XIAOMI TRUSTWORTHY AI WHITE PAPER

2021.05

Contents

Summary

As a global leading smartphone manufacturer, Xiaomi is dedicated to developing Trustworthy Artificial Intelligence (AI) technologies (hereinafter referred to as "Trustworthy AI") to benefit and empower every user. To this end, Xiaomi adheres to the internationally recognized ethical standards in the development and application of AI technology. Taking into account of EU's *Ethics Guidelines for Trustworthy AI*, combined with Xiaomi's practice and culture, we have set up four basic principles for Xiaomi Trustworthy AI, covering security and safety, privacy, fairness and explainability. These principles will be implemented throughout the the course of research, development and application of all Xiaomi services and products involving AI technology.

This white paper comprehensively describes how to apply the above basic Trustworthy AI principles to different scenarios of Xiaomi AI services, including Voice Call Noise Reduction, Camera Image Optimization, Face Unlock and Fingerprint Unlock. Xiaomi has taken technological and non-technological measures to ensure the security and safety, privacy, fairness and explainability of the algorithm and operation flow in each scenario.

With regard to technological measures, Xiaomi has built security architecture to ensure the security of the algorithm operating environment and user information. Xiaomi AI model is deeply integrated into the device and only runs locally. The data processed by the AI algorithm will not be backed up or transferred to any other location. The algorithm can only be activated under the authorization of users, and only processes data necessary for the purpose of providing services in compliance with the principle of data minimization. Before the algorithm is released, Xiaomi records and manually verifies the training data, training process, and training results of the algorithm under sufficient tests. In the Application chapter, we will give a detailed description of the technical measures for implementing Trustworthy AI under each scenario.

With regard to non-technological measures, Xiaomi has built a complete management system, including an AI Ethics Committee and a Security and Privacy Committee, to supervise our AI operation flow and achieve best practice. In order to continuously safeguard the implementation of Trustworthy AI principles, Xiaomi continuously improves user engagement, internal audit, risk control and other relevant mechanisms. To maintain the reliability of our AI products and services in the face of technological and social changes, we actively accept public supervision, communicate with our users, obtain official certifications, publish white papers, update privacy policies when necessary, and take every possible measure to strengthen user confidence in our AI products and services.

Overall, Xiaomi scrupulously adheres to the ethical norms of the AI industry throughout the research, development and application of AI. We focus on humanism and strive to ensure that our AI technologies are always used in a way that protects the wellbeing and basic rights of our users.

Declaration

This document only serves as reference guidelines for public to understand the basic principles of Xiaomi Trustworthy AI, and the technical measures, capacity building, user data security and privacy protection involved in implementing Trustworthy AI. Based on the current hardware architecture and Trustworthy AI technology, Xiaomi provides corresponding introductions. However, in view of potential problems such as technology upgrades, product iterations, changes of applicable laws and regulations and consistency of wording, Xiaomi hereby expressly declares that we do not offer any guarantees, whether explicitly or implicitly, to the completeness, accuracy or applicability of the content of this document.

In accordance with relevant laws, Xiaomi and its affiliates (hereinafter collectively referred to as "Xiaomi") own the intellectual property rights for all original content by Xiaomi in this document, including but not limited to images, architecture designs, descriptive texts, etc.. No organization, company or individual may extract, translate or copy the content of this document, in part or in whole, without the prior written consent of Xiaomi.The content of this document may change, subject to the upgrades and adjustments to Xiaomi products or services or other reasons, Xiaomi has the right to add, modify, delete or nullify the content of this document. Please download the latest version from the official website in time.

If you find any errors in this document or have any questions about the content of this document, please contact Xiaomi directly at security@xiaomi.com.

01

Principles

1. Principles

As a global leading smartphone manufacturer, Xiaomi relentlessly builds amazing products with honest prices to let everyone in the world enjoy a better life through innovative technology. Xiaomi is dedicated to developing trustworthy artificial intelligence technologies to benefit and empower every user. To this end, Xiaomi has used AI technologies in the following four services: Voice Call Noise Reduction, Camera Image Optimization, Face Unlock and Fingerprint Unlock. Throughout the development, design, manufacturing, operation and service stages of AI, Xiaomi ensure that AI technologies are always used to enhance and enrich the user experience of electronics products. Xiaomi adheres to the internationally recognized values in EU's *Ethics Guidelines for Trustworthy AI* during the course of development and application of AI. Combined with the practice and culture of Xiaomi, we have also set up four basic principles of Xiaomi trustworthy AI, covering **security and safety, privacy, fairness, and explainability**. These principles will be implemented throughout the development and application of all Xiaomi AI services.

- **Security and Safety**

Xiaomi is firmly dedicated to ensuring security and safety throughout development and application of trustworthy AI technologies, providing users with safe and trustworthy AI products and services and making sure that our trustworthy AI will not do any harm to society. We undertake research and development in line with the best practices for secure AI, ensuring that the use of Xiaomi AI technologies is within the limits of enhancing and enriching the experience of our consumers. In order to ensure the safety and to avoid the security threat caused by system out of control, Xiaomi continuously improves the maturity, robustness and anti-interference ability of AI technology on the basis of evaluating the security risk of AI, ensuring that AI can be supervised and taken over by human beings in time. In the meantime, we have adopted various security protection measures and supervisory mechanisms to control and test the processes, evaluate security risks regularly and avoid accidental consequences resulting from the risks, ensuring the reliability and accuracy of the results.

- **Privacy**

Xiaomi always puts user privacy protection at the heart of our technologies, products and services. We are dedicated to protecting our users' privacy and personal data in line with high standards (e.g.EU's *General Data Protection Regulation*) throughout the entire life-cycle of AI and we aim to achieve best practice, rather than mere compliance with laws and regulations. Xiaomi has established strict user data protection policies and a Security and Privacy Committee to supervise their implementation. We regularly conduct internal and external audits on privacy compliance, proactively participate in the establishment of relevant industry standards and ensure that Xiaomi and its affiliates respect and protect user privacy. We comply with the principle of data minimization, AI models only collect the data necessary for providing relevant services. We never use users' data to train AI models. All training data comes from legitimate sources and has been reviewed for compliance. We try our utmost to avoid risks that may arise during the transmission of user data by deploying AI models on the local device, and we use multiple encryption technologies to ensure the security of user data.

- **Fairness**

Xiaomi always believes that AI should treat everyone fairly, reduce bias and avoid unfair influences. AI technologies, when properly calibrated, can help improve the fairness in decision-making, process and evaluate facts faster and more effectively, or allocate resources more fairly. For example, all data used to train AI models is screened by professionals to ensure its comprehensiveness and fairness and to avoid discrimination and bias against particular groups.

- **Explainability**

The lack of transparency inherent in AI systems, which is often known as the "black box" problem, may compromise the credibility of AI products for users. Xiaomi is devoted to making our AI technology as explainable as possible to the extent that technololgy allows. We keep records of all processes throughout the whole life cycle of AI systems to ensure that the output and logic of AI technology can be better understood, thus improving the traceability of the output in order to identify and solve any problem that may arise. At the same time, we tell our users where our AI systems operate, what tangible functions they can realize, and what changes they will bring to users via product information, marketing communications and multiple other channels.

EU Framework of Trustworthy AI 7 Key Requirements	Xiaomi Trustworthy AI 4 Basic Principles
Human agency and oversight	Security
Technical robustness and safety	
Privacy and data governance	Privacy
Diversity, non-discrimination and fairness	Fairness
Societal and environmental well-being	
Accountability	Explainability
Transparency	

Chart 1 Trustworthy AI Principles

02

Governance

2. Governance

Xiaomi has established Trustworthy AI Ethics Committee (or "Ethics Committee") in order to provide users with secure, privacy-protective, fair, and explainable Trustworthy AI services. The Committee identifies with the internationally recognized values in the EU's *Ethics Guidelines for Trustworthy AI*, fully respects social ethics, culture, and social norms in different regions, established the four principles of Trustworthy AI of Xiaomi, and is dedicated to providing all of our users with high-quality AI services. Xiaomi's Trustworthy AI Ethics Committee has established an internal supervision mechanism for Trustworthy AI, which requires that all AI research be used only to improve the user experience of consumer electronic products.In order to minimize the occurrence of risk, members of the Ethics Committee assist business teams to jointly identify potential risks and develop countermeasures, and supervise the implementation of the measures at all stages of Trustworthy AI technology research, development and application.

In addition, in order to ensure the implementation of Xiaomi's Trustworthy AI principles, Xiaomi has built a sound Trustworthy AI Management System,including data protection technology, standard process and procedures, assessment and review mechanisms, etc. With regards to the provision of business operating environments and services that are in compliance with laws, regulations and industry standards, Xiaomi has implemented global compliance management and is subject to regular review by external regulatory bodies. The infrastructure, development, operation and maintenance of Xiaomi's Trustworthy AI services comply with the international authoritative certification system and have obtained the international certifications of ISO27001 and ISO27018 from the British Standards Institution (BSI). The MIUI operating system and its built-in applications, which are equipped with Xiaomi's Trustworthy AI services, have been reviewed and verified by TrustArc, the world's leading data privacy management company. Xiaomi's privacy policies and privacy practices comply with TrustArc's standards for assessing corporate privacy and data governance practices and Xiaomi has been awarded a certified privacy seal.

Concurrently, Xiaomi has established guarantee mechanisms, such as user participation, internal audit and continuous evaluation. By doing so, Xiaomi has ensured security and safety, privacy, fairness and explainability of algorithms and operation processes in all scenarios.

- **User participation:** users can give feedback to us through Services & feedback app, customer service, Mi community and other means, when they encounter any problems using Xiaomi TrustWorthy AI service. We will stay open to suggestions from our users, and adjust the algorithm based on feedback, so as to gradually optimize the algorithm and improve the user experience.
- **Internal Audit:** we have an internal algorithm audit mechanism, which is used to evaluate the algorithm, data and design process in order to ensure the clear division of responsibilities in all steps and urge the implementation of measures and policies.
- **Continuous evaluation:** in the process of mobile phone sales and maintenance, we will track user feedback and social feedback, analyze the user requirements, and continuously evaluate the credibility and potential risks of AI algorithm, so as to review the application status of the algorithm and respond in time.

In addition, Xiaomi solicits security issues and information from security researchers around the world through Xiaomi Security Response Centre (SRC), HackerOne, Email and other channels. Xiaomi will assign the confirmed security issues a high priority and solve them as soon as possible.

Contact Xiaomi Security Center: https://sec.xiaomi.com/, https://hackerone.com/xiaomi, security@xiaomi.com

03

Application

3. Application

Xiaomi apply AI algorithm to the following services: Voice Call Noise Reduction, Camera Image Optimization, Face Unlock and Fingerprint Unlock. Xiaomi always adheres to the basic principles of Trustworthy AI in the process of developing and deploying these services. Xiaomi is making unremitting efforts in the research and development of AI technology and continually taking a variety of technical and non-technical measures so as to ensure the security and safety, privacy, fairness and explainability of the application of AI technology and ultimately achieve the protection of human dignity, freedom, security and other basic rights.

3.1 Voice Call Noise Reduction

3.1.1 Usage Scenario

Voice Call Noise Reduction, being an integral part of our smartphone communication system, is an ancillary tool engaged during calls. It aims to suppress ambient noise and improve the quality and performance of the voice call between the parties to the call. It does not alter, distort, or make any other changes to the content of conversation so as to ensure it has no effect on the user's subjective judgement.

3.1.2 Technical Measures for Implementing Trustworthy AI

Xiaomi avoids external attacks on the model by deeply integrating the model within the DSP chip. Also, the model only processes and outputs the input sound in real time locally on the device, without any storage or transmission of users' data. Xiaomi only uses training data sets that are properly and legally collected for the algorithm training. The algorithm is further ensured to be fair and explainable through multiple rounds of screening and

adjustment of training data sets and adequate tests of the algorithm in accordance with a strict process.

3.1.2.1 Security Architecture

The Voice Call Noise Reduction algorithm (hereinafter referred to as the "noise reduction algorithm") is deeply integrated in mobile phone's DSP chip and performs system interaction using Qualcomm standard interface. In order to prevent threats from external modifications or attacks, the kernel code is not accessible to the public.

The noise reduction algorithm only runs locally on the device. It only processes and outputs the voice call data in real time without collecting users' other information. It does not preserve any information or transmit it to Xiaomi server, thereby fundamentally eliminating the risks associated with the transmission and storage of data. The noise reduction algorithm is only applied to calling scenarios and invoked only for calls. When in use, the algorithm only uses limited phone resources and will release them after the call ends.

3.1.2.2 Algorithm Testing and Verification

The sources of training data for noise reduction algorithms include: 1. The purchase of relevant language datasets through official channels, while we refuse to use illegally obtained voice data; 2. Audio training data manually recorded by the algorithm research and development team. The purpose of the use of such data has been explained to the subject of the recording, and consent has been obtained before the data is recorded, ensuring that legal requirements are met and that the principle of privacy is strictly enforced from the earliest stages of the AI life-cycle.

As the training data is anonymous, we manually perform subjective listening tests on those data, and organize, label and filter training data to ensure the quality and accuracy of training data and avoid errors in real-world applications of noise reduction algorithms. This is also beneficial to adjustments of algorithm in later stages.

In addition, in order to achieve fairness in noise reduction algorithm, training data includes a wide range of voice segments from people of different genders, ages, timbres and frequencies. To ensure the accuracy of noise reduction algorithm, training data is collected at different locations (such as restaurants or construction sites) and time periods, so that our noise reduction algorithm can work properly in different complex external scenarios.

Noise reduction algorithms undergo multiple rounds of testing prior to being released. These tests include, but are not limited to, performance testing (to test algorithm performance and enhancements), integration testing (to test actual performance and enhancements in hardware environments), and scenario acceptance testing (to test actual human auditory perception). Through these tests, we hope to identify and resolve potential problems early and guarantee the services we ultimately provide to our users are secure, stable and reliable.

3.1.2.3 Explaination Methods

3.1.2.3.1 The Security & Safety and Privacy of Noise Reduction Agorithm. We control the operation of the algorithm by controlling the parameters, and based on the results of various tests and feedback from users, we constantly adjust and optimize the noise reduction algorithm to ensure that the use of the algorithm does not go beyond our control. The noise reduction algorithm will not collect any user information after it is released, ensuring the privacy,security and safety and confidentiality of user information and their calls.

3.1.2.3.2 The Fairness of Noise Reduction Algorithm We ensure the fairness of our noise reduction algorithm through various measures, for instance the comprehensiveness of training data. Our training data includes human voices of different genders, ages, languages and accents, as well as ambient noise of different locations and periods of time.

3.1.2.3.3 The Explainability of Noise Reduction Algorithm We have appropriate mechanisms to record and preserve the various aspects of the noise reduction algorithm (training, testing and so forth), training data and solutions to problems. This allows us to achieve backtracking (including, but not limited to, the reproduction of problems) and ensure that the source of the problem is quickly and accurately identified and handled in a timely manner. We are able to explain the effects of the noise reduction algorithm during its application.

The Voice Call Noise Reduction service strictly adheres to the processes and standards set by the Xiaomi Trustworthy AI Ethics Committee for AI technology. In addition to the above technical measures, non-technical measures such as user participation, internal audit and continuous assessment are used to ensure the implementation of the principles of security and safety, privacy, fairness and explainability of our AI technology.

3.2 Camera Image Optimization

3.2.1 Usage Scenario

The Camera Image Optimization AI algorithm (hereinafter referred to as the "image optimization algorithm") in the MIUI is mainly used for the following features: Supermoon, AI Camera, Documents Mode, Portrait Mode and Beautify feature. The purpose of this feature is to meet users photographing needs. Users can now easily take amazing photos without complicated post-processing.

- **Supermoon Mode** This feature enables users to capture crisp and clear moon scenes with smartphones.
- **AI Camera Mode** This feature allows users to capture more scenes by automatically identifying the category of a particular scene and adding different filters for the different categories.
- **Documents Mode** This feature automatically detects document boundaries and enhances the document inside the boundaries, such as presentation slides, paper documents, etc.
- **Portrait Mode** Based on the bokeh algorithm, this feature separates the main subject from the picture while blurring the other parts of the scene. In this way, it can highlight the main subject of the photo.
- **Beautify Algorithm** This feature applies skin smoothing, face slimming, eye enlargement and other effects to the facial features of the person being photographed to meet the user's beautifying needs when photographing faces.

3.2.2 Technical Measures for Implementing Trustworthy AI

Xiaomi is committed to ensure the security of the algorithm's operating environment. Before pressing the capture button, the image data will not be stored by the camera and will not leave the device, and the users' personal information will not be collected. At the same time, the training of the algorithm only uses training data sets from regular sources that are legally collected, and does not collect or use user image data. In order to ensure the fairness and accuracy of the algorithm, before the algorithm is released, Xiaomi completely records and conducts multiple rounds of manual verification of the algorithm's training data, training process and training results, and then releases the algorithm after it passes the test.

3.2.2.1 Security Architecture

The image optimization algorithm is integrated into the device and only runs locally on the device. In addition, the MIUI system cannot directly store images that are not captured by the camera. The data processed through the algorithm is only stored locally on the device when authorized by the user and will not be backed up or uploaded elsewhere.

Image Optimization Algorithm Operates in a Secure Environment. The algorithm is the underlying service being invoked. The algorithm is deeply integrated into the MIUI system as independent and sealed SDK.The MIUI system has signature verification process and it cannot be modified. This effectively defends against external attacks while ensuring the security of the algorithms and user data.

3.2.2.2 Algorithm Testing and Verification

The Fairness of Training Data. Training data for AI camera image optimization algorithms is obtained through official channels (open source datasets, compliant procurement and so forth). The research and development team labels training data and selects datasets that meet the requirements to ensure its fairness and comprehensiveness.

- Unfairness or bias issues are not applicable for scenes that target non-human subjects, such as the Documents Mode, AI Camera and Supermoon features.
- As the bokeh algorithm only separates the main subject from the picture, and the training datasets for the algorithm do not involve the labelling of facial features, they are applicable to people in different regions and with different complexions without bias or discrimination issues.

- The beautify algorithm performs specific optimizations for different complexions and different groups of people, and has been tested by testing teams in different regions throughout the world. An example of this would be the retention of the red dots on people's foreheads in India, ensuring that the algorithm fully respects local cultures.

The Security of Training Results. Research and development teams are fully involved throughout the design, training and tuning processes for the image optimization algorithm. After the algorithm is encapsulated, it is integrated into the mobile phone system and must undergo several rounds of rigorous testing before it goes live. Testing includes trial testing by in-house employees, sample testing by photographers, DxO testing (an independent external company specializes in measuring the effectiveness and quality of smartphone cameras and lenses), image quality testing, objective performance and stability testing, and so forth. In order to provide users with a better user experience, Xiaomi continuously improves and optimizes its algorithm's features. Xiaomi accesses the updated contents of the algorithm before releasing each update, and then provides users with the update through the system according to the standard procedure.

3.2.2.3 Explanation Methods

3.2.2.3.1 The Security & Safety and Privacy of Image Optimization Algorithm. The image optimization algorithm is integrated into the device and only runs locally on the device. The data processed through the algorithm is only stored locally on the device when authorized by the user and will not be backed up or uploaded elsewhere, in order to defend against external attacks. And users have full right and to decide whether use these features. For some image optimization algorithms, users can continue to adjust the algorithm's effect after turning on corresponding features.

- Features such as Supermoon, AI Camera, Documents Mode, Portrait Mode, Beautify feature and more all have toggle buttons on the camera interface, and can be turned on or off independently through UI interaction, giving users full autonomy.

- The Portrait Mode allows users to automatically adjust the intensity of the blur effect by changing the aperture size on the UI interface.

- When using the Beautify function, users are given full autonomy and can independently adjust the intensity of the beautifying effect to be applied to specific parts of their faces through the corresponding button.

3.2.2.3.2 The Explainability of Image Optimization Algorithm. Xiaomi has appropriate mechanisms to record and preserve each stage of the algorithm's development and application and the related training data to backtrack and reproduce problems. This ensures that the source of a problem can be quickly and accurately identified and handled in a timely manner.

3.2.2.3.3 The Fairness of Image Optimization Algorithm. During the datasets acquisition and labeling process, qualified datasets are rigorously filtered by professionals, and the algorithm is tested several times before going live to ensure the accuracy of algorithm training and results. In order to ensure fairness among different users, we continue to perform the corresponding algorithm debugging and optimization processes for different regions, complexions and cultural groups, to avoid algorithm bias to the greatest extent possible.

Camera Image Optimization Service has strictly followed the procedures and specifications formulated by Trustworthy AI Ethics Committee forTrustworthy AI technology. In addition to this, it has also ensured the implementation of AI technology's security and safety, privacy, fairness and explainability through user participation, internal audit, continuous evaluation and other non-technical measures.

3.3 Face Unlock

3.3.1 Usage Scenario

Face Unlock is designed to optimize the Xiaomi smartphone user experience based on the AI facial recognition algorithm. This feature intelligently detects and matches facial features with high precision, providing users with a more convenient way to unlock their devices, without requiring users to enter long and complex numeric or graphical passwords. But since the algorithm can not completely avoid the small probability of false detection caused by similar appearances, the security of Face Unlock is lower than that of pattern passwords, digital passwords, fingerprint or mixed passwords in certain circumstances. While continuously improving the security and accuracy of facial recognition algorithm, we prompt the corresponding effects and risks of Face Unlock, ensuring that users can freely choose whether to use the service. In addition, in order to enhance the security and privacy of users, Face Unlock is restricted in the following scenarios:

1) When the user's device has just been turned on or restarted;

2) If the device has not been unlocked using a password for more than 72 hours;

3) If the Face Unlock function fails to unlock the user's device four times in a row.

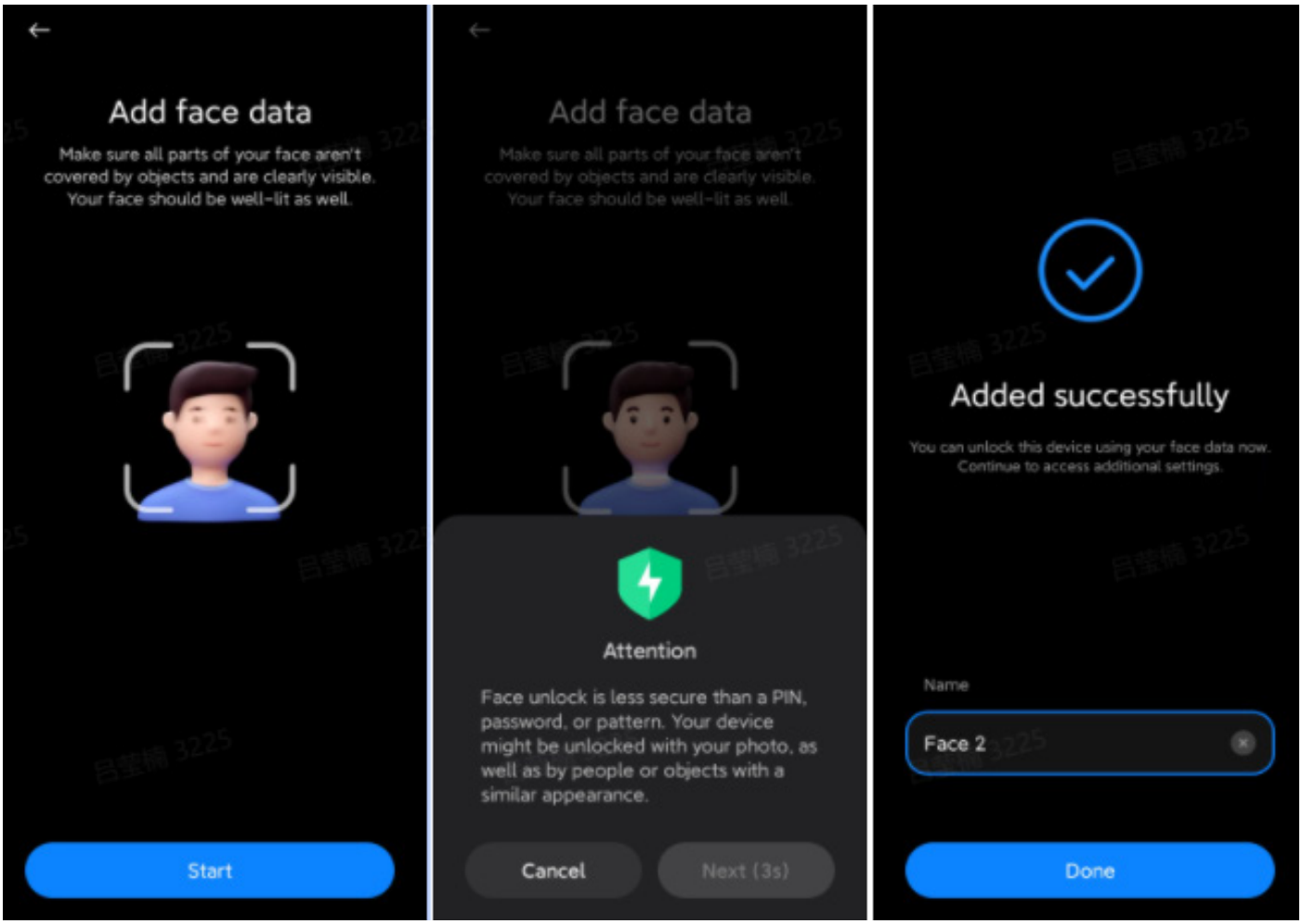

Figure 3–1 Face Unlock Interaction

3.3.2 Technical Measures for Implementing Trustworthy AI

3.3.2.1 Security Architecture

The facial recognition AI mode is integrated and operates locally on the device. After extracting facial feature information, the facial recognition algorithm encrypts the information and irreversibly saves it to the device. It does not retain the original facial biometric information, nor does it backup or upload the user's facial feature data to any other platform.

3.3.2.2 Algorithm Testing and Verification

- **Secure Training Data** The training database of the facial recognition algorithm is purchased through official channels. Training data includes data relating to different countries, ages, genders and complexions worldwide, in this way we could ensure the inclusiveness, comprehensiveness and fairness of the source of training data, and mitigate any risk of unfairness which arises in the practical application of the facial

recognition algorithm. We declare not to collect any user's facial feature information for use in algorithm training.

- **Secure Training Process** Facial recognition algorithm has undergone multiple rounds of testing prior to release. These tests include but not limited to development tests, integration tests, subjective joint debugging tests and objective laboratory tests, thereby ensuring the accuracy, security and reliability of the algorithm. The test scenarios include live batch processing, comparison batch processing,opened/closed-eye batch processing, and tests with different distances, light, angles, facial expressions, facial occlusion and accessories, etc.

- **Secure Training Results** Facial recognition algorithm adopts an unlock-level facial comparison security and live security algorithm. After repeated optimization training, the algorithm strives to reduce the False Acceptance Rate (FAR) and False Reject Rate (FRR) to the minimum and has achieved an FAR of 0.00000526 and an FRR of 0.00649585. The algorithm also includesopened/closed-eye detection, which does not record or unlock the device when eyes closed.

- **Algorithm Optimization Upgrade** Xiaomi continues to reduce the false discovery rate (such as the small probability of false detection caused by similar appearances) through algorithm optimization and upgrading. If the optimized algorithm still fails to solve the false detection problem, we will guide users to switch to the password unlock mode. In addition, we will timely state any unsolved problem due to the algorithm capability bottleneck, so as to reduce the risk caused by algorithm false detection.

3.3.2.3 Explaination Methods

3.3.2.3.1 The Security and Privacy of Facial Recognition Algorithm Before the Face Unlock function is officially released, there is manual supervision and intervention in the process of training, testing and verification to ensure that the application effect of the algorithm is safe and controllable. Face Unlock can only be opened with the consent of the user, and can only be used after the user actively enters the face template. Face Unlock is only used to unlock the smartphone and does not involve payment and other functions. Users can choose to turn on/off this service anytime.

3.3.2.3.2 The Explainability of Facial Recognition Algorithm We collect feedbacks and provide solutions to users concerning any problem in Face Unlock via Customer Service, Service & Feedback, Community Forums and other channels. In fault analysis, if necessary and with the user's explicit consent, the user will actively provide us with the face information for fault diagnosis. After concluding fault diagnosis and analysis, we will delete the user's facial feature data with the promise not to add it to the training dataset for the facial recognition algorithm.

3.3.2.3.3 The Fairness of Facial Recognition Algorithm. Xiaomi has developed strict testing procedures to minimize the algorithm's FAR and FRR to the greatest extent possible. To ensure security, the core application scenario of the face recognition algorithm is set at 20 cm to 80 cm, while the face unlock/detection function is not available over 1.5 m. By fielding feedback from users in various regions, we constantly optimize the algorithm and strive to ensure that facial recognition algorithm meets the needs of all Xiaomi users.

The Face Unlock service strictly abides by the procedures and rules for trustworthy AI technology set by Xiaomi Trustworthy AI Ethics Committee. In addition to the above technical measures, it also takes user engagement, internal audit, continuous evaluation and other non-technical measures to ensure the implementation of trustworthy AI technology, including security and safety, privacy, fairness and explainability.

3.4 Fingerprint Unlock:

3.4.1 Usage Scenario

Fingerprint Unlock is based on biometric identification technology ,after the user turns on this funtion, they only need to place their fingers on the fingerprint sensor to quickly unlock their device without requiring the user to enter a long and complex numeric or graphical password each time. Moreover, in order to protect the security and privacy of users, the Fingerprint Unlock service is restricted in the following scenarios:

1) When the user's device has just been turned on;

2) If the device has not been unlocked using a password for more than 72 hours;

3) If the fingerprint unlock function fails to unlock the user's device five times in a row.

3.4.2 Technical Measures for Implementing Trustworthy AI

By building a security framework for Fingerprint Unlock, Xiaomi ensures the security of the algorithm operating environment and the storage environment of fingerprint template. When using the fingerprint unlocking function, the user's fingerprint templatewill be stored in a secure environment and only run locally on the device, so that the fingerprint template cannot be accessed by external applications. In addition, fingerprint unlock algorithm undergo multiple rounds of testing prior to being released. Xiaomi records and manuallyverifies the training data, training process, and training results of the algorithm.

3.4.2.1 Security Architecture

Local Operation. Xiaomi's fingerprint recognition AI model is integrated and operates locally on the device. While in use, the user's fingerprint data will not leave the device, nor will it ever be backed up or uploaded to any other platform. When adding a fingerprint template, the device only saves the extracted fingerprint feature information, not the original fingerprint biometric information.

Safe Operating Environment. Xiaomi's fingerprint security framework extends Android's native fingerprint security architecture and uses it as a basis for expansion. The AI fingerprint recognition algorithm operates on the Fingerprint TA in a TEE environment. TEE is a micro-operating system developed based on ARM TrustZone technology. Through the isolated built-in hardware mandatory in the CPU, TEE provides an effective and system-wide security method to ensure the security of user fingerprint characteristic information record, storage, and verification at all stages to defend against external attacks. Xiaomi's fingerprint security framework is shown in Figure 2.

- **Storage Security.** The fingerprint template is encrypted by the AES-256 encryption algorithm and then stored in a Secure File System (SFS) in the TEE environment. Encryption is achieved by invoking KeyStore. The fingerprint template is signed with the device's dedicated private key that makes the template unusable on other devices and unavailable to any other user registered on the same device. Encrypted fingerprint template can only be accessed by the Fingerprint TA. Even if the smartphone is rooted, the attacker cannot read the fingerprint templates through the kernel or platform, thereby securing the user fingerprint templates stored on the device.
- **Authentication Process Security.** The entire fingerprint authentication process is performed in the TEE environment. During this process, applications that support fingerprint authentication can only initiate fingerprint authentication requests and receive authentication results throught the Fingerprint TA in the TEE environment. These applications cannot directly access the fingerprint templates,realising the security of the fingerprint authentication process.

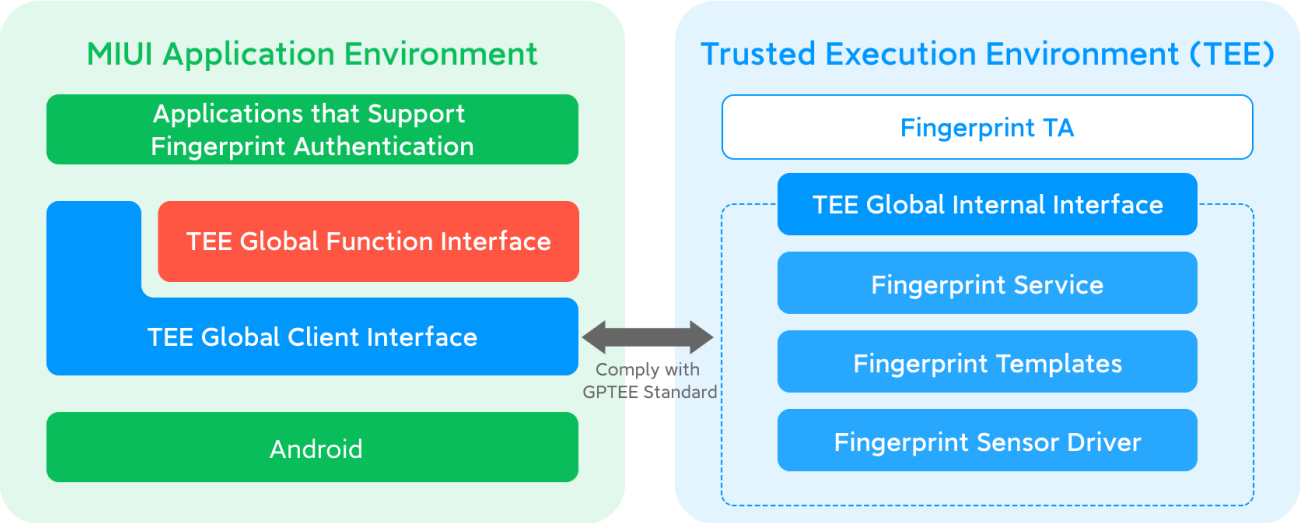

Figure 3-2 Xiaomi Fingerprint Security Architecture

3.4.2.2 Algorithm Testing and Verification

- **Secure Training Data** The algorithm undergo multiple rounds of testing prior to being released. The training database of the algorithm is procured through official channels. Xiaomi declare not to collect any users' fingerprint data for algorithm training.

- **Secure Training Results** Verification results for fingerprint recognition algorithms are based on the requirements of international FIDO standards for biometrics, ensuring that the algorithm has passed the test with regard to FAR (False Acceptance Rate) and FRR (False Rejection Rate) before being released. FIDO standards for biometrics mandate an FAR <3% and an FRR <1/10,000. In order to provide users with more reliable fingerprint unlock services, Xiaomi has constantly optimized its algorithm to ensure that the FAR<3% and FRR <1/50,000,achieving higher levels.

- **Algorithm Optimization Upgrade** During the testing of the algorithm, we covered common scenes that may cause misrecognition (such as orange peel, protective cover, etc.). And on this basis we have added foreign object attacks tests (phone bubble film, strands of hair, etc.), 2D anti-forgery tests (create black and white background print pictures based on the user's non-cooperative residual imprint.), durability tests (the scratching or cracking of the tempered glass screen protector,etc.), cover more test scenarios to ensure the security of the algorithm. At the same time, special optimizations have been made for some special scenarios such as strong light, low temperature, dry fingers of optical fingerprints, etc., to further improve the accuracy and reliability of the algorithm.

3.4.2.3 Explaination Methods

3.4.2.3.1 The Security and Privacy of Fingerprint Recognition Algorithm. The Fingerprint Unlock function must be fully tested and pass both machine and manual acceptance tests before being released. The algorithm is integrated and runs in local TEE environment. The user’ s fingerprint templetes are stored in a secure environment and will not be uploaded or backed up to any other platform. We will obtain the device logs if users report problems via the Service & Feedback. However, the logs will not contain any information of users' fingerprint characteristics.

3.4.2.3.2 The Explainability of Fingerprint Recognition Algorithm. We collect feedbacks and provide solutions to users concerning any problem in Face Unlock via Customer Service, Service & Feedback, Community Forums and other channels, helping users to fully understand the application effect of the fingerprint recognition AI model.The FAR and FRR indicators of Xiaomi's AI fingerprint recognition algorithm meet the requirements under international FIDO standards for biometrics, and the functions and effects of the algorithm can be explained accordingly.

3.4.2.3.3 The Fairness of Fingerprint Recognition Algorithm. By establishing supervision mechanism, Xiaomi manually supervises and records the research, development and testing process of the algorithm to ensure that the application effect of the algorithm is controllable. In addition, when setting the device's unlock method, the user may opt to turn the Fingerprint Unlock function on or off at any time on the phone's Settings the path is '**Passwords & security** – > **Fingerprint Unlock**. We combine feedbacks from users in various regions to continuously optimize the algorithm, and strive to meet the needs of all Xiaomi users with fingerprint recognition AI technology.

The fingerprint unlock service strictly complies with the procedures and specifications established by the Trustworthy AI Ethics Committee of Xiaomi for Trustworthy AI technology. In addition to the above technical measures, it also ensure the security and safety, privacy, fairness and explainability of AI technology through non-technical measures such as user participation, internal audit, and continuous evaluation.

04

Conclusion

4. Conclusion

Xiaomi is dedicated to providing comprehensive, safe and easy-to-use digital software and hardware products users.

In the research, design, manufacturing and operation of AI technology, Xiaomi lways uphold fair, safe, privacy-protecting and explainable Trustworthy AI technology to enhance and enrich the user experience of Xiaomi consumer electronic products. This White Paper comprehensively demonstrates the design and application of the Trustworthy AI at Xiaomi.

Xiaomi strives to embed the four basic principles of Trustworthy AI into the hearts of every business unit, every employee, and every partner. As mentioned above, Xiaomi has established Trustworthy AI Ethics Committee and an internal supervision mechanism, continuously improves the security and privacy management system, and has integrated the basic principles of trusted AI, security and privacy strategies into the development and application of AI algorithms and products. We conduct strict security and privacy audits on our partners, and actively monitor and solve new security issues to ensure that user data is guaranteed throughout the life cycle. In order to adapt to the evolving security situation, Xiaomi will continue to improve its capabilities of TrustworthyAI technology and security technology and the security and privacy protection functions of products and services, and optimize the security and privacy management system.We will also continue to communicate with the public about the progress via official certifications, white papers, privacy policies, and other means to build user confidence in our products and services.

Xiaomi firmly believes that respecting and protecting the security of user's information and user privacy is the only approach to build long-term trust in Xiaomi products and services. Therefore, Xiaomi insists on the provision of fair, safe and secure, privacy-protective and explainable Trustworthy AI and has continuously increased its investment in security and privacy. We are dedicated to transferring Xiaomi's best practices, and technical capabilities in Trustworthy AI to our partners, in order to provide users with reliable, safe AI products and services.

05

Abbreviations

5. Abbreviations

Abbreviation	Full name	Definition
AES	Advanced Encryption Standard	A commonly used symmetric encryption algorithm. A variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits.
AI	Artificial Intelligence	A wide-ranging branch of computer science concerned with building smart machines capable of performing tasks the typically require human intelligence.
API	Application Programming Interface	A set of functions and procedures that allow for the creation of applications that access data and features of other applications, services or operating system without accessing source code.
DSP	Digital Signal Processor	A digital signal processor (DSP) is a specialized microprocessor chip, with its architecture optimized for the operational needs of digital signal processing.
DXO	A French company dedicated to photography	DxO created DxOMark.com, which provides image quality ratings for standalone cameras, lenses, and mobile devices that include cameras.
FAR	False Accept Rate	the percentage of identification instances in which unauthorised persons are incorrectly accepted.
FRR	False Reject Rate	the percentage of identification instances in which authorised persons are incorrectly rejected.
OS	Operating System	System software that manages computer hardware, software resources, and provides common services for computer programs.

Abbreviation	Full name	Definition
ROM	Read-only memory	A solid-state semiconductor memory that can only read data stored in advance.
SDK	Software Development Kit	is a collection of software development tools in one installable package. They facilitate the creation of applications by having a compiler, debugger and perhaps a software framework
SFS	Self-certifying File System	is a global and decentralized, distributed file system for Unix-like operating systems, while also providing transparent encryption of communications as well as authentication
TA	Trusted Application	A highly secure application program that runs in a TEE environment.
TEE	Trusted Execution Environment	A secure area on the main processor of a mobile device exists in parallel with the mobile OS, providing an isolated execution environment to ensure isolated execution, integrity of trusted applications, confidentiality of trusted data, secure storage, etc
UI	User Interface	In the industrial design field of human – computer interaction, a user interface is the space where interactions between humans and machines occur.