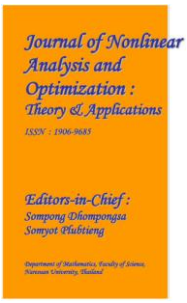
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1, No.15 : 2024
ISSN : **1906-9685**



HIDDEN CIPHERTEXT POLICY ATTRIBUTE-BASED WITH FAST DECRYPTION FOR PERSONAL HEALTH RECORD SYSTEM

V.Sarala [1], Ch Lalith Ganesh [2],

[1]**Assistant professor, MCA DEPT,** Dantuluri Narayana Raju College**, Bhimavaram, Andharapradesh**
Email: - vedalasarala21@gmail.com
[2]**PG Student of MCA, Dantuluri** Narayana Raju College**, Bhimavaram, Andharapradesh**
Email: - challalalithganesh@gmail.com

ABSTRACT

Since cloud computing has been playing an increasingly important role in real life, the privacy protection in many fields has been paid more and more attention, especially, in the field of personal health record (PHR). The traditional cipher text-policy attribute-based encryption (CP-ABE) provides the fine-grained access control policy for encrypted PHR data, but the access policy is also sent along with cipher text explicitly. However, the access policy will reveal the users' privacy, because it contains too much sensitive information of the legitimate data users. Hence, it is important to protect users' privacy by hiding access policies. In most of the previous schemes, although the access policy is hidden, they face two practical problems:

1) these schemes do not support large attribute universe, so their practicality in PHR is greatly limited and

2) the cost of decryption is especially high since the access policy is embedded in the cipher text. To address these problems, we construct a CP-ABE scheme with efficient decryption, where both the size of public parameters and the cost of decryption are constant. Moreover, we also show that the proposed scheme achieves full security in the standard model under static assumptions by using the dual system encryption method.

1 INTRODUCTION

What is Secure Computing?

Computer security (Also known as cyber security or IT Security) is information security as applied to computers and networks. The field covers all the processes and mechanisms by which computer-

based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters. Otherwise, in the computer industry, the term security -- or the phrase computer security -- refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

Diagram clearly explain the about the secure computing

2 RELEATED WORK

Generalized key delegation for wildcarded identity-based and inner-product encryption

AUTHORS: M. Abdalla, A. De Caro, and D. H. Phan

Inspired by the fact that many e-mail addresses correspond to groups of users, Abdalla introduced the notion of identity-based encryption with wildcards (WIBE), which allows a sender to simultaneously encrypt messages to a group of users matching a certain pattern, defined as a sequence of identity strings and wildcards. This notion was later generalized by Abdalla, Kiltz, and Neven, who considered more general delegation patterns during the key derivation process. Despite its many applications, current constructions have two significant limitations: 1) they are only known to be fully secure when the maximum hierarchy depth is a constant; and 2) they do not hide the pattern associated with the ciphertext. To overcome these, this paper offers two new constructions. First, we show how to convert a WIBE scheme of Abdalla into a (nonanonymous) WIBE scheme with generalized key delegation (WW-IBE) that is fully secure even for polynomially many levels. Then, to achieve anonymity, we initially consider hierarchical predicate encryption (HPE) schemes with more generalized forms of key delegation and use them to construct an anonymous WW-IBE

scheme. Finally, to instantiate the former, we modify the HPE scheme of Lewko to allow for more general key delegation patterns. Our proofs are in the standard model and use existing complexity assumptions.

3 IMPLEMENTATION STUDY

Existing System:

Since Attribute-Based Encryption was first proposed by Sahai and Waters [6], it has been seen as the most promising approach for fine-grained access control in the field of cloud computing. With the continuous improvements of ABE, currently, there are mainly two basic types of ABE schemes, Key Policy ABE (KP-ABE) [24], [26] and Cipher text Policy ABE (CP-ABE) [7], [10], [13]. In KP-ABE scheme, keys are associated with access structure and cipher texts are associated with a set of attributes. The first KP-ABE scheme was proposed by Wang and He [24]. But in this scheme, the trusted authority fully determines the combination of attributes associated with the cipher text, because the access control associated with the key are generated by the center for each legitimate decryption user. Then Sahai et al. proposed another KP-ABE scheme, in which the decryption keys of users' could express any access formulas over attributes, including non-monotone ones.

Disadvantages:

In the existing work, access control policy isn't sent along with cipher text explicitly, in other words, no unauthorized user can obtain useful information about the access structure. Some other schemes with the same performance have been proposed by other researchers, which are called Anonymous Attribute-Based Encryption.

The system is not secured due to lack of hidden policy, fast decryption.

PROPOSED SYSTEM & ALOGIRTHAM

Access structure: Each attribute in the proposed system contains two parts, attribute name index and its attribute value. And Each attribute has multiple candidate values. Every decrytor only knows the attribute name index of his own and his attribute value. Moreover, the values of the attributes in the access policy defined by the encryptor are hidden, and they are not sent with the cipher text. Only the access matrix and the defined function are sent to the decryptor along with the cipher text. What's more, the proposed scheme can handle any access control policy that can be expressed as a linear secret sharing scheme.

4.1 Advantages:

Hidden cipher text policy attribute-based encryption scheme provides a good way to solve the problem, where it achieves privacy protection by hiding access control policy.

The system is more secured due to HIDDEN CIPHERTEXT POLICY ATTRIBUTE-BASED ENCRYPTION.

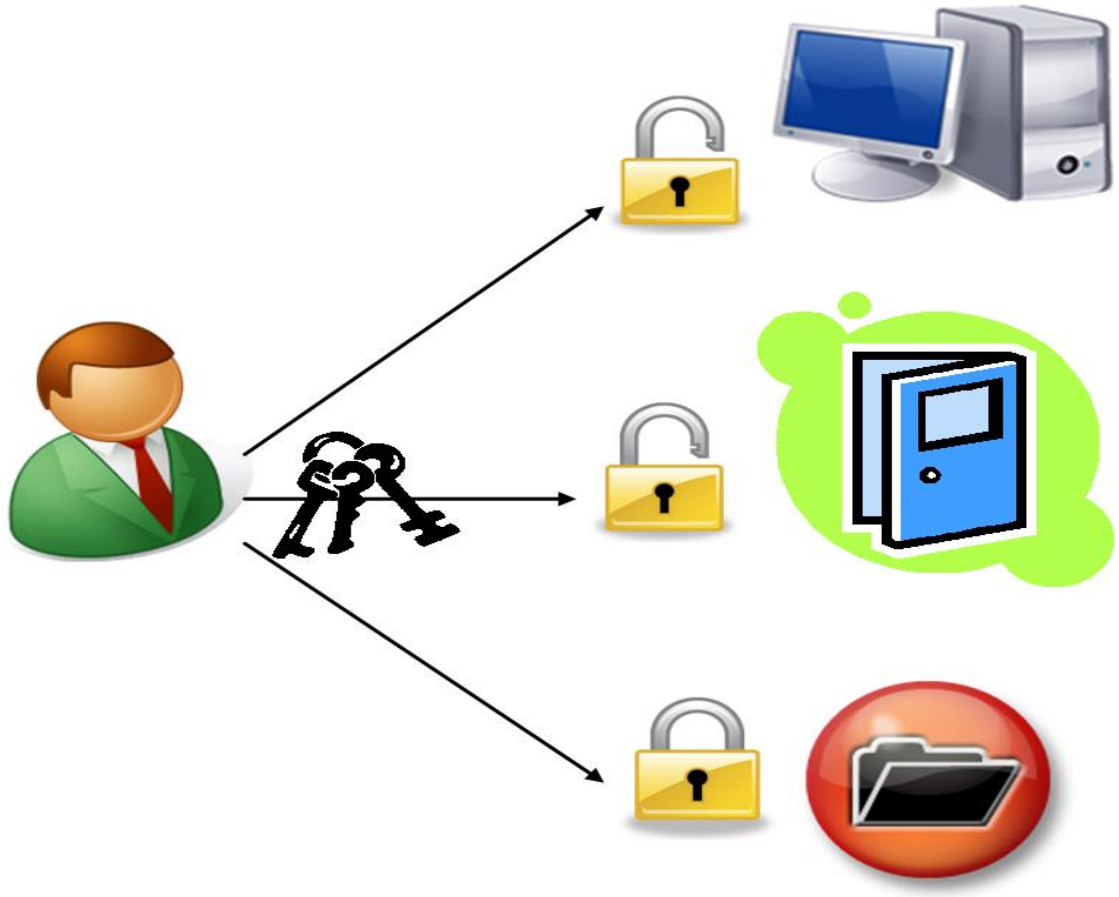


Fig1: SYSTEM ARCHITECTURE

4. IMPLEMENTATION

4.1 MODULES:

- Owner
- User
- Admin

MODULES DESCRIPTION:

Owner:

- Owner Will Sign up and Wait for the authorization (key) of admin.
- After Getting key Owner can login using the key, and upload any personal file by encrypting using ABE with wildcard characters on the cloud.
- Owner will check the progress status of the file upload by him/her.
- Owner logout the session.

User:

- ❖ User will register and wait for the authorization (key) of admin.
- ❖ User will login and access file using the same attribute for decrypt
- ❖ User view the file and download the file
- ❖ User logout the session.

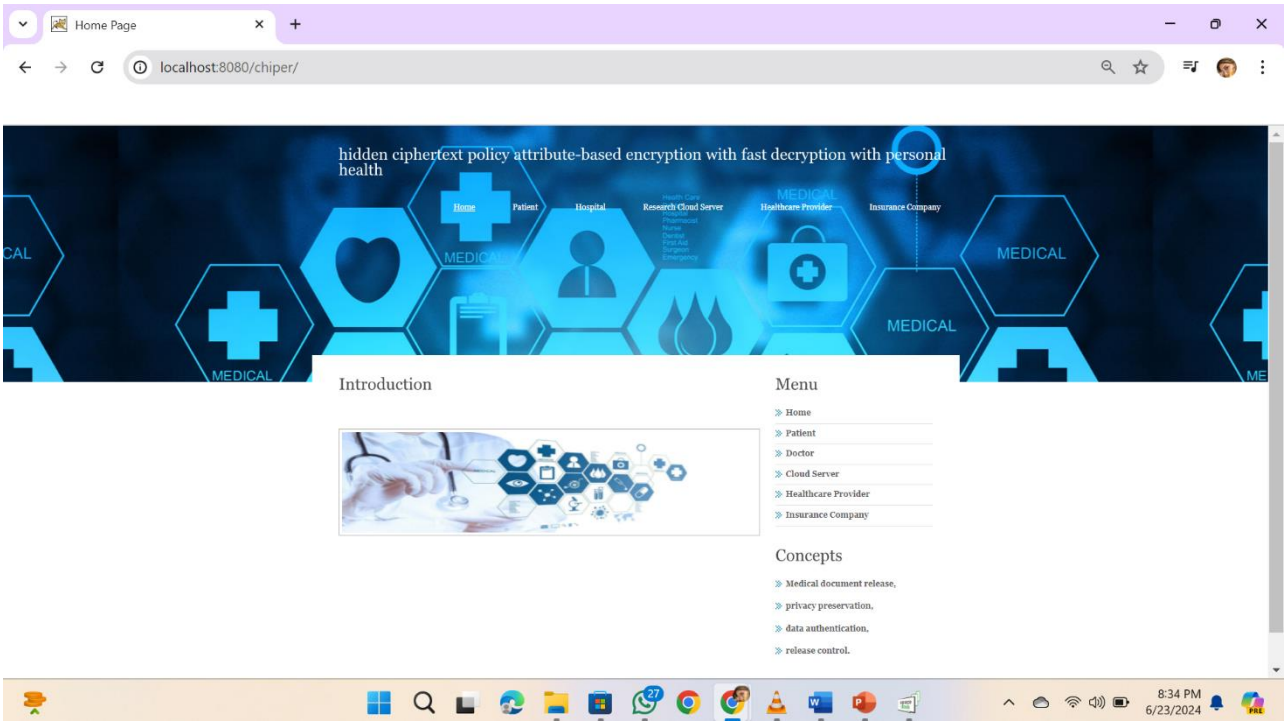
Admin:

- ❖ Admin Will Login on the admin's page.
- ❖ He/she will check the pending requests of any of the above person.
- ❖ Admin check the download/session history user for future referral
- ❖ Admin logout session

5 RESULTS AND DISCUSSION

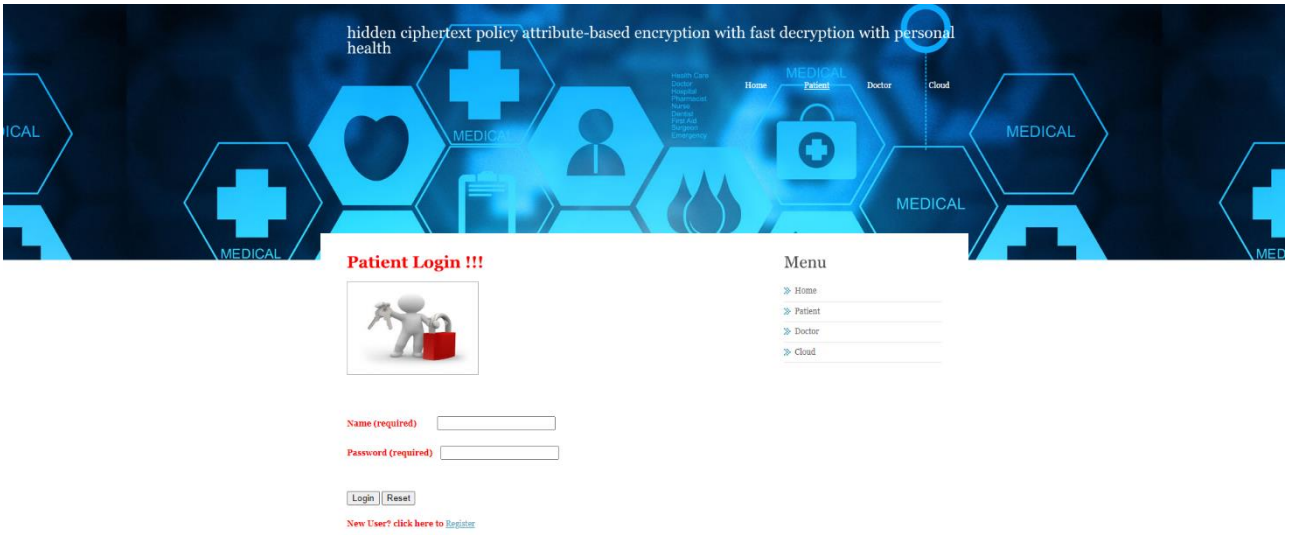
SCREEN SHORTS

HOME PAGE:



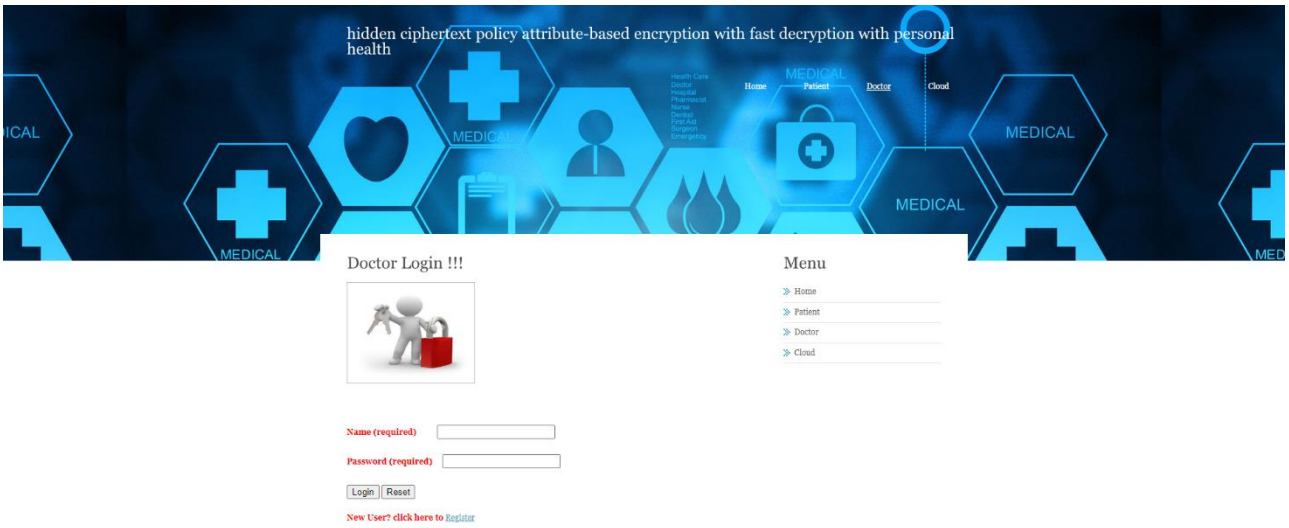
PATIENT REGISTERATION:

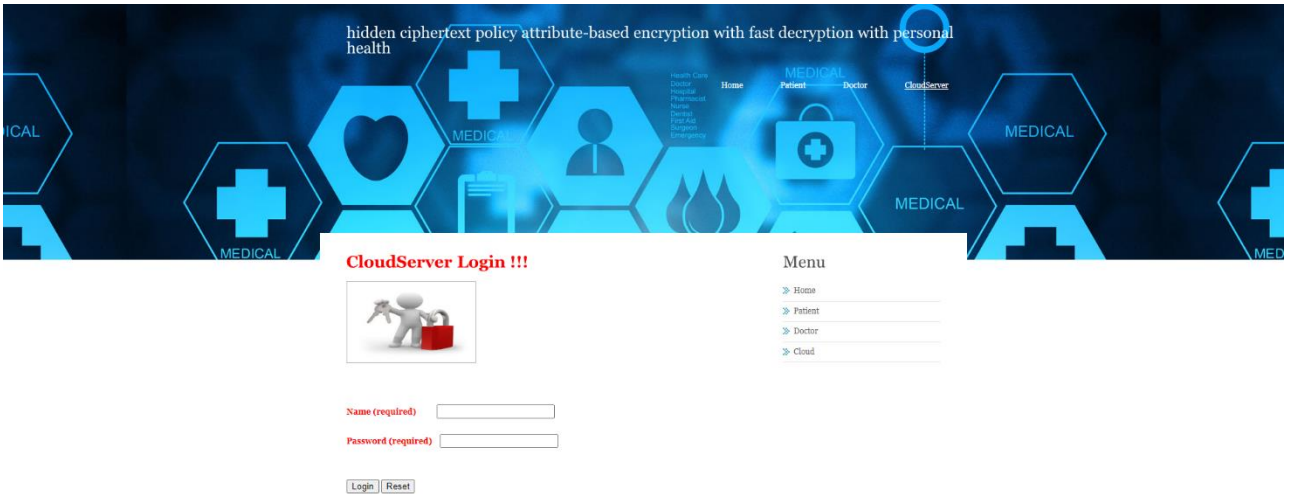
PATIENT LOGIN:



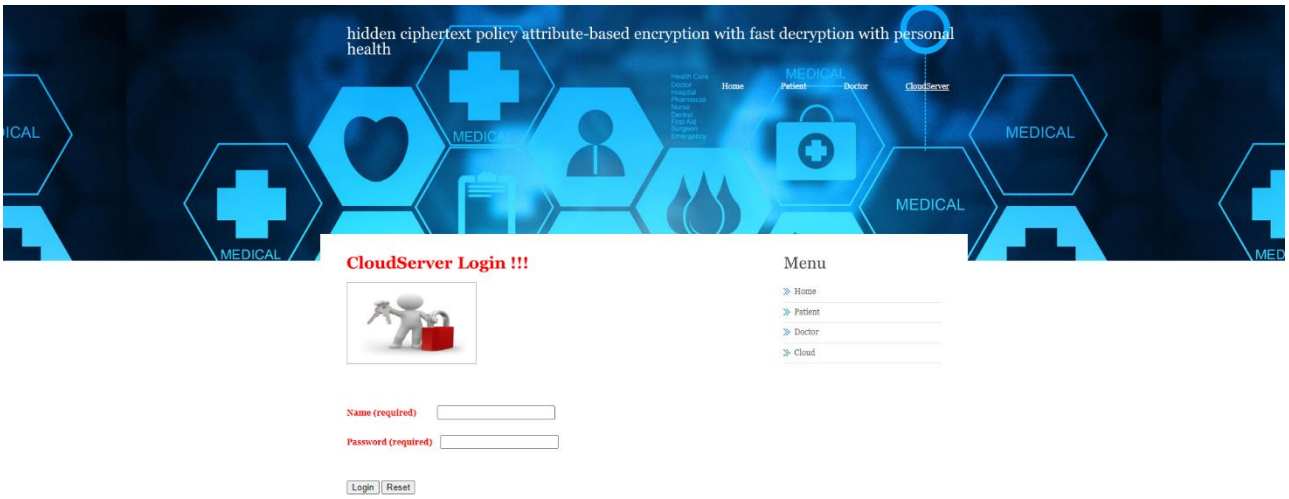
DOCTOR REGISTRATION:

DOCTOR LOGIN:

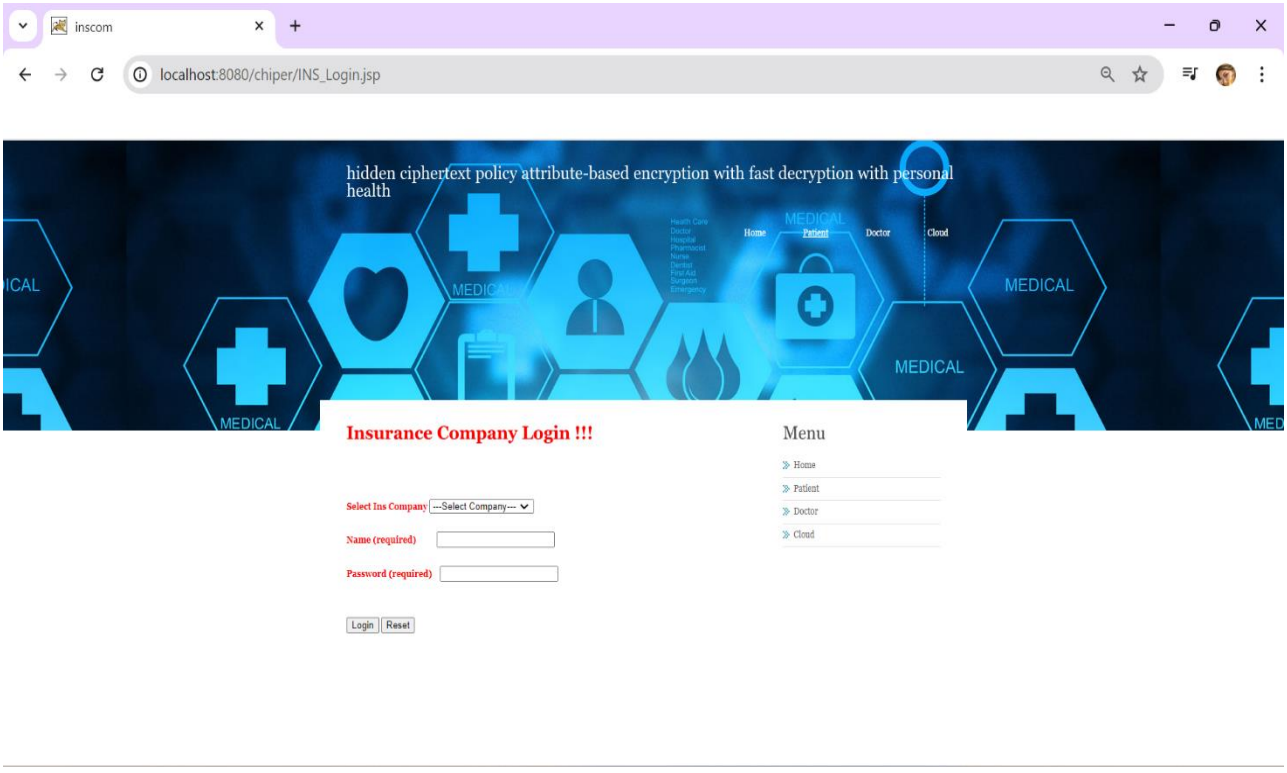




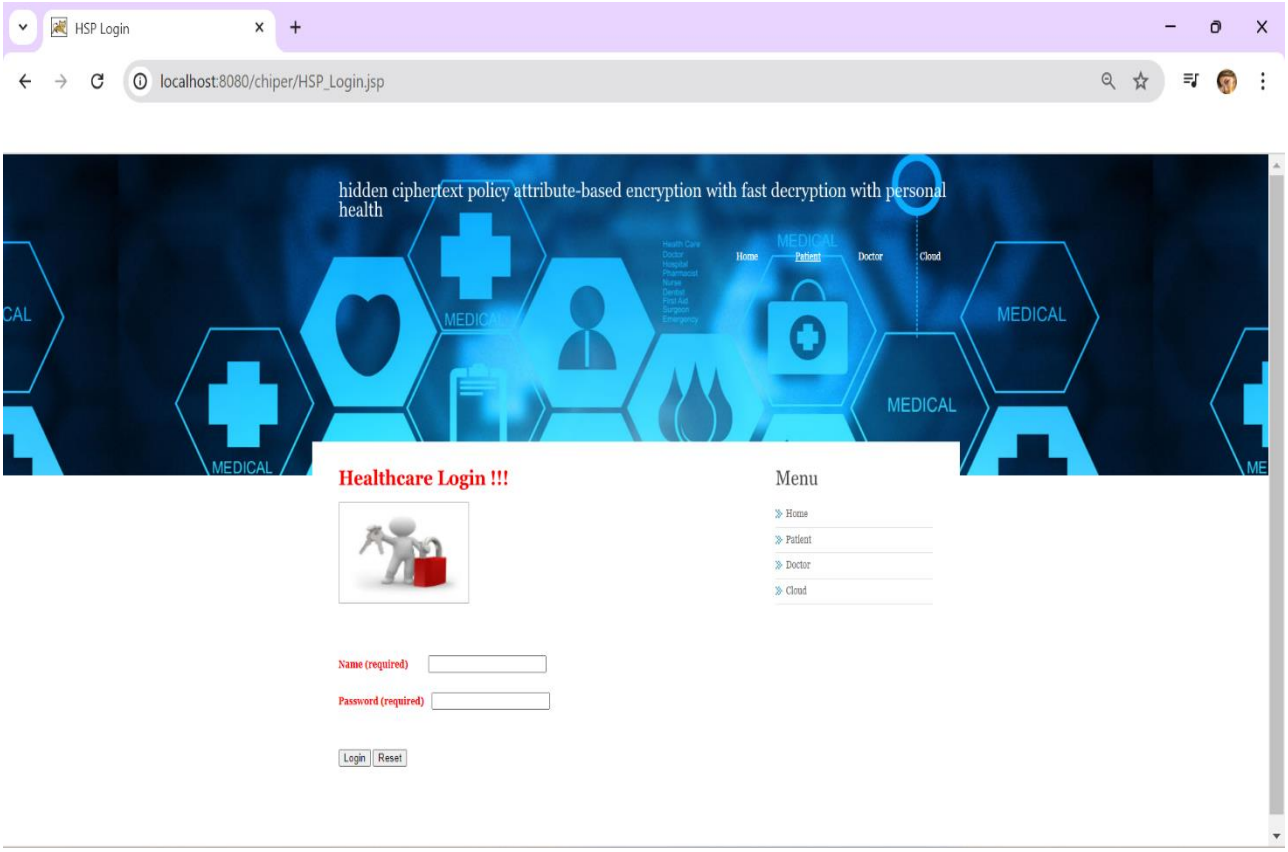
CLOUDSERVER LOGIN:



INSURANCE COMPANY LOGIN:



HEALTHCARE LOGIN:



6. CONCLUSION

CONCLUSION

In this paper, we presented two new constructions of Ciphertext Policy Attribute Based Encryption for the AND-Gate with wildcard access policy. Our first scheme achieves constant ciphertext size, but cannot hide the access policy. On the other hand, our second scheme can even hide the access policy against the legitimate decryptors. We proved that our second construction is secure under the Decisional Bilinear Diffie-Hellman and the Decision Linear assumptions. One shortcoming of our second construction is that its ciphertext size is no longer constant, then proving this construction in fully secure.We leave the solution for this problem as our future work.

7. REFRENCES

1. **1** M. Abdalla, A. De Caro, and D. H. Phan, “Generalized key delegation for wild carded identity-based and inner-product encryption,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 6, pp. 1695–1706, Dec. 2012.

2. N. Attrapadung, B. Libert, and E. de Panafieu, “Expressive key-policy attribute-based encryption with constant-size ciphertexts,” in Public Key Cryptography (Lecture Notes in Computer Science), vol. 6571. Berlin, Germany: Springer-Verlag, 2011, pp. 90–108.
3. J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attributebased encryption,” in Proc. IEEE Symp. Secur. Privacy (SP), May 2007, pp. 321–334.
4. D. Boneh and M. K. Franklin, “Identity-based encryption from the Weil pairing,” in Proc. 21st Annu. Int. CRYPTO, 2001, pp. 213–229.
5. C. Chen et al., “Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures,” in Topics in Cryptology (Lecture Notes in Computer Science), vol. 7779, E. Dawson, Ed. Berlin, Germany: Springer-Verlag, 2013, pp. 50–67.
6. C. Chen, Z. Zhang, and D. Feng, “Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost,” in Proc. 5th Int. Conf. Provable Secur. (ProvSec), 2011, pp. 84–101.
7. L. Cheung and C. Newport, “Provably secure ciphertext policy ABE,” in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2007, pp. 456–465.
8. N. Doshi and D. Jinwala, “Hidden access structure ciphertext policy attribute based encryption with constant length ciphertext,” in Proc. Int. Conf. Adv. Comput., Netw. Secur., 2012, pp. 515–523.
9. K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, “A ciphertext-policy attribute-based encryption scheme with constant ciphertext length,” in Proc. 5th Int. Conf. ISPEC, 2009, pp. 13–23.
10. A. Ge, R. Zhang, C. Chen, C. Ma, and Z. Zhang, “Threshold ciphertext policy attribute-based encryption with constant size ciphertexts,” in Proc. 17th Austral. Conf. Inf. Secur. Privacy, 2012, pp. 336–349.
11. V. Goyal, A. Jain, O. Pandey, and A. Sahai, “Bounded ciphertext policy attribute based encryption,” in Proc. 35th Int. Colloq. Auto., Lang. Program. (ICALP), 2008, pp. 579–591.