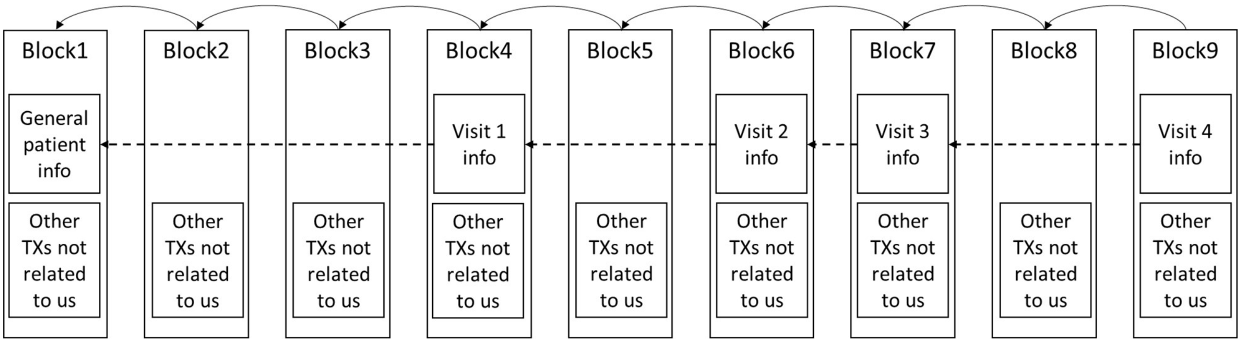
CSEN 1001 – Computer and Network Security

Project Description

The objective of the project is to create a blockchain application for Electronic Healthcare Records (EHR).

EHRs contain all information pertaining to a patient in the healthcare system. This includes general information about the patient (name, age, weight, height, sex, initial medical measurements such as blood pressure, pulse, oxygen, glucose, etc.), but also includes information about every visit to a healthcare professional. The information about every visit includes any readings that the patient takes in the clinic/hospital (blood pressure, glucose, temperature, pulse, etc.), the reason for the visit (periodic checkup, management of a case such as hypertension or diabetes, or patient is complaining about something), the doctor's diagnosis, and the prescription. The prescription may include medications (with doses and intake periods), referrals to other doctors/specialists, follow-up appointments, and lab tests. Note that a lab test would be considered a separate visit to the healthcare system.

The goal of this project is to create a blockchain application for the EHR operations mentioned above. For each patient, an initial transaction is to be added to a block in the blockchain that contains the general patient information. Then, for each visit a patient makes in the system, another transaction will be added to the most recent block with the information of that visit. The transaction for each patient will be chained in a similar way to the transactions of a user on the Bitcoin blockchain. The following figure illustrates how the blockchain would look like after adding the EHR of one patient.


Block1
General patient info
Other TXs not related to us
Block2
Other TXs not related to us
Block3
Other TXs not related to us
Block4
Visit 1 info
Other TXs not related to us
Block5
Other TXs not related to us
Block6
Visit 2 info
Other TXs not related to us
Block7
Visit 3 info
Other TXs not related to us
Block8
Other TXs not related to us
Block9
Visit 4 info
Other TXs not related to us

You may assume that the transactions are uploaded to the blockchain via a healthcare professional (doctor/nurse). Like transactions in any blockchain, they should have the security services of integrity and non-repudiation. This means that transactions that are uploaded cannot be modified (which is the case in any blockchain) and that transactions are digitally signed by the person who uploads them.

In addition, since we are dealing with EHRs, there is an additional requirement of confidentiality (normally not found in blockchain applications), since patient records contain sensitive information that cannot be viewed except by the authorized personnel. Thus you will have to figure out the proper set of cryptographic tools to achieve that. This means that we should be able to verify the transaction (the digital signature, validity of contents, chain to previous transactions), without reading the content of the transaction itself. There is a cryptocurrency known as ZCash that does something similar to that. You are advised to look into it. Please note that authorized personnel should still be able to read the EHRs.

Rules:

1. You are strongly advised to read about the operations of existing blockchain systems such as Bitcoin and Ethereum. You have to learn how integrity and non-repudiation are achieved for every transaction, how chaining blocks achieve a tamper-proof structure, how transactions are chained, the process of mining and adding blocks, and voting on a block.
2. You may deploy your application on an existing blockchain such as Ethereum or design your own private blockchain
3. Anything that is not explicitly specified in this document is considered a point to be designed, and you are free to design it in any way you think is proper. You will be evaluated in the end about whether or not the specified security objectives are achieved.
4. This is a security project, not a programming assignment. Thus, you are expected to design the security aspects of this project that have not been explicitly specified.
5. You may work in teams of minimum 2 students and maximum 5 students. Cross-tutorial groups are accepted.
6. The evaluation in the end will be done in one of two ways (you choose): either every team member will specify the part of the project that they were responsible for and will be evaluated only on this part (in which case every student may get a different grade), or you will be evaluated as a group, in which anyone may be asked about any part of the project and has to answer, and the group will get the same grade. Please note that in both cases, 30% of the project grade will be about the overall quality of the submitted project, and this part will be the same for all group members.
7. The details of what the EHR should contain are arbitrary. You may assume some general information for each patient (choose minimum 6 items of information as listed above), and some general information for each visit/lab test. The important aspects are the security objectives and how they are achieved.
8. The deadline to submit the team members is 31 March, 2022 (details of how to submit team members will be sent later).
9. There will be no milestones for the project, just the final submission/evaluation which will be in the last week of the semester (exact date will be sent later). However, you are strongly advised to consult the course instructors about your progress and your choices throughout the semester. If you do not check your progress, you are responsible for the outcome and whether or not it satisfies the project objectives.