Our proposed architecture, in Figure 1, consists of patients, hospitals, insurers, and compliance entities, as well as a database (cloud) where data received from entities is stored and processed. Eventually, a subset of data that complies with the system specification, defined by its entities' roles and requirements, is added to a blockchain system component. Derivation of the blockchain from the cloud storage is policy-specific, resulting in various challenges that we address in this proposal. In the blockchain subsystem, we envision a peer-to-peer (P2P) network in which blockchain nodes communicate data (transactions/blocks) with one another. **Use Scenario.** To start, we concretely provide a use scenario defining the roles of each subsystem and entity. In this scenario, we consider a person (patient) involved in a road accident. In providing emergency medical services, the person is first attended by a team of first responders who would administer first aid then possibly transport the patient to a hospital. At the hospital, the emergency room (ER) team collects information from the first responders and the patient to assess the patient's conditions and provide the appropriate treatment. Once the patient is treated, she is discharged and a billing statement is issued to the insurance provider, with explanation of claim communicated with the patient. Finally, a compliance entity may investigate the process to ensure that each entity dutifully executed its responsibilities.

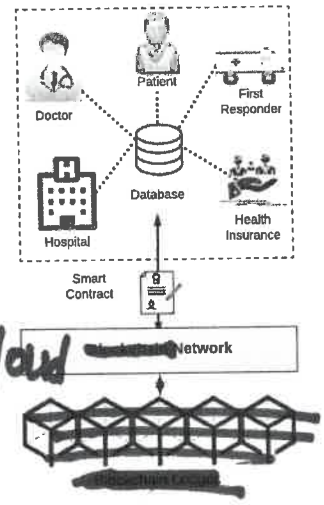


Figure 1: *Proposed Architecture.*

**System-wide Ideal Requirements.** The above scenario and use case dictate various ideal system requirements. First, the first responders need to swiftly provide the first aid to the patient and transport her over to the hospital for further assessment. To achieve this requirement, it would be ideal that the first responders are able to swiftly acquire additional information about the patient (e.g., basic medical record, including known allergies, current medications, etc.) for effective delivery of first aid treatment. The ER team would need to quickly assess the situation and follow prescribed medical procedures. For that, it would be ideal if the team has timely access to the patient's medical history, data describing the patient's current medical condition, and data gathered by the first responders, in order to facilitate the treatment. Upon treating the patient, insurance information is collected from the patient, coverage is verified, and medical bill is sent to the insurance company, along with explanation of claims sent to the patient. It would be ideal to have a seamless acquisition of such information in real-time. Upon disputes between any of those entities, or even to ensure quality of service and compliance, a compliance entity might be involved, requesting various pieces of information concerning the treatment of the patient. For that, it would be ideal to provide complete and untampered with medical data to the compliance entity in a timely manner.

**Medical IoT.** Medical IoT helps us achieve some of the aforementioned requirements. The medical IoT architecture is enabled by accurate medical sensors, covering various functions such as blood pressure, temperature, body position, electrocardiogram (ECG), galvanic skin response (GSR), etc., which are attached to the patient. Along with those sensors and associated data, the medical IoT system includes various analytics on the patient, including descriptive, diagnostics, event-triggers, predictive analytics. The medical IoT system involves human operators to read and assess low-level sensed data and high-level analytics, making further decisions, recommendations, diagnostics, and assessments. Those operators could be the first responders, ER team, etc. Part of the requirements is fulfilled by making available a consolidated electronic medical record in real-time upon authorization, as well as insurance providers, as shown in Figure 1.

cloud **[redacted].** In our system, long-term data storage, data availability, confidentiality, integrity, and provenance are necessary requirements. For data storage that ensures low-latency data access with high availability guarantees, we propose to use large-scale data systems, such as distributed cloud storage. For data provenance, centralized techniques are impractical, for they are vulnerable to single point of failure. Our system utilizes a blockchain ledger, which naturally resists the single point of failure. Given the use scenario above, in the following we outline the different data types in our proposed system, the system design challenges that need to address, and reach a general overview of an initial blockchain construct.

**Data Types.** Various records are generated, updated, and stored, requiring provenance. Those records include sensed data, medical records, insurance data, permission data (for access), analytics, insurance transactions, etc. For scalability, our design separates the application data from provenance data, where the blockchain stores *transactions* for provenance. Data records in our system are highlight in the following. ❶ Sensed data: the medical sensors generate real-time data streams used for analytics and diagnostics and to facilitate medical uses cases. Each sensed data record includes basic patient information, sensor information, time information, value (sensor-dependent), uniform resource identifier (URI), and authenticity and integrity markers. ❷ Analytics data: this data record includes reference to the sensed data records and results of analytics procedures; e.g., descriptive analytics (summaries), diagnostics, event-based actions, and predictive analystics output. ❸ Medical record data: this record includes biographical data, demographics, administrative and billing data, medical history, current medications, immunization dates, allergies, and a URI. ❹ Medical service data: this record includes information of services rendered, including a reference to a medical record, a reference to analytics records, details of tests, treatments and procedures. ❺ Insurance data: this record includes a reference to the medical record data, and stipulations and attributes of the insurance policy. ❻ Insurance claims: this record includes the equivalent of a medical billing data, with a reference to medical service data and billing information associated with rendered medical services. ❼ Permission data: this data includes access authorization of different system entities such as hospitals (doctors, nurses, administrators, etc.), insurers, compliance officers, etc. to other records.

**Blockchain Design Choice.** Our proposed system has a smart contract that will generate transactions sent over a network to the blockchain. The blockchain subsystem will consist of peers that will execute a consensus algorithm to confirm a transaction. The blockchain provides a provenance service that captures *mutually agreed* upon state of the cloud database. The provenance can be used for conflict resolution, fault detection, and data recovery. For instance, under attack on the cloud database, the blockchain can be used to recover some of essential data, and prove the tamper of other types. However, in order to realize such a bold vision and application, we expect to first address the following challenges.