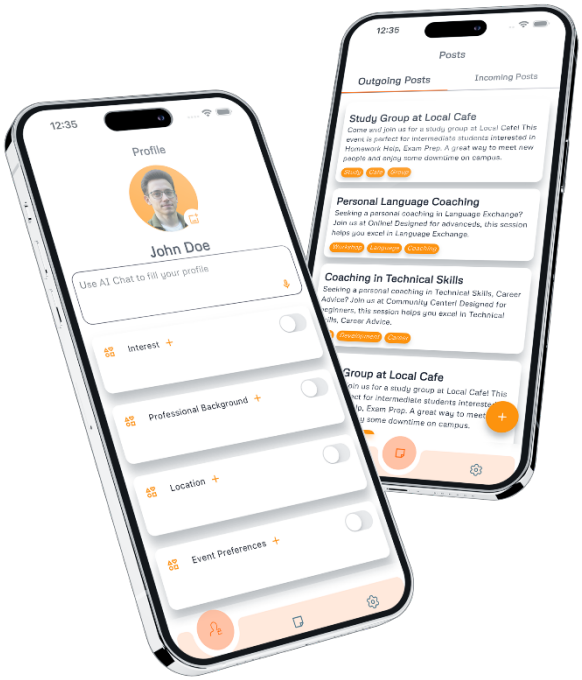
# Lucii

link-up . create . interact . inspire



# Contents

1. Introduction and problem definition ..... 2

2. Basics ..... 3

2.1 Centralized vs. decentralized solutions: Security, trust, efficiency ..... 3

2.2 The matrix protocol ..... 5

2.3 AI on Edge ..... 6

3. Lucii: Link-up - create - interact - inspire ..... 7

3.1 Overview - Functionality ..... 7

3.2 Development phases - AI models ..... 9

4. Lucii: Implementation and user journey ..... 13

5. Conclusion and outlook ..... 18

# 1. Introduction and problem definition

The aim of the InduKo project was to promote innovation through collaboration. However, in order for collaboration and communication to take place, the right people must first connect with each other. The university landscape is characterized by a high level of diversity: students, lecturers, researchers, administrative staff, alumni, corporate partners and external experts each bring different skills, interests and perspectives to the table, which offer enormous potential for (interdisciplinary) collaboration and innovative solutions. However, this potential often remains untapped due to a lack of suitable mechanisms to bring the right people together. Instead, there are often fragmented approaches that only address isolated parts of this network, which means that many fruitful collaborations remain undiscovered. A major obstacle is that people with similar interests or complementary skills often do not meet, even if they work at the same institution. Interdisciplinary research and innovation projects or student start-up initiatives, for example, could benefit considerably from targeted networking opportunities, or students preparing for challenging exams could more quickly find collaborators for specialized study groups or tutoring. Alumni, who provide valuable professional contacts, mentoring, or internship opportunities, often face organizational hurdles that complicate engagement with potential collaborators. More efficient networking could also make it easier for corporate partners to identify young talent whose profiles are tailored to specific positions. The benefits of efficient networking extend far beyond the boundaries of individual universities.

Although universities, colleges and research institutions are increasingly relying on digital platforms to facilitate exchanges between teachers, students and researchers from different disciplines, conventional communication tools - such as emails, central messaging applications or forums managed by institutions - are often neither sufficiently suitable nor privacy-friendly, and they focus much less on bringing people together initially and more on communication once networking has already taken place. At the same time, central platforms are usually operated by institutions, leading to a loss of user control over their data. For understandable reasons, many platforms operated by public institutions refrain from very extensive profiling functions because the management of highly sensitive data entails a responsibility and liability risk that public educational institutions are neither willing nor able to assume - especially in view of potential weaknesses in IT security or possible cyber attacks. However, successful networking requires precisely this detailed data on the interests, skills, research focus, language skills, experience and personal characteristics of those involved.

Another challenge is the fragmentation of data sources. Currently, students exchange information informally in chat groups, for example, while student councils and initiatives distribute their announcements via various channels. Alumni networks are often limited to contact lists and companies rely on individual collaborations that often do not make use of the breadth of the academic network. Research projects and results are often published on various platforms, including project and institute websites, scientific repositories or conference sites. The visibility of researchers is further limited by the fact that their profiles are spread across different platforms such as university or research

websites or LinkedIn. This fragmented information landscape makes it difficult to bring people or resources together efficiently. In some cases, however, current projects are deliberately not published anywhere because the work is still at an early stage. Nevertheless, in such cases it can often be very helpful to find collaborators for a start-up idea or a research project, for example.

At the same time, there is a natural skepticism towards central platforms that could bundle all information, and not without reason. Centralized solutions are prone to data protection problems because a single breach of security can have catastrophic consequences. A centralized system is undoubtedly efficient, but carries a significant risk of losing sensitive data to third parties. In particular, the integration of modern AI technologies such as large language models exacerbates this problem because such models store information in parameter space, making it almost impossible to delete personal data retrospectively.

The tension between the need for networking and the requirements for data protection and security is complex. The aim would be to find a solution that exploits the enormous networking potential in the university context and at the same time ensures the best possible data protection and security for those involved in order to promote communication and collaboration. Before we present this solution, which was developed as part of a sub-project of the InduKo project (Innovation through Collaboration) funded by the Stiftung für Innovation in der Hochschullehre on the basis of the matrix messaging protocol, we will first briefly describe aspects of centralized and decentralized solutions. Building on this, the matrix protocol is presented as a suitable communication architecture that is characterized by its decentralized, open and federated structure. In addition to the matrix messaging protocol, another central component of our problem solution is the concept of AI on Edge, in which the AI is executed directly on the end devices in order to minimize the central data flow and protect the privacy of the users. Finally, the mobile application "Lucii" (link-up - create - interact - inspire) developed by us illustrates how these concepts can be put into practice in order to address the challenges mentioned with modern tools in the best possible way.

# 2. Basics

## 2.1 Centralized vs. decentralized solutions: Security, trust, efficiency.

A central solution to the problem outlined above would require a system that collects, processes and manages all relevant data about the actors in one place. In such a scenario, users could create detailed profiles containing information on interests, skills and other personal characteristics. These profiles would be collected by a central entity that analyzes them with the help of AI algorithms to connect suitable people, groups or projects. The advantage of such an approach lies in its efficiency. Central platforms can analyse large amounts of data, create precise suggestions and enable highly personalized matching by using comprehensive models such as large language models. Thanks to the

technologies available today, the implementation of such a centralized system would be well supported by numerous proven technical solutions or tools. Cloud computing services, pre-trained AI models and established, very powerful platform structures from various large providers offer a robust basis for implementing such systems efficiently and scalably with manageable effort.

However, the risks are considerable; centralized data storage makes the system more susceptible to external attacks, for example. Cyber criminals could access personal information, manipulate it or use it for improper purposes. Such a system also harbours risks of internal misuse, such as unauthorized employees gaining access to sensitive data. The storage of data in centralized AI models also raises the problem already mentioned: Once data has flowed into a model, it cannot be easily removed. The diffuse storage of information in the parameter space of neural networks prevents simple and targeted deletion, as would be the case, for example, when deleting a data record from an SQL database. In addition, users must trust the platform operator, even if the corresponding data protection agreements are very well formulated in the interests of the users to ensure that this agreement is actually adhered to and does not offer any legal loopholes. This lack of transparency and autonomy undermines trust in the platform and can lead to a reluctance to disclose information. The risk of poorer data quality as a result should not be underestimated: If users are reluctant to provide complete or correct information due to data protection concerns or a lack of trust, this significantly reduces the effectiveness of the system and can lead to poorer or incorrect recommendations.

Centralized systems concentrate all data traffic and control in one place, which not only makes them more vulnerable to attacks, but also to failures. As soon as a core system is disrupted or a security incident occurs, this has an immediate impact on all users and stakeholders. Such a centralized architecture results in a single point of failure. Decentralized approaches, on the other hand, distribute responsibility and spread the system across many components , which increases overall resilience, as no single failure automatically leads to a collapse of the entire ecosystem

A centralized approach also raises complex questions from a legal perspective. It raises the fundamental question of who "owns" the data fed into the system or who holds the ownership rights to it. In addition, responsibility for errors, misuse of data or breaches of legal requirements can become a considerable burden, which could deter public institutions in particular from operating a centralized system.

Another key aspect concerns access control. In a complex university environment with numerous organizational units, departments, projects and external partners, defining rights, roles and responsibilities is a challenging task. Controlling who is allowed to view, process and pass on which information is usually extremely time-consuming in a centralized, monolithic system. This challenge is exacerbated if the framework conditions, personnel responsibilities or legal requirements change over time.

Overall, the central concentration of data leads to a structure that is technically efficient, easy to implement and easily scalable, but in many respects harbors considerable risks, dependencies and

uncertainties. Especially in the sensitive university context, which is characterized by high diversity, autonomy and innovation, these disadvantages weigh heavily. Ultimately, the architecture of a centralized system leads to an inherent weakness that cannot be remedied by technical security measures alone. A decentralized approach solves many of these problems by shifting the processing, storage and control of personal data entirely to the users' end devices. This eliminates the need for a central data pool as a single point of failure, for example, as there is no concentrated instance on which "worthwhile" attacks could focus or whose failure could paralyze the entire system. In addition, each person retains full control over their own data and can make changes or carry out deletions without having to rely on a central point. This not only eliminates key vulnerabilities such as susceptibility to outages and attacks, limited data sovereignty, legal uncertainties, complex access structures and the problem of making it difficult to remove personal information once it has been entered into a central LLM. Instead, an environment is created in which data protection, privacy and autonomy are inherently strengthened, thus creating the basis for a sustainably trustworthy and flexibly adaptable networking ecosystem.

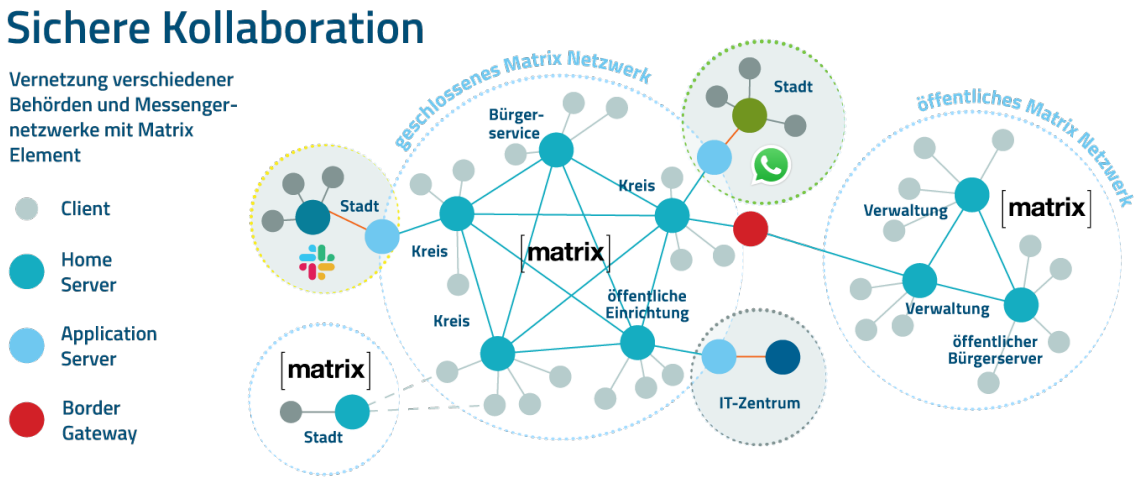
Security and confidentiality must also consistently cover the transportation of data in order to ensure a trustworthy system. End-to-end encryption is of central importance here, as it ensures that only the end devices involved have access to the decrypted content. It goes without saying that even the servers carrying out the transmission must not be able to view the data. With its end-to-end encrypted transmission and proven communication architecture, the matrix messaging protocol provides an excellent basis for secure, trustworthy and scalable networking solutions.

## 2.2 The matrix protocol

The Matrix protocol has become an established basis for decentralized, secure and flexible real-time communication. It offers an open infrastructure based on federated networks and interoperable interfaces. This approach promotes data privacy, data sovereignty and long-term scalability. This is precisely why Matrix is of interest to individuals, companies, governments and non-profit organizations alike.

Technically, the protocol is based on a REST-like JSON API that ensures standardized exchange between clients and servers. Matrix rooms act as basic communication units and can receive text messages, files, voice calls, video conferences or bots. Thanks to their flexibility, they can be used to map individual conversations, entire communities or even complete organizational structures. The matrix messaging protocol offers end-to-end encryption directly on the end devices so that only the people involved can read the content. However, E2EE is not necessarily preset for all rooms. Open, public spaces are sometimes deliberately operated without encryption so that they are easier to find and more people can participate easily.

"Federation" is a central element of Matrix. It ensures reliability, scalability and prevents dependency on centralized locations. Everyone can decide for themselves whether they want to operate their own server or use an existing one, without losing the ability to communicate with participants on other instances. For organizations, this results in a platform that can be used both internally and externally. A self-hosted matrix server offers control over your own data. Sensitive information can be stored in your own IT infrastructure, which is particularly important for companies, authorities and non-profit organizations that have to comply with strict data protection regulations or legal requirements. This is probably why Matrix is now increasingly being used in government contexts. One example is the French government, which operates its own communication solution based on Matrix with "Tchap". In Germany, the "BundesMessenger" was launched under the responsibility of BWI - a federally owned IT service provider that works primarily for the German armed forces and other authorities. This tool is also based on the Matrix protocol, is specially tailored to the requirements of public administration and the federal messenger for authorities based on it can be used without additional fees. In addition, gematik, which is responsible for the digitalization of the healthcare system, uses the protocol for the so-called TI Messenger. This project aims to enable secure and interoperable communication in the healthcare sector while at the same time meeting the high standards of data protection and data security.




*Source: https://nordeck.net/matrix-loesungen/*

## 2.3 AI on Edge

For a long time, powerful AI applications were run almost exclusively in central data centers or not on mobile devices, mainly due to the hardware required. In recent years, however, there has been a trend towards "AI on Edge" or "Edge AI". This refers to AI processing directly on the end device itself, e.g. on a smartphone or tablet. In addition to advantages such as the ability to use it offline, one of the key drivers behind this change is the increased desire for more privacy: if all calculations are

performed locally, no sensitive data needs to be sent to remote servers, which reduces the risk of data leaks and strengthens users' trust in the respective AI application. As the models run directly on the end device, they can also be better tailored to individual preferences and usage habits without permanently transmitting this information to external services. In addition, local data processing becomes noticeably more secure: even if external systems are compromised, the sensitive information remains in the hands of the user.

This development has been made possible by increasingly powerful modern end devices, which are increasingly capable of executing even complex AI models. Both Apple and Google, for example, are investing in corresponding hardware and software solutions that enable machine learning on mobile processors. Apple is pursuing this approach with "Apple Intelligence"; these AI-supported functions make it possible to perform tasks such as composing and summarizing texts directly on the device. Google has also made significant progress in the area of Edge AI. With the introduction of Gemini Nano and the Google AI Edge SDK, developers can integrate generative AI functions directly into mobile applications. These tools also make it possible to perform tasks such as text rephrasing, intelligent responses and text summaries locally on supported devices. These developments and the increased commitment of leading companies illustrate the growing importance of AI on Edge. As devices become more powerful, it is expected that the trend towards local execution of AI models will continue to grow, opening up new opportunities for personalized, secure applications.

# 3. Lucii: Link-up - create - interact - inspire

## 3.1 Overview - How it works

The concepts described above are put into practice in the Lucii mobile application. Lucii was specially developed to promote collaboration without passing on sensitive personal or institutional data to central servers. The architecture ensures that profiles and calculation results are stored locally; critical calculations take place in protected storage areas where neither encryption keys nor intermediate results can be viewed externally. By dispensing with central data storage, Lucii reduces the risk of data leaks, unauthorized access and violations of data protection guidelines such as the GDPR. At its core, Lucii relies on lightweight neural network models that are specially optimized for low-resource environments such as mobile devices or IoT nodes. The development progressed step by step from "Convolutional Neural Networks (CNNs)" to more sophisticated "DistilBERT" transformer architectures and optimized frameworks such as "Gemini Nano". Lucii uses the matrix messaging protocol for communication, allowing messages to be exchanged securely and scalably.

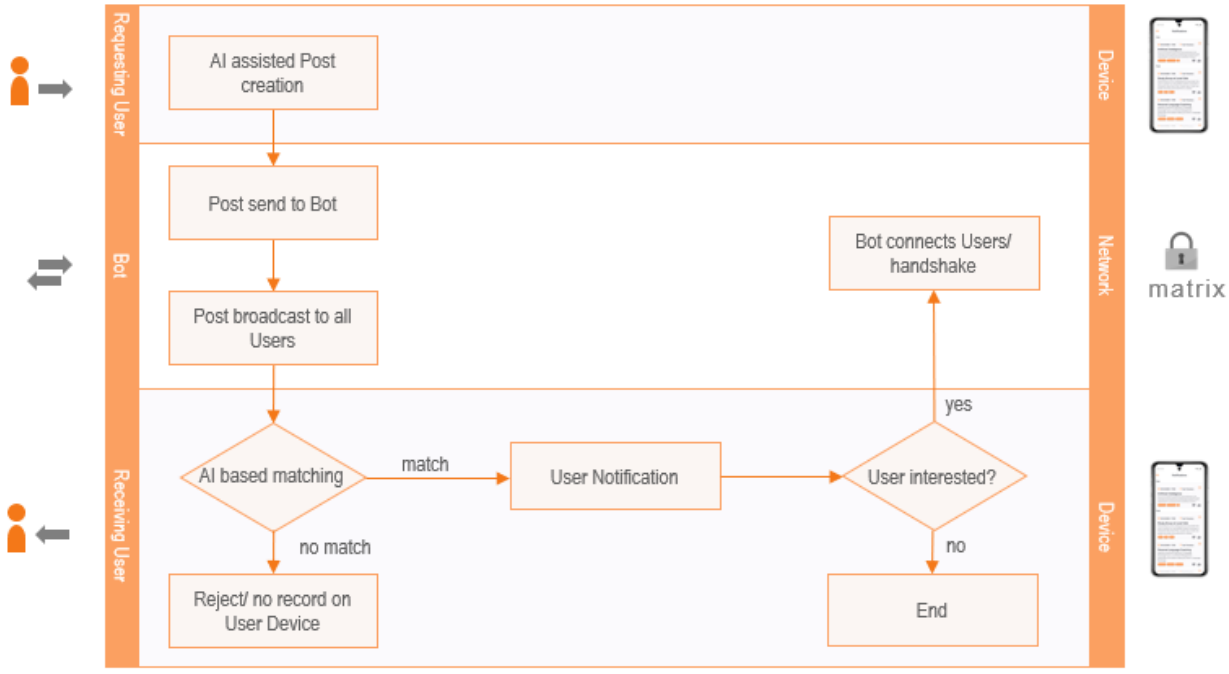
The practical implementation of matching takes place in several stages. Users first store their profile data locally on their device, including, for example, skills, interests and project priorities. The profile creation itself is also supported by AI - the users enter a descriptive text and the AI on the device

extracts the matching keywords; this data can also include very sensitive information because it never leaves the device, only so-called "posts" are encrypted and fed anonymously into the network via the matrix protocol.

Anyone can create a post to formulate a specific request - be it the search for a research partner, the search for a learning group, a reference to a workshop or the offer of a collaboration. These posts are digital entries created by users to send requests to other users. They take on the function of a notice board, so to speak, with the crucial difference that they are neither publicly visible nor contain personal contact information and that AI on Edge ensures efficient matching.

The Matrix protocol ensures that posts are distributed securely and decentrally. The local AI decides whether a post matches a person by comparing the post with the profile data stored on the device. The AI models described above are used to recognize semantic connections between the posts and the user's interests. As a result, thematically related posts are also recognized, even if they are formulated differently. If the AI detects a match, the person concerned receives a notification about the relevant post without the creator finding out about it. Unlike traditional networks or platforms, where public lists are searched or direct contact requests are made, Lucii works according to the principle that only thematically relevant posts are displayed via notification. Only when both parties confirm their interest can they gradually exchange further information in an anonymous chat.

With this system, Lucii replaces conventional methods of making contact with intelligent, anonymous and decentralized matching via posts. It combines the outdated principle of a bulletin board with modern AI technologies and encrypted communication so that users can make targeted connections without having to disclose personal information.




*Matching - Schematic diagram*

Lucii demonstrates how advanced technologies such as the Matrix protocol and on-device AI such as DistilBERT or Gemini Nano can be successfully combined to create a data protection-friendly, secure and efficient networking tool in the university environment

## 3.2 Development phases - AI models

As already mentioned, the development process for the Lucii app involved several stages. Each phase built on the knowledge gained in the previous phase and rectified the weaknesses identified there. In this way, accuracy, speed (latency) and memory requirements were gradually optimized. This chapter describes the respective model setups, training methods and optimization measures. It also presents the key figures that were used to evaluate and compare the individual development stages. Synthetic data sets generated with GPT-3 were used to train and evaluate the model. These simulate a variety of user profiles and events so that no real personal data had to be collected, stored or processed. The evaluation focuses on metrics that measure the performance of the system in real-time profiling and matching events to users. The F1 score is used to measure the balance between precision and recall. Recall specifically measures the ability of the system to correctly identify all relevant events. Latency is analyzed to ensure that the system performance meets the requirements for real-time operation. In addition, a similarity matrix is used to assess the accuracy of user profile creation and matching.

**Phase 1: Basic CNN model**

The first step was to develop a basic CNN that performs basic user profiling and event mapping tasks. Although Convolutional Neural Networks are typically used in image processing, they can also recognize relevant text patterns using convolutional kernels applied to word embeddings.

In this phase, a synthetic data set was used that mapped user interests, location preferences, event types and professional specializations, among other things. Pre-trained embeddings (e.g. Word2Vec) were used to obtain meaningful language representations. The most important steps in data pre-processing included tokenization, the removal of stop words and stemming or lemmatization.

The CNN architecture comprised an embedding layer that converted the text into feature vectors, followed by two convolutional layers with ReLU activation that extracted local text patterns in the tokenized sequences. Pooling layers were then used to reduce the dimensions and highlight relevant feature expressions. One or more fully connected layers were used for the actual classification and provided probabilities for different classes via softmax activation.


*Architecture of the CNN model used in phase 1*

The model was trained with the Adam optimizer and the categorical cross-entropy as a loss function. In addition, an early-stopping mechanism was implemented to prevent overfitting. The hyperparameters (e.g. number and size of filters, learning rate, batch size) were specifically fine-tuned, which ultimately led to moderate accuracy.

| Category | Accuracy |
|---|---|
| Interests | 84% |
| Location Preferences | 78% |
| Event Preferences | 80% |
| Professional Background | 79% |
| Social Preferences | 82% |

*Phase 1 CNN Performance Metrics*

The computational effort and model size remained at an acceptable level. The average inference time was 1.2 seconds; the model size was 5 MB, making it compatible with mid-range devices. However, the model had difficulties with nuanced natural language input and showed limited adaptability.

This first version served as a reference point. The deficits identified in dealing with complicated linguistic structures were the deciding factor in the next phase to switch to a more powerful method that can better represent contextual information.

**Phase 2: DistilBERT approach with improved language processing**

To overcome the limitations of the CNN model identified in phase 1, DistilBERT was introduced in phase 2 - a compressed, transformer-based architecture based on BERT (Bidirectional Encoder Representations from Transformers). DistilBERT offers a good compromise between computational effort and semantic accuracy and enables significantly improved recognition of complex speech input directly on the end device.

In contrast to the previous CNN approach, DistilBERT requires more complex pre-processing. The input data is first decomposed using WordPiece tokenization, with special symbols such as [CLS] and [SEP] marking sentence or section boundaries. DistilBERT then calculates contextual embeddings that capture bidirectional dependencies. A downstream classification layer (one or more Fully Connected Layers) processes these embeddings and outputs classification values (logits) for prediction.


*Architecture of the DistilBERT model used in phase 1*

Initially, DistilBERT was fine-tuned on synthetic datasets generated using GPT-3, simulating a variety of researcher profiles and event descriptions. Pruning and quantization techniques were used to downsize the model for use on mobile and embedded devices, reducing the model size from around 330 MB to around 30 MB. The model was then converted to TFLite format for more resource-efficient inference.

Despite these optimizations, the computing requirements of DistilBERT are higher than those of the original CNN, which is particularly noticeable on devices with low performance.

| Category | Accuracy |
|---|---|
| Interests | 92% |
| Location Preferences | 88% |
| Event Preferences | 90% |
| Professional Background | 90% |
| Social Preferences | 87% |

*Phase 2 (DistilBERT) Performance Metrics*

The accuracy improved to 99.5% and the average inference time was 2.5 seconds. Although the model achieved higher accuracy, its higher computational requirements made it difficult to use on less powerful devices and the static updates limited real-time adaptability. Despite the clear progress in terms of speech understanding and classification quality, this shows new limits in terms of computing power and memory requirements, which are to be further optimized in the following development steps

**Phase 3: Optimization with the Gemini Nano Model**

Phase 3 dealt with the optimization of the Lucii application for use under real conditions. Gemini Nano, a lightweight model developed for edge computing, was integrated to ensure high classification accuracy with reduced computational requirements and latency. The goal was to reliably run the AI model on mobile devices without sacrificing profiling accuracy. Gemini Nano combines convolutional and transformer-based components in a hybrid architecture, which enables efficient text classification. Quantization and pruning reduced the model size to 10 MB, while knowledge distillation was used with DistilBERT as the teacher model and Gemini Nano as the student, controlled by cross entropy and Kullback-Leibler divergence.


*Architecture of the DistilBERT model used in phase 1*

An interactive feedback mechanism was also introduced as part of this phase, allowing users to refine their profiles using natural language input. Secure communication based on the Matrix protocol ensures that matching results can be transmitted in real time.

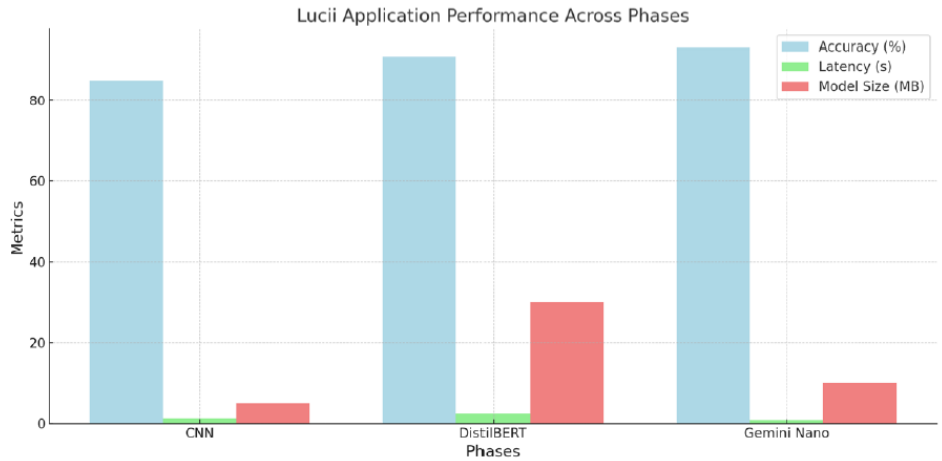
| Category | Accuracy |
|---|---|
| Interests | 95% |
| Location Preferences | 93% |
| Event Preferences | 94% |
| Professional Background | 92% |
| Social Preferences | 91% |

*Phase 3 Gemini Nano Performance Metrics*

The match confidence increased to 99.56%, while the average inference time decreased to 0.8 seconds. These results show that Gemini Nano successfully overcomes the challenges of the previous phases and also offers high performance on mobile devices.

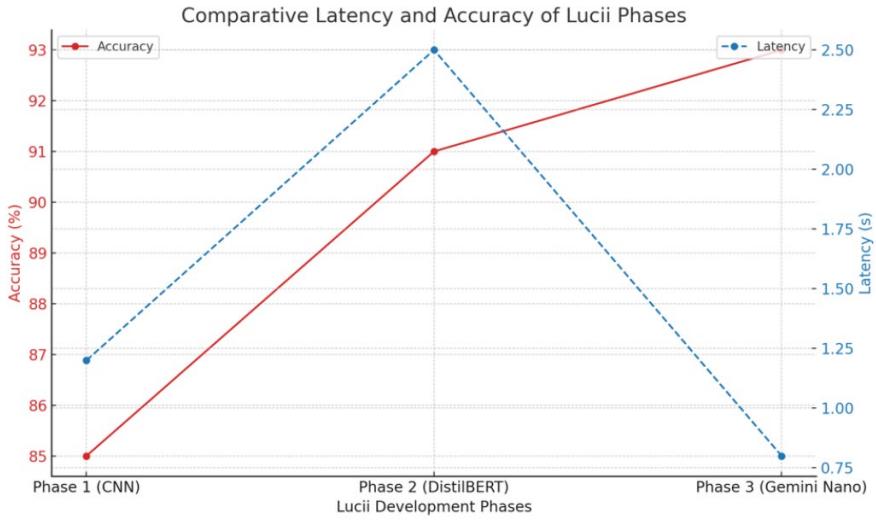
**Results across the development phases**

The Gemini-Nano model showed the best balance between accuracy and efficiency and is therefore particularly suitable for use directly on the device.




| Metric | Phase 1 (CNN) | Phase 2 (DistilBERT) | Phase 3 (Gemini Nano) |
|---|---|---|---|
| Accuracy | 85% | 91% | 93% |
| Latency (s) | 1.2 | 2.5 | 0.8 |
| Model Size (MB) | 5 | 30 | 10 |

The experimental evaluation of the framework proves its effectiveness through high accuracy and low latency times.



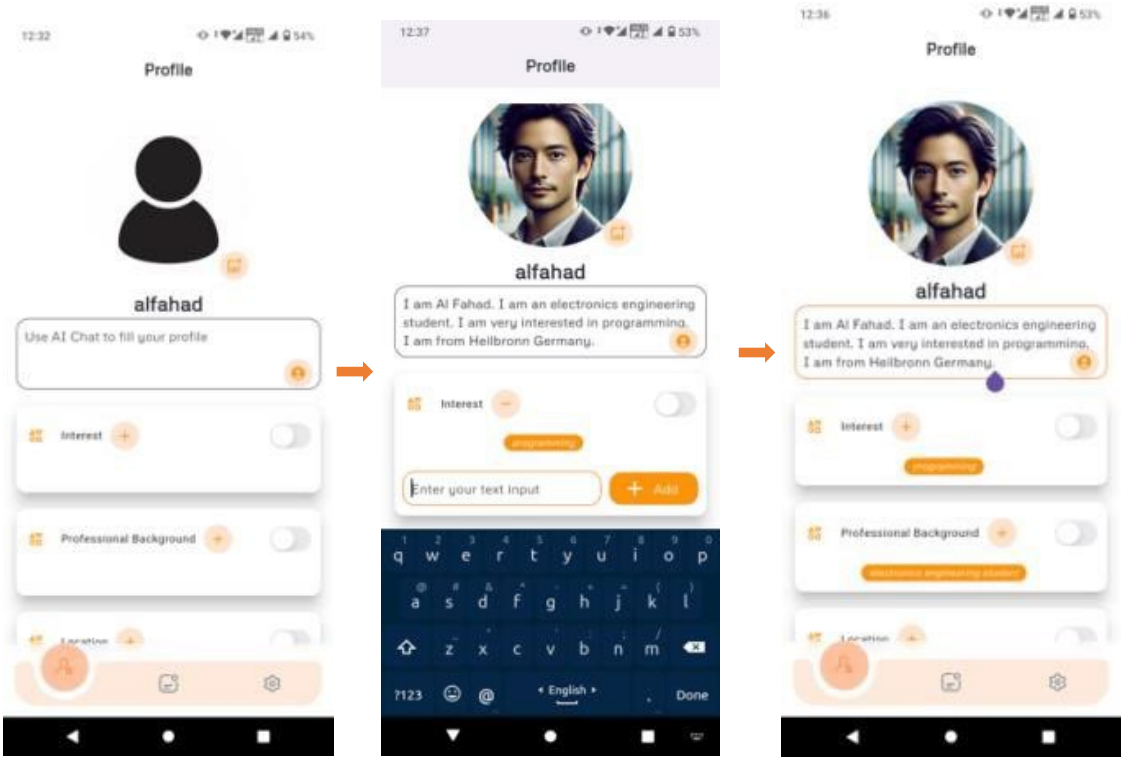

# 4. Lucii: Implementation and user journey

The iterative development of Lucii's AI models, culminating in the implementation of Gemini Nano, enables the system to provide privacy-friendly, yet generally accurate and responsive event matching directly on users' devices. At the same time, the communication infrastructure and security measures were further developed and an interactive feedback process was introduced. Federated communication via the matrix protocol was also tested in controlled trials. External data transfers are carried out via SSL and HTTPS, while anonymized tokens and temporary IDs ensure that no personally identifiable information (PII) is disclosed.

In the final version of Lucii, the user journey includes all essential functions: From creating a profile to creating posts and interactive message management, all steps of a realistic workflow are covered.

**Profiling**

Users start by entering their interests, professional background, location and preferences in natural language. Gemini Nano processes this information locally, extracts relevant keywords and stores them securely.




*Empty profile* *Text* input/keyword recognition Profile

Keyword recognition and categorization accuracy averaged 93%, matching the performance of the final Gemini Nano model. On mid-range smartphones, latency remained below one second, ensuring the responsiveness required for a seamless user experience.

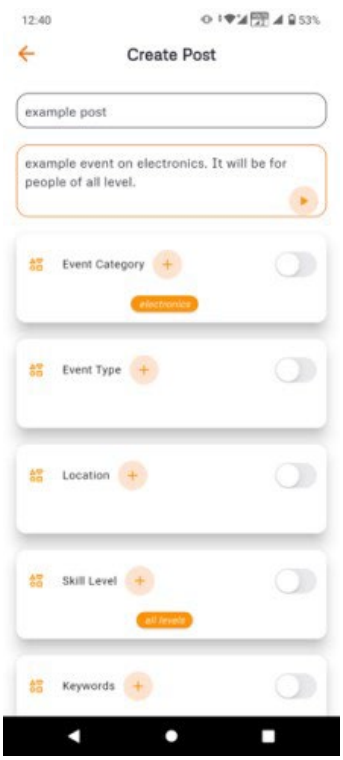
The screenshot on the left shows the empty profile with the predefined categories such as interests and professional background. In the middle, you can see how the system automatically extracts relevant keywords directly on the device by entering a text, for example an existing description from a job portal that you could copy and paste. This procedure not only makes work easier, it also leads to more consistent entries and higher data quality. Typing errors or unclear formulations due to manual input can thus be largely avoided by this type of AI-based, systematic categorization; this is a significant advantage over purely manual input procedures and contributes to the reliability of the entire system. Profile information can also be temporarily deactivated via corresponding switches if matching is not currently desired with regard to these categories.

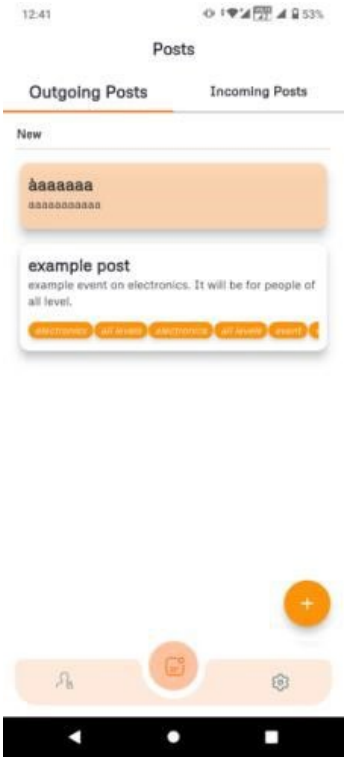
Profile updates secured by JWT authentication prevent unauthorized changes. Experiments have shown that model re-inference after the addition of keywords provides updated recommendations in less than a second, enabling real-time customization.

**Creation of outgoing posts**

With so-called posts, users publish contributions that function like a digital notice on a virtual pin-board, with the difference that this information cannot be viewed by everyone. Posts can be used to find fellow campaigners for start-ups, research projects, study groups or other initiatives, for example, if there are special interests, expertise or health restrictions and people are looking for collaboration or contact. These posts are automatically tagged when they are created, as is the case with profile information. Anonymized tokens are used instead of user IDs to protect personal information and identity.

Experimental evaluations showed that the automatic tagging precisely matched the interests in over 90% of the cases tested, demonstrating that the semantic understanding provided by Gemini Nano delivers high accuracy.

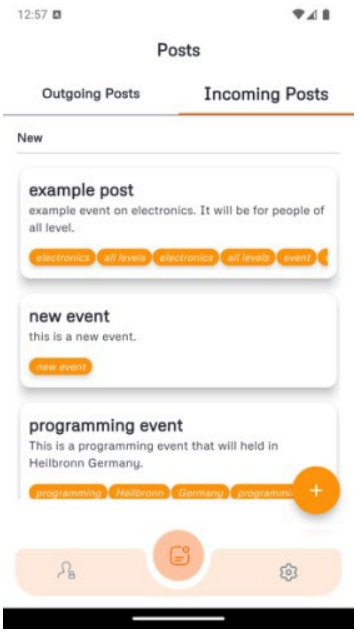



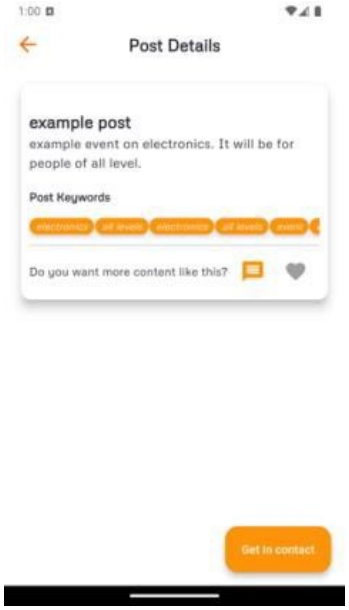

*"Create New Post"* *Text* input/keyword recognition "Outgoing Posts"

**Incoming posts**

Only if the local AI on the device recognizes a match between a post and the information stored in the profile will an incoming post be displayed on the end devices. Users can check the new incoming posts and identify events or cooperation opportunities that match their profiles. Relevance is the key success criterion here: In over 92% of the simulations carried out, the suggested posts were judged to be relevant and contextually appropriate to the respective interests.




*"Incoming Posts"*




*"Post Details"*

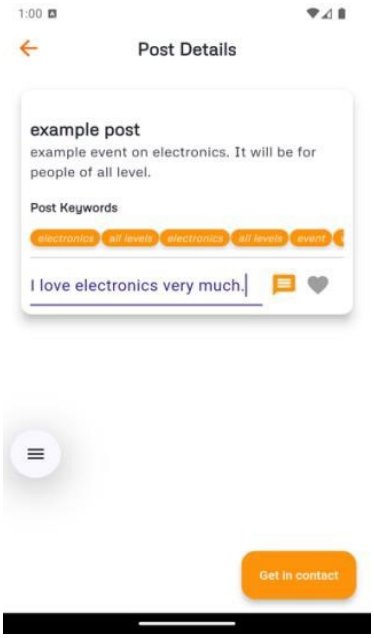
**Anonymous contact via chat**

If a user considers an incoming contribution to be interesting, there is first the option of anonymous contact via chat to clarify any further details before actual contact details are exchanged. Stable encryption and a token-based identity system are used for private conversations between anonymous participants. The latency in establishing the end-to-end encrypted communication channels remained consistently low, with average transmission times of less than 200 milliseconds.


*Possibility to exchange anonymous messages*

**Feedback and recommendation refinement**

Users have the opportunity to leave natural language feedback in order to refine future recommendations. This option goes beyond the traditional "like" or "don't like" label and enables more extensive model improvements. Gemini Nano processes this input locally, updating its internal representations without exposing the data externally.




*Feedback and recommendation refinement*

**Safety test**

To ensure that data protection and security requirements are met, a series of penetration tests and vulnerability scans were carried out. The SSL/TLS configurations were checked and 100% secure transmission was confirmed. JWT tokens were exposed to replay attacks in isolated environments without logging unauthorized profile changes. The use of anonymized tokens also prevented personally identifiable information (PII) from being exposed in simulated attacks. Furthermore, the backend validation in the area of event processing showed no evidence of injection or DoS vulnerabilities. The consistent use of HTTPS for all external requests effectively prevented the unauthorized reading of personal data. In the final implementation, none of the attack attempts lead to an impairment of the anonymity or integrity of the data.

# 5. Conclusion and outlook

The project results show that the innovative linking of the matrix messaging protocol with AI on Edge can specifically improve the networking of people in higher education without jeopardizing data protection. Traditional platforms that rely on large amounts of data and cloud-based processing do not offer a satisfactory solution here, as they create dependencies, pose security risks and are often incompatible with data protection and ethical requirements. The decentralized solution concept presented here offers an innovative alternative. By combining the matrix protocol for secure, federated communication with AI on Edge, a system is created that combines data protection and user-friendliness. Lucii shows that intelligent, AI-supported matching processes can be user-friendly even without centralized data storage. Anonymous communication, secure encryption and the ability to improve the quality of recommendations through natural language feedback offer additional innovative improvements for networking in the university environment.

Lucii has demonstrated the feasibility and potential of such a solution; a larger test outside of development, i.e. a practical test with a broader user group, is required in order to make targeted improvements and further develop the system into a stable, operational solution. Future work could also involve testing Lucii in various application scenarios - for example in a university network, with cooperating companies, non-profit organizations or research networks. Advances in the hardware of mobile devices, more efficient model compression and the integration of explainable AI approaches offer further opportunities to improve the system in the future.