ManaTEE | CONFIDENTIAL COMPUTING CONSORTIUM

ManaTEE 2025 Annual Review

Mingshen Sun

ManaTEE is an open-source *trusted research environment* for secure and verifiable data analytics.

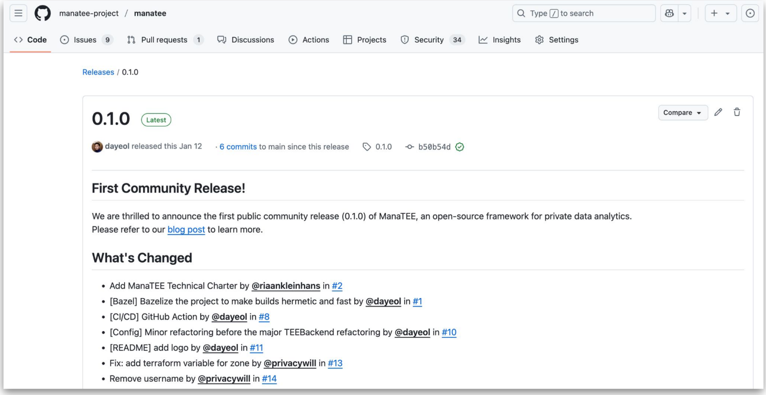
It leverages Privacy Enhancing Technologies like *confidential computing* and differential privacy to protect sensitive data while maintaining usability.

Project Progress since joined CCC (Nov 2024)

- No change in Technical Charter.
- No budget allocation from CCC relevant to ManaTEE.
- No outstanding license issue.
- No progress in OpenSSF Best Practices Badge. Start working in the following year.
- Project liaison changed to Mingshen Sun <mingshen.sun at tiktok.com>.
- Technical updates: First community release, new AI use case, code refactoring, new TEE backend (TDX), documentation, homepage, etc.
- Outreach: Multiple outreach activities.

Highlights of Technical Updates

- First community release: 0.1.0
  - File restructured, code refactoring, bazel, CI integration, documentation, etc.
- minikube local testing environment
- Homepage launched: https://manatee-project.github.io/manatee/
- New TEE backend (Intel TDX): PR #59
- New use case for verifiable AI model evaluation: PR #60



0.1.0

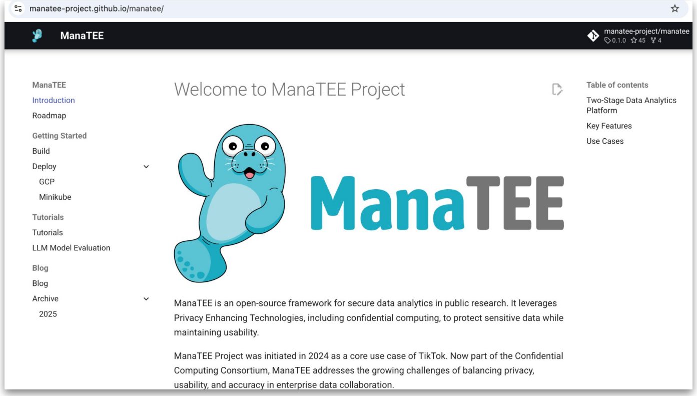
dayeol released this Jan 12 · 6 commits to main since this release 0.1.0 b50b54d

First Community Release!

We are thrilled to announce the first public community release (0.1.0) of ManaTEE, an open-source framework for private data analytics. Please refer to our blog post to learn more.

What's Changed

- Add ManaTEE Technical Charter by @riaankleinhans in #2
- [Bazel] Bazelize the project to make builds hermetic and fast by @dayeol in #1
- [CI/CD] GitHub Action by @dayeol in #8
- [Config] Minor refactoring before the major TEEBackend refactoring by @dayeol in #10
- [README] add logo by @dayeol in #11
- Fix: add terraform variable for zone by @privacywill in #13
- Remove username by @privacywill in #14



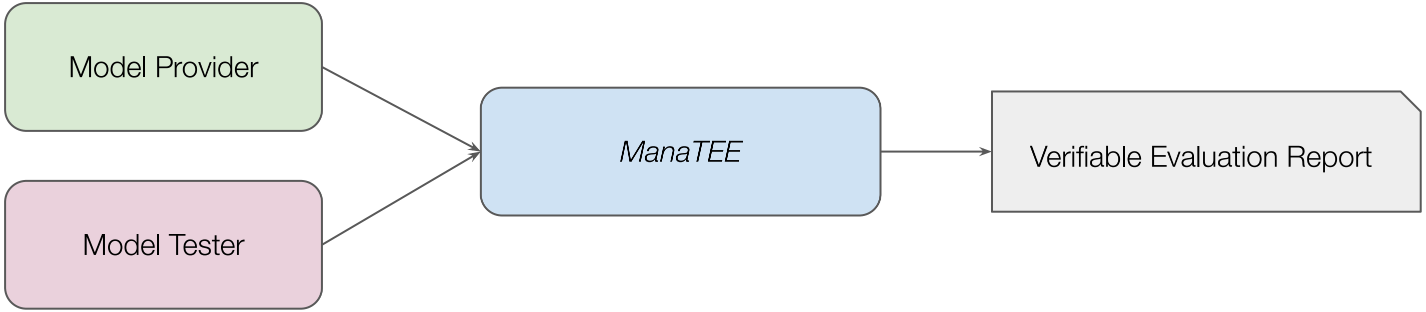
Welcome to ManaTEE Project

ManaTEE is an open-source framework for secure data analytics in public research. It leverages Privacy Enhancing Technologies, including confidential computing, to protect sensitive data while maintaining usability.

ManaTEE Project was initiated in 2024 as a core use case of TikTok. Now part of the Confidential Computing Consortium, ManaTEE addresses the growing challenges of balancing privacy, usability, and accuracy in enterprise data collaboration.

New Use Case: Verifiable AI Model Evaluation

- Verifiable evaluation on AI models in ManaTEE.
    - Fairness, trust & safety, bias evaluation, etc.
    - Integrity and confidentiality of public and private models.
    - Improved trustworthiness through hardware-signed attestation report.



Highlight of Outreach Activities

- FOSDEM 2025 @ Belgium
- Confidential Computing Summit 2025 @ San Francisco
- Asia Tech x Singapore 2025 @ Singapore
- AI Infra Summit 2025 @ Santa Clara (planned)

Roadmap

- Continue improving the AI model evaluation workflow.
- Explore new use cases in trusted research environments.
- Integrate with new TEE backends and cloud providers.
- OpenSSF Best Practices Badge.

Thanks!