

PoliceChain: Blockchain-Based Smart Policing System for Smart Cities

Arnab Mukherjee


RCC Institute of Information Technology
Kolkata, India
mukherjeearnab911@gmail.com

Raju Halder


Indian Institute of Technology Patna
Bihar, India
halder@iitp.ac.in



Introduction

- The most crucial smart service, among many others, which smart cities must adopt is a ***smart and robust policing system***.
 - Aim to increase **accountability, transparency, and trust** concerning the **storage, safeguarding** and **sharing** of evidence and intelligence related to ongoing investigations, criminal cases and justice information among the stakeholders.
 - This allows the citizens to interact with law enforcement agencies securely (even without visiting them physically) and to avail all related services.
- 


Why Smart Policing?

- A significant gap in the police-population ratio exists.
 - Often it is not possible to visit the nearest police station from the place of occurrence of the offence.
 - Lack of coordination between various states and law enforcement agencies.
 - Investigations may get influenced behind the scene.
 - Evidence, forensic reports and investigation case files may be tampered with.
 - Delay in investigation and lack of transparency.
- 

Related Works and Motivation

1. Maisha Tasnim, et al. (SpaCCS 2018):
 - Criminal record storage system using blockchain technology which allows only authorities (e.g., law enforcement agencies and courts) to add and maintain criminal data.
 - Other general users (e.g., individuals, airports, visa application centers etc.) can access them whenever needed.
2. A. T. Dini, et al. (CACIDI 2018):
 - Storage of criminal records and information related to it on a blockchain platform.
3. Belchior et al. (OTM 2019):
 - Maintaining of justice audit logs
 - Distributing Justice information among multiple stakeholders.
4. E. Nyaletey, et al. (IEEE ICBC 2019):
 - Storage and access of Forensic data.

Although no one considers a complete system for policing, taking into account the whole scenario.




Motivation

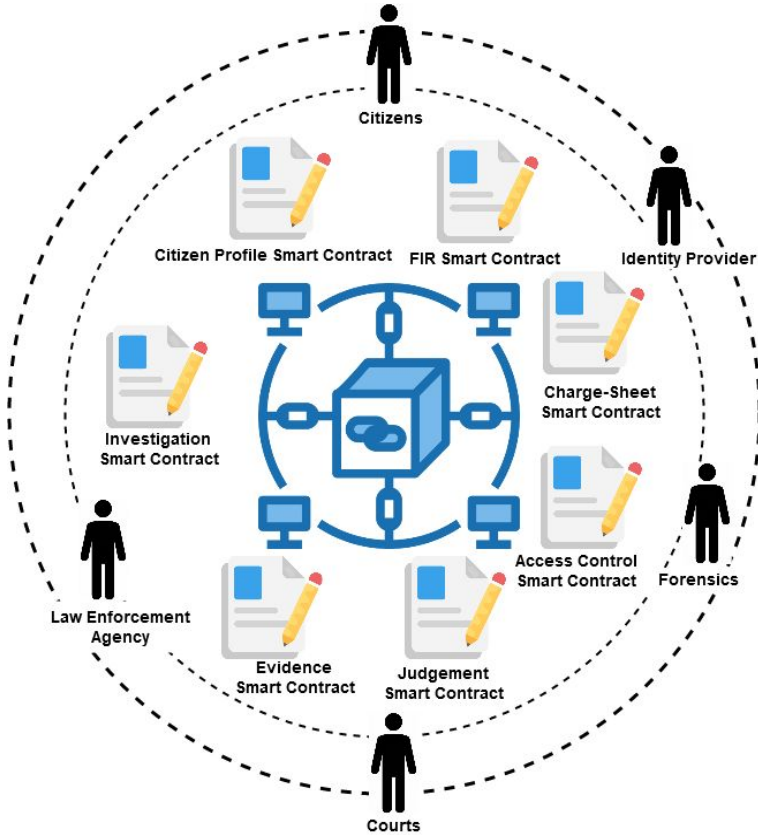
- Blockchain technology has emerged as a ground-breaking disruptive technology since 2008
- Wide range of applications: Supply-Chain, Land Registry, Insurance, E-Governance, Health Care, Smart Agriculture, and many more.
- Benefits:
 - Blockchain, along with its support to smart contracts, is about building a trusted system in an untrusted world.
 - Removes intermediaries and enabling greater coordination between parties.
 - No centralized authority, provides data-persistence, immutability, auditability, etc.,



Contributions

1. We propose a novel blockchain-based smart policing system, as part of Smart City services.
 2. **The system allows various stakeholders:** citizens, law enforcement agencies, intelligence agencies, forensic departments, government bodies and judges.
 3. **The system supports various crucial services:** filing FIR, initiating investigations, adding forensic reports, delivering justice, etc., related to smart policing.
 4. We adopt **Attribute-Based Access Control (ABAC)** policy, to ensure the rightful access to the information on the platform.
 5. We present a proof of concept of our proposal using **Hyperledger Fabric**, and we perform an experimental evaluation to demonstrate the performance of the system.
- 

Proposed Approach: Overall System Components



Smart Contracts:

1. Citizen Profile Smart Contract
2. FIR Smart Contract
3. Access Control Smart Contract
4. Judgement Smart Contract
5. Evidence Smart Contract
6. Investigation Smart Contract
7. Charge-Sheet Smart Contract

Stakeholders:

1. Citizens
2. Law enforcement Agencies
3. Forensics
4. Court
5. Identity Provider

Stakeholders

1. **Citizens:**

- a. Filing an FIR, submit evidence to an active investigation, or view judicial information relevant to them.

2. **Law Enforcement Agencies:**

- a. Collection of evidences
- b. Creation of charge-sheets based on the FIRs and investigations
- c. Sending the case to the judiciary.

3. **Forensics:**

- a. Provide additional evidence to an investigations which include analysing and reporting physical evidence from a crime scene
- b. Biological samples and other trace of evidence.



Stakeholders continued.

4. **Courts:**

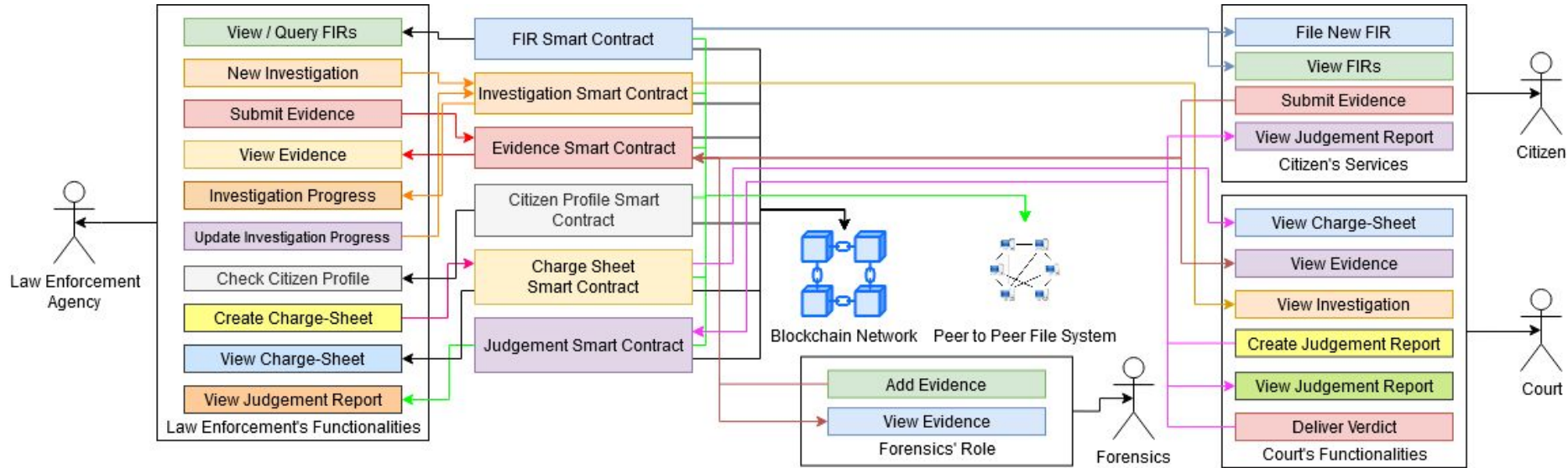
- a. Interface between police's investigation and court's judicial activities.
- b. On producing charge-sheets by the police, court passes through a number of trials, provides final judgement and declares verdicts.

5. **Identity Provider:**

- a. responsible for creating and maintaining the profiles of the citizens of the country.
- b. The citizens will be able to join and perform their respective functionalities, once their profiles are created by the Identity Provider.



Smart Contract Functionalities



This figure describes how functionalities of different stakeholders connect to the smart contracts of the blockchain network.

Access Control

- Since access control to critical information on the platform is a crucial aspect, we consider **Attribute-Based Access Control (ABAC)**.

U:	Set of users.
O:	Set of objects.
E:	Set of environmental conditions.
$\bar{U}\bar{A}$:	$\{a_1^u, a_2^u, a_3^u, \dots, a_n^u\}$ is an ordered list of user attributes.
$\bar{O}\bar{A}$:	$\{a_1^o, a_2^o, a_3^o, \dots, a_m^o\}$ is an ordered list of object attributes.
$\bar{E}\bar{A}$:	$\{a_1^e, a_2^e, a_3^e, \dots, a_p^e\}$ is an ordered list of environmental attributes.
V_i^x :	$\{v_{i1}^x, v_{i2}^x, v_{i3}^x, \dots, v_{ik}^x\}$ is the set of values that can be taken up by the attribute a_i^x , where $x \in \{u, o, e\}$.
OP:	Set of allowable operations on the object.
P:	$\{r_1, r_2, r_3, \dots, r_l\}$ is a set of rules that governs the access to an object depending on the values of the user- and the object-attributes and the prevalent environmental conditions.

ABAC Access Control

- $\vec{UA} = \{\text{user-type, department, designation}\}$
- $\vec{OA} = \{\text{document-type}\}$
- $\vec{EA} = \{\text{day}\}$

Rule: Police personnel under state-police with designation 'officer' can create, read and write FIR copy only on 'weekday', i.e.

user-type = police \wedge department = state-police \wedge
designation = officer \wedge document-type = FIR \wedge day =
weekday \wedge OP = *

- $V_1^u = \{\text{citizen, police, forensic, judge}\}$, set of possible values for user attribute 'user-type'.
- $V_2^u = \{\text{traffic-police, state-police, cyber-forensics, forensic-biology, apex-court, district-court}\}$, set of possible values for user attribute 'department'.
- $V_3^u = \{\text{police-officer, forensic-scientist, handwriting-expert, chief-justice, associate-justice}\}$, set of possible values for user attribute 'designation'.
- $V_1^o = \{\text{FIR, evidence, judgement}\}$, set of possible values for object attribute 'document-type'.
- $V_1^e = \{\text{weekday, weekend}\}$, set of possible values for environment attribute 'day'.

ABAC Algorithm

Algorithm 1: Algorithm CheckPolicy

Data: ABAC Policy P , ABAC Request R

Result: Allow or Deny

```
1  $\langle \overline{U}\overline{A}.val, \overline{O}\overline{A}.val, \overline{E}\overline{A}.val, action \rangle \leftarrow R$ 
2 permission  $\leftarrow true$ 
3 for rule  $\in P$  do
4   Let rule be of the form  $\langle f_1(\overline{U}\overline{A}, \overline{v}^u), f_2(\overline{O}\overline{A}, \overline{v}^o),$ 
    $f_3(\overline{E}\overline{A}, \overline{v}^e), op \rangle$ .
5   if  $\overline{U}\overline{A}.val \neq f_1(\overline{U}\overline{A}, \overline{v}^u)$  then
6     permission = false;
7     break;
8   end
9   if  $\overline{O}\overline{A}.val \neq f_2(\overline{O}\overline{A}, \overline{v}^o)$  then
10    permission = false;
11    break;
12   end
13   if  $\overline{E}\overline{A}.val \neq f_3(\overline{E}\overline{A}, \overline{v}^e)$  then
14    permission = false;
15    break;
16   end
17   for operation  $\in action$  do
18     if operation  $\notin op$  then
19       permission = false;
20       break;
21     end
22   end
23 end
24 Return permission;
```

Implementation Details

Implemented using the **Hyperledger Fabric blockchain platform**

The whole development consists of three parts:

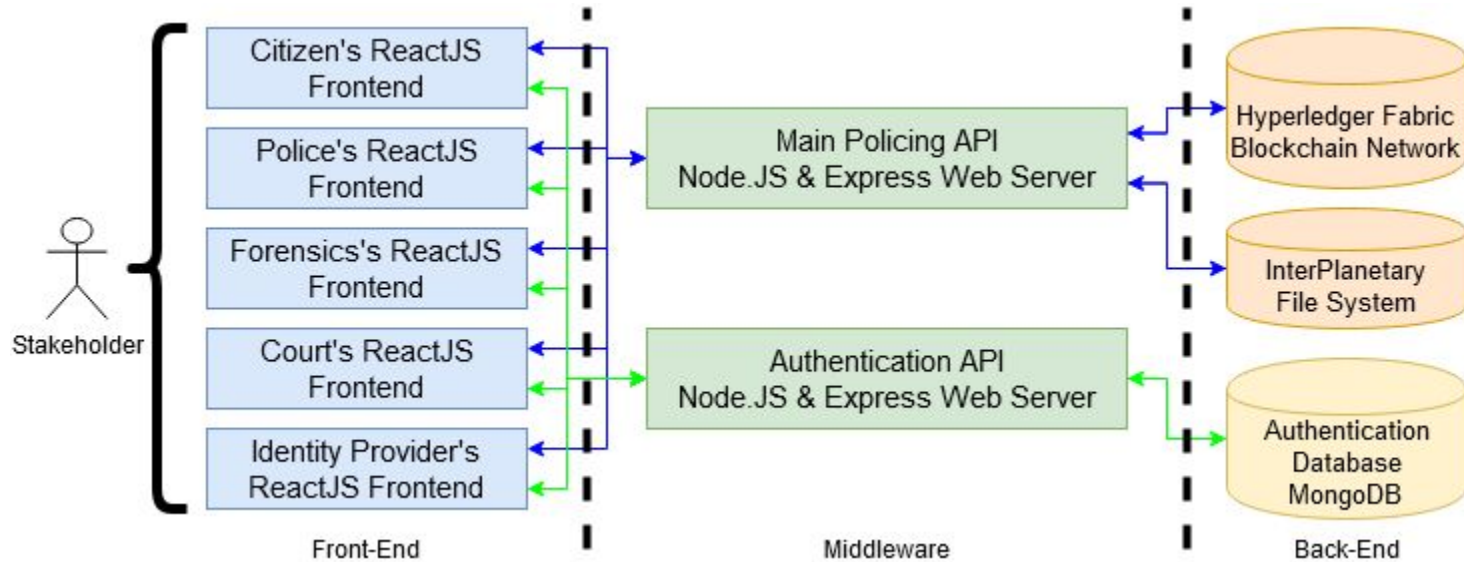
- Hyperledger Fabric blockchain network (back-end)
- Node.JS REST API (middle-ware)
- React JS web-based GUI (frontend)

To store various documents and reports, we use **InterPlanetary File System (IPFS)**.



Prototype Architecture

<https://github.com/mukherjeeearnab/policing-network>



5 stakeholders and 7 smart contracts

Test-Bench Specification

The experiment is conducted on a machine with

CPU: AMD Phenom(TM) II X6 1090T clocked at 3.6 GHz

Memory: 8 GB 1333 MHz dual-channel memory

Storage: Western Digital Green 240GB SATA III SSD

Operating System: Canonical Ubuntu Server 20.04 LTS



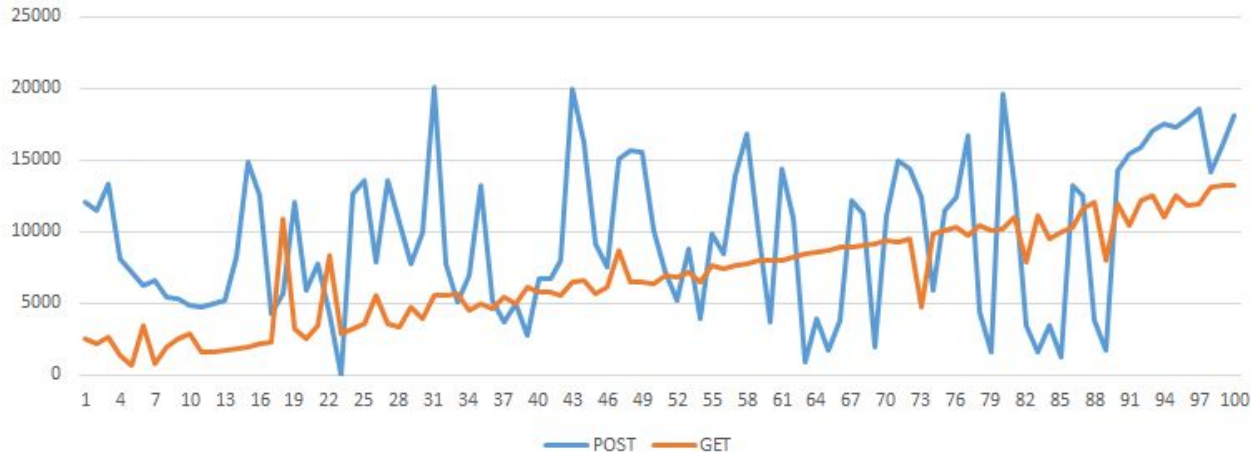
Performance Evaluation (JMeter)

- We assess response times over number of requests issued at various time instances by sending **HTTP** requests using **Apache JMeter**
- Load, ramp-up period and loop count were set to **4000** threads, **1** second and **1** respectively.



Number of Requests v/s Response Time (ms)

- The response time **increases** as the number of requests increase for **GET** requests.
- However, the response time for **POST** requests have an **alternating** curve.



Performance Evaluation (Hyperledger Caliper)

A performance test on our blockchain network using **Hyperledger Caliper** under three different operations read, query and write.

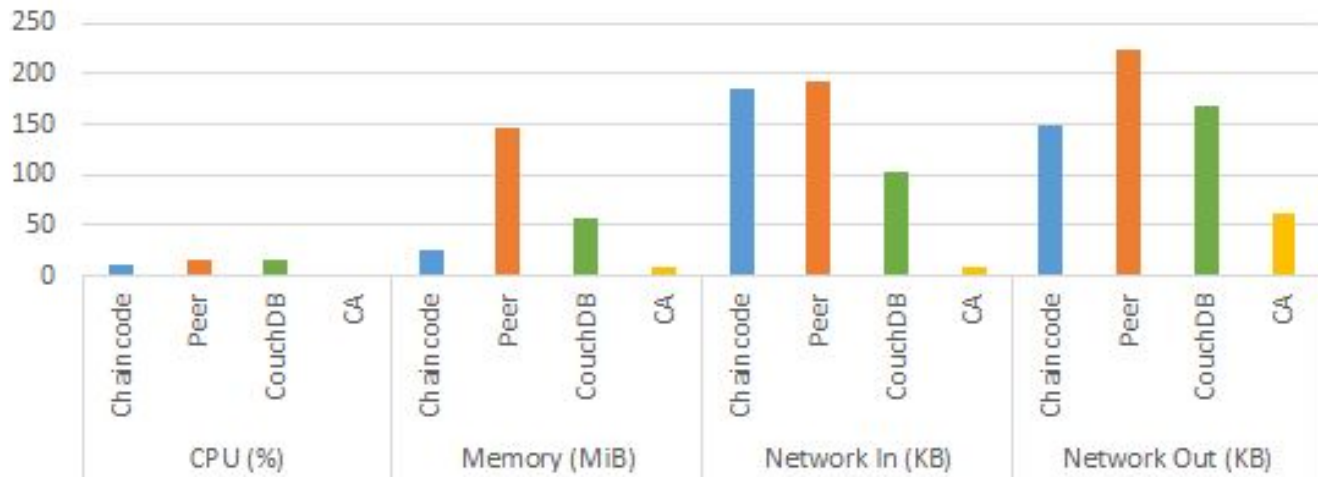
Name	Succ	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
read	100	0	34.7	4.23	0.36	1.48	23.7
query	100	0	100.3	6.43	1.17	1.63	66.4
write	86	14	24.8	20.7	4.67	11.56	6.51

TPS denotes **transaction per second**.



Resource Consumption

Resource consumption during the conduction of tests on the blockchain network using **Hyperledger Caliper**.



Conclusion

- We propose a smart policing system by leveraging the power of blockchain technology and smart contracts
- The proposed system establishes transparency, trust and accountability in the system.
- The experimental results on response times for a number of requests issued at various time instances are encouraging.
- To the best of our knowledge, this is the first proposal of its kind.
- Currently, we are in the process of extending it to support more services, e.g. smart passport management system, automated police verification, etc.



Thank You!

