E-voting App Based on Blockchain

A comprehensive solution for secure electronic voting leveraging blockchain technology. Developed by Nedelcu Mihail Rares, IT&C Security Master program.

Introduction

Secure Platform

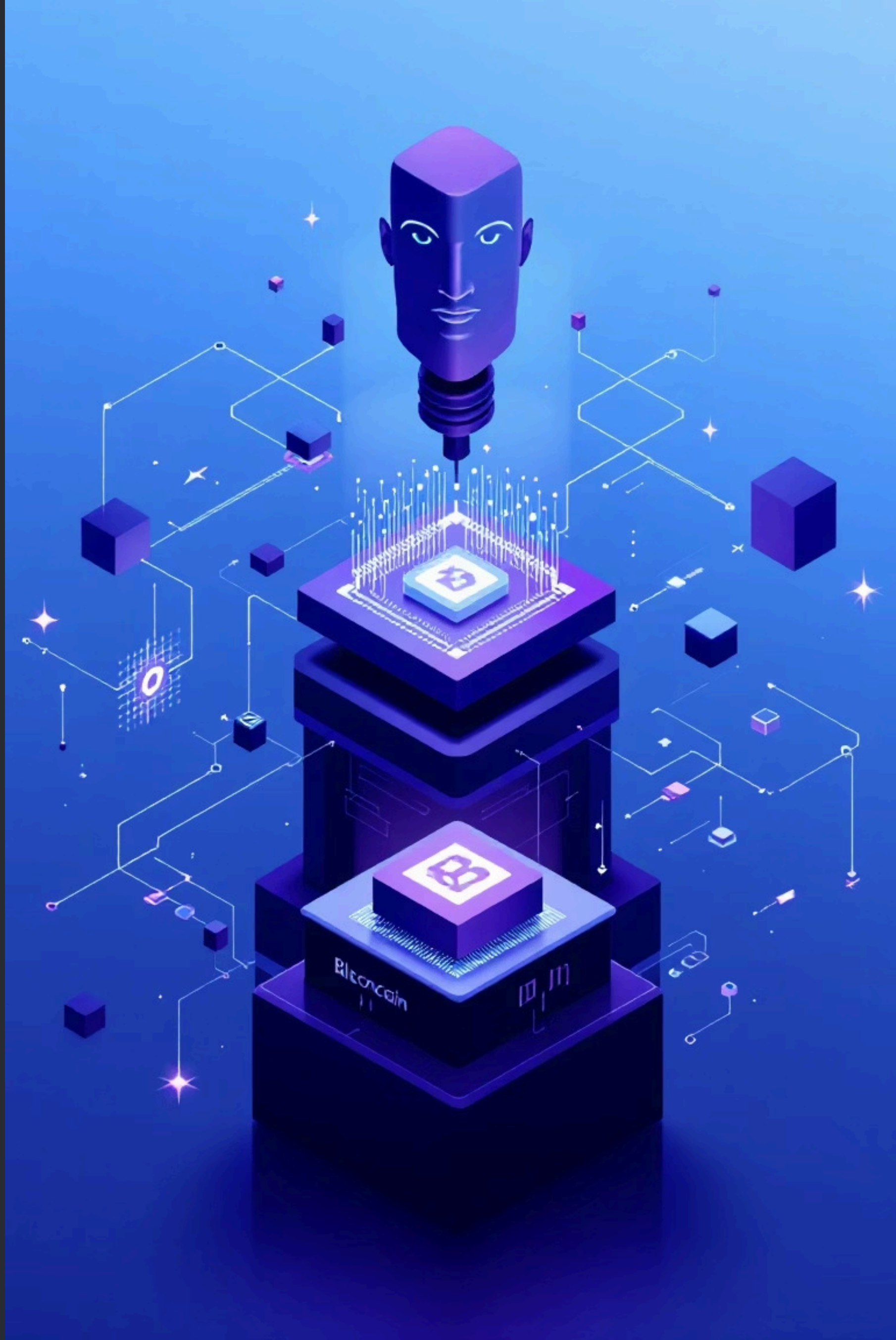
Built on Spring Boot microservices architecture with multiple security layers to ensure vote integrity.

Identity Verification

Advanced facial recognition technology to verify voter identity and prevent impersonation.

Blockchain Trust

Immutable record of votes stored on Ethereum blockchain for complete transparency and auditability.



Objective and Problem Description

Identity Verification

Authenticate users with multi-factor systems to prevent impersonation attacks.

Data Security

Protect sensitive voter information and ballot data through encryption and secure storage.

Vote Integrity

Prevent manipulation of cast votes through immutable recording mechanisms.

User Trust

Build public confidence in digital voting through transparency and auditability.

Methods and Technologies Used

Backend Framework

- Spring Boot
- JWT authentication
- RESTful APIs

Data Management

- PostgreSQL database
- Redis caching
- Docker containers

Identity Verification

- OpenCV facial recognition
- Tesseract OCR

Blockchain Integration

- Ethereum network
- Web3j library
- Maven dependency management

Solution Architecture

Frontend Application

User interface for registration, authentication, and voting operations.

Backend Microservices

Four specialized services handling distinct aspects of the voting system.

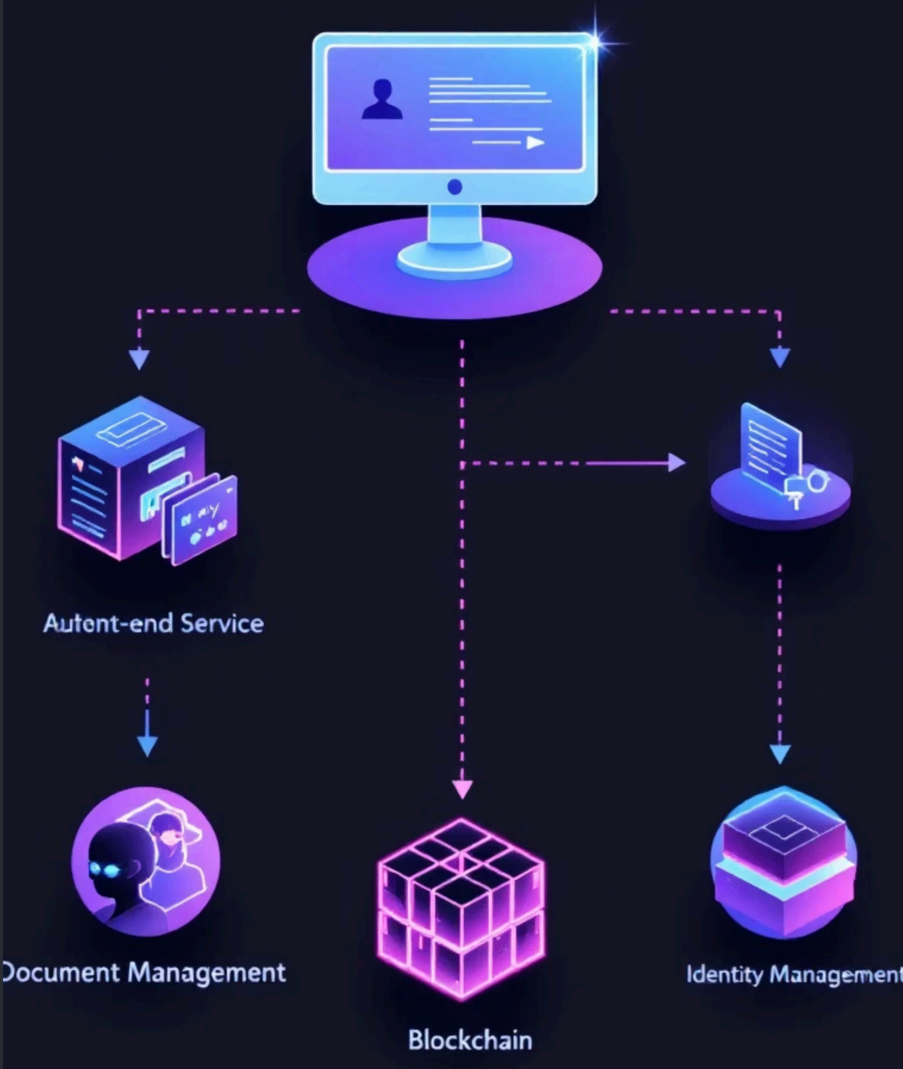
Secure Communication

RESTful APIs with JWT authentication between all system components.

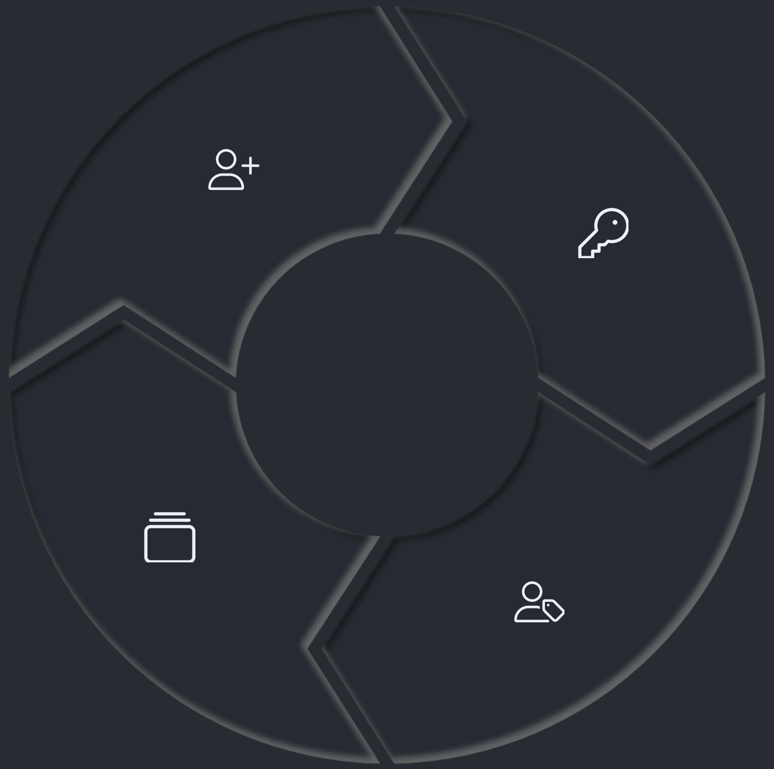
4

Data Storage

Distributed databases and blockchain for different data types.



Auth Microservice



Registration

Secure account creation with email verification step.

Authentication

JWT-based login with Time-based One-Time Password (TOTP) for 2FA.

Authorization

Role-based access control for different system functions.

Audit Logging

Comprehensive activity tracking for security analysis.

Identity & Document Services

Document Upload

Users submit government ID documents through secure encrypted channels.

Data Extraction

Tesseract OCR extracts document information and photos for verification.

Face Matching

OpenCV compares document photos with live selfies using advanced algorithms.

Secure Caching

Redis stores verification data temporarily for performance optimization.

Blockchain Voting Service

Identity Validation

Confirm user has completed all verification steps.

Vote Casting

Secure ballot submission through encrypted channels.

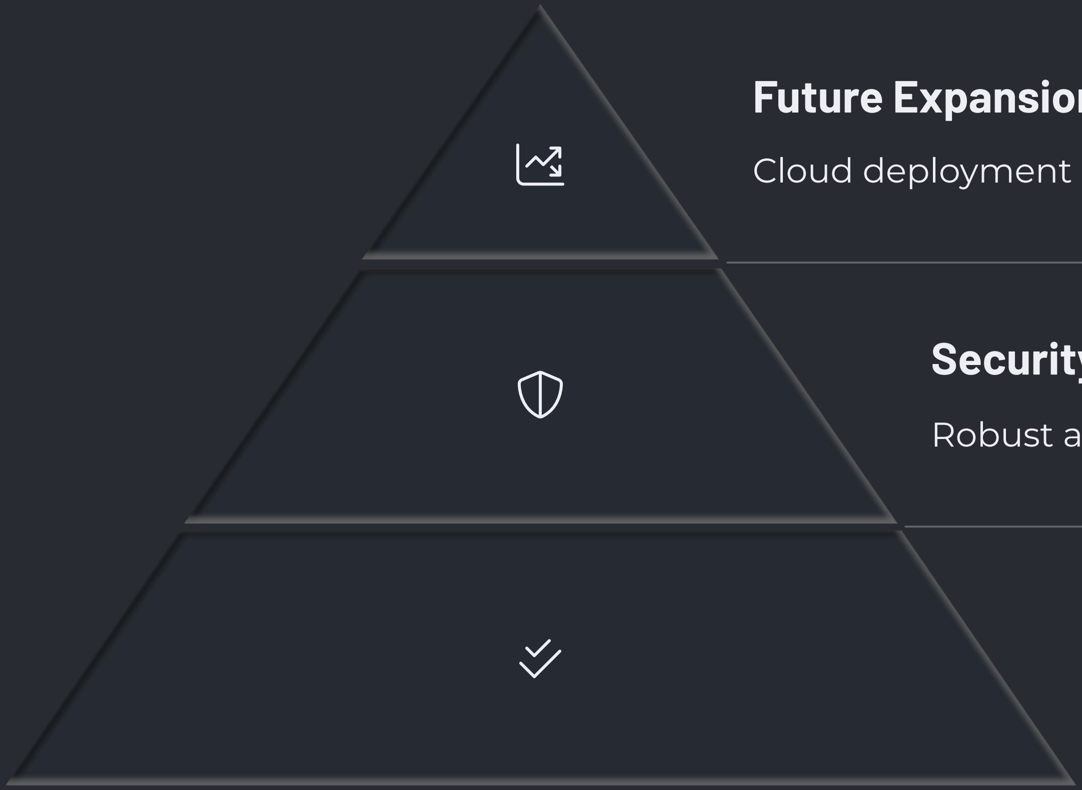
Blockchain Recording

Vote data stored in Ethereum smart contracts.

Verification

Public audit capability without compromising voter privacy.

Conclusions



Future Expansion

Cloud deployment and user scaling capabilities.

Security Validation

Robust architecture withstanding common attack vectors.

Core Achievements

Real-time face verification and immutable blockchain voting.

The system successfully combines multiple security layers to create a trustworthy e-voting platform. Face verification and blockchain technology provide a robust foundation for digital democracy.

References

Nakamoto, S. (2008)	Bitcoin: A Peer-to-Peer Electronic Cash System
King, S. et al. (2012)	PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake
Wood, G. (2014)	Ethereum: A Secure Decentralised Generalised Transaction Ledger
Atzori, M. (2015)	Blockchain Technology and Decentralized Governance
Spring Security (2023)	Official Documentation for JWT Authentication
OpenCV Foundation (2023)	Facial Recognition Implementation Guidelines