Practical Exercise 1 - Threat Modeling

Owner: Group 4
Reviewer:
Contributors: Adam Mendoza, Luis Palafox, Wilhelm Pangilinan
Date Generated: Thu Feb 13 2025

Executive Summary

High level system description

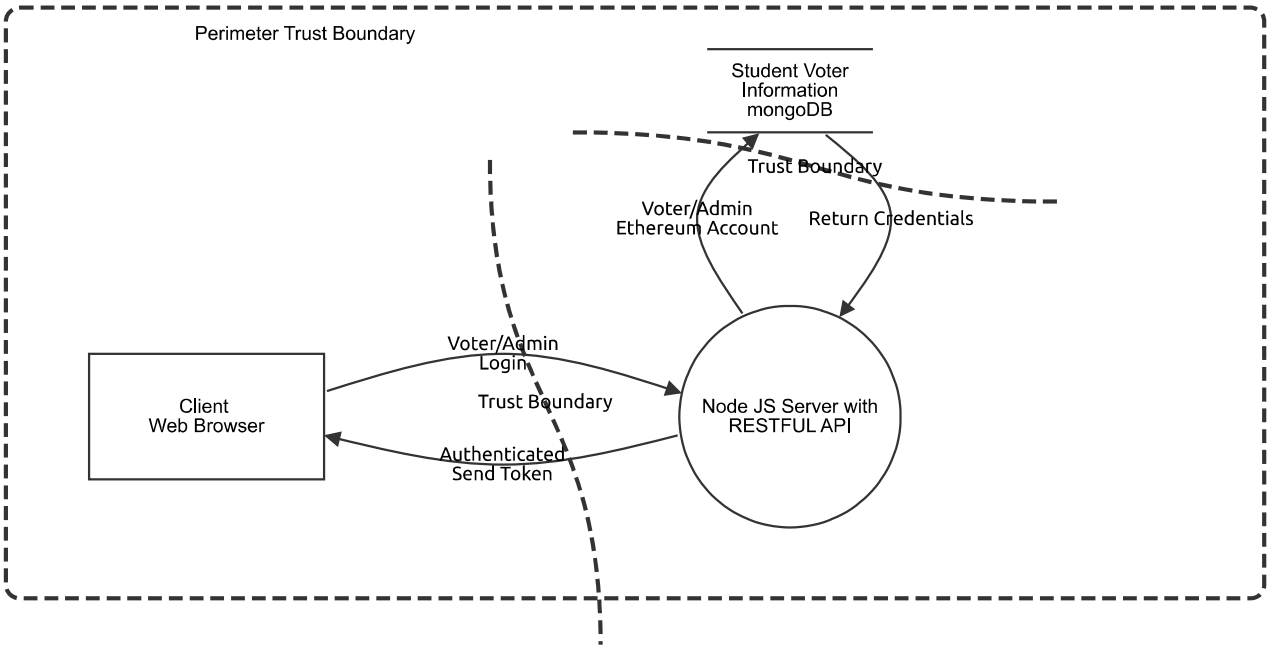
A MongoDB database will pre-register student voters and authenticate their eligibility. A web app built with HTML5, CSS3, JavaScript, and Handlebars will enable authentication and voting. A Node.js server with a RESTful API will handle login and voting status, while Web3.js will interact with an Ethereum node to process transactions via smart contracts. The transaction status will be relayed back to the server and displayed on the web app.

Summary

Total Threats	0
Total Mitigated	0
Not Mitigated	0
Open / High Priority	0
Open / Medium Priority	0
Open / Low Priority	0
Open / Unknown Priority	0

1, 2. Voter Authentication and Election Administrator Authentication

The voter/administrator logs in with administrator-provided credentials to access their dashboard.



1, 2. Voter Authentication and Election Administrator Authentication

Client Web Browser (Actor)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Node JS Server with RESTFUL API (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Authenticated Send Token (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Return Credentials (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Voter/Admin Login (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Voter/Admin Ethereum Account (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

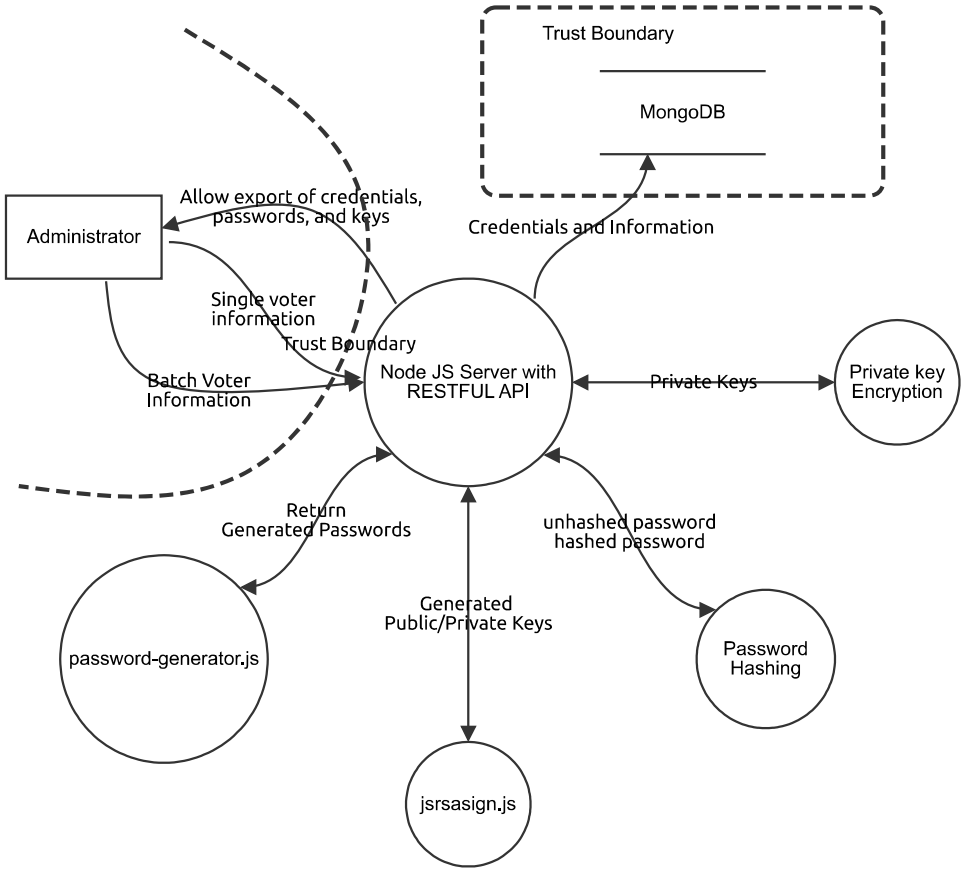
Student Voter Information mongoDB (Store)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

3. Voter Registration

The administrator registers voters individually or in batches, generating credentials, keys, and securely storing them.



3. Voter Registration

Node JS Server with RESTFUL API (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Administrator (Actor)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Single voter information (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Return Generated Passwords (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Generated Public/Private Keys (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Allow export of credentials, passwords, and keys (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

unhashed password hashed password (Data Flow)

Description: using PBKDF2withHmacSHA256.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Private Keys (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Credentials and Information (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Batch Voter Information (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

password-generator.js (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

jsrsasign.js (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Password Hashing (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Private key Encryption (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

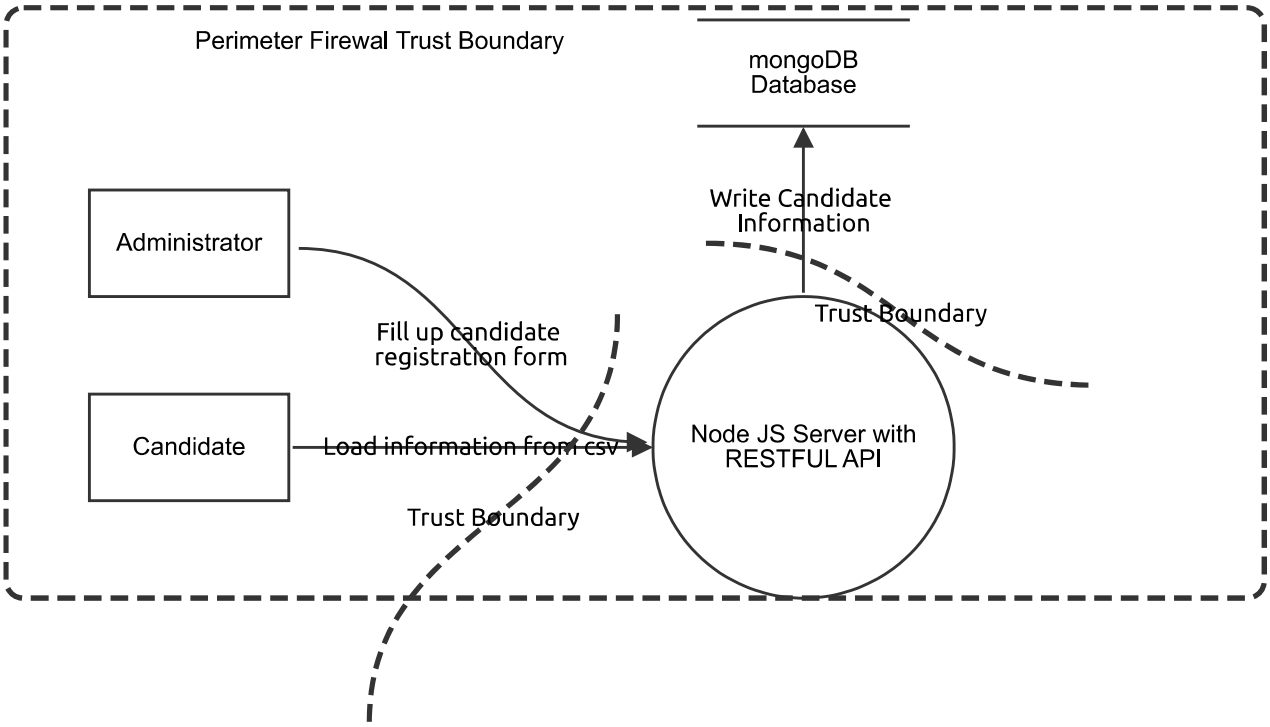
MongoDB (Store)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

4. Candidate Registration

The administrator registers candidates individually or via a CSV file, storing their details in the database.



4. Candidate Registration

Node JS Server with RESTFUL API (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Candidate (Actor)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

mongoDB Database (Store)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Write Candidate Information (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Load information from csv (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Fill up candidate registration form (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

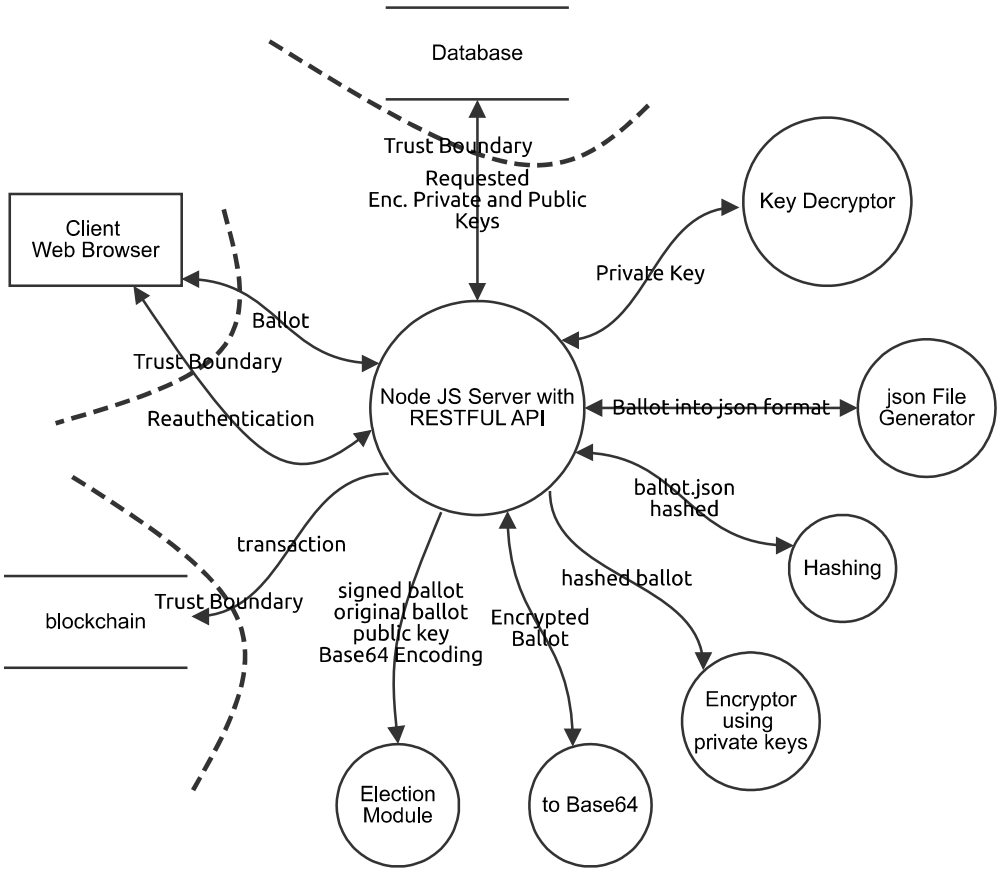
Administrator (Actor)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

5. Vote Casting

The voter submits a ballot, which is digitally signed, encoded, and recorded in the blockchain.



5. Vote Casting

Client Web Browser (Actor)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Node JS Server with RESTFUL API (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Ballot (Data Flow)

Description: Filtered / Submitted

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Reauthentication (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Requested Enc. Private and Public Keys (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Private Key (Data Flow)

Description: Private key is decrypted and sent back to the controllerr\

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Ballot into json format (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

ballot.json hashed (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

hashed ballot (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Encrypted Ballot (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

signed ballot original ballot public key Base64 Encoding (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

transaction (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Database (Store)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Key Decryptor (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

json File Generator (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Hashing (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Encryptor using private keys (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

to Base64 (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Election Module (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

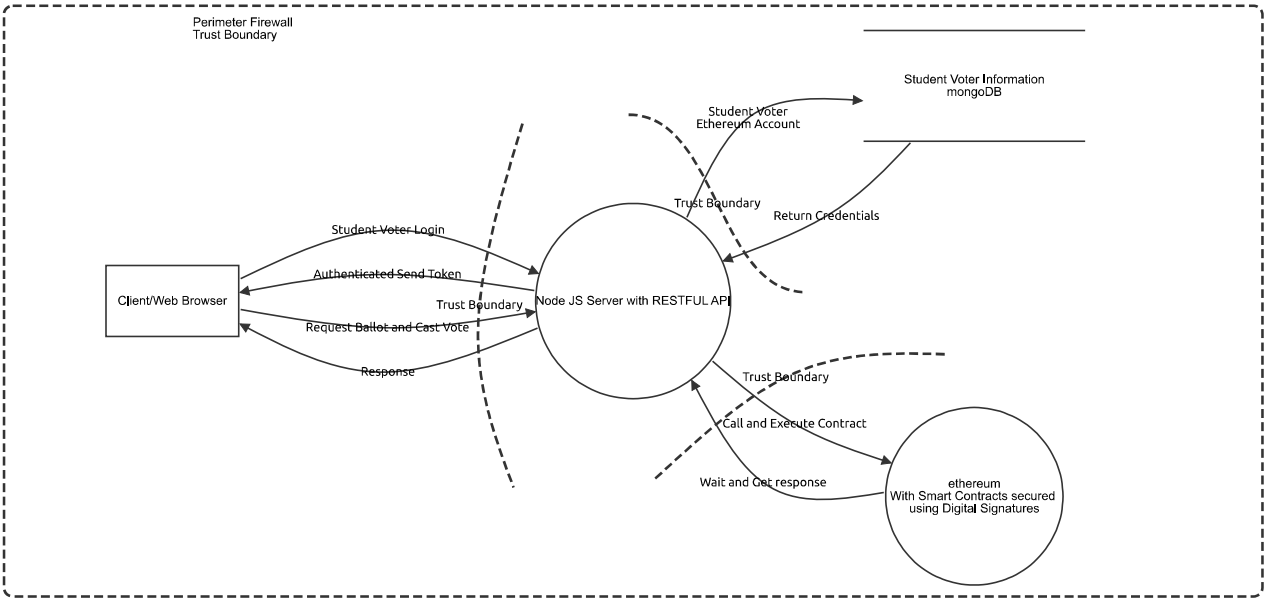
blockchain (Store)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Student Voting System with Web Authentication

A MongoDB-backed web application uses Node.js, Web3.js, and Ethereum smart contracts to authenticate student voters and securely process their votes



Student Voting System with Web Authentication

Client/Web Browser (Actor)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Node JS Server with RESTFUL API (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

ethereum With Smart Contracts secured using Digital Signatures (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Authenticated Send Token (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Request Ballot and Cast Vote (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Response (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Call and Execute Contract (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Wait and Get response (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Student Voter Login (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Student Voter Ethereum Account (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Return Credentials (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Student Voter Information mongoDB (Store)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations