Application of Ciphertext Policy Attribute Based Encryption in Cloud based Electronic Health Record

Lê Mậu Anh Phong

Nguyễn Duy Huy

For Cryptography Presentation

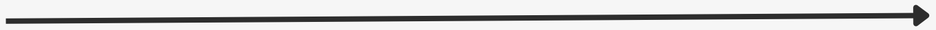
2023 June 17

Context

- Electronic Health Records
- Profiles
- Internal information
- ...

Nhiều dữ liệu

- Availability
- Cost saving

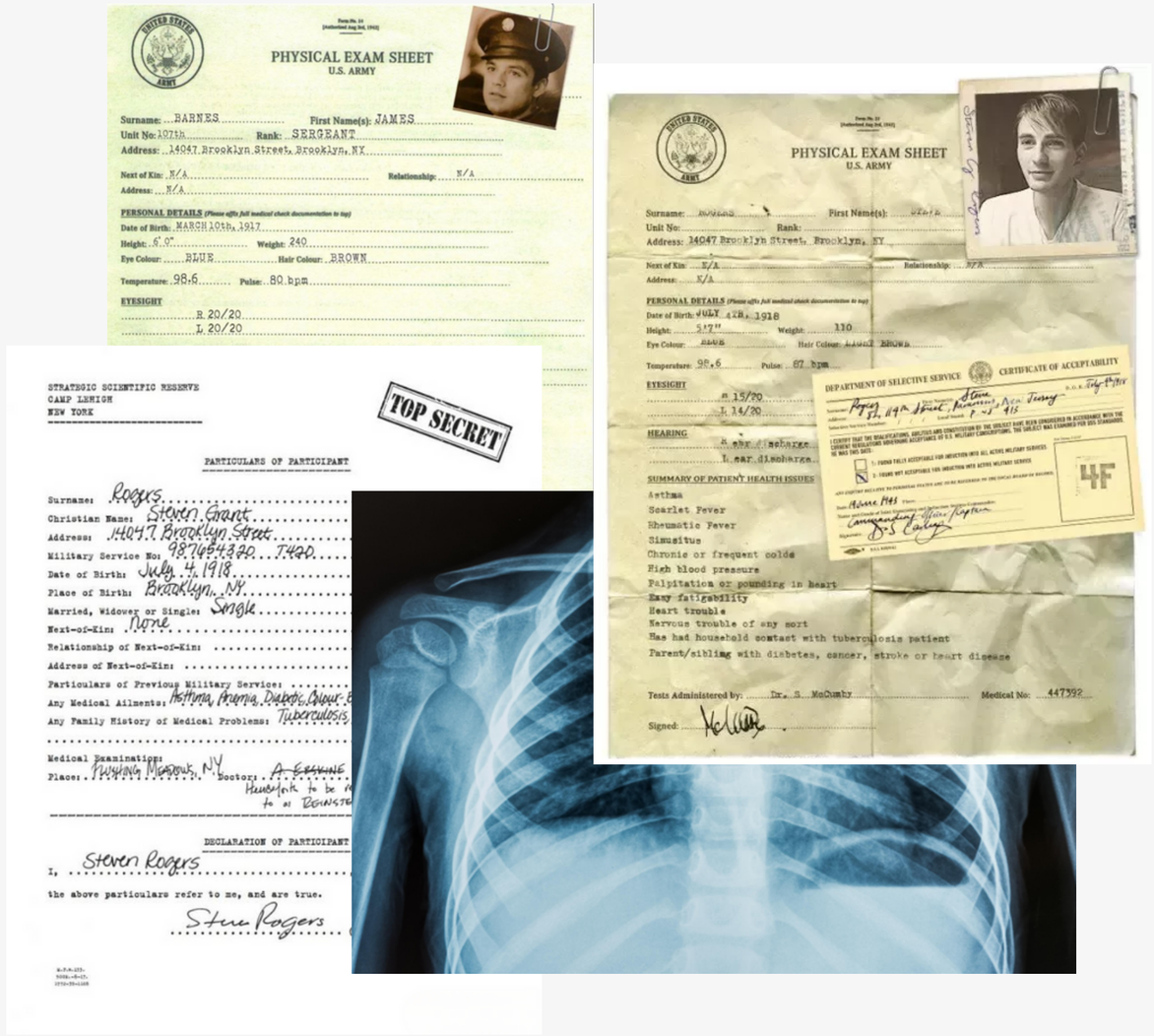


Cloud

What do we protect?

- Patient's health record:
  - Personal information
  - Medical diagnosis
  - Laboratory results
  - Treatment plans
- Doctors, nurses, staff… profiles
- Financial information
- Other profiles, …

…



Data owner

- Doctors, nurses
- Researchers

...

Fetch, upload data

Semi trusted: try to extract data

Cloud service providers

users spoofing

Fetch data

try to fetch or upload data

Data user

- Patients
- Patient's relatives
- Financial department

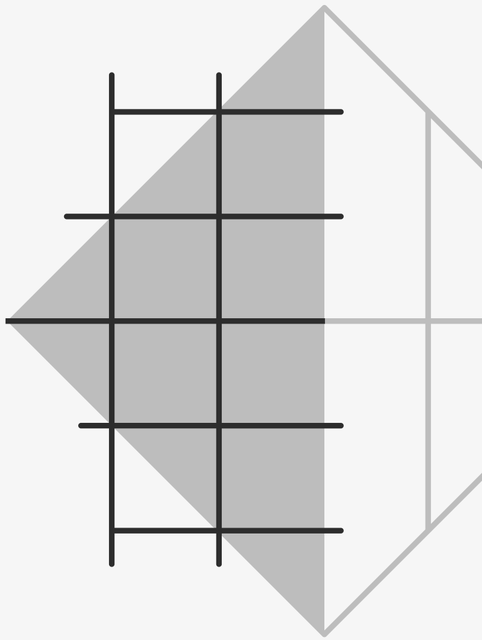
...

users spoofing

Threat

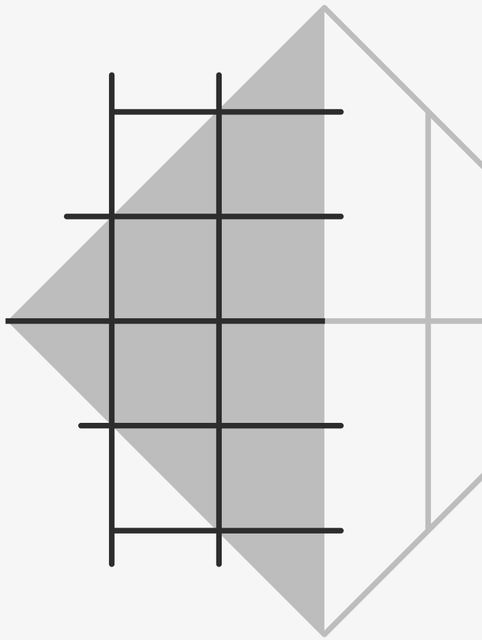
Security goals

- Ensure patient privacy
- Secure EHR data on Cloud Storage with confidential
- Only authorized parties are able to access patient health data



Solution

- Use CP-ABE to encrypt data before uploading to cloud
- Use HTTPS to secure transmission
- Use JWT + ABAC to authenticate, authorize to cloud

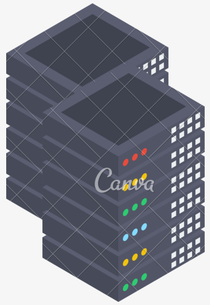


- Doctors, nurses
- Researchers
- Financial department
- ...

JWT Token + User key

Login

Fully trusted



Authority servers

All of connections using HTTPS

JWT Token + Encrypted data

Encrypted data

Semi trusted: try to extract data

Authentication module	Storage module

Cloud service providers

JWT Token + User key

Login

- Patients
- Patient's relatives
- ...

JWT Token

Encrypted data

Authority server will sign JWT, and authentication module will verify it

HTTPS

- Create free DNS records using DuckDNS.
- Use SSLForFree to generate key and cetificate.

JWT

- Algorithm: Ed25519
  - openssl genpkey -algorithm Ed25519 -out ed25519key.pem
  - openssl pkey -in ed25519key.pem -pubout -out ed25519pubkey.pem

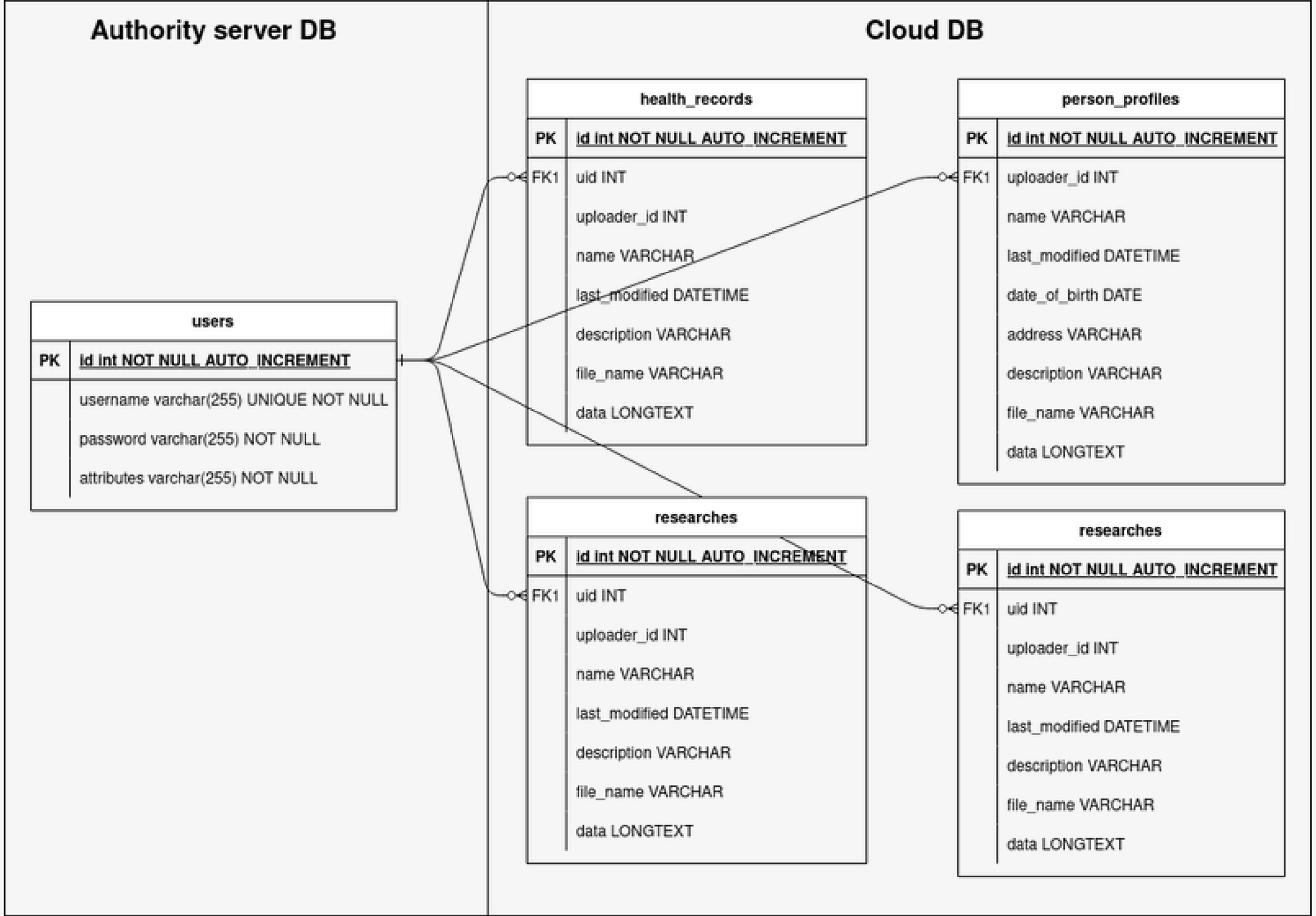
Permissions

- Read: Any user can download the data, but only those who have the right access policy can decrypt it.

- Write/Upload: Controlled by the ABAC Engine (PyCasbin) on the cloud web server. People are only allowed to write their data in specific categories.

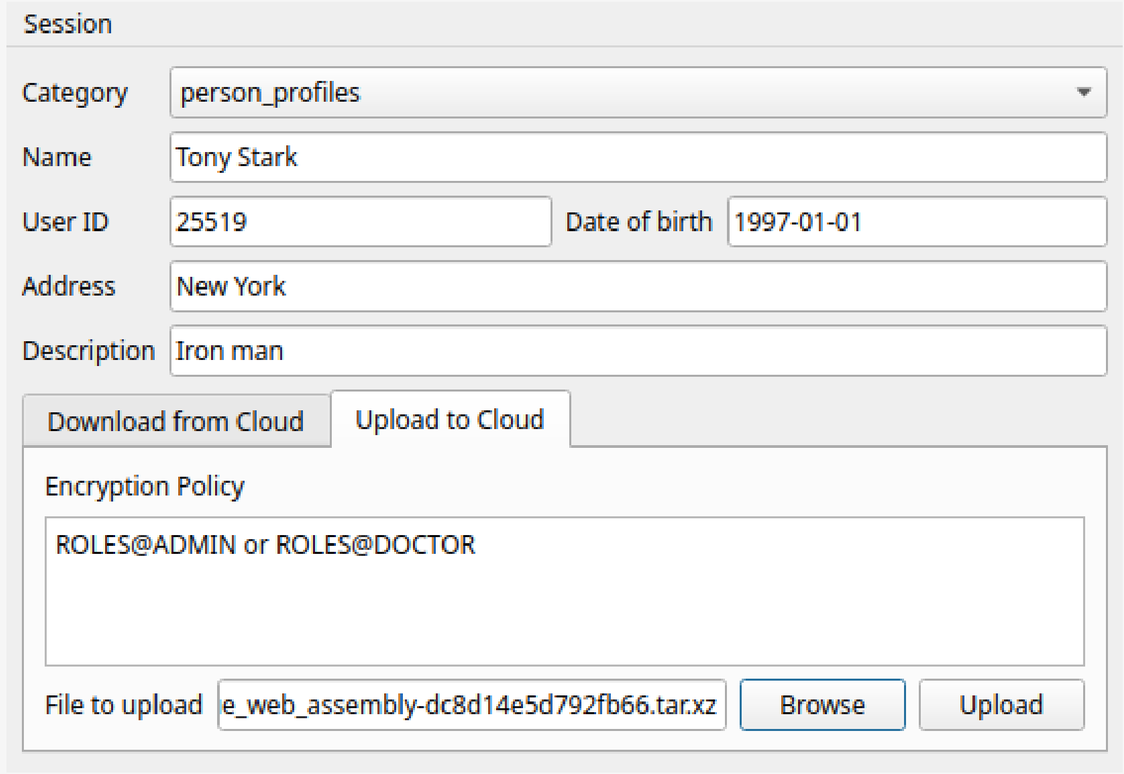
Database

- Stores some info about users (ID, uploader ID), and encrypted data (name, modified time).
- Encrypted data is encoded to base64 form


Authority server DB
Cloud DB
users
PK
id int NOT NULL AUTO_INCREMENT
username varchar(255) UNIQUE NOT NULL
password varchar(255) NOT NULL
attributes varchar(255) NOT NULL
health_records
PK
id int NOT NULL AUTO_INCREMENT
FK1
uid INT
uploader_id INT
name VARCHAR
last_modified DATETIME
description VARCHAR
file_name VARCHAR
data LONGTEXT
person_profiles
PK
id int NOT NULL AUTO_INCREMENT
FK1
uploader_id INT
name VARCHAR
last_modified DATETIME
date_of_birth DATE
address VARCHAR
description VARCHAR
file_name VARCHAR
data LONGTEXT
researches
PK
id int NOT NULL AUTO_INCREMENT
FK1
uid INT
uploader_id INT
name VARCHAR
last_modified DATETIME
description VARCHAR
file_name VARCHAR
data LONGTEXT
researches
PK
id int NOT NULL AUTO_INCREMENT
FK1
uid INT
uploader_id INT
name VARCHAR
last_modified DATETIME
description VARCHAR
file_name VARCHAR
data LONGTEXT

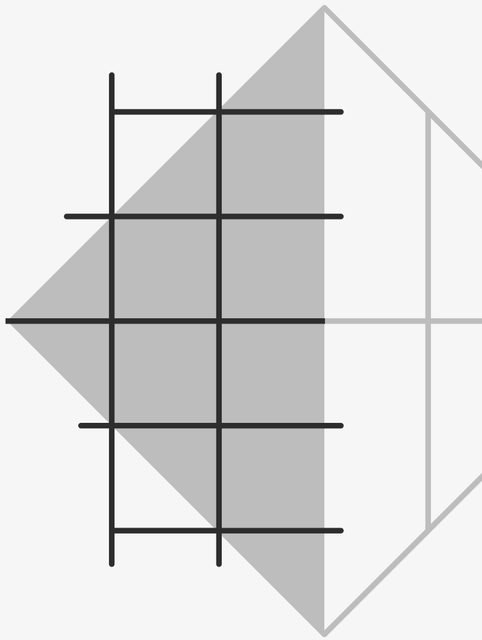
Client

- Login to AS and get the token, public key and private key
- Encrypt + upload data to cloud
- Download + decrypt data
- Searching data on cloud



Application context

- A healthcare organization that maintains (EHRs) for its patients
- Diverse set of users, including doctors, nurses, researchers, administrative staff, and patients, ...
- Requiring varying levels of access to the EHRs
- EHRs are storing on the third-party cloud storage



Test scenario

- Set up a test environment for the EHR system
- Create a sample dataset of patient records
- Tests the EHR system using dataset and analyze the results

Cloud Implementations Details

Programming Language	Python	
Isolated Environment	Docker	Phong + Huy
HTTP Server	Flask Gunicorn Nginx	Phong + Huy
JWT verification	OpenSSL PyJWT (Ed25519)	Phong
Secure Connection (HTTPS)	DuckDNS SSLForFree	Phong
Database	MariaDB	Huy
Cloud ABAC	PyCasbin	Huy + Phong

AS Implementations details

Programming Language	Python	
Isolated Environment	Docker	Huy + Phong
HTTP Server	Flask Gunicorn Nginx	Phong + Huy
JWT signing	JWT	Phong
Secure Connection (HTTPS)	DuckDNS + SSLForFree	Phong
Database	MariaDB	Huy

Client Implementations details

Programming Language	Python	
Data Encryption/Decryption	Charm-Crypto CP-ABE	Huy
Client application	Qt	Huy

Cloud System specifications

Cloud	Google Cloud Platform - VM
Operating System	Debian GNU/Linux 11 (bullseye)
CPU	Intel(R) Xeon(R) CPU @ 2.20GHz
Memory	8GB RAM
Storage:	20GB

AS System specifications

Operating System	Ubuntu 20.04.5 LTS (WSL2)
CPU	11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz 2.42 GHz
Memory	5GB RAM
Storage:	SSD 250GB

Client System specifications

Operating System	Arch Linux x86_64
CPU	AMD Ryzen 5 5600H 3.300GHz
Memory	16GB RAM
Storage:	SSD 500GB

References

[1] Bethencourt, J., Sahai, A., & Waters, B. (2007, May). Ciphertext-policy attribute-based encryption. In 2007 IEEE symposium on security and privacy (SP'07) (pp. 321-334). IEEE.

[2] Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2012). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE transactions on parallel and distributed systems, 24(1), 131-143.

[3] Alshehri, S., Radziszowski, S. P., & Raj, R. K. (2012, April). Secure access for healthcare data in the cloud using ciphertext-policy attribute-based encryption. In 2012 IEEE 28th international conference on data engineering workshops (pp. 143-146). IEEE.

[4] Yuan, E., & Tong, J. (2005, July). Attributed based access control (ABAC) for web services. In IEEE International Conference on Web Services (ICWS'05). IEEE.