SOFTWARE REQUIREMENT SPECIFICATION

FOR

***AVAULT**-A BLOCKCHAIN BASED CRIME REPORTING SYSTEM*

ITERATION 1

TEAM-14 MEMBERS

63.VINAYAK M V

28.DIYA PRATHAP

40.MOHAMMED IRFAN T K

52.P SREERAM

44.MUHAMMED SHAHZA

GENERAL INTRODUCTION

INTRODUCTION

Crime rates are steadily increasing worldwide, and accessibility to law enforcement services remains a challenge, especially in vast and densely populated regions. Many crimes go unreported due to a lack of secure and efficient platforms, leading to delays in justice and manipulation of complaints. Traditional reporting methods are often inefficient, lacking transparency and accountability. To address these issues, blockchain technology offers a decentralized and tamper-proof solution, ensuring data security, anonymity, and integrity. By leveraging blockchain, crime reporting can become more transparent, secure, and accessible, fostering trust between citizens and law enforcement authorities.

PROBLEM STATEMENT

The absence of a secure and trustworthy crime reporting system leads to multiple challenges, including unreported crimes, tampering with complaints, and inefficiencies in law enforcement responses. Existing systems often fail to maintain the anonymity of victims, making individuals hesitant to report crimes due to fear of retaliation. Additionally, centralized systems are prone to data manipulation and unauthorized access. The need for a decentralized, immutable, and user-friendly platform that allows secure crime reporting while maintaining confidentiality is crucial. This project aims to develop a blockchain-based crime reporting system that enhances transparency, security, and efficiency in law enforcement.

GOALS AND OBJECTIVES

The primary goal of this project is to design and deploy a blockchain-based crime reporting system that ensures secure, anonymous, and tamper-proof crime reporting. The system will allow users to submit reports along with multimedia evidence while maintaining end-to-end encryption. Key objectives include:

- Implementing asymmetric encryption to safeguard user data.
- Enabling anonymous reporting while ensuring authentication and verification.
- Storing crime reports on a blockchain ledger to prevent data manipulation.
- Providing law enforcement with a secure and verifiable platform for investigating reports.
- Enhancing public trust in crime reporting systems through transparency and security measures.
- Ensuring accessibility with a user-friendly interface for all sections of society.

EXISTING SYSTEM

LITERATURE SURVEY

Several studies have explored the use of blockchain technology in crime reporting and law enforcement, emphasizing its potential to enhance transparency, security, and efficiency. Hingorani et al. (2020) proposed a blockchain-based police complaint management system that prevents manipulation of crime reports. Their study highlighted how decentralized ledgers and smart contracts can ensure data integrity, preventing unauthorized modifications. Similarly, Swati et al. (2024) examined the role of blockchain in forensic evidence management, demonstrating how immutable storage can improve trust in legal investigations while addressing challenges such as key management and system scalability.

Amin et al. (2023) introduced the XCRM system, which leverages Hyperledger Cacti to enable seamless interoperability between different blockchain networks for crime reporting. Their research focused on the use of digital signatures and decentralized identity management, ensuring secure and verifiable complaint submissions. Dpushpa et al. (2023) explored the implementation of blockchain-based police complaint registration, using Ethereum smart contracts to create tamper-proof crime databases. Their study also discussed real-world challenges, including system adoption and integration with existing law enforcement infrastructure. Mil et al. (2025) further extended the application of blockchain to criminal record management, ensuring that investigation histories and past reports remain secure and immutable. Their research emphasized how blockchain can prevent evidence tampering, a critical issue in many judicial proceedings.

These studies collectively highlight how blockchain can revolutionize crime reporting by addressing key issues such as data security, anonymity, and inefficiencies in traditional systems. Despite its advantages, researchers also acknowledge potential challenges, including computational overhead, user education, and integration with existing police databases.

COMPARISON WITH EXISTING SYSTEM IN INDIA

India’s current crime reporting system is largely centralized, relying on police stations and government portals such as the Crime and Criminal Tracking Network and Systems (CCTNS). While these platforms provide a digital framework for complaint registration, they remain vulnerable to data manipulation, unauthorized access, and bureaucratic inefficiencies. In contrast, blockchain-based systems offer immutable record-keeping, ensuring that once a crime report is submitted, it cannot be altered or deleted. This significantly enhances the reliability of crime data and prevents potential corruption or negligence in law enforcement.

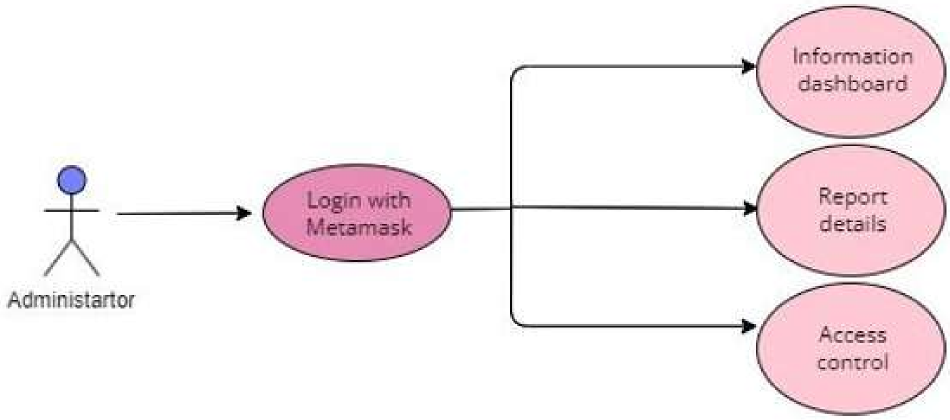
Anonymity is another major concern in India’s existing system, as complainants are often required to disclose their identity, making them hesitant to report crimes due to fear of retaliation. Blockchain-based systems address this issue by using cryptographic key-based identities, allowing victims to submit reports securely while maintaining privacy. Moreover, accessibility remains a challenge in the traditional system, as many individuals, especially in rural areas, find it difficult to visit police stations. A blockchain-based platform, accessible online, ensures wider reach and convenience, allowing users to report crimes from any location.

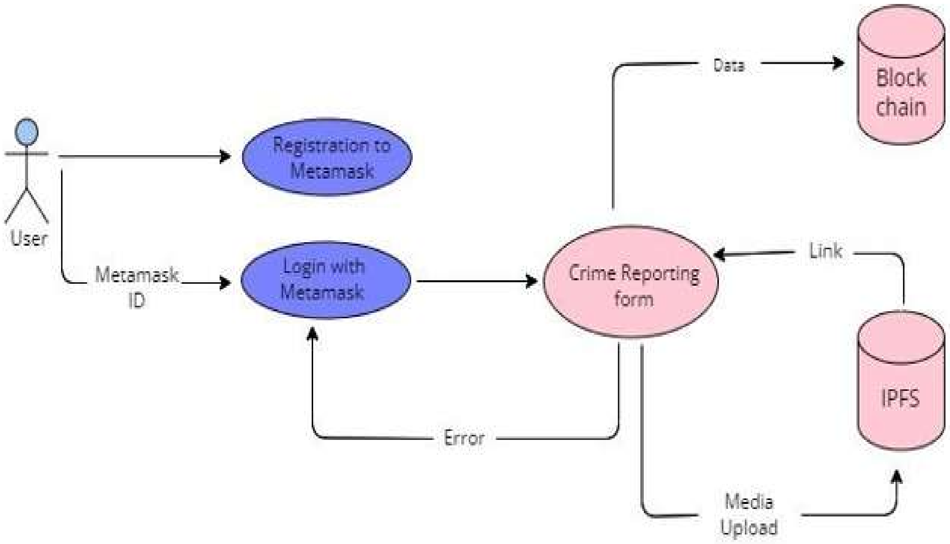
Response time is also a key differentiator. The current system in India suffers from delays due to bureaucratic processes and manual handling of complaints. Blockchain-based systems, on the other hand, can utilize smart contracts to automate case verification and assignment, significantly reducing processing times. Security is another area where blockchain has a distinct advantage. While centralized databases are prone to hacking and data breaches, blockchain's decentralized architecture and asymmetric encryption provide enhanced protection against unauthorized access.

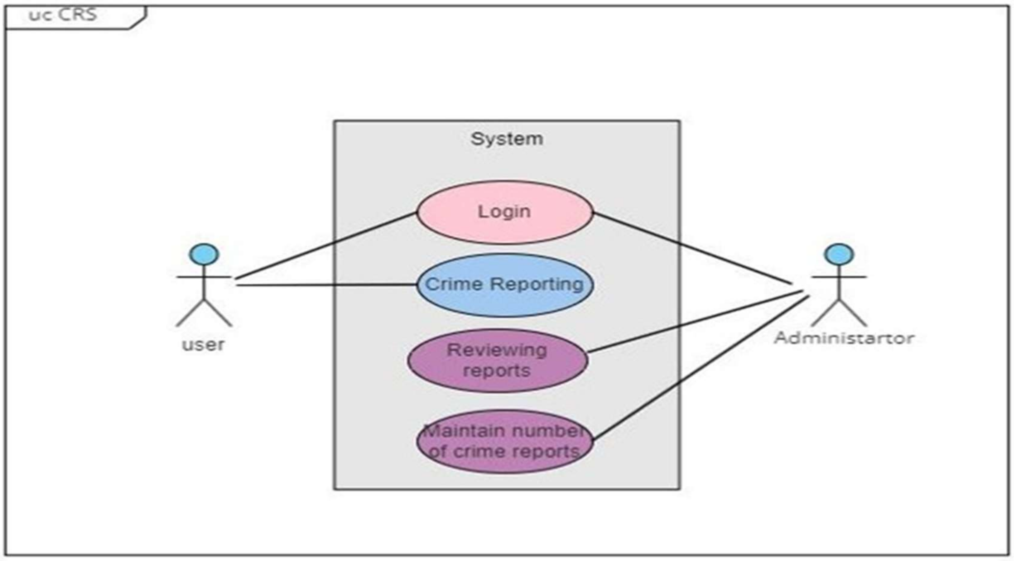
Public trust in the Indian crime reporting system has been a longstanding issue due to past incidents of police negligence and corruption. Blockchain technology can help rebuild this trust by ensuring transparency, as all transactions and modifications on the platform are recorded and verifiable. Additionally, blockchain-based crime reports, supported by digital signatures and cryptographic hashing, can hold legal validity, eliminating the need for excessive paperwork and physical documentation.

In conclusion, blockchain-based crime reporting systems present a significant improvement over India's current system by enhancing security, anonymity, accessibility, and efficiency. However, for successful implementation, challenges such as public awareness, law enforcement training, and integration with existing police infrastructure need to be addressed.

USE CASE DIAGRAM

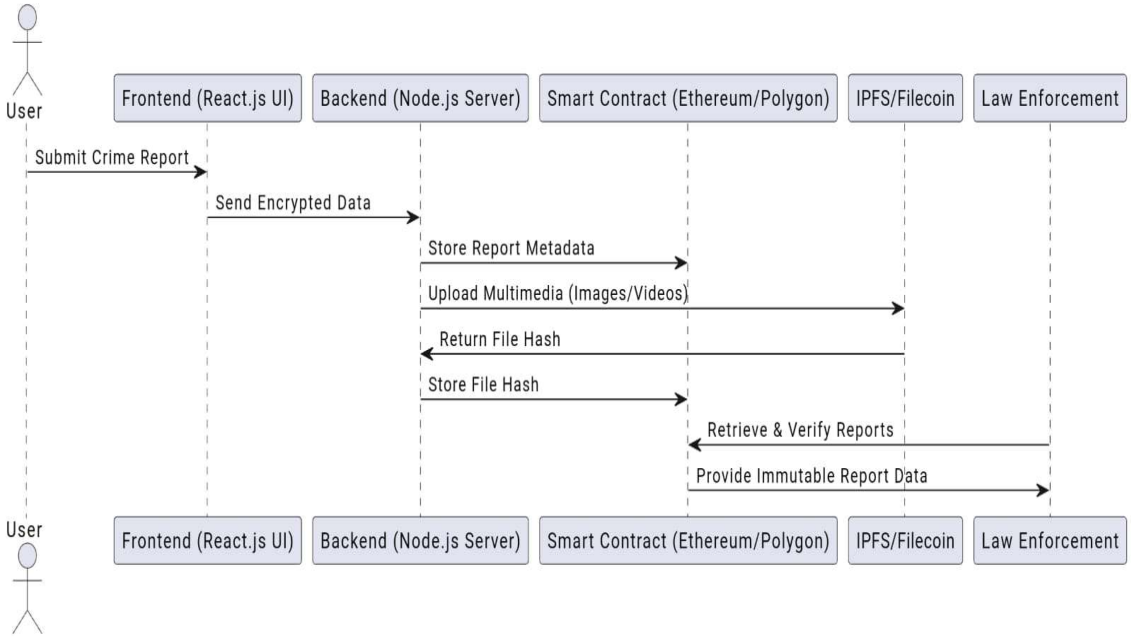




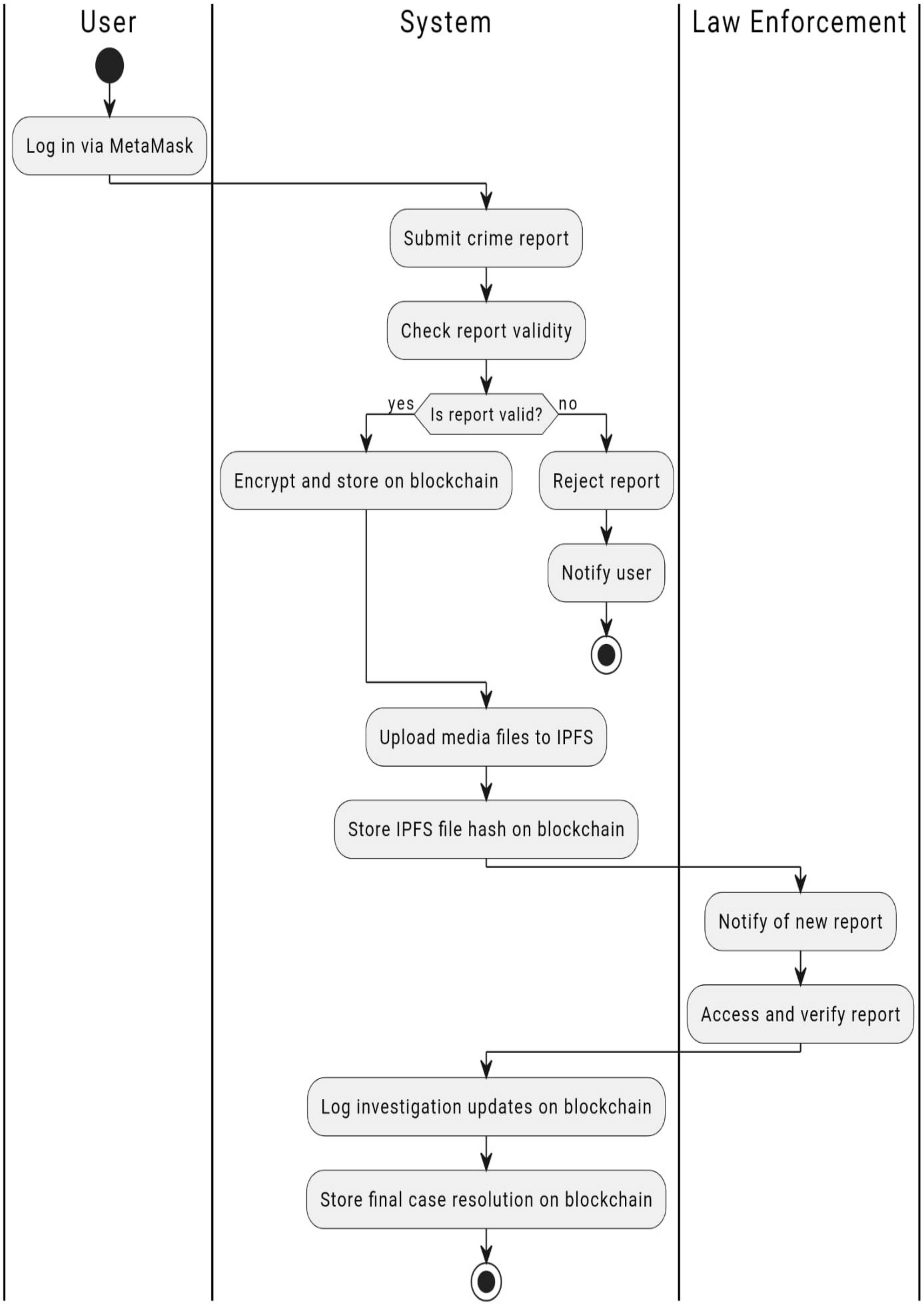


use case diagram

SEQUENCE DIAGRAM



ACTIVITY DIAGRAM



REQUIREMENT ANALYSIS

HARDWARE REQUIREMENTS FOR USER

- **Processor:** Minimum dual-core (2 GHz or higher)
- **RAM:** At least 2 GB (4 GB recommended for smooth operation)
- **Storage:** Minimum 200 MB free space for application installation
- **Network:** Stable internet connection (minimum 2 Mbps speed)
- **Operating System:** Windows 10 or above, macOS 10.13 or above, or Linux (Ubuntu 18.04+)

SOFTWARE REQUIREMENTS

- **Programming Languages:** JavaScript, Solidity, Python
- **Frameworks & Libraries:** ReactJS, Node.js, Web3.js
- **Blockchain Platform:** Ethereum (Smart Contracts using Solidity)
- **Database:** MongoDB 4.0+
- **Security Tools:** OpenSSL for encryption, OAuth for authentication
- **Cloud Services:** AWS or Google Cloud for deployment
- **Storage Solutions:** IPFS for storing encrypted files

HARDWARE REQUIREMENTS DURING DEVELOPMENT

- **Processor:** Quad-core (3.0 GHz or higher recommended)
- **RAM:** Minimum 8 GB (16 GB recommended for smooth multitasking)
- **Storage:** SSD with at least 512 GB space
- **Graphics:** Dedicated GPU (if using machine learning or complex data visualization)
- **Internet Speed:** High-speed broadband (minimum 10 Mbps for efficient cloud interaction)
- **Operating System:** Windows 10 or above, macOS 10.13 or above, Linux (Ubuntu 20.04+ recommended)

IMPLEMENTATION DETAILS

DATASET

- **Crime Report Dataset:** Contains structured information about past crime reports, types, locations, and timestamps.
- **User Identity Dataset:** Stores encrypted user credentials and anonymous identifiers for authentication.
- **Blockchain Transactions Dataset:** Maintains a ledger of all submitted reports, ensuring tamper-proof storage.
- **Multimedia Evidence Repository:** Stores images, videos, and supporting documents in an encrypted format.

MODELS REQUIRED

- **Encryption Model:** Uses RSA-2048 asymmetric encryption for securing user-submitted reports.
- **Blockchain Smart Contract Model:** Defines the structure of crime reports, user verification, and immutable storage.
- **Machine Learning Model (Optional):** Predicts crime trends based on historical data and helps prioritize cases.
- **Identity Verification Model:** Uses cryptographic signatures for user authentication.

TOOLS

- **Backend:** Node.js with Express.js for handling API requests.
- **Frontend:** ReactJS for building a user-friendly interface.
- **Blockchain:** Ethereum smart contracts (Solidity) for secure and immutable storage.
- **Database:** MongoDB for storing non-sensitive user details and metadata.
- **Encryption Libraries:** OpenSSL and Crypto-JS for securing user data.
- **Storage:** IPFS (InterPlanetary File System) for decentralized storage of multimedia evidence.
- **Authentication:** OAuth for secure user access.
- **Deployment:** AWS or Google Cloud for hosting backend and blockchain nodes.

This implementation ensures security, anonymity, and efficiency in crime reporting using blockchain technology.