ZKML Bootcamp

Signature Verification

Group 10

Edward
Sky
Tanmoy

ZKML Signature Verification Project

- Identifying Signatures Using Zero-Knowledge Machine Learning

Project Overview

- Zero-knowledge proof system for handwriting/signature verification
- Built using EZKL framework
- Developed and demonstrated on Google Colab
- Privacy-preserving authentication system

The Challenge

- Traditional signature verification lacks privacy
- Need for trustless verification without revealing original signature
- Authentication without compromising security
- Making ML verification compatible with blockchain systems

Our ZKML Approach

- Machine learning model to identify signature characteristics
- Zero-knowledge proofs to verify authenticity without revealing data
- Circuit-based implementation for on-chain verification
- Privacy-preserving verification system

Technical Architecture

- Model Training : Neural network for signature classification
- Circuit Creation: EZKL for converting ML model to ZK circuits
- Proving System : Generate ZK proofs of signature authenticity
- Verification : Verify proofs without accessing original signatures

Dataset & Materials

- Signature dataset: Handwriting Recognition
- Pre-trained ML model for signature recognition
- EZKL framework for circuit generation
- Google Colab environment for demonstration

Project Demonstration

- Google Colab notebook walkthrough
- Example signature verification process
- Performance metrics and accuracy results
- Privacy guarantees demonstration

Conclusion & Next Steps

Conclusion

- Privacy-preserving signature verification using ZKML
- Practical implementation with EZKL on Google Colab
- Balancing security, privacy, and usability
- Open-source contribution to ZKML ecosystem

Future Development

- Integration with blockchain for immutable verification records
- On-chain verification of signature proofs
- Mobile application for real-time signature verification
- Extension to other biometric verification methods