**Electronic Medical Bureau**

- Vijayakumar Pattanashetti

Geetha N

Kiran Mohan

Vivek J

1. ***Abstract***

High security electronic management in healthcare sector is still an expectation. However, there exists technologies that are used for electronic healthcare management which still lack in privacy, interoperability, tracking, unambiguous and complete record keeping. Outcome-based contracts, real-time atomic clearing and settlement are also the still expected major requirements.

Electronic Medical Bureau (EMB) is a blockchain based approach for **one** healthcare information exchange platform that ensures high value of **confidentiality, privacy, interoperability, integrity** over **immutable** patient’s medical records, which improves the quality as well as reduces the cost of healthcare. The solution also implements **hashing** and **Aadhaar authentication** to fortify the secure sharing of healthcare data. The solution promises anonymized consistent accessibility to healthcare providers, partners, payers and patient to **secured and updated unambiguous patient's medical records** in trusted, secure & consensual way with ability of immediate access to wide range of normalised, patient’s non-identifiable information. The platform also allows automatic gathering, replication and distribution of data from **Electronic Data Capture** (EDC) machines with **extreme control** for **appreciable tracking**.

1. ***High Level Solution Architecture and Solution Approach***

The overall solution architecture along with few other architectures of flows are detailed below with relevant pictorial depictions.

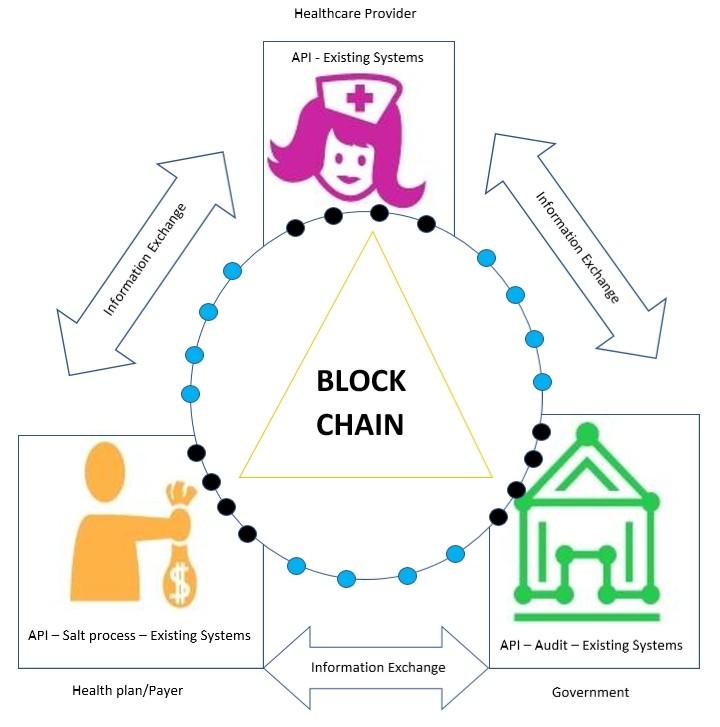
* 1. ***Outline - As a whole***

Fig.1. Outline of Solution

As a whole, the Fig.1. depicts implementation of blockchain technology to achieve the desirous features in electronic healthcare information exchange systems(detailed above and explained individually below). This is built as a platform for the three main participants and for necessary information exchange between them without violating privacy and security of patient's identity between the healthcare provider, the government and the health plan/payer. The patient isn’t included in this online platform as he/she interacts directly, if required patient gets his/her brief medical details via SMS to Aadhaar registered mobile number.

The healthcare provider interacts with government for authentication(Aadhaar), verification and extraction identifiable details of patient during enrollment. If enrollment is found to be successful, then the extracted identifiable data such as photo, name, gender, DOB is tokenized (detailed in page no. 4) and securely stored on blockchain to ensure anywhere and anytime accessibility(detailed in page no. 8&9). The interaction between the healthcare and the health plan/payer that involves patient’s direct participation also is depicted in detail in page no. 5&6. The interaction between the government and the health plan/payer involves authentication, verification and information exchange of healthcare related statistics, research, claimable offers, government policies.

**Note:**

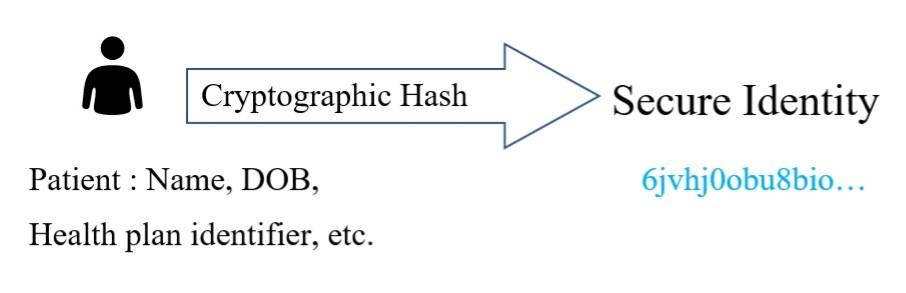
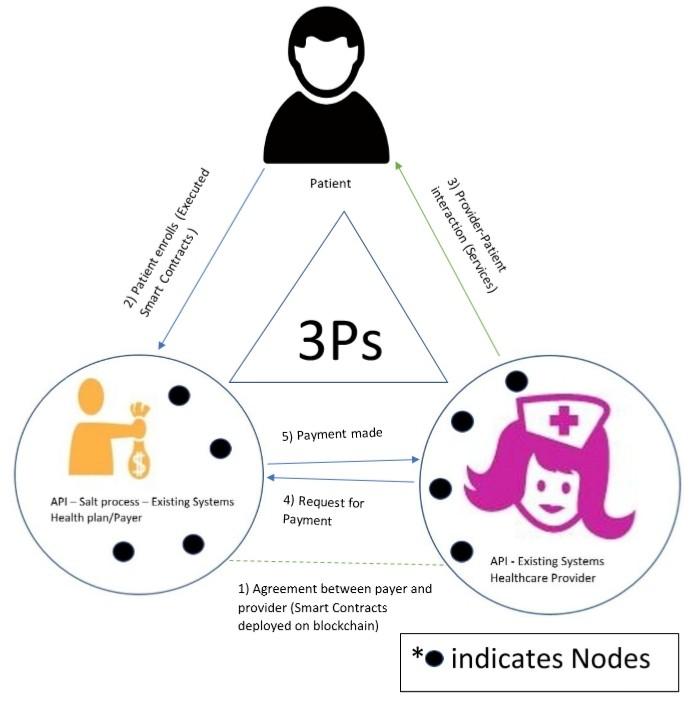
* Salting/Salt process in blockchain is the practical method to provide high security.
* Nodes ( ) contain Smart Contracts for information exchange between three main participants.
* Third party/Vendor nodes ( ) contain Smart Contracts for sharing limited information with on-boarding vendors for innovation, research and supply(pharmaceuticals).
  1. ***Tokenization for privacy***

Fig.2. Tokenization Flow

The tokenization process is carried out to securely store the personal information of the patient/healthcare provider/health plan/payer such as name, relevant IDs, etc… in the blockchain. This is done through cryptographic hashing. The illustration of tokenization flow is depicted in the Fig.2. This serves confidentiality to patient.

* 1. ***Patient, Provider and Payer Interactions***

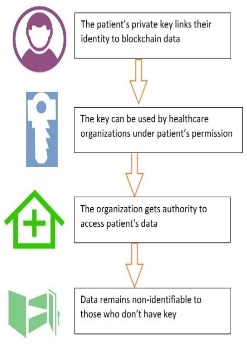
***(3Ps' interactions)***

Fig.3. 3Ps' Interaction

The 3Ps' interaction process can have greatest impact on the healthcare management. As detailed in the Fig.3., the 3Ps include the patient, the healthcare provider and the payer. The well organized interaction/communication between these 3Ps can influence the existing systems to implement the solution. As a initiation/first step, the payer and the healthcare provider accept to the agreements (deployment of smart contracts). Later, patient enrolls to the health plan (Execution of smart contracts). Further, the services are rendered to the patient. Now, its time for healthcare provider to get paid from payer. So, the healthcare provider claims the payer for payment which is paid as a response from the payer. The entire process is known as 3Ps' interaction (here).

* 1. ***Authorization to access Patient’s data and Nationwide Interoperability***

Fig.5. Authorization Flow



Whenever it’s the time to access the patient’s identifiable data from blockchain by healthcare organizations, they can use the private key (password/fingerprint) under his/her permission. Otherwise, identifiable data remains non-identifiable. (Refer Fig.5.) This serves privacy to the patient.

To serve patient with nationwide interoperability, blockchain found its importance. After patient being served by healthcare provider, the clinical data is tracked. The tracked data along with patient’s public ID (after being authorized) is processed by smart contracts. Finally, as a result the data is stored in blockchain where the patient’s public ID is pre-stored.

Further, the healthcare organizations and institutions from anywhere at anytime can request for accessibility to patient's non-identifiable (specially health records) data via APIs. Once the request is approved, the organizations/institutions can access and use the non-identifiable data for research and innovation.

