CENTER FOR
DIGITAL SAFETY & SECURITY

AUSTRIAN INSTITUTE OF TECHNOLOGY

ARTIFICIAL INTELLIGENCE

Applications, Services and Solutions

Headquarter of AIT Austrian Institute of Technology in Vienna, Austria.

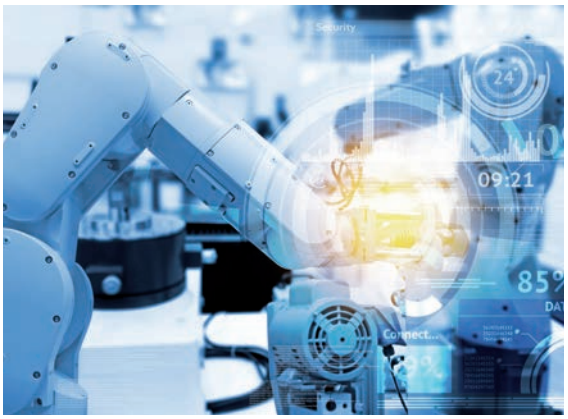
INTRODUCTION

Today Artificial Intelligence (AI) is applied in almost all industrial sectors and social subsystems.

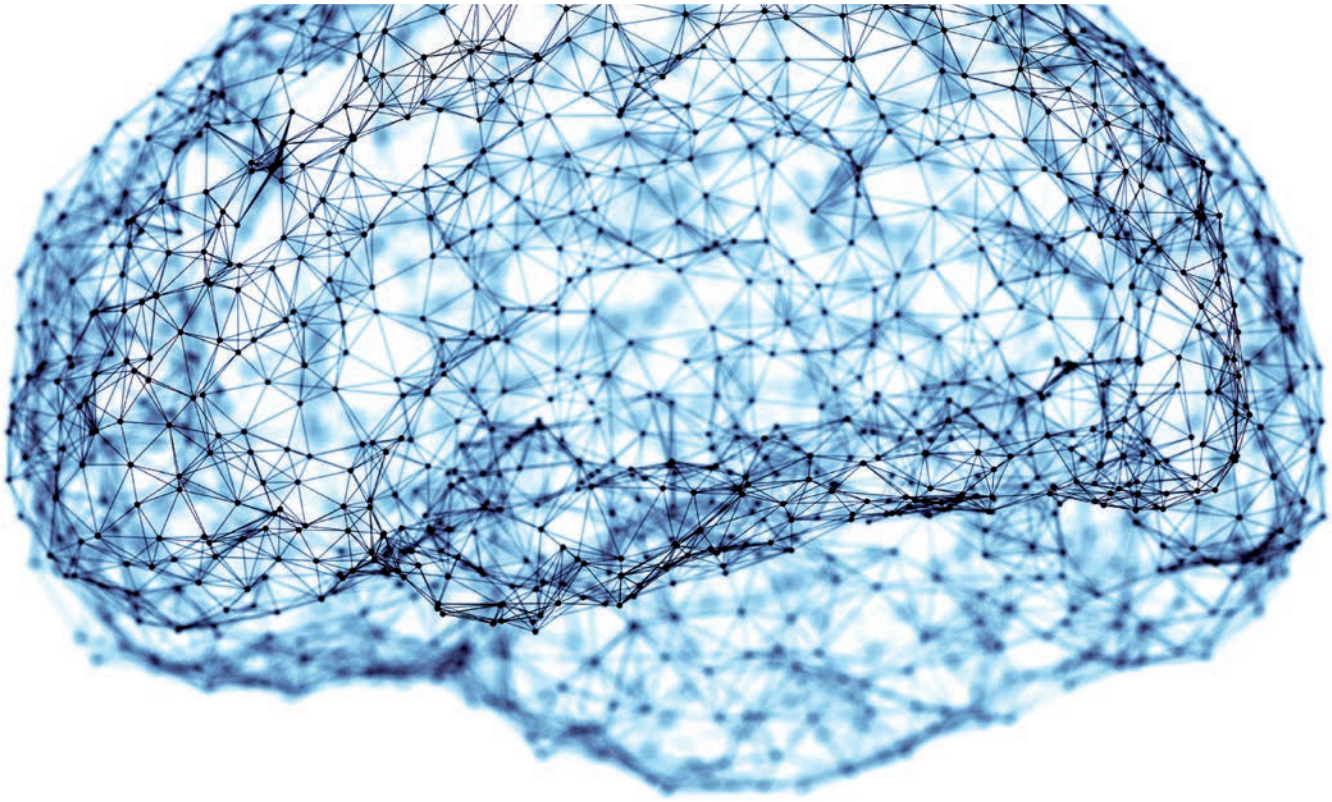
It is used in areas including traffic and transport (e.g. autonomous driving), robotics, industrial automation (smart factories), public safety, crisis and disaster management, cybersecurity (e.g. protection of industrial control systems), in a range of banking, insurance and legal business applications, as well as in fields including education, social services, energy, the environment and healthcare provision. Its primary intention is, of course, to enhance customer convenience.

The Center for Digital Safety & Security at AIT has comprehensive expertise in data science and AI, and is working to develop state-of-the-art AI-based services and solutions. The strategic key areas for new AI technologies lie in dedicated application areas such as monitoring (e.g. cybersecurity), allowing large data volumes to be analysed in real time and identifying patterns as well as deviations. By using self-learning models, AI systems are also suitable for finding and extracting relevant information from large volumes of data (data mining), and interpreting the abstract patterns that have been identified. Another key function of AI lies in the ability to make predictions, such as forecasting future trends. The interpretation capability of AI systems is the most significant factor. This allows AI systems to analyse and interpret complex, unstructured data deriving from images, videos, audio and text files, as well as sensor data. Perhaps the most important function of AI is, however, interaction with the physical environment, such as with robots or sensors for the efficient control and navigation of highly automated systems, with both human interaction (e.g. via gestures, speech, facial expressions) and interaction between machines within M2M constellations.

The following pages provide an overview of state-of-the-art AI-based services and solutions developed at AIT Center for Digital Safety & Security together with and for partners in business and industry.



APPLICATIONS, SERVICES AND SOLUTIONS



ARTIFICIAL INTELLIGENCE FOR NETWORK ANALYSIS

Telecommunication networks are the biggest data carriers in society today, with trillions of events occurring every second, even in medium-size networks. With such a wealth of big data, learning-based and AI-enabled networking is a cornerstone of better, more reliable, and safer networks and services. However, AI for network data is complex as it involves all of the major learning and big data challenges (the 4 Vs): massive volumes of complex and heterogeneous data (Volume and Variety), fast and highly dynamic streams of data (Velocity), lack of ground truth for learning (Veracity), as well as highly unbalanced data, a lack of visibility due to massive adoption of end-to-end encryption, and more.

AIT can help your organisation unleash the power of AI in a variety of networking-related domains:

NETWORK SECURITY (AI4NETSEC)

AI can largely increase the detection accuracy of attacks and other threats flowing through the network, without sacrificing the robustness of the analysis (i.e., false alarms). AI can rapidly identify complex threats and detect previously unseen attacks, as well as deal with obfuscated and adversarial learning environments, and consequently helps to drastically improve your business security. Furthermore, AI-based network security does not necessarily mean black-box behaviour: you can still fully track and understand the decisions taken by your security system, thanks to explainable AI (XAI) concepts and techniques.

NETWORK ANOMALY DETECTION & DIAGNOSIS (AI4NETADD)

The automatic detection and diagnosis of the ever-growing number of anomalies faced by network operators is a paramount challenge. By enabling the analysis of highly-dimensional data with both real-time and large-scale requirements, AI and big data principles and platforms can significantly improve the visibility and understanding of such complex and rare events, empowering a quick troubleshooting process.

NETWORK MONITORING AND ANALYSIS (AI4NETMON)

Network Traffic Monitoring and Analysis (NTMA) is a key component in network management and is needed to guarantee the correct operation of large-scale and/or complex networks. Applications such as performance monitoring, traffic classification and network policing require real-time and scalable monitoring approaches. Anomaly detection and security mechanisms require operators to quickly identify and react to unpredictable events while processing millions of heterogeneous events. In addition, NTMA systems must be capable of collecting, storing, and processing massive sets of historical data for learning and post-mortem analysis. At AIT we design scalable online and offline data mining and machine learning-based techniques and platforms to monitor and characterize extremely large volumes of network traffic data.

INTERNET QUALITY OF EXPERIENCE (AI4NETQOE)

Quality of Experience (QoE) is a well-known concept that permits operators to understand and assess the functioning of networks and services from the standpoint of the end user or service customer. QoE development has been traditionally limited to small-scale controlled environments, but today QoE-based network measurements represent a paramount source of information for Internet service and content providers. Here at AIT, we are experts in QoE for networks at scale, incorporating the QoE paradigm into the design, analysis and operation of real-world networks, services, and distributed systems. AI-based Internet-QoE relies on big data analytics to generate useful user-centric insights from large-scale network measurements, even under the increasing prevalence of end-to-end encryption.

References (excerpt)

ÆCID - Automatic Event Correlation for Incident Detection; https://aecid.ait.ac.at/

BIG-DAMA – Big Data Analytics for Network Traffic Monitoring and Analysis; https://bigdama.ait.ac.at/

MobiQoE – Monitoring and Analysis of Quality of Experience in Mobile Networks; http://mobiqoe.ait.ac.at/

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Dr. Pedro Casas
Tel. +43(0) 50550 4104
Giefinggasse 4, 1210 Vienna
pedro.casas@ait.ac.at
www.ait.ac.at/dss

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Dr. Dr. Florian Skopik
Tel. +43(0) 50550 3116
Giefinggasse 4, 1210 Vienna
florian.skopik@ait.ac.at
www.ait.ac.at/dss

AI FOR NATURAL LANGUAGE PROCESSING (NLP)

Discovering valuable information within unstructured, heterogeneous text is a challenging task, given the vast amount of textual data that we must cope with in today's information society. AIT provides the expertise and support for a broad range of use cases by applying a variety of machine-learning techniques – including algorithmics, mathematics and statistics – to discover topics and semantic relationships, and to extract meaningful, structured information.

With the advent of more powerful computing hardware, deep learning has emerged as a new and promising machine-learning paradigm in natural language processing (NLP). The use of neural network-based machine learning is not new, but with the application of new approaches for learning vector representations of words in very large text collections, deep learning has been proven to deliver excellent results in machine-learning tasks such as classification or the detection of semantic relationships between words.

While deep learning has changed the manner in which NLP is carried out, it is only part of the solution. AIT offers advice on the many classic tasks that still play a fundamental role, such as corpus building and cleaning, pre-processing, tokenization and stemming. Classic information retrieval measures such as co-occurrence statistics, TF-IDF (term frequency–inverse document frequency), bag-of-words (BoW) representation, or part-of-speech tagging (PoS) are still important parts of the NLP toolset. Depending on the specific use case, these are individually applied as input for Deep Neural Networks (DNN), or in conjunction with other machine-learning algorithms such as Support Vector Machines (SVM).

AIT solutions enable the analysis and overview of new text document collections using unsupervised machine learning methods. Topic modelling allows us to reveal important concepts, terms and relationships that occur in a collection of documents.

Using pre-defined or manually assigned labels, classification algorithms support the structuring and filtering of large text collections into sub-groups. This is also important for building a domain-specific, cleaned corpus for use in a specific application domain. Once such a well-defined text corpus exists, it can be used to implement supervised machine learning tasks. These include, for example, Named Entity Recognition (NER) in which, based on external knowledge, words are assigned to abstract classes such as names of persons or organizations, events, machine parts in industry or medical terms in healthcare.

AIT´S ANNOTATION PLATFORM

One of our primary goals is to minimize the effort required for the manual annotation and labelling of text, because this task relies on manual work and domain knowledge. One method of achieving this goal is to provide efficient and user-friendly labelling tools. Recogito is our annotation platform which uses existing gazetteers and dictionaries to aid in the process of producing the high-quality ground-truth training data required for supervised machine-learning tasks. This task can be supported by active learning, where the learning algorithm actively suggests significant terms to the user who is then able to confirm, reject or refine effectively, and by transfer learning, which allows us to leverage generic language models which can then be tailored to domain-specific languages and document types with significantly less effort.

References (excerpt)

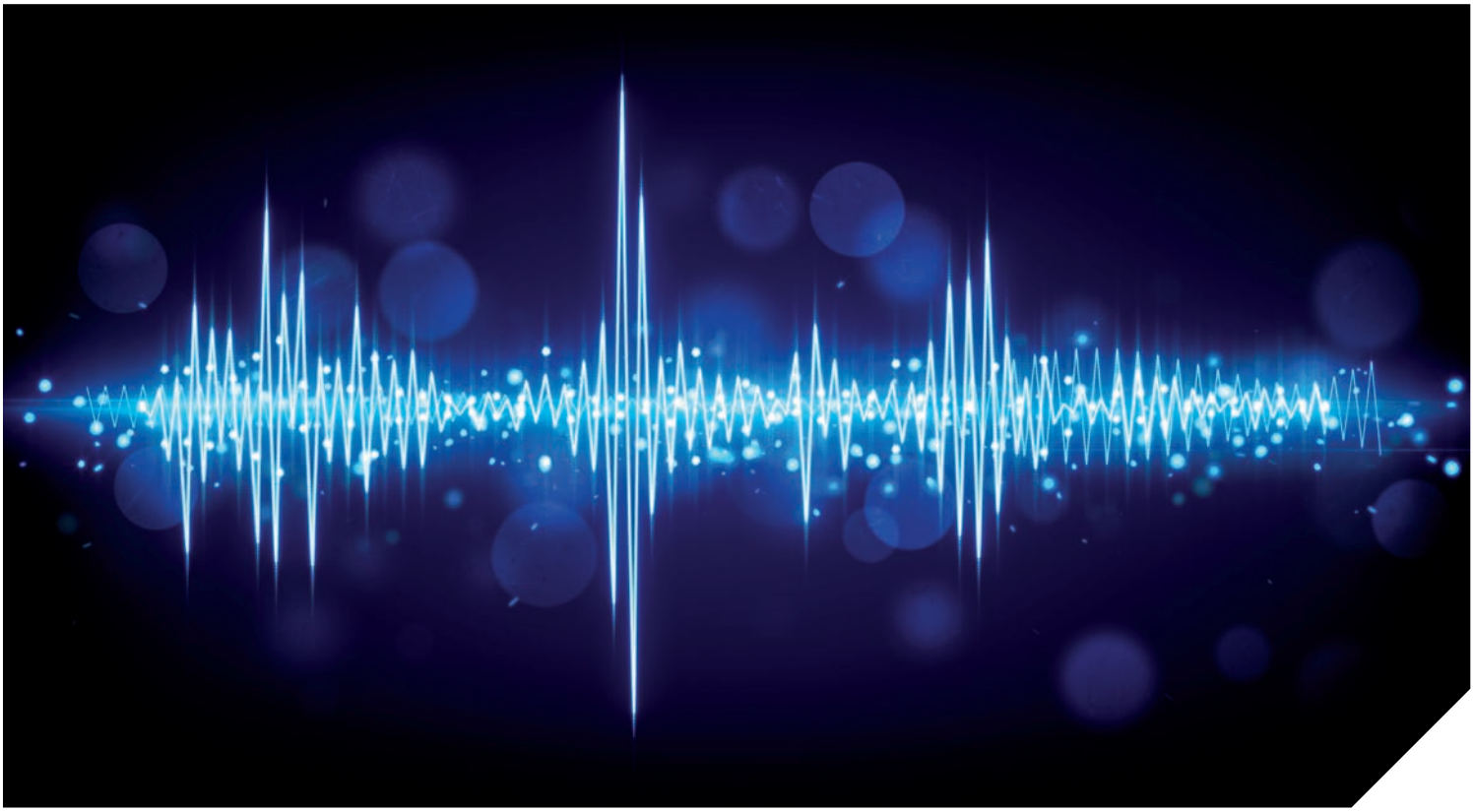
COPKIT (H2020) – Intelligence-led Early Warning and Early Action system for Law Enforcement Agencies; https://copkit.eu/

TRAVELOGUES (FWF) – Perceptions of the Other 1500–1876; http://www.travelogues-project.info/

Pelagios Projects – a collection of multiple projects under which the Recogito platform was developed: http://commons.pelagios.org/ (Andrew. W. Mellon Foundation), https://pelagios.org/

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Dr. Sven Schlarb
Tel. +43(0) 50550 4179
Giefinggasse 4, 1210 Vienna
sven.schlarb@ait.ac.at
www.ait.ac.at/dss

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
DI Alexander Schindler
Tel. +43(0) 50550 2902
Giefinggasse 4, 1210 Vienna
alexander.schindler@ait.ac.at
www.ait.ac.at/dss



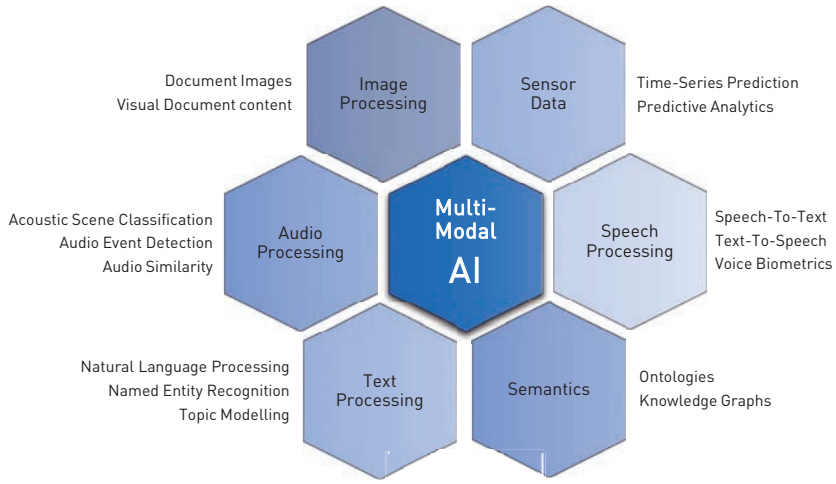
MULTI-MODAL AI FOR SECURITY APPLICATIONS

AIT has developed a scalable security platform for implementing multi-modal AI at a market-ready level, and with features that address the requirements of end users including service providers and stakeholders such as law enforcement agencies (LEAs). The core task of the platform is to analyse and prioritize large volumes of audio-video content delivered, for example, by witnesses to a terrorist attack such as the Boston Marathon bombing incident. Experience shows that such incidents result in several thousands of hours of video material. This development relies on several areas of AIT expertise:

Image Analysis: Videos are searched for visual features. Designated objects are detected and tracked. A flexible analysis component plug-in layer allows for the simple inclusion of additional algorithms such as license plate number extraction or facial recognition.

Audio Analysis: a special focus of the platform is audio analysis. Non-visual events such as gunshots and explosions are indexed to facilitate search, using methods based on deep neural networks to detect relevant acoustic events. Additionally, relevant video sequences can be selected to identify other sequences with similar audio content. This is useful as an aid in personal identification, for example. Videos with similar audio will be recorded at the same place and at the same time, possibly providing a different angle on the same person. We also offer audio fingerprinting techniques that allow the system to synchronize multiple data sources based on audio events.

Scalable Data Processing: Managing large volumes of video data requires the use of appropriate technologies. We have experience in various scalable architectures including Hadoop, Spark, and Airflow. Additionally, neural network models optimized on GPUs, such as the audio models for event detection and scene classification noted above, are integrated with this distributed, scalable architecture, which is otherwise based on commodity hardware.



A scalable system architecture uses multiple distributed open source platforms in order to manage these requirements. It is based on multimedia data, assumed to be available after a terrorist or criminal attack. Among other data, this will include videos from eye witnesses as well as videos from public and private surveillance cameras. These large volumes of multimedia data are uploaded into a distributed file system. During import, image and audio features relevant for the training of deep learning models are extracted, and other necessary pre-processing steps are executed. The neural networks used for audio analysis and video tracking are trained and executed on integrated GPU clusters. A query interface, based on standards such as JSON and GraphQL, accesses this database and serves as the interface to external systems.

References (excerpt)

VICTORIA – Video analysis for Investigation of Criminal and TerrORIst Activities; https://www.victoria-project.eu/ (EU H2020)

FLORIDA; https://www.kiras.at/gefoerderte-projekte/detail/d/florida/ (funded under the Austrian KIRAS security programme of the Federal Ministry of Transport, Innovation and Technology)

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Dr. Ross King
Tel. +43(0) 50550 4271
Giefinggasse 4, 1210 Vienna
ross.king@ait.ac.at
www.ait.ac.at/dss

MULTI-MODAL AI FOR DOCUMENT MANAGEMENT

Document management systems need to be able to store, archive, process, and extract information from digital-born as well as scanned, image-based documents. Documents and their relevant parts need to be searchable and to be presented appropriately with respect to their context and document type. In recent times, AI in general, and machine learning in particular, has opened up new possibilities for better supporting users and providing more efficient tools for managing large collections of heterogeneous documents.

AIT offers a full range of software and expertise, from document acquisition to access. Its portfolio comprises modular and flexible components for creating domain-specific document processing workflows that are ready to scale up and work on very large document collections. Multi-modal AI is applied to this domain in three primary areas.

First, the quality of OCR (optical character recognition) has improved significantly in recent years, also with the help of AI. While digital-born and good quality scans can be reliably transformed into text, challenges remain for low quality scans or photographs taken from documents. Here multi-modal AI can help by using a combination of techniques (OCR and Image Analysis) to achieve better overall performance. At AIT, we use these techniques to address challenging tasks such as gaining structured information from tables contained in document images or extracting semantically meaningful blocks including the sender, addressee, and subject line of a scanned letter.

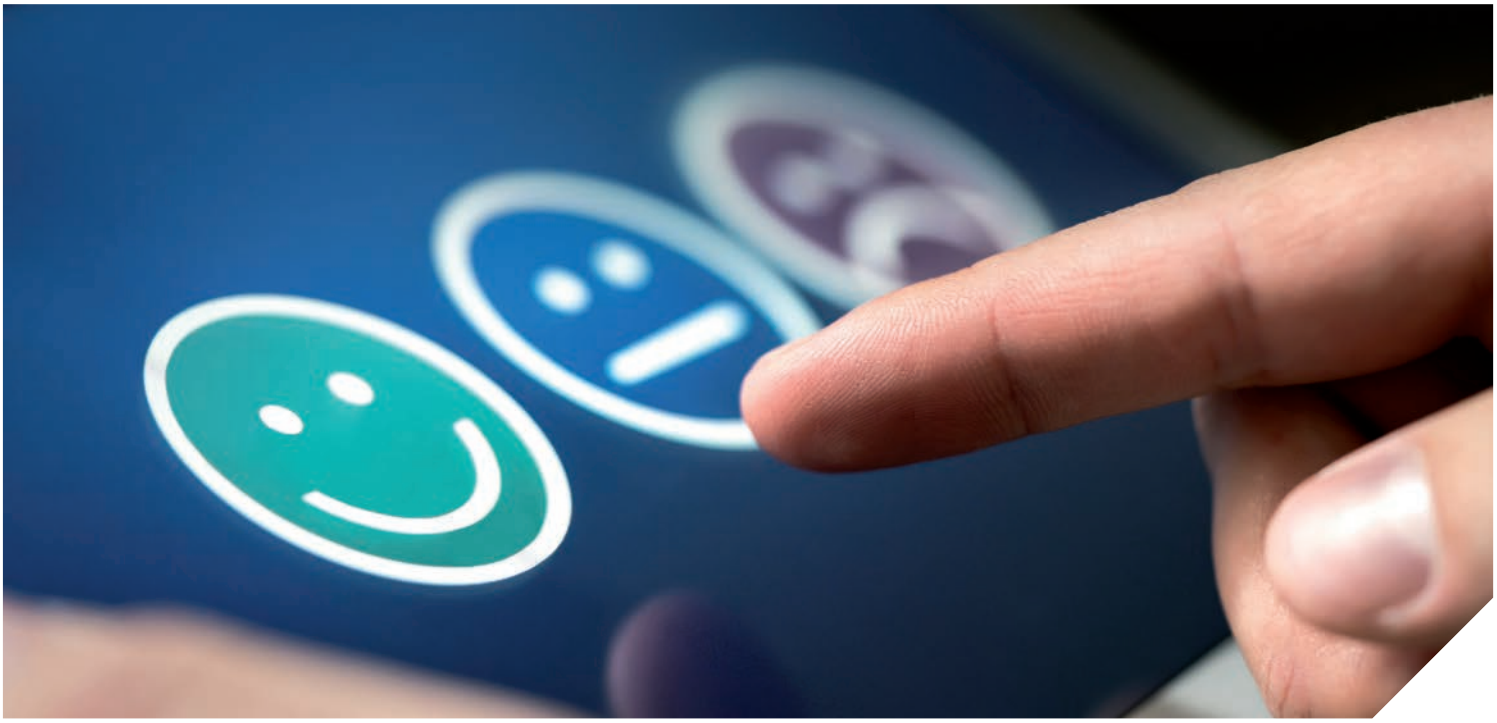
Second, AI is now at the heart of "document understanding". Domain-specific language and document structure and layout models are required to reach a good level of performance in document classification, clustering, information extraction, and natural language analytics tasks. This in turn requires the creation and management of adequate training data and, in many cases, a scalable storage and compute environment for pre-processing and for the creation of machine learning models. AIT can advise your organization on how to manage this new aspect of data and software maintenance.

Third, AI is indispensable for the access and retrieval of documents, and AIT can support the introduction of this new approach in your knowledge management landscape. This includes, for example, search technology that relies heavily on natural language processing techniques, such as NGrams, Gazetteers and dictionaries, and on Named Entity Recognition, where we leverage well-known open source search and retrieval frameworks such as SolR and Elastic Search.

References (excerpt)

E-ARK – European Archival Records and Knowledge Preservation; https://www.eark-project.com/ (EU CIP), https://e-ark4all.eu/

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Dr. Sven Schlarb
Tel. +43(0) 50550 4179
Giefinggasse 4, 1210 Vienna
sven.schlarb@ait.ac.at
www.ait.ac.at/dss



MULTI-MODAL AI FOR CUSTOMER SERVICE

Customers are the most important asset in any industry. Customer service is the art of fulfilling your customer's expectations by delivering professional, helpful, high quality service and assistance before, during, and after the customer's requirements have been met.

Here at AIT, we are exploring Artificial Intelligence approaches that combine multiple data types, such as images, audio streams and text, so-called "multi-modal AI", so that your business can provide an enhanced and efficient customer service.

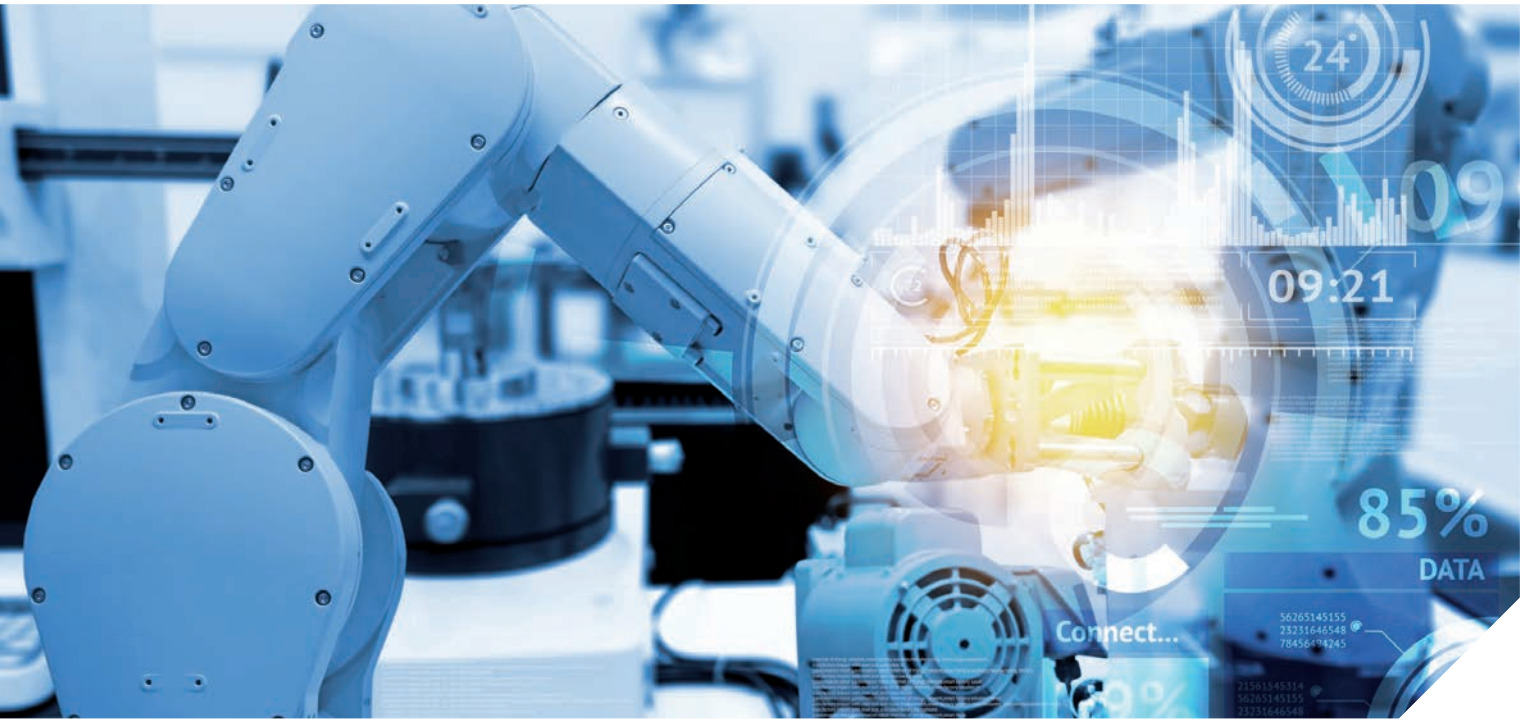
For example, how can you automatically determine who is the sender or recipient of a letter when technologies such as Named Entity Recognition (NER) provide only names? In this case more context is required. Often the sender uses a different font, a certain style or even a logo in the letterhead. This layout information is not available in pure text data, but by combining text analytics with visual analytics, the text is set within a broader context and the two names can be distinguished.

Multi-modal AI combines information from multiple modalities, such as images, audio, text, sensors, etc. Traditionally complex to realize, this field is currently experiencing rapid advances due to the success of deep neural networks which facilitate multiple modalities within a single model.
With teams specialized in the individual modalities, we work together intensively to improve our multi-modal approaches and redefine the state-of-the-art.

References (excerpt)

Text and speech recognition software for international provider of enterprise content management software and financial service provider

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
DI Alexander Schindler
Tel. +43(0) 50550 2902
Giefinggasse 4, 1210 Vienna
alexander.schindler@ait.ac.at
www.ait.ac.at/dss



AI FOR PREDICTIVE MAINTENANCE IN INDUSTRY 4.0

Prospective maintenance refers to a holistic approach to monitoring the history and condition of industrial equipment in order to determine when maintenance activities should be carried out. This approach promises cost savings compared to routine or time-based preventive maintenance regimens, because maintenance tasks are performed only when required and expensive post-breakdown interventions are avoided.

AIT trains and applies machine-learning models to detect degradations of machines or machine parts, allowing them to predict future equipment failures. This provides an informed basis for proactive decisions by maintenance planning and can thus reduce the costs related to unexpected machine breakdowns. For example, maintenance can be brought forward, or additional resources can be requested. An additional cost saving occurs when maintenance is avoided for machines in a healthy condition.

Creating a forecasting model requires comprehensive analysis and processing of existing data. In this step, AIT experts gather information from different data sources that are then standardized, visualized and statistically analysed. The data quality is also assessed, and our customers receive an analysis of this data quality and methods for the systematic examination of the data.

The explorative analysis is used to create and evaluate machine-learning models. Of particular note are "deep learning" approaches, which yield excellent results in many cases, and classical models that allow interpretation. Interpretability is desirable in many applications because decisions become human-readable and confidence in the model is strengthened.

Together with the domain expert, the current maintenance strategy is depicted in realistic benchmarks. The evaluation of the models is based on real customer data and in reference to these benchmarks. In order to estimate the effort of an implementation to production, a deployment concept is created based on the requirements of the forecast model and the customer's local infrastructure. Our expertise and offering:

- Data analysis & visualization operating on top of data streams
- Data quality checking
- Artificial Intelligence models predicting time-to-failure (TTF) and remaining useful lifetime (RUL)
- Automatic health monitoring (health factor generation)
- Building decision support models that consider algorithmic predictions
- Performance metrics, test methods, data sets, and reference documentation to verify and validate deployed methods

References (excerpt)

Machine learning and deep learning tools for international technology manufacturers and technology companies

COGNITUS (FFG IKT der Zukunft) – Deep learning technology for predicting outages of machineries based on sensor data streams

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Dr. Bernhard Haslhofer
Tel. +43(0) 50550 4192
Giefinggasse 4, 1210 Vienna
bernhard.haslhofer@ait.ac.at
www.ait.ac.at/dss

AI FOR SAFETY & SECURITY IN CYBER-PHYSICAL SYSTEMS

Artificial Intelligence, together with safety & security requirements, is significantly shaping the systems used in Industry 4.0, highly automated cyber-physical systems, and the Internet of Things (IOT). The Center for Digital Safety & Security has extensive experience in the development and operation of safe and secure systems. For many years specialists at the Center have been working in standardization in order to shape tomorrow's compulsory standards, as well as developing practical solutions and advising companies on the introduction of compliant processes and implementing engineering projects.

The Center's portfolio includes:

- Training in Artificial Intelligence (AI) for industrial applications, cybersecurity, standard-compliant work
- Verification technologies suitable for AI methods, and which themselves apply AI approaches in order to increase efficiency
- Standard-compliant workflows including tool support, e.g. using AI-based document evaluation
- Tools for automatic, model-based threat analysis of system designs (Security by Design) with an automatically updating threat database (subscription model)
- Real-time monitoring of analogue and digital signals (runtime monitoring)
- Data analysis and machine learning (including explainable AI)
- Secure architectures for legacy systems (secure gateways, etc.)
- Security analyses of network designs, machine code analysis, source code reviews/audits, penetration testing, ISO training
- Tools for automated cybersecurity threat analysis in the automotive field

The special processes, technologies and tools developed at AIT allow the safety & security of systems to be monitored in real-time, during operation, and are currently being deployed globally.

References (excerpt)

Enable-S3 – European Initiative to Enable Validation for Highly Automated Safe and Secure Systems; https://www.enable-s3.eu/ (H2020, ECSEL Joint Undertaking)

THREATGET – Threat Analysis and Risk Management Tool; https://www.threatget.com/, https://cybersecurity.lieberlieber.com

Installations at Tier 1 manufacturers and automotive suppliers

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Dr. Willibald Krenn
Tel. +43(0) 50550 4109
Giefinggasse 4, 1210 Vienna
willibald.krenn@ait.ac.at
www.ait.ac.at/dss

Editorial management: Michael W. Mürling | Images: iStock.com, AIT, Johannes Zinner | Place of publication: Vienna, August 2019

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Mag. (FH) Michael W. Mürling
Marketing and Communications
Center for Digital Safety & Security
Phone +43 50550 4126
Giefinggasse 4, 1210 Vienna, Austria
michael.muerling@ait.ac.at
www.ait.ac.at/dss

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Dr. Markus Kommenda
Business Development
Center for Digital Safety & Security
Phone +43 50550 4180
Giefinggasse 4, 1210 Vienna, Austria
markus.kommenda@ait.ac.at
www.ait.ac.at/dss