E-HEALTHCARE

Xiyuan Feng, 85919234

Yinan Zhang, 87818979

Jiayu Zhou, 65492156

INTRODUCTION

E-healthcare makes it possible for patients to receive off-clinic health evaluation and a hierarchical structure is a common way to give different physicians different levels of authorization to access Patients' Health Record (PHR). However, this kind of hierarchical structure is not secure enough since PHR can be leaked from higher hierarchy generally by directly sharing data after access or by sharing private key to lower hierarchy letting them have the authorization to access. To solve these problems, out team makes PHR to be track-able and access control is being established. To fulfill these, our team set up a Patient Privacy Protection system based on Hybrid Cryptography, Attribute Based Access Control, Document, Digital Watermark, Pairing Based Cryptography.

E-HEALTHCARE

Hybrid Cryptography

Attribute Based Access Control

Document Digital Watermark

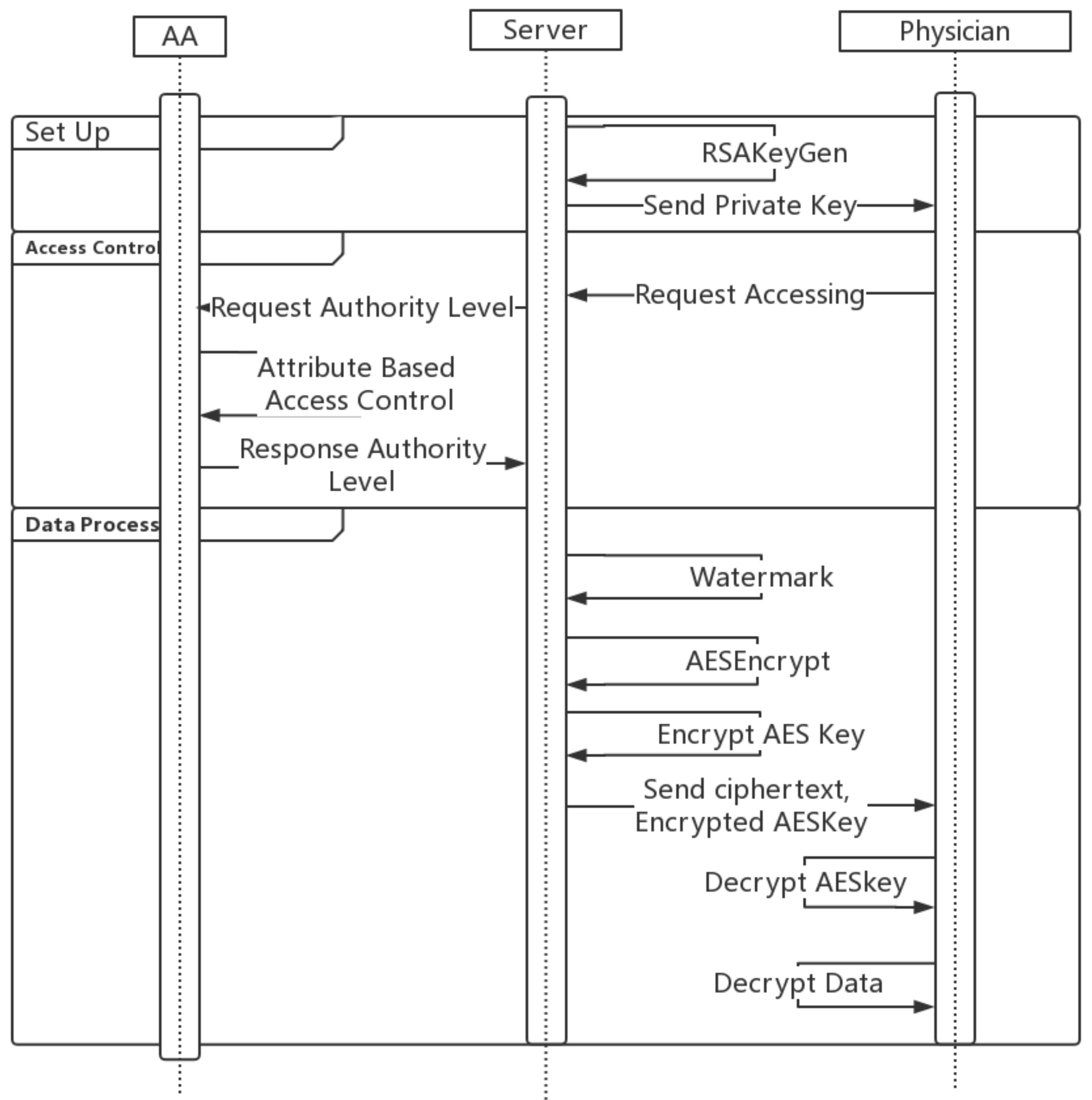
Pairing Based Cryptography

OBJECTIVES

Our goal is to prevent patient's data from leaking. Furthermore, if data unfortunately is leaked, the person who leaks is identifiable.

DESIGN

System Flow Chart



RSAKeyGen: Randomly generate RSA public key $rsapk$ and RSA private key $rsask$. $RSAGenKey(randompool) \rightarrow rsapk, rsask$. And send private key $rsask$ to physician.

Access Control: Doctor provides three credentials(DocID, Password, Workplace). Attribute Authority checking the access policy to determine doctor's authority level and how much data he can access.

Add a Watermark: A digital dictionary is used to store synonyms and possible represent forms of words. Before embedding the watermark, words in the documents will be analyzed for whether they can be replaced by other words or not. After the watermark message is transformed into a binary number, each bit of the number will decide whether each possible word is replaced or not.

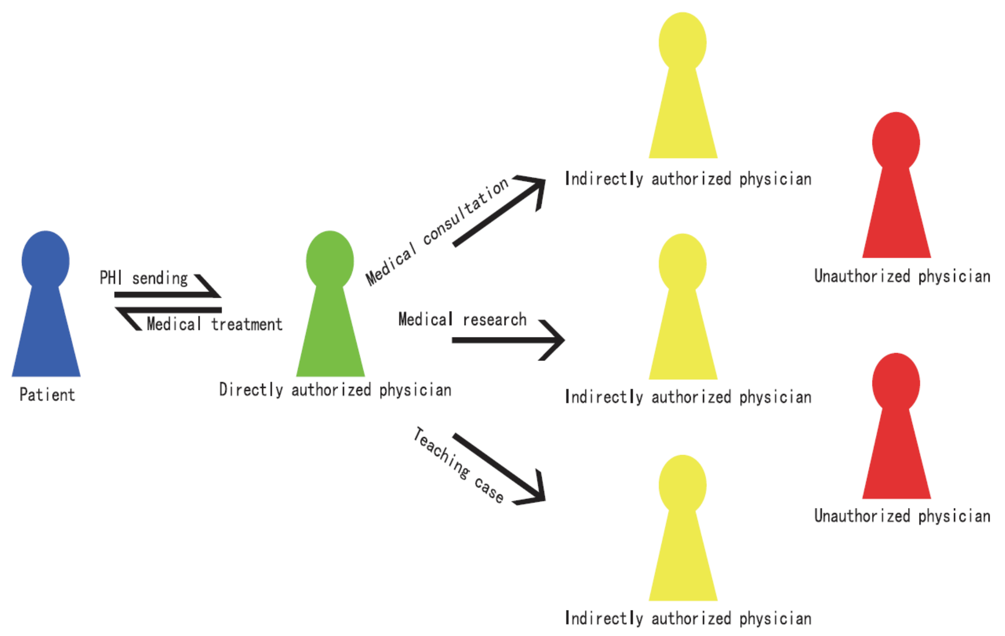
AESencrypt: Randomly generate AES key $aesk\_id, aesk\_data$. $AESGenKey(randompool) \rightarrow aesk\_id, aesk\_data$. Encrypt information of patients by AES. $AESenrypt(aesk\_id, aesk\_data, patient\_id, patient\_data) \rightarrow ciphertext\_id, ciphertext\_data$

RSAencrypt: When we receive the request of physician, we'll judge their attribute and decide if they have the authority to get all the information or part of them. Then use RSAencrypt those part of informaion. $RSAencrypt(rsapk, aesk\_data, (aesk\_id)) \rightarrow aesk\_data\_cipher, (aesk\_id\_cipher)$. And then send $(ciphertext\_id), ciphertext\_data, (aesk\_id\_cipher), aesk\_data\_cipher$ to the physician.

RSAdecrypt: When physician receive the information. They can first decrypt the AES key by their RSA private key. $RSAdecrypt(rsask, (aesk\_id\_cipher), aesk\_data\_cipher) \rightarrow (aesk\_id), aesk\_data$.

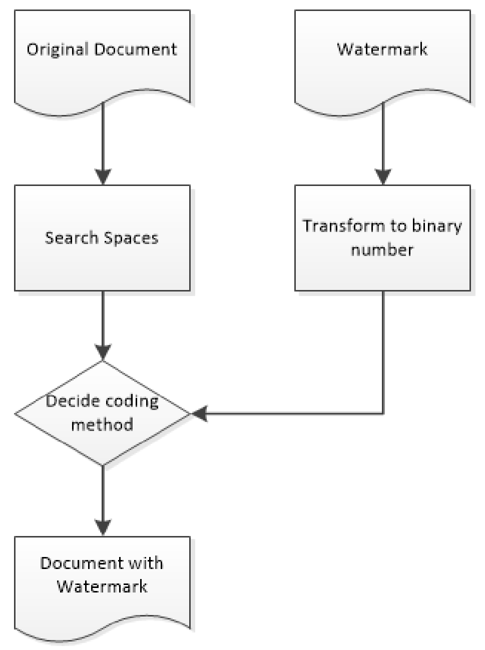
AESdecrypt: Then the physician can use the AES key to decrypt. $AESdecrypt((aesk\_id), aesk\_data, (ciphertext\_id), ciphertext\_data) \rightarrow (patient\_id), patient\_data$

Technical Details



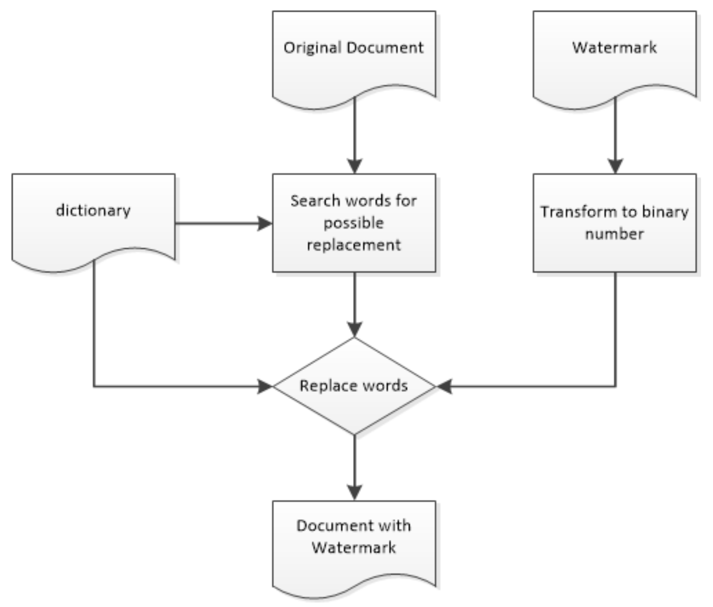
Multiple security and privacy levels in E-Healthcare

Let {P1, P2, . . . , Pn} be a set of parties. A collection A ⊆ 2{P1,P2,...,Pn} is monotone if ∀ B,C : if B ∈ A and B ⊆ C then C ∈ A. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) A of non-empty subsets of {P1, P2, . . . , Pn}, i.e., A ⊆ 2{P1,P2,...,Pn} \ {∅}. The sets in A are called the authorized sets, and the sets not in A are called the unauthorized sets.



Format-Based Watermark

Format-based watermark algorithms use color, size and other attribute of documents to embed the watermark. Since we are using plaint text documents based on ASCII codes, I decides to use the codes which don't represent alphabets to embed watermark. The watermark message is transformed into a binary number. Then each bit of the number will decide whether each space(' ') in document is represents by code 0(null) or code 32(space).



Semantics-based Watermark

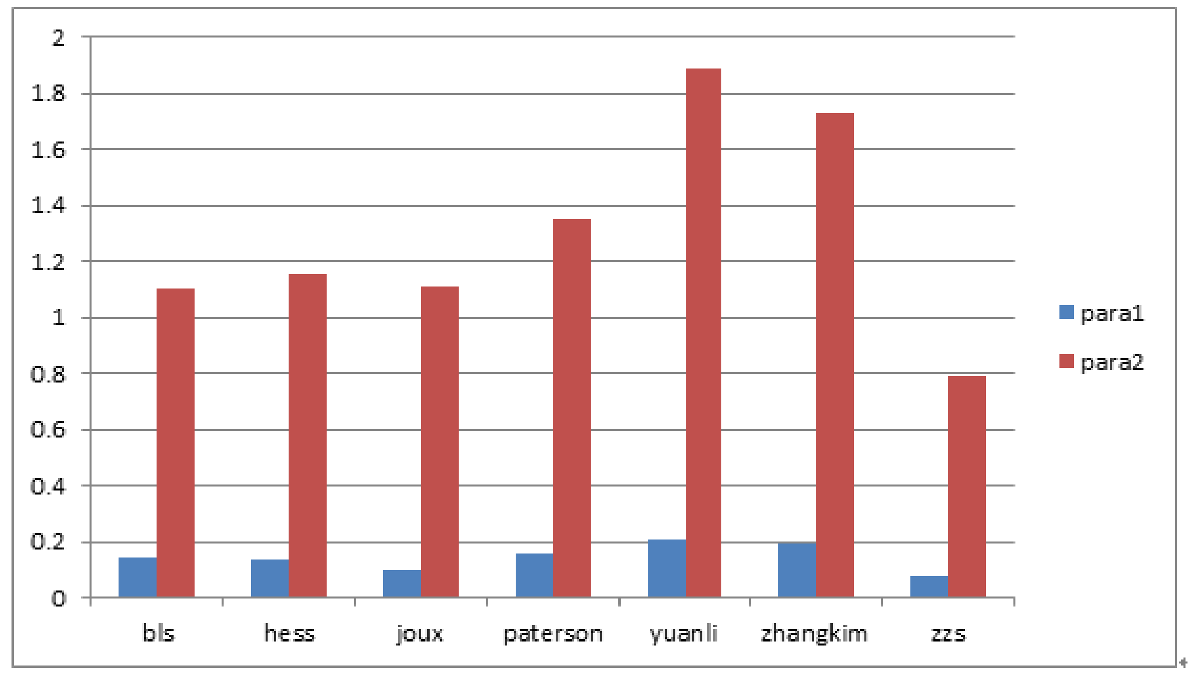
Semantic-based watermark algorithms analyze the structure of sentences and try to modify nouns, verbs and other words in sentences to embed the watermark. Because medical records are not like articles. Most sentences in medical records are incomplete while most information are represent by words but not sentences. I design a word-based algorithm to embed the watermark. In this algorithm, a digital dictionary is used to store synonyms and possible represent forms of words. Before embedding the watermark, words in the documents will be analyzed for whether they can be replaced by other words or not. After the watermark message is transformed into a binary number, each bit of the number will decide whether each possible word is replaced or not.

Analysis

1.Besides building this E-Healthcare system, we also use the pbc library and try to run several paring based signature or negotiation keys structure to see how it works.

The structure includes:

1. Boneh-Lynn-Shacham short signatures
2. Hess identity-based signatures
3. Joux tripartite Diffie-Hellman
4. Paterson identity-based signatures
5. Yuan-Li identity-based authenticated key agreement
6. Zhang-Kim identity-based blind/ring signatures
7. Zhang-Safavi-Naini-Susilo signatures



2. we also compare the two watermark algorithm. The format-based algorithm is fast while not changing the original content. Although the watermark will not be destroy by clipboard cutting and pasting, it can still be easily changed if the coding method is known. The semantics-based watermark has much stronger robustness since it's impossible to tell which words are replaced without the original document. However, the semantic-based watermark algorithm is slow while changing the original content. A bad dictionary of replacement may change the meaning of the document.

CONCLUSION

In this project, we constructed a E-Healthcare system with following feature:

1. Hybrid cryptology speeds up the encryption process.
2. Access control guarantee the data security when people access data with different purposes.
3. Watermark makes data trace possible.