presidency of the Council of the EU. In his opening remarks, Mr Pur presented an overview of the Slovenian experience in using AI for law enforcement purposes. He emphasised that Slovenian authorities have long recognised the importance of AI and have supported the Commission in this endeavour by organising a workshop on AI for law enforcement.

Setting the scene, Mr Pur suggested that due to the large amount of information that is being produced every minute, including by numerous cameras and sensors, AI is becoming indispensable for the effective performance of duties by law enforcement authorities. Mr Pur continued by outlining the definition of AI systems according to the proposed AI Act, which includes a wide range of software based on novel machine learning techniques including deep learning, as well as older approaches such as expert systems. This means that many systems used by law enforcement authorities for investigative purposes, can be classified as high-risk systems that must meet specific requirements. The strength of AI systems lies in the fact that they can uncover hidden relationships by analysing large amounts of data from various sources, thereby improving the efficiency of investigations by identifying relevant information in large amounts of unstructured data. At the same time, the main weakness of AI is that their decisions are not always reliable nor explainable. Therefore, Mr Pur argued, important decisions must be based on transparent AI systems and all information must be confirmed by humans.

Mr Pur continued his presentation stating that on the one hand, AI systems provide opportunities for improving performance of law enforcement and public security. On the other hand, unethical and illegal use of AI systems brings new threats, such as deepfakes, or misuse of AI by terrorist groups and organised crime. The easiest way to address these threats would be to ban AI systems. However, in that case we would also prohibit the use of AI applications that can help identify victims of sexual abuse. Hence, the easiest way is not always the best way. Therefore, Mr Pur argued, we need to improve our understanding of AI. To illustrate his point, he offered the following example – machine learning systems often rely on historical data to predict the future; however, in crime, the modus operandi can change daily, and therefore patterns from the past are not necessarily relevant in the future. Mr Pur stated unambiguously that we need to steer clear from black-box solutions that provide outputs that cannot be explained. However, this doesn't mean that we should abandon AI as such, as there are numerous techniques that provide transparent and explainable results. When used appropriately, such techniques are almost risk-free. Therefore, he argued, understanding different AI techniques is paramount for their effective implementation in an ethical and trustworthy manner.

To expand on this argument further, Mr Pur offered an example of a system-based on machine learning techniques for named entity recognition, which helps investigators identify links between different natural persons and legal entities in a large corpus of unstructured data. According to the proposed AI Act, such a system would still be classified as high-risk, despite the fact that the system only provides input for human decision-making process. Furthermore, AI systems can in fact enhance privacy, for example, by anonymising documents through the removal of named entities.

Mr Pur also presented an example focused on the Advance Passenger Information (API) and Passenger Name Records (PNR) data and the identification of suspicious passengers using historical data. Here, the AI system is used to detect patterns that are then used as additional information by the passenger information unit to identify whether certain passengers might pose a threat or not.

Concluding his presentation, Mr Pur emphasised that today we cannot imagine law enforcement authorities without AI, because nowadays, investigating criminal activity involves huge amounts of data. The proposed regulatory framework for AI will result in a significant increase in paperwork needed to clear the use of high-risk AI Systems. Ultimately, proper understanding of the functioning of AI systems is necessary for the ethical and trustworthy application of AI systems in law enforcement.

Project Presentation: ITFLOWS – IT Tools and Methods for Managing Migration Flows

Dr Cristina Blasi, Autonomous University of Barcelona

Dr Cristina Blasi Casagran is assistant professor in EU law at the Autonomous University of Barcelona, and she holds a PhD in Law from the European University Institute (Florence, 2015) where she specialised in EU privacy and data protection law. Dr Blasi is currently coordinating a H2020 project IT Tools and Methods to Manage Migration Flows (ITFLOWS)[1] and that was the topic of her presentation which opened with a short video presentation[2] outlining the key objectives of the project.

ITFLOWS is a H2020 project aiming to provide accurate predictions and practical management solutions for migration flows in the EU in the phases of reception, relocation, settlement and integration. The project, which was launched in September 2020 and will run until 2023, is currently in the early development stage, focusing on the collection of data that will be used in the development of a user-friendly IT tool – the EUMigraTool – created to support NGOs and municipalities in assisting migrants arriving to the EU. For policymakers, the project will translate the results of the data analysis and the developed solutions into practical policy recommendations distributed in the form of policy briefs.

The EUMigraTool has two main objectives: first, to offer accurate predictions of migration flows; second, to identify tensions and potential violence between migrants and local citizens in EU Member States.

a) When it comes to predicting migration flows, the project focuses on the countries that have historically been major sources of migration into the EU, intending to identify the drivers of migration from these countries. In addition, the project also analyses the countries that are targets of migration flows, namely Greece, Italy and Spain, delving into the specific reasons why these particular countries are most frequently chosen as main destinations. The data collected in the framework of this project will serve as input for the development of predictive algorithms. The preliminary objective is to predict migratory flows at least one week in advance, with the ultimate goal of making predictions for up to 1 month in advance by the project's end.

b) The component developed for the prediction of tensions will focus on three Member States, namely Greece, Italy and Spain, and will use sentiment analysis techniques in order to identify the general sentiment around the topic of migration. This will be done using a wide range of data sources, including data on public attitudes collected via regular surveys, as well as real-time data, such as data collected from Twitter, Google trends, and GDELT[3] which is particularly helpful in identifying large-scale events, such as natural disasters and protests that may trigger migration flows.

In order to ensure that the EUMigraTool meets the requirements or user-friendliness and minimal technical knowledge, the project has engaged a number of NGOs and municipalities who serve on the project's board and will be actively involved in testing the tool once it's ready. In addition, the project has also set up a policy working group that will be supporting the project from the policy perspective.

Dr Blasi continued her presentation with an overview of simulations of public sentiment towards migration, which can be used by municipal authorities and NGOs in re-location and integration efforts. Additionally, Dr Blasi also presented an analysis of data from refugee camps that can be used by national authorities in identifying best approaches for handling migrants depending on their age group, gender, etc. Concluding her presentation, Dr Blasi mentioned that in June 2022 the project will organise a workshop in Brussels for EU policymakers from Member States and institutions, as well as NGOs operating in the field of migration.

[1] For more information, please visit the official website of the ITFLOWS project itflows.eu
[2] The video is available online using the following hyperlink: youtube.com/watch?v=2KVKWuSQSZo
[3] Global Database of Events, Language and Tone gdeltproject.org

Q&A Session

The first question focused on whether the developed models will factor in the impact of extreme events such as military conflicts, and what role will AI play in such cases.

Dr Blasi responded that the project is currently collecting data, including data on different conflicts, that will be used to develop models to provide insights on the impact of extreme events (e.g., military conflicts) on migration flows. Dr Blasi went on to further explain that the tool would benefit from a manual entry system that would allow adding various events as they happen.

The second question inquired whether the EUMigraTool will be adaptable to other countries of origin and destination of irregular migration that are currently not included in the project.

Dr Blasi confirmed that the EUMigraTool will be adaptable to other countries as well. Since it is impossible to address all EU countries within the scope of one project, the countries were chosen for practical reasons and based on discussions with experts. After the project is completed, the scope will be expanded to all 27 EU Member States, as the main aim of the project is to provide a practical tool for NGOs that operate across the EU.

The final question addressed the issue of using Twitter as one of the main data sources, while excluding other social media platforms. Was this a data-driven choice based on the use of specific platforms in chosen Member States?

Dr Blasi argued that Twitter was chosen as a relevant data source, as it provides information on the intentions of potential migrants, as well as on attitudes towards migration in the countries of destination. Ultimately the ambition is to include other social media platforms to provide a more comprehensive picture of both of migrant intentions and risks of tensions.

Industry Presentations

Fujitsu Technology Solutions – ManageNow® Data Analytics

Mr Fritz Benker, Head of Platforms Operation Service Central & Eastern Europe

Mr Fritz Benker presented Fujitsu's ManageNow data analytics platform that integrates a variety of structured and unstructured data sources in a data lake, enabling to run nearly real time analytics with interactive dashboards. The solution features a wide variety of data analytics tools and methods (both statistical and AI/ML), as well as predictive capabilities that can be used for predictive analytics in the operation of diverse systems. ManageNow can be deployed as a software-as-a-service (SaaS) either on a private or on a public cloud, and also onsite at the customer's data centre.

Considering that ManageNow is a data analytics platform, data scientists can deploy ML/AI models developed in different environments, such as R or python, and use the interactive dashboards for presenting the outcomes of their predictive analytics. However, it is important to note that ManageNow is not an AI development environment.

Using a range of open source technologies that provide the necessary functionalities, Fujitsu developed an enterprise-level solution that is highly scalable, allowing the addition of new nodes to the cluster without downtime. As a result, ManageNow solution can be run on a 24/7 basis, as updates can be installed without disrupting the workflows.

At the end of his presentation, Mr Benker introduced a few use cases, including one focused on IoT (Internet of Things) operations, which integrates dedicated IoT components relevant in industrial manufacturing, such as Bosch and Schneider Electric.

Decisively Australia – Legislation to Execution. Automating Decision-making Processes

Mr Joel Nation, Chief Technical Officer

Australian company Decisively focuses on helping the public sector make better decisions using artificial intelligence. Mr Nation opened his presentation outlining some of the challenges for modern public sector IT systems. First, most of these systems operate as black boxes, resulting in scepticism towards the decisions made. Usually such systems, even if they are rules-based, are developed by IT programmers, which raises questions of transparency. As a result, there is often doubt whether the decisions made using automated systems are actually in line with legislative intent and current regulations.

Another problem is that the standard approach is rather slow, often taking the double amount of time to develop a system as it takes to get legislation through parliament. In addition, rules tend to change quite frequently, meaning that the systems need regular updates. As exemplified by the COVID-19 pandemic, rules can change very quickly, in particular when it comes to borders and health. Therefore, we need to develop ways to implement such changes quickly, and analyse their impact on decision-making processes in IT systems. What is more, in this process it is important to ensure traceability, i.e. to ensure that automated decisions can be traced back.

Decisively has essentially decided to approach such rules as a service, providing a centralised service that different systems can use to make accurate, transparent and auditable decisions, as compared to the current approach where different systems operate based on different rules that are often hard to track and reconcile. Mr Nation explained that Decisively relies on natural language in legislation to encode rules that will be used in decision-making systems, allowing decisions to be linked directly back to a specific provision in a legislative act.

Continuing his presentation, Mr Nation outlined additional functionalities featured in the Decisively system, such as the possibility to perform counterfactual or 'what if' analysis, enabling to evaluate policy changes in terms of their effectiveness and efficiency. The rules-based system can also be complemented with an AI component, for example, to perform risk assessment in visa application procedures, where an AI system can analyse the behaviour of the applicant in real time in order to identify whether the applicant is trying to game the system. Other functionalities of the system include integration with financial analytics tools that can perform simple automated analyses of bank account transaction data; document analysis using OCR and natural language processing in order to identify potential fraud; entity matching across different documents, all of which are particularly relevant in the context of processing visa applications. Concluding his presentation, Mr Nation stated that Decisively does not use AI for automated decision-making, instead, AI is used to support the decision-making process by providing relevant information and risk assessment.

Atos - Big Data Analytics for Risk Assessment in Border Management Context, Migration Analysis and Forecasting

Mr Michel Jardon, Public Sector Solution Manager

Mr Jardon opened his presentation with an overview of the Atos approach to integrated border management, which is divided into three pillars: control points at borders, unregulated borders, trade and customs. The technologies developed by Atos were introduced by way of specific case studies. First, the asylum management case in Germany, where Atos provided the German Federal Office for Migration and Refugees with a system for asylum seeker validation to be used in cases when documents are incomplete or missing. The system integrates voice and dialect recognition, face recognition, as well as using the asylum seeker's mobile phone to validate their origin in a multi-factor validation process. When it comes to language/dialect recognition, the system can distinguish between 22 languages and six dialects of Arabic.

Continuing his presentation, Mr Jardon introduced an AI use case focusing on computer vision solutions for regulated and non-regulated border crossing points that can be implemented in different scenarios with CCTV cameras, such as airports, public spaces, green borders, etc. The system, based on object identification with pre-defined scenarios, is able to detect and monitor movement of people and goods (e.g. unattended luggage in airports or abandoned vehicles in public spaces) and is can be trained to identify certain objects and the pre-defined scenarios in video stream.

Going forward, Mr Jardon provided an overview of a data platform for implementing different data analytics solutions, including those mentioned before. The data platform is built around micro-services architecture, and incorporates a wide range of supporting technologies such as federated AI, edge computing and blockchain, where those are relevant. Mr Jardon closed his presentation with a discussion of ethical applications of AI as an essential component when considering the implementation of AI. In particular, Mr Jardon emphasised that before we develop and deploy an AI system, we should consider whether the technology will be used to benefit the public, whether the use of data is legitimate or are there possibilities for misuse, and whether data analytics provides the necessary evidence that is unbiased and explainable.

Almaviva Group - Artificial Intelligence Available Solutions for Justice and Home Affairs Challenges

Ms Giulia Zimei, International Business Development Manager
Mr Fabio Previtali, AI Solution Architect & Davide Buscaglia, Global Sales Account Manager

AlmavivA Group is one of the major and longstanding IT service providers for the Italian Government and Public Administration, in the areas of internal security, law enforcement and cyber security, pursuing innovation by integrating and evolving complex legacy systems with emerging technologies. Ms Zimei outlined the overall scope of activities of Almaviva Group in the area of data analytics and AI, focusing on two central aspects of the JHA domain: a) visa process digitalisation, and b) data management and semantic ontology data models.

For the visa process digitalisation, Almaviva has developed an AI training and learning automation platform (T&LA), enabling the automation of the ML process from the first stage of acquiring data to the deployment of a model in production. The platform incorporates the full range of machine learning algorithms, starting from the classical random forest to artificial neural networks. The platform also allows for automatic monitoring of models in production, removing the requirement for manual interventions.

This AI platform was further introduced through three use cases. First, automatic document validation that checks the document's validity, incl. names and personal identity numbers. Second, document coherence validation that performs an automated consistency check across all documents submitted by the applicant, including whether the sequence of document submission is correct and pattern identification to ensure that the documents are valid. Third, automatic verification of submitted photos for aging, masking, etc., using convolutional neural networks to identify changes.

In the final part of the presentation, Mr Buscaglia gave an overview of the solutions focusing on data management and semantic ontology data models that can be used to query data lakes containing structured and unstructured data using natural language. The proposed solution provides an overview of all possible connections related to a specific entity (e.g. an individual crossing a border that may be of interest to authorities). Concluding the presentation, Mr Buscaglia pointed out that the AI solutions provided by Almaviva can be integrated with voice biometrics and speech recognition.

Panel Discussion and Q&A

The concluding panel discussion on using AI for advanced data analytics in the area of internal security was led by Mr Igor Taranic, Senior Research Officer at eu-LISA.

First, the issue of trust and social acceptance of AI was addressed.

Mr Jardon (Atos) drew a connection to larger public mistrust in government and advocated for increasing trust in government to help citizens realise that innovative technologies, such as AI, can be used for the common good, e.g., identifying disturbances in public areas using video streamed data from CCTV. When talking about deploying the Fujitsu dashboard system in the border management context, Mr Brenker replied that this area of application is very similar to law enforcement. The quality of dashboards ultimately depends on the quality of input data that is behind the dashboard.

The discussion continued with a question addressed to Decisively, focusing on AI capabilities that need to be developed to enable AI to interpret legislation.

Responding to this question, Mr Nation (Decisively) indicated that two aspects must be taken into consideration. First, there is not enough legislation for training AI systems. Second, legislation is very specific about requirements and conditions that need to be met in order make a certain decision. Therefore, we need to be able to test these AI/ML solutions and verify that they make the right decisions according to the rules contained in the legal acts.

Next, the panel discussed the use of mobile/smart phones for identity validation.

Mr Jardon (Atos) explained that mobile phones are used for identity verification of asylum applicants only in cases where other means of verification are not available. Such identity verification is voluntary and uses only data that has been posted publicly (e.g. social media posts). A follow-up question addressed the challenge of dialect verification to which to Mr Jardon (Atos) responded that the accuracy of dialect detection for Arabic is very strong, but this system is always used in combination with a human translator.

Finally, the panellists discussed the areas where AI deployment is not yet possible.

Mr Nation (Decisively) suggested that the implementation of AI application ultimately comes down to risk tolerance of decision-makers. In some areas, e.g., child protection or long-term visa applications, mistakes can be very costly, although the number of decisions steps is not that large and therefore the use of AI is not justified. In contrast, AI systems can be deployed relatively safely in processing visa applications of regular travellers or tourists where associated risks, including wrong decisions, are relatively low. Mr Brenker (Fujitsu) seconded the point, arguing that we should avoid the application of AI in areas where its efficiency has yet to be proven and where errors in automated decision-making can have serious consequences for individuals. Mr Nation (Decisively) followed-up explaining that a significant number of tasks can be automated in any area, e.g., analysis of document authenticity, biometric matching, etc., and AI is useful in reducing the human workload related to such routine and repetitive tasks. However, we should steer clear from using AI in areas and tasks where human decisions are indispensable, which on average constitute a relatively small share of all tasks.

Session II

Privacy-preserving Approaches and Technologies for Data Analytics and AI

11 November 2021

Keynote Presentation: Accountability for AI Use in the Area of Security

Prof. Dr Saskia Bayerl, Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research (CENTRIC)

Dr Saskia Bayerl is a Professor of Digital Communication and Security at the Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research (CENTRIC). Her research interests lay at the intersection of human-computer interaction, organisational communication and change, with a special focus on ICT implementation, privacy, and the management of transparency.

Prof. Bayerl gave a presentation of her research into accountability principles for AI (AP4AI Framework). The objective is to develop a robust set of agreed and validated framework of accountability principles for AI, integrating a wide range of inputs from practitioners to regular citizens. Ultimately, the aim is to develop a practical compliance and assessment tool for security practitioners. The core consortium of the research project comprises CENTRIC, Europol, Eurojust, and the European Union Agency for Fundamental Rights.

The AP4AI Framework project is divided into three distinct cycles. First, expert consultations (25 countries) and review of state of the art (corpus of 135+ documents) to lay the groundwork. Second, citizen consultations in the form of an online survey with approx. 6000 citizens from 30 countries (EU MS, UK, USA, Australia), and in the final stage, framework validation by subject-matter experts. Currently, the first cycle is near completion and preparations are underway for commencing citizen consultations.

The focal point of Prof. Bayerl's research is the need for an AI assurance framework in order to develop public trust in a system that carries considerable risks and harms. To be effective, accountability must be bound to enforceable obligations, making it actionable. In a nutshell, accountability provides a practical mechanism to ensure that legitimate interests (as well as concerns, fears and hopes) of all stakeholders are factored in throughout the full decision-making process about the AI capabilities used by law enforcement agencies.

While there are some existing AI frameworks developed by, for example, the European Parliament, Council of Europe, OECD, Interpol and several national governments, e.g., UK, Australia, Canada, Germany, etc., perhaps the most comprehensive is the one prepared by the European Commission's High-Level Expert Group on AI. In 2019, this group pinpointed accountability among seven key principles for AI, defining it as mechanisms to ensure responsibility and accountability for AI systems and their outcomes.

Finally, Prof. Bayerl introduced some select propositions stemming from her research, such as having a double structure on EU level and national level (e.g., akin to the human rights framework), broad compliance by organisations with appropriate remedies in place for individuals, exceptions for emergencies, although generic 'national security' justifications would not be acceptable as they are too vague.

In her concluding remarks Prof. Bayerl stressed that this is not a one-off effort and going forward, she is looking into the creation of support mechanisms for AP4AI assessments, in conjunction with continuing consultations and evaluations for updates and improvements.

During the subsequent Q&A session, Prof. Bayerl addressed questions regarding accountability and AI.

The first question inquired about balancing accountability and innovation in AI.

To start, Prof. Bayerl stressed the need to distinguish between using AI in specific high-risk domains and a universal approach to AI. On the other hand, accountability should not be seen as counter to innovation. In fact, the two are closely intertwined because accountability entails responsibility to keep improving the systems for increased benefits. So actually, accountability and innovation complement each other.

The second question addressed the issue of high-risk systems and the need for more rigorous accountability in such contexts.

According to Prof. Bayerl, in such cases it is paramount to ensure proper governance and conduct a thorough analysis of the risks. All innovation entails risk, but we must decide what risks we are willing to take and who will carry the risks – those are issues that must be addressed and injustices redressed. Another good question to ask is what are the risks or consequences if we don't go forward with the proposed innovation. Elaborating on a question from the audience with regard to who defines the risks, Prof. Bayerl stressed that risks must be defined collectively by involving different groups.

When asked whether accountability might limit AI,

Prof. Bayerl argued that it is not a limiting approach at all, and the aim is to set it up as an empowering approach that ensures the use of AI in a way that doesn't create any problems. As such, accountability is an important part of responsible AI use, offering a valuable framework to guide operation and further development.

Industry Presentations

Leonardo – Embedding Privacy in Data-driven Digital Transition Processes

Ms Arianna Pedrini, Security Governance (EU Institutions and Agencies)

Leonardo is a global technology company operating in the areas of aerospace, defence and security, offering global security solutions for both military requirements and civil applications, ensuring the security and resilience of physical and digital infrastructures via complete protection against hybrid threats and critical events.

Modern organisations faced with an increasing amount of different norms and they need a one-stop-shop solution for managing an increasing variety of risks. Ms Pedrini presented several compliance risk assessment tools that ensure accountability by design and come with embedded data protection features, pre-defined checklists, alerts, etc. These tools are well-suited to monitor processes over longer periods and generate recommendations for devising prioritised action plans.

For operations, Leonardo has developed an AI decision support system (DSS), a cybersecurity platform that provides real-time dynamic overview and situational awareness, making use of AI to pull together different sources of data to support decision making. Given an infrastructure to monitor, AI DSS collects, correlates and analyses data to build a comprehensive overview of cyber risks, providing organisations with decision-making support that helps ensure business continuity and minimising cyber impacts.

Another data protection tool developed by Leonardo is the Privacy Query Platform (PQP) – a data protection layer based on Machine Learning/Natural Language Processing that can be used to safeguard citizen privacy for datasets that are accessed by external entities for statistical or research purposes.

GMV – uTile PET

Mr Luis Grañana Martín, Business Partner & uTile Product Owner

Mr Grañana's presentation focused on data protection solutions in the context of data-sharing. GMV has developed a tool called uTile that facilitates secure data-sharing between organizations, allowing machine learning (ML) algorithms and analytical models to be developed by using sensitive data from distributed sources. In addition, it enables making secure calculations based on distributed sensitive data without exposing or moving it.

With uTile, ML models are trained locally using federated learning. Federated learning is an algorithmic solution that trains ML models by sending copies of a model to the place where data resides and performing training at the edge, thereby eliminating the necessity to move large amounts of data to a central server for training purposes, i.e., raw data never leave host premises and all connections are run through coordination nodes.

To provide stronger security guarantees to data owners, uTile uses Secure Multi-Party Computation (SMPC) and Private Set Intersection (PSI), a powerful cryptographic technique which enables interested parties to find intersections between their datasets without exposing their raw data to the other party (such as location, ID, card number, etc).

During his presentation, Mr Grañana presented several use cases. For instance, an example of federated learning where a central server orchestrates the training of a model based on input from three data owners. Another example was of encrypted inference where the data owner requests an inference result from the model over the Internet but retains the confidentiality of patient data. Other applications include, for example, data owned by independent entities or different units within the same entity in various jurisdictions or confidential data about the same type of entities/objects distributed across silos, etc.

secunet Security Networks – Privacy by Design

Mr Dominik Lawatsch, AI Business Development Manager
Ms Sina Youn, Senior Privacy & Technology Strategist @ brighter.AI

secunet is Germany's leading cyber security company, offering a combination of products and consulting services, including extensive expertise in sophisticated and sustainable border control solutions for capturing and processing biometric data, as well as solutions for mobile identity checks and verification.

Mr Lawatsch presented an overview of AI solutions developed by secunet for anonymised image and video analysis using privacy-focused artificial intelligence to demonstrate how to reconcile the use of photo and video data with data protection requirements.

To train AI models, we need large amounts of data that is as free as possible from artefacts. However, the storage and processing of such personal data is subject to restrictions, although GDPR (recital 26) allows for an exception for anonymous information.

The solution developed by secunet – Deep Natural Anonymization – uses AI-based anonymization that detects and replaces captured face imagery automatically with artificially created natural-looking "masks", thereby removing personal data and resulting in natural, high-quality anonymization of persons. As a result, the evaluability of metadata remains intact while the protection of personal identity is ensured. For example, compared to precision blurring which is re-constructible, Deep Natural Anonymization leaves sociographic and situational features intact, and is not re-constructible.

Panel Discussion and Q&A

The concluding panel discussion focusing on privacy-preserving technologies for data analytics was led by Dr Aleksandrs Cepilovs, Capability Building Officer - Research and Development at eu-LISA.

The panellists discussed whether it is possible to ensure complete privacy and data protection using current technologies.

The panellists agreed that protection is never 100% guaranteed and the risks are always there. In this situation, it is important to find the right balance between risks and benefits. Standards and regulations (e.g. anonymization) can help in this regard by providing a guiding framework and AI can help in achieving these objectives (e.g. federated learning) by delivering a very high level of data protection. As such, public sector can lead the way and promote these kinds of technologies for the benefit of society. Considering the EU's achievement in its approach to data protection, the next step could be certification to ensure public trust in AI systems.

Subsequently, the panellists were asked to elaborate on the topic of federated learning and its applications.

The panellists were in agreement that the most suitable approach is determined by individual use cases. For example, GMV using AI federated learning in combination with Secure Multi-Party Computation (SMPC). In addition, the panellists found that federated learning has great potential, especially since it creates opportunities for international cooperation by facilitating data-sharing from distributed sources. However, in such instances it is important to balance privacy and security considerations with performance needs, with one panellist suggesting synthetic data built by AI as a possible solution.

Lastly, a question from the audience regarding anonymized images and videos, specifically how to prevent accidental similarities with real persons (or license plates).

Responding to this question, Mr Lawatsch and Ms Youn (secunet) explained that secunet's Deep Natural Anonymization technology automatically anonymizes faces and licence plates in images and videos while retaining relevant visual information and context intact. In theory this means that contextual information could be used to identify anonymized objects but the probability of that exact licence plate in combination with that exact car type occurring in real life or being traceable is extremely low. In case of anonymization, the threshold is at the difficulty of reconstructing the original identity, which must require high effort.

Session III

Artificial Intelligence in IT Operations – AIOps

18 November 2021

Industry Presentations

Moderated by **Ms Anna Beata Kolodziej,** IT Officer, Business Relations Management Sector, eu-LISA

NTT Data – AIOps as Autonomous IT Operations Facilitator

Mr Luis Cancela Vallespín, Manager, Infrastructure & Cloud Services

Mr Vallespín's presentation focused on how AIOps can drive operational excellence trough the optimisation of technology and operations. In this context, an important concept is IT operations maturity. By evaluating the maturity level of IT operations, it is possible to chart a course to achieve the highest level of maturity – autonomous service. The first step towards autonomous IT operations is digitalisation through transforming IT processes by eliminating routine work. This stage entails IT service orchestration (incl. service catalogue automation) and defining IT operations as architecture (incl. standard frameworks) to yield such benefits as cost reduction, agility, scalability and overall quality improvement. The next step is AIOps as the key facilitator for autonomous IT operations by combining big data and AI functionality to provide data-driven decisions and trigger digital operations routines. As a result, it automates broad range of operational processes and tasks, incl. performance monitoring, event analysis, service management, and automation.

Thus, autonomous operations are achieved by combining digital operations with AIOps to achieve operational excellence. This is done in three stages. First, data is aggregated, then analysed, and finally, the results are acted upon, i.e., automated pattern discovery, anomaly detection, root cause determination, prescriptive advice, etc.

Mr Vallespín's went on to outline six main benefits of AIOps platforms: 1) better causality (to identify probable causes of incidents), 2) reduced noise (e.g., false alarms), 3) data-driven decision-making, 4) proactive problem resolution, 5) improved anomaly detection 6) extrapolation of future events to prevent potential breakdown.

Next, Mr Vallespín presented several AIOps use cases for IT service management (incl. auto triage, etc.), for operations and support (incl. end-to-end monitoring, automated root cause analysis, anomaly detection, capacity management, etc.), and for service desk support, AIOps provides digital assistant (chatbots) that helps save 30% of time dedicated to end-user requests. Overall, AIOps contributes to incident avoidance and improves resolution time (40%).

To conclude his presentation, Mr Vallespín presented an operational intelligence solution developed by NTT Data – Flens, a real-time modular and multilayer Big Data solution that enables the application of AI to each business layer for making predictions and identifying anomalies. Its automated decision-making enables achieving maximum operational efficiency and productivity, while also reducing operational noise and complexity.

At the end of the presentation Mr Vallespín was asked to give a real example how AI has helped pro-actively, and he responded that the main advantage is in the anticipation of anomalies. Also improved capacity management as a result of constant analysis of data, which enables better planning of resources.

PWC EU Services – Shared AI Platforms. Experience from European Piloting

Mr Andreas Braun, Director, PwC Luxembourg

Mr Braun provided an overview of the collaborative Advanced Data Analytics Platform developed for the European Commission, a process covering the whole chain from prototyping to active use. The objective was to develop a central AI solution for risk assessment that feeds from a multitude of distributed data sources and must interface with systems at different IT maturity levels.

The result was an onsite collaborative AI platform based on an "Infrastructure as Code" composed of +40 servers, offering seamless integration of 15 open source and proprietary solutions, built around a tailor-made portal and the common goal to work on advanced AI matters.

The platform includes the following key features: 1) strong data governance and platform security (secure and hermetic projects environment with restricted access); 2) vendor agnostic, allowing all components to be replaced; 3) near-real time processing supports time-critical decision-making; 4) multi-data source integration, incl. external systems managed by other parties; 5) collaboration between different stakeholders with secured access control; 6) production-ready.

The developed AI platform enables the Commission to support MS in the design and implementation of real use cases, where added value can be derived from AI advanced analytics and near real-time analyses, e.g. tailored reports and dashboards for crisis management, machine learning capabilities, etc.

Having concluded his presentation, Mr Braun was asked to elaborate on the mechanism to protect restricted data. Responding to this question, Mr Braun pinpointed data virtualisation and data encryption as key elements of data protection. By design, all created datasets are made available only to the designated user group. There's no such thing as public data by default, and access is granted only on a case-by-case basis. All data is restricted, and opened up only upon necessity to select users.

Sopra Steria Benelux – AI for IT Ops

Mr Simon Marsol, Director Public Sector
Mr Thierry Luc, CTO - Infrastructure and Security Services

Sopra Steria is a European leader in digital transformation with a comprehensive portfolio of end-to-end service offerings: consulting, systems integration, software development, infrastructure management and business process services. In the internal security domain, Sopra Steria contributes to further developing centralised databases and services around border control and migration, both for EU institutions and MS.

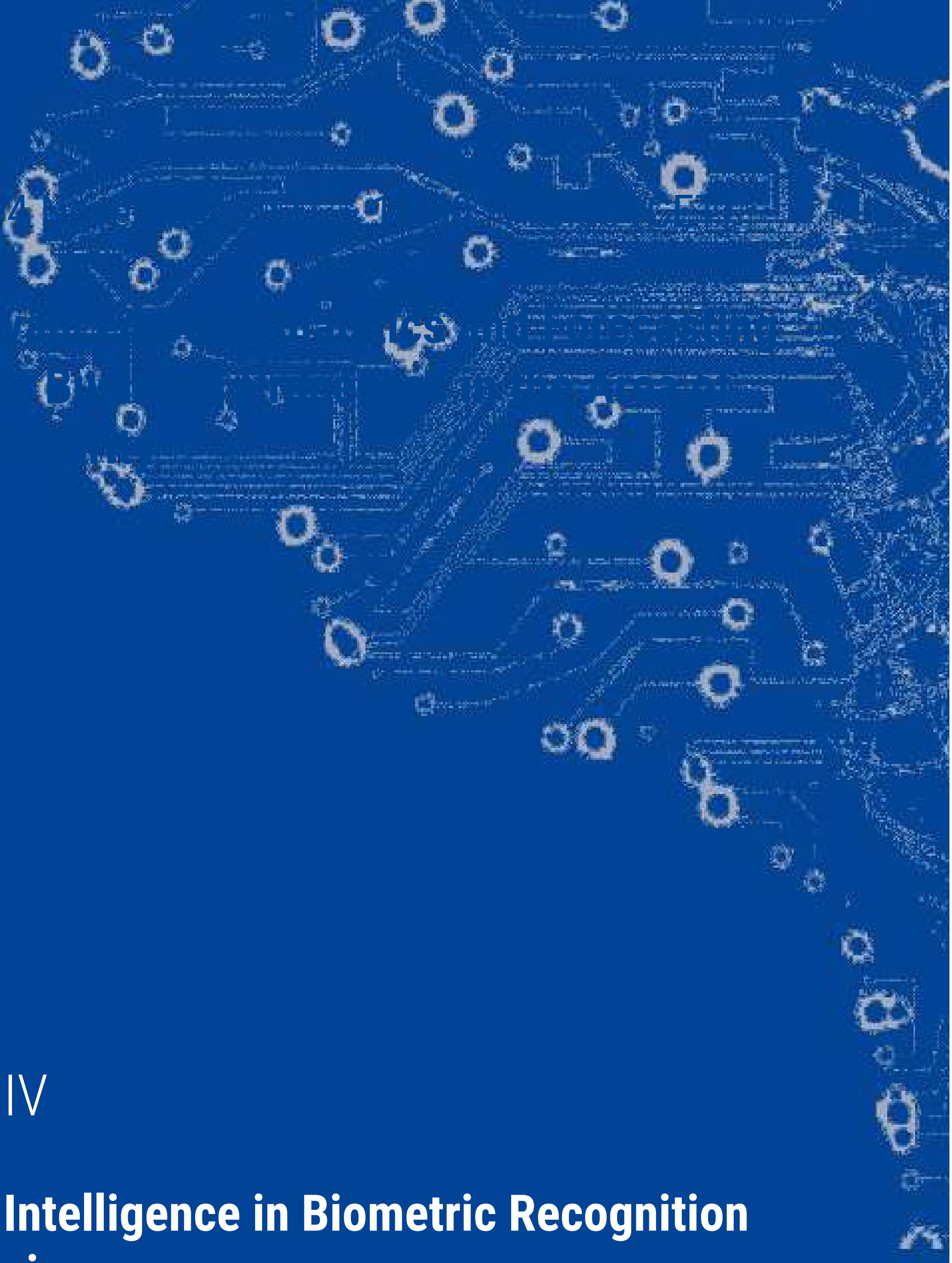
AIOps combines big data and machine learning to automate IT operations processes and the main use cases for AI operations include performance analysis, incident/anomaly detection, causality, and automation, while benefits include enhanced performance monitoring, predictability of incidents, capacity planning, incident resolution, etc.

Sopra Steria provided an overview of three AI Ops use cases. First, AIOps for end-user support to improve performance of support agents and offer next generation support to end-users (incl. chatbot) by providing a seamless user journey. As such, it is basically a decision-making tool allowing real-time monitoring of service quality, using AI technology and virtual assistants.

Second, AIOps for infrastructure operations to facilitate transition from managing traditional IT to new IT that is performance oriented and based on user experience, characterised by standardisation, automation, data analysis and management (AI), predictive models, etc. As such, the end-to-end operations AIOps model is a platform combining several tools to offer a range of capabilities. The artificial intelligence engine allows moving from silo supervision to end-to-end supervision across the value chain.

The final use case focused on AIOps for cybersecurity operations, covering such features as automation, machine learning, incident detection and response, vulnerability management and threat intelligence.

Overall, AIOps facilitates increased efficiencies and higher quality services through business monitoring based on end-to-end supervision, while also leading to a true transformation of teams.



Session IV

Artificial Intelligence in Biometric Recognition Technologies

25 November 2021

Project Presentations: AI Supporting the Evaluation of Face Recognition Technology

Mr Haoyu Zhang, Prof. Christoph Busch – Norwegian Biometrics Laboratory (NTNU)

The research project run by Prof. Christoph Busch and Mr Haoyu Zhang – AI Supporting the Evaluation of Face Recognition Technology – focuses on the ability of convolutional neural networks to generate features in facial images that are similar to bona fide ones. In addition to eu-LISA who sponsors the project, the consortium includes also Steinbeis Biometric Research Centre at Darmstadt University, Mobai, PLUS University in Salzburg, Austria, and NTNU.

The development and testing of biometric recognition systems relies on large-scale biometric datasets, and although there are many public ones (e.g., India's biometric ID system Aadhaar with over 1bn enrolled), their use is limited because biometrics are deemed sensitive personal data that cannot be shared with research or testing institutions. The collection of equivalent datasets is technically challenging and very resource-intensive, and its use is similarly bound by privacy restrictions. However, recent advances in convolutional neural networks offer a way forward by enabling the generation of synthetic images that can be used for training biometric recognition systems.

The past five years have seen significant progress in the generation of synthetic facial images, that for a human being synthetic images have become indistinguishable from real ones. This research aims to perform an objective evaluation of synthetic images. Standard testing methodologies have already been developed for fingerprint images (e.g., NFIQ2.1 and the corresponding standard ISO/IEC 29794). However, when it comes to facial imagery, only industry-developed proprietary algorithms exist. Thus, in order to have a vendor-agnostic approach, it is necessary to develop a NFIQ equivalent for face images. Currently, a standard defining testing methodology for facial images is being developed (ISO/IEC 29794- 5) to complement the standards on biometric sample quality (19794-5:2011 and 39794-5:2019).

Mr Haoyu Zhang presented an overview of the methodology used in the study for the generation of synthetic images and their evaluation. First, a database was created by generating non-mated samples using StyleGAN and StyleGAN2. In addition, a representative bona fide dataset was used from the Face Recognition Grand Challenge (FRGC). Altogether 50,000 images were generated for each synthetic dataset with different truncation factors. These datasets were then evaluated using three different methodologies, including FaceQnet v1 (an end-to-end deep learning model), SER-FIQ (an unsupervised approach), and an implementation based on the ISO/IEC TR 29794-5:2010.

In the first stage, the evaluation of non-mated samples using the three approaches mentioned above produced the following results. The distribution of scores between FRGC and StyleGAN2 for FaceQnet are very similar, with the FRGC data set performing slightly better. For the ISO/IEC TR 29794-5:2010 implementation, distribution of scores are also very similar, with the StyleGAN2 performing slightly better and more consistently. At the same time, the SER-FIQ approach shows that the FRGC data set performs better than the synthetic data set.

The second step was the evaluation of mated samples. In this case, when evaluating with FaceQnet, the FRGC bona fide dataset exhibited slightly higher quality. Similar results were attained when evaluating with SER-FIQ, where FRGC data set evaluation resulted in higher score distribution than synthetic datasets. However, when evaluating with the ISO/IEC TR 29794-5:2010 implementation, synthetic datasets appear to have significantly higher quality. One of the takeaways from evaluating mated samples is that real datasets contain more intra-identity variability, whereas in synthetic datasets, only limited intra-identity variability is introduced through semantic editing. Nevertheless, it is still relatively difficult to simulate intra-identity variance.

For non-mated samples, the applicability of synthetic data generated by StyleGAN and StyleGAN2 is similar. Only minor differences exist between the synthetic and selected set of bona fide samples, meaning that synthetic facial images are of high quality, that there are minor differences in estimated biometric sample quality, and that the variety of identity information is limited when the synthetic dataset is generated with a low truncation factor. As for mated samples, it is evident that they can be generated without any significant loss of identity information. However, one challenge still remains – bona fide data has higher intra-identity variation than synthetic data.

Although the study yielded some promising results, it is still not sufficient for testing operational systems. There are two essential requirements that need to be met when testing operational systems before entry into operation. First, the system must work with acceptable transaction times or throughput rate, which is usually tested with synthetic data as in this study. The second factor is biometric performance (FMR/FNRM) or, in case of identification mode, false positive and false negative identification rates. In this case we cannot extrapolate from the small dataset to a large dataset that would exist in the operational system. Owing to that, there is no viable alternative to conducting tests using actual large-scale biometric datasets, however, researchers, don't have access to such large-scale data sets.

Technology Foresight on Biometrics for the Future of Travel

Dr Luigi Raffaele, Research Officer, Frontex

Dr Luigi Raffaele is a Research Officer at Frontex's Research and Innovation Unit, where he oversees the development and implementation of Research and Innovation (R&I) in the area of border security.

The project – Technology Foresight on Biometrics for the Future of Travel – was carried out during 2021 in collaboration with 9 EU MS and Schengen Associated Countries, the European Commission, eu- LISA, Europol, the European Union Agency for Fundamental Rights, as well as Interpol, International Civil Aviation Organization (ICAO), and the U.S. Department of Homeland Security.

This research was motivated by two factors. First, the growing cross-border mobility of individuals and the demand for seamless border crossing necessitates digital identity management solutions, as well as no-gate physical solutions for automatic and seamless checks at border-crossing points. Second, the COVID-19 pandemic has created a need for technological solutions that are compatible with policies and measures implemented during the pandemic, while also ensuring effective safeguarding of the EU's external borders.

Owing to that, biometric technologies are the key enabler for automated processing of individuals at border crossing points. This foresight project constitutes an anticipatory response with a view to providing the European Border and Coast Guard community with knowledge on how to best utilise biometric technologies in the future, as well as helping to identify research and innovation activities in the area of biometrics in the short, medium and long term.

The analysis identified four 'must-haves' for biometric technologies: 1) seamlessness; 2) compliance with fundamental EU values and regulations; 3) applicability within pandemic-related restrictions; 4) low vulnerability to adversary attacks. These characteristics were used throughout this foresight project as reference points when analysing different biometric technologies.

The review of the state of the art in biometric technologies resulted in a three-level taxonomy encompassing 57 biometric technologies grouped into biomolecular, morphological and behavioural. In order to explore these technologies at system level, the taxonomy was augmented with a two-level taxonomy of biometrics-enabled technological systems. In addition to the state-of-the-art review, the project also performed a clustering of technologies on the basis of patentometric and bibliometric analysis, to identify most active parties in the field and their geographical distribution. Not surprisingly, the four largest technology companies (i.e. Microsoft, Amazon, Google and Apple) hold the largest number of patents in the area of biometrics.

Subsequently, four scenarios for the future of travel, border checks and biometrics were defined with a view to 2040 to be used in later stages of the project. Scenario definition was followed by a Delphi survey, which helped prioritise certain technologies. The experts who took part in the Delphi survey identified the following technologies as closest to mainstream and having a relative advantage in their specific application: infrared face recognition; 3D face recognition; contactless friction ridge recognition; iris recognition in the NIR spectrum; iris recognition in the visible spectrum.

Following the Delphi survey and prioritisation, an in-depth analysis of the key technological clusters was performed with the aim of envisaging future developments in terms of applications, functions, products and systems. This phase resulted in three main outcomes: visual technology roadmap; list of expected key opportunities and challenges from today to 2040; and a comparative analysis of the key envisaged developments under the conditions of the four scenarios. This was further complemented by capability readiness analysis for each of the technology clusters, domains (i.e. research, industry, institutions), scenario, and in two time frames (2022-27; 2028-33).

Q&A Session

The first question inquired about the most reliable biometric modalities from the perspective of Frontex, and what kinds of combinations with biometrics are being considered in addition to the EES requirements (i.e. facial imagery and fingerprints).

In response to this question, Dr Raffaele explained that the five technology clusters prioritised in the study are the ones that Frontex considers as the most reliable biometric modalities for application in border checks. These modalities are also in alignment with the current mainstream modalities in industrial research. In addition, application of other technologies, such as AI and privacy-preserving or privacy-enhancing technologies, in combination with biometric technologies, will further improve the operational performance of border control systems.

Responding to the second part of the question, Dr Raffaele suggested that the study considered multi- sensor deployments enabling multi-modal biometric recognition. The experts involved found that a combination of iris, fingerprint and facial recognition might have the highest potential for improving biometric accuracy, with 3D face recognition also relevant. In addition, iris in combination with periocular recognition was considered as relevant in combination with facial recognition. Another perspective from which multi-modal combinations were considered was the contactless or remote biometric identification.

The final question focused on whether Frontex is planning to pilot some of these modalities in real life environments in the near future.

Dr Raffaele responded that at this point in time it is too early to speak about pilot projects. Before deciding on possible future pilot projects, the results of the technology foresight should be analysed first. At the EU level, under the Horizon Framework Programme, there will be calls to further advance research in the specific biometric applications for seamless border checks, which Frontex strongly supports.

Industry Presentations

IDEMIA – AI & Biometrics

Mr Vincent Bouatou, Head of Strategic Innovation, Public Security and Identity

IDEMIA views security globally by factoring in the customer's environment and how they specifically use technology. In a world of ever-increasing online interaction, security primarily means protecting identities, which is why IDEMIA focuses on Augmented Identity.

Mr Bouatou opened his presentation with an overview of how developments in AI have affected biometrics. First, the performance of face recognition algorithms has improved significantly with the introduction of AI, in particular the deep learning ML algorithms, with false negative identification rate moving from 3.89% to 0.16% between 2018 and 2021. In addition, AI has significantly improved robustness against environmental factors, and also ageing. It has also ushered in new changes, such as facial recognition of masked individuals, leading to threefold reduction in error rates within six months. Another area where AI has had a significant impact is presentation attack detection.

Additionally, AI has significantly improved the performance of consumer grade terminals such as smartphones, which can now be used for professional applications, such as biometric identification, which is a change in paradigm. This is also due to most modern high-end smartphones having a neuro-processing unit that facilitates fast and efficient deployment of deep learning technology.

Furthermore, AI has helped improve the detection of voluntary or involuntary alteration of fingerprints. Thanks to AI, biometric recognition is now used for passenger facilitation, removing the need to present a physical identity document, allowing instead to rely only on biometric identifiers (incl. from one-to-one to one-to-many identification without loss in performance). Finally, we have video analytics to identify persons, vehicle license plates, objects, etc.

Mr Bouatou continued his presentation suggesting that beyond improvements in biometric performance, AI has also allowed us to enhance privacy protection. For example, anonymization of real-time video streams by removing people's faces, or replacing individuals with avatars in a CCTV stream, thus removing all identifying information and maintaining the privacy of individuals captured in the video stream.

Mr Bouatou also argued that AI applications in biometrics have taught us several valuable lessons. For example, from the perspective of the GDPR, biometrics have always been considered sensitive data, which has led to the development of technologies for processing biometric data (e.g., full homomorphic encryption, secure multiparty computation, etc.). The area of performance assessment has benefitted through having a range of standards on performance of biometric systems already available, including standards on performance testing and reporting, presentation attack detection, etc.

Concluding his presentation, Mr Bouatou highlighted three key points. First, biometric recognition has been an AI-based technology even before the introduction of deep learning algorithms. Second, AI will be a critical feature of applications used by European authorities for ensuring internal and border security. Lastly, the recently proposed AI Act will facilitate the formalisation of the AI ecosystem by introducing best practices, however, it should be balanced in order not to stifle innovation and performance.

FUJITSU – Palm Secure: Use Your Hand to Unlock the World

Mr Pieter Joris, Distribution Account Manager at Fujitsu Belgium

Mr Joris presented Fujitsu's biometric recognition technology PalmSecure which is based on palm vein recognition. He opened his presentation by outlining five key requirements determining the usability of biometric recognition modality. First, it should be universal in the sense that every person possesses this trait. Second, it should enable reliable differentiation between different individuals. Third, the quality of modality in terms of performance (i.e. recognition) should be measurable. Fourth, it should not change significantly over time. Last, in order to be practical, it should also allow for fast operation. He continued with an overview of the technical solution behind the palm-vein recognition technology. The rest of the process is common to other biometric modalities, meaning that after the image of palm veins is captured using infrared imaging, a template is stored and converted into a hash hey, which can then be stored on a device (e.g. a smart card).

There are several advantages to using palm vein identification. First, it offers high levels of security as it is hidden under the skin, it is unique (even in case of identical twins), it doesn't change over time, and it allows for simple liveness detection. Second, it is very precise due to the complexity of palm vein structure, with more than five million reference points, and since palm veins are significantly thicker than fingers, making them more easily identifiable. Lastly, it offers a number of usability benefits, such as contactless and intuitive operation, as well as high level of privacy due to the fact that palm vein image cannot be captured without the use of IR imaging.

In the context of border control, by anchoring identity in biometrics, palm vein could be used in combination with other biometric modalities, complementing other modalities with such benefits as impossibility of loss of the identifier, as well as impossibility of spoofing or modification. A PoC is currently ongoing at the European Parliament, using palm vein for authentication in access control.

Mr Joris also presented a scenario where palm vein technology was used to secure access to a football stadium, which presents challenges that are similar to border crossing processes, such as the need for fast processing, convenience and ease of use, low FRR and lowest possible FAR, no impact of lighting conditions, and possibility to integrate with other systems. In the specific use case presented, the football club has over 180 thousand members. Despite the relatively high number of enrolled members, the system maintains very high quality and speed of verification, although this figure is clearly significantly lower than in case of border-crossing scenarios.

mobai
Multimodal
Biometric
Authentication

Mobai – Industry Perspective on Face Morphing and Mobile ID Checks

Mr Brage Strand, CEO of Mobai
Prof. Raghavendra Ramachandra, Chief Scientist

Opening the presentation, Mr Strand posed a question: what if we couldn't trust passports anymore?

Prof. Ramachandra continued with an explanation of what face morphing is and how it can be used in border-crossing scenarios. He further explained that different types of image modification can have different effects, for example, sharpening of the image due to changing lighting might not affect the performance of an automated facial recognition system or even manual recognition, whereas morphing the images of several individuals may have a significant effect. By morphing the images of two individuals, a single identity document can be used by both individuals, as the facial recognition system may verify both individuals as a match to the photo provided in the identity document. This is possible due to the vulnerabilities in the passport issuance process, which accepts printed images with passport applications, or uploading images via an online application system, as is the case in the UK.

There are two common approaches to morphing attack detection (MAD): single image MAD and differential MAD. In single-image MAD, different types of algorithms are applied to evaluate whether the passport image it is a bona fide image or a morph.

In differential MAD, different algorithms are applied to analyse two images: one captured using a trusted device (e.g. ABC gate), and another image stored on a passport chip.

Prof. Ramachandra went on to introduce a study, where experts and non-experts in facial recognition were asked to identify morphed images. The study demonstrated that even experts specialised in manual examination and face comparison could identify only 72.56% of morphed images in case of differential MAD, and 64.63% in case of single MAD.

In concluding the presentation, Mr Strand provided an overview of different methods for tackling MAD. First, enrolment using a trusted device. Second, training people working with manual examination of documents. Third, using automatic morphing detection systems, with ABC gates as the most obvious places for introducing such systems. Similarly, morphing detection can be implemented in a differential MAD scenario, when a picture made by a third party is used. In this case differential MAD can be applied to an image provided by the applicant and the image taken using a trusted device when picking up a passport, significantly improving morphing attack detection.

secunet Security Networks – Morphing Attack Detection in Practice

Mr Michael Schweiger, Senior Product Manager, Homeland Security Division

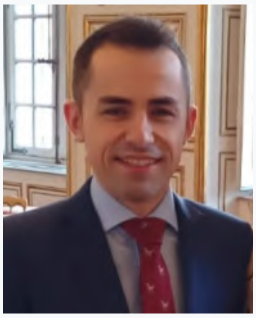
A morphing attack is when an identity document is created using a morphed image, which can then be used by two individuals for travel purposes with a significant likelihood that it will be verified by automated recognition solutions, for example, an ABC gate. Mr Schwaiger went on to explain that it is not simply a theoretical problem, but something that national authorities have to deal with on a daily basis. He elaborated on this point using an example from Slovenia, where they have detected 40 morphed images, all of them related to organised crime.

Similar to the previous presentation by Mobai, Mr Schweiger suggested three countermeasures to tackle MAD. First, opting for live enrolment when issuing identity documents. This is especially problematic in case of TCNs crossing Schengen borders using automated systems in the context of the EES. Second, training human experts to perform morphing attack detection, which may have a significant positive effect on the performance of human experts. Third, using AI in automated MAD.

Mr Schweiger continued his presentation with an explanation of how MAD is implemented in the ABC gate solution provided by secunet. In this particular implementation, border control officers have a review screen where they can see what is happening at each of the gates, including the verification of travel documents, checking of facial biometrics against the image stored on the passport chip, presentation attack detection and morphing attack detection. Presenting the results of testing the algorithm in operation, Mr Schweiger suggested that the algorithm is suitable for daily use, as at the threshold of 2% for FPR, the system is able to detect 85-88% of available morphs. In terms of error rates, this means Attack Presentation Classification Error Rate (APCER) of 12-15% at Bona Fide Presentation Classification Error Rate (BPCER) of 2%. The 2% BPCER can be considered as optimal in border control scenarios, allowing to identify up to 88% of morphs already at the level of ABC gates.

Closing his presentation Mr Schweiger outlined the future outlook for MAD. First, automated MAD will be the reality quite soon. Nevertheless, detecting high quality morphs remains a challenge. Another objective is to continue re-training the algorithms to further reduce the APCER rate at realistic target BPCER rate for operational settings. In this regard two challenges remain to be addressed: frontal images and face masks. MAD systems can also be further improved by incorporating learning from high-performing human experts, as well as using different methods for generating morphs that can be used for algorithm training. Last but not least, automated MAD is only one part of the story, which needs to be accompanied by live enrolment and training of human experts to ensure highest level protection against morphs.

Panel Discussion and Q&A



The concluding panel discussion focusing on AI in biometric recognition technologies was led by Dr Ramon Blanco, IT Officer at eu-LISA's Planning and Standards Unit.

First question addressed to IDEMIA focused on the social acceptability of biometric recognition in the context of CCTV, in particular making sure that faces are not recorded.

Responding to this question, Mr Bouatou explained that the solution presented is in development stage and is not yet in active use. He suggested, however, that this issue should be addressed at policy level, in particular by defining requirements for implementing anonymization. For example, if anonymization is implemented at camera level, then there should be little concern that anyone could get to un-anonymized data at any point. Another way to address this issue would be to encrypt the original video after anonymization, and in this case regulations should define access to decryption. The main takeaway is that with the introduction of AI, we will have not only better-performing biometric technologies, but also more privacy-preserving biometric technologies.

The second question inquired about the tools used by criminals to create morphed images. According to Mr Strand (Mobai) there are a number of open source tools available, including openCV.

Prof. Ramachandra added that the choice of tools depends on the technical competency of the criminals. For example, less technically advanced criminals use open source tools, while more advanced criminals use deep learning-based approaches, which are also available as open source. When it comes to presentation attacks in palm-vein biometrics, they are difficult to orchestrate because replicating vein patterns is technically not feasible.

The third question focused on IDEMIA's R&D work on the use of biometrics in other domains, such as gesture recognition or recognition of symptoms of illnesses.

Mr Bouatou (IDEMIA) explained that IDEMIA's research focuses on biometric applications in video analytics. He stressed that IDEMIA is not a health company, and it is not working on healthcare related applications. However, when it comes to gesture recognition, IDEMIA's video analytics research is focusing on identifying what is happening in a video stream. Mr Strand (Mobai) followed up on this question, zeroing in the identification of malicious intent. He argued that the problem of lie detection is an extremely challenging problem for AI, and we should be extremely cautious when developing and deploying such solutions. Mr Strand (Mobai) expanded on that, pointing out a wide range of cultural idiosyncrasies when it comes to lying, e.g., movement and speech patterns, etc. All of those elements are relevant from an investigator's point of view, making it extremely hard to capture with an automatic system trained in gesture analysis.

The next question inquired about the future outlook in the development and application of AI in the area of biometric technologies.

The representative from Fujitsu proposed that the main challenge for PalmSecure is the high number of identifiers against which an individual would need to be identified in case of one-to-many scenario. Here the challenge is to ensure similarly low level of False Acceptance Rate. Mr Schwaiger (secunet), in turn, pointed out that behavioural analytics is one of the more challenging areas. For example, a person may exhibit signs of nervousness because they are traveling with a fake passport, but it may also be due to the fact that they are using an e-gate for the first time. This is why secunet is focusing on core problems such as MAD or PAD, where there is ground truth and it is possible to develop well-performing algorithms with reliable results.

Another question from the audience focused on the persistent biases in biometric systems, as proven by scientists, related to race or gender.

Mr Bouatou responded that one needs to be very clear about defining specific applications where bias has been identified, and bear in mind that not all of these applications are biometric or facial recognition. For example, in the recent evaluation performed by NIST, it was shown that error rates due to gender or race are extremely small, as it is affected by the size of the dataset against which identification is performed, as well as whether the results of the algorithms are calibrated, which can also address the issue of bias, including in real time. The NIST evaluation concluded that there is hardly any measurable difference in the performance of facial recognition algorithms based on gender or race.

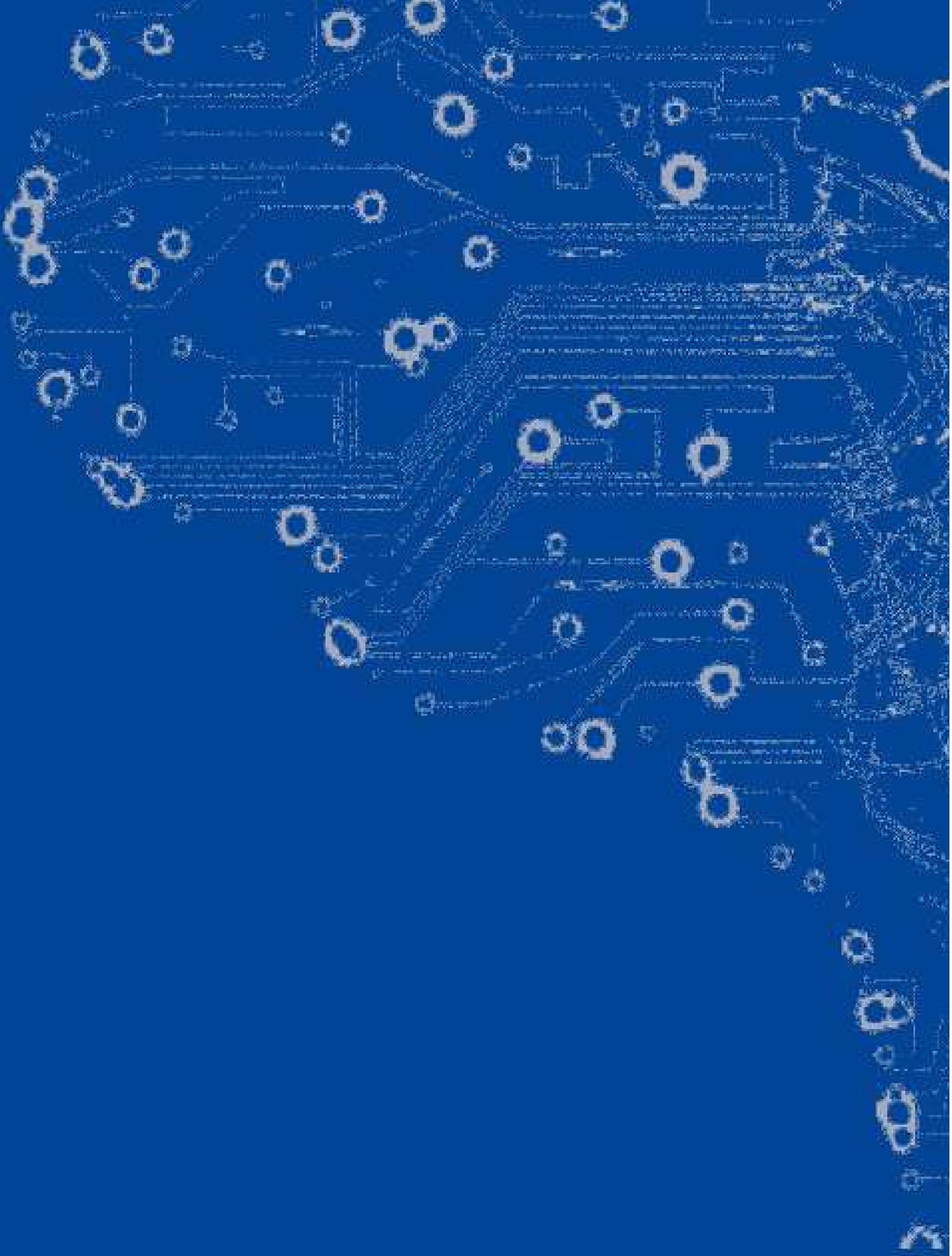
The final question in the discussion focused on presentation attack detection (PAD) in contactless fingerprint scanners.

According to Mr Bouatou this is a problem that is much harder to solve. IDEMIA has been working on contactless fingerprint technology for 10 years, and PAD algorithms built into the technology are able to detect most presentation attacks. However, PAD in a scenario when fingerprint capture is being performed using an unknown device in an unsupervised environment, is very difficult to control. In general, PAD is strong in case of trusted devices with known illumination. Of course, this doesn't mean that mobile devices cannot be used because a trustworthy operator operating a mobile device for remote contactless fingerprint acquisition can work just fine. In such cases, there's no reason to worry about PAD because the operator would notice if there is an issue. However, otherwise it is not possible to say that there's a bulletproof solution for PAD in contactless enrolment.

Closing Remarks

Mr Luca Tagliaretti, Deputy Executive Director, eu-LISA

In closing this iteration of eu-LISA's Industry Roundtable, Mr Tagliaretti argued that eu-LISA is tackling challenges that are important not only in Europe but on a global scale. These are challenges that none of us can resolve alone, which is why public-private partnership is the best way forward. In that sense, eu-LISA's Industry Roundtable offers a bridge to new ideas and technologies, suggesting avenues for new research and approaches. Therefore, research and development are one of the key priorities for the Agency. Mr Tagliaretti went on to underscore that AI is an extremely topical issue for eu-LISA and its stakeholders, especially in light of the proposed EU Artificial Intelligence Act. The Agency's position on this issue is clear: we should not regulate AI as such, instead we should regulate specific applications of this technology, bearing in mind the public interest and our mission. Therefore, it is important to keep discussing these issues to further our understanding, as we did during this event, and this is why events like the eu-LISA Industry Roundtable are very important for raising awareness and increasing trust, helping us in our work towards our common objectives.



Publications Office
of the European Union

Catalogue number: EL-AN-21-002-EN-N
ISBN 978-92-95217-93-5
ISSN: 2600-2728
DOI:10.2857/105750