EIH-PS8: Smart Birth Registration and Vaccination Monitoring

Rahul Dutta, Arindam Roy, Subhodeep Mondal and Shrabana Goswami

University of Calcutta

Idea Description

Smart Birth Registration and Vaccination Monitoring: The proposed approach presents a decentralized Smart Birth Registration and Vaccination Monitoring application using **Ethereum Blockchain** and **Inter Planetory File System (IPFS)**. The proposed system presents an all-in-one Blockchain based digital platform for secure, low cost and efficient way of registering, issuing and verification of birth certificates and vaccine records while maintaining its **integrity**, **fraudlessness** and **immutability**. The actual birth certificate and vaccine records are stored in IPFS which makes them **tamper-proof**. The hash of the records acting as its pointer is stored on Ethereum Blockchain and due to Blockchain's decentralized nature, integrity and fraudlessness of the records are maintained while **eliminating any forgery** of certificates and records. **Smart Contracts** have been implemented in Ethereum to **speedup and auto-enforce entire registration process**. Users can **retreive birth certificates and vaccination records within minutes** and also, allow third party authorities such as Colleges, Companies, access to them.

Technology Stack

Back-end technologies stack

- Blockchain: Ethereum[1].
- Frameworks: Truffle Suite[1].
- Programming Languages: Solidity[2], Javascript.
- Server: Ganache(Private Ethereum Network)[3], ExpressJS,
- Database: Inter Planetory File System (IPFS)[2], MongoDB.

Front-end technologies stack

- Markup language: HTML 5
- Style sheet language: CSS

---

[1]Truffle Suite, https://www.trufflesuite.com/

[2]Solidity, https://solidity.readthedocs.io/en/v0.6.2/

[3]Ganache, https://www.trufflesuite.com/ganache
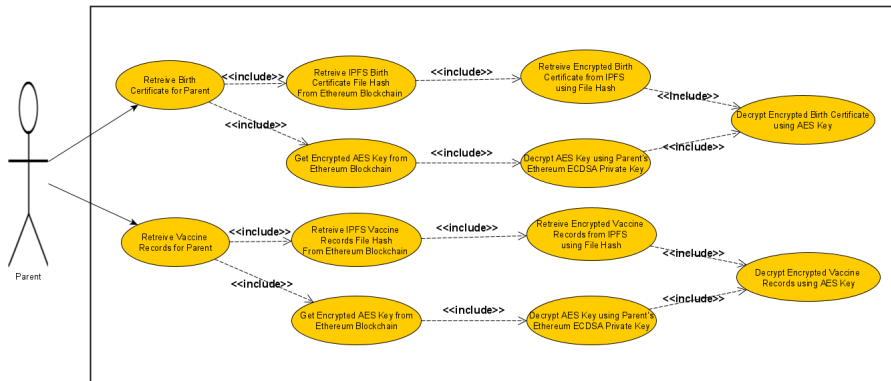
Use Case Diagram
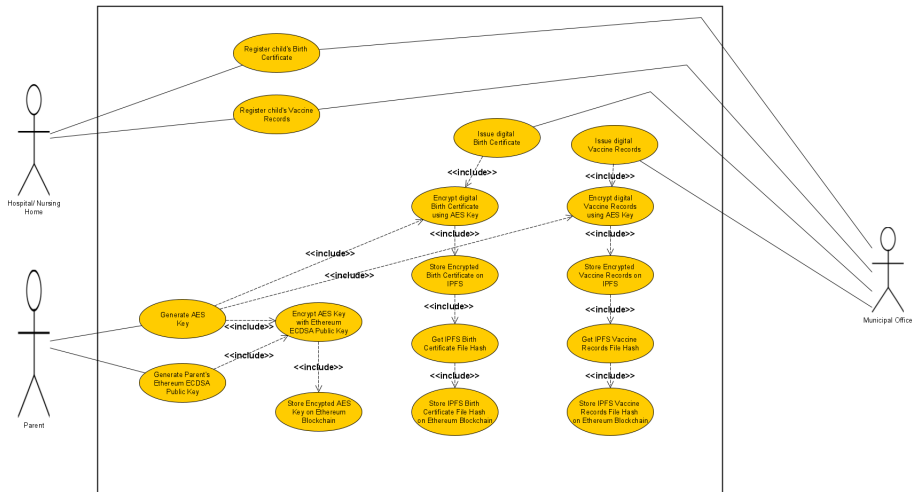
Figure: Use Case Diagram

Figure: Use Case Diagram

Allowing third party access

- For sharing the digital birth certificate and vaccine records to third parties such as educational institutes or for identity verification, **all the above steps will be repeated but instead of parent's Ethereum Public key, the third party's Ethereum Public key will be used to encrypt AES key**.

Risk Analysis

- Low probaibility of high transaction cost of smart contract function.
- Medium probability of Scalability being a risk(Current Ethereum Transaction Per Second=20 (approx)). It would require sharding of Ethereum as a possible solution.

Novelty

- **Secured** due to use of assymetric cryptography and AES.
- **Tamper-proof** due to immutable nature of IPFS and hash pointers in Ethereum Blockchain.
- Eliminates **Forgery**.
- **Auto-enforced** due to if-then-else property of smart contracts.
- **Byzantine Fault tolerance**.

📄 Gavin Wood et al.
Ethereum: A secure decentralised generalised transaction ledger.
Ethereum project yellow paper, 151(2014):1–32, 2014.

📄 Juan Benet.
IPFS - content addressed, versioned, P2P file system.
CoRR, abs/1407.3561, 2014.