Indian Journal of Science and Technology, Vol 8(35), DOI: 10.17485/ijst/2015/v8i35/82743, December 2015
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

An Innovative Proposal for Secure Cloud Authentication using Encrypted Biometric Authentication Scheme

S. Kavin Hari Hara Sudhan[1]* and S. Saravana Kumar[2]

[1]Information Technology, St. Peter's University, Chennai – 600054, Tamil Nadu, India; kavinmtech@gmail.com
[2]Department of Computer Science Engineering, SVEC, Tirupati – 517102, Andra Pradesh, India; saravanakumars81@gmail.com

Abstract

Background/Objectives: Cloud computing has been emerging technology in recent years. But security is the main concern for the user not to accepting the cloud computing systems. Among them lack of trust and multi tenancy are the major issues, altogether comes under authentication problem **Methods/Statistical Analysis:** These problems are mainly in third party management model and self managed models as well. In order to overcome such tribulations Biometric is the major concern. Even in biometric research group is very much concentrating on security of biometric templates. For the security of biometric template, The two encryption algorithms such as AES, RSA have been imposed on templates. **Findings:** The biometric template will be safe in transit and storage as well in both cloud consumer and cloud provider side to improve the reliability of cloud. **Applications/Improvements:** If such approach has been adopted then confidence regarding the usage of cloud will be greater than before.

Keywords: Authentication, Biometric, Cloud, Encryption, Privacy, Security

1. Introduction

Cloud computing is the method of delivering applications and computing resources over the internet. It provides services to the customer in following types like SAAS, PAAS and IAAS[1,2].

Cloud computing has four types of deployment models such as public cloud, private cloud and hybrid, community cloud[3]. If the customer wants to use the cloud environment then he should trust the cloud that his own data belongings will be safe enough while computation, storage and transportation[4].

As such cloud consumers may have faith in cloud providers but not the intruders. If the user wants to protect his valuable information then perfect authentication mechanism is must[5,6]. Whatever may be the authentication there will be loop line to compromise. Since cloud is having highly confidential information it has to be protected to the core. Much more security related issues arise only because of lag in authentication[7]. The improved and secure authentication scheme will resolve almost all security problems.

So biometric is the best choice of authentication[8]. Even though Biometric is the secure authentication scheme but the biometric templates are not that much secure[9]. In our proposed model we developed a mechanism for highly secure biometric template by means of dual encryption in both user side as well as cloud server side. End to end safety ensures better security to the template in storage and transit.

2. Existing Work

With reference to NIST cloud architecture and cloud security architecture the major issues which affects the reliability of cloud will be because of the lag in better authentication methodology[10].

The notorious nine, the article published by Cloud Security Alliance(CSA)[11], which talks about issues and problems related to the adoption of cloud computing. The

*Author for correspondence

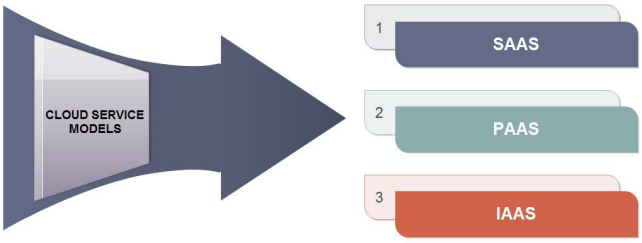

Figure 1. Cloud service model.

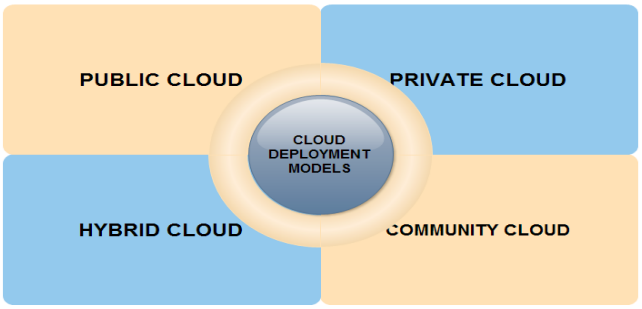

Figure 2. Cloud deployment model.

major problems discussed in notorious nine are related to authentication and authorization. If we have great authentication and authorization schemes then all related problems can be rejected[12].

There are much more proposal are there related to cloud computing and authentication towards cloud environment[13]. But biometric authentication is the scheme with high security and reliability. Even biometric authentication is also there for better security in cloud environment. But template protection by means of dual encryption is not available since.

Every country in the world is moving towards biometric personal identification systems. At the same time people are put in great threat of template safety[14]. Even Israel and British biometric database have been stolen by the clandestine users[15,16]. In order to protect the templates used in biometric authentication systems we are proposing dual encryption method that will be helpful in protecting cloud environment in the mode of authentication[17,18].

3. Proposed Model

The problem that affects the trust goodness of adopting cloud is authentication. This problem can be minimized to the core by means of implementing the following method protocol. In such method we are incorporating two encryption algorithms for the safety of biometric template used in biometric samples for authentication.

The overall authentication mechanism has been subdivided into two major subdivisions

- The user is first using the cloud (registration).
- The user keep on logging in for the further usage (log in).

At first during registration the biometric sample is given from the consumer side that is going to be encrypted by public key which is received from the authentication server [Epub (temp)].

Then [Epub (temp)] is forwarded to the server side, where it is decrypted by the private key of its own (Dpr1 [temp])[19]. Then the decrypted template is once again encrypted by the servers private key and stored in the database along with user name and password for further usage (Epr2 [temp]).

Where,
temp = Biometric template,
Epub = Encryption using public key of authentication server,
Dpr1 = Decryption using private key of authentication server,
Epr2 = AES encryption using private key of server.

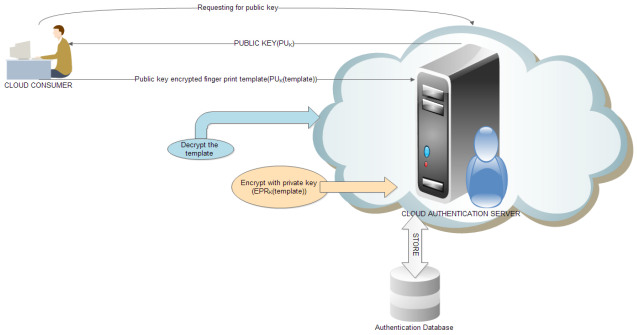

Figure 3. Registration Phase.

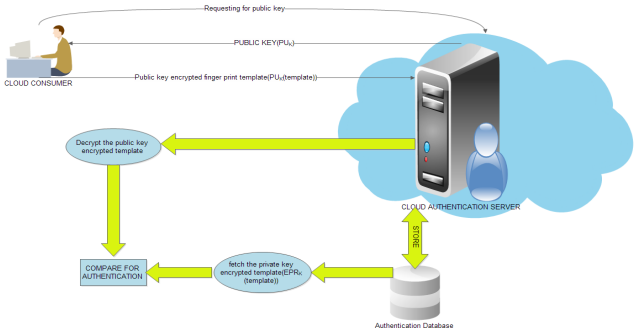

Figure 4. Log in phase.

While login after the first registration the same principle is followed that is, from consumer side biometric template is given as input then it is encrypted by using public key of server [Epub (temp)] it should be forwarded to the server side then it will be decrypted by the private key of cloud authentication server[Dpr1 (temp)].

In this stage two cases are possible that is there will be a dilemma between security as well as accuracy. If we want high security than accuracy that is false rejection rate will be slightly high. But no one will be ready compromise with security.

Then the comparison of template will be the done only in the decrypted format. Since every time different types of randomized public and private keys have been generated so that based on avalanche effect a small change in the plain text as well as key will create drastic change in the cipher text.

Two different algorithms have been used in our system, for asymmetric key encryption and decryption RSA is used and for symmetric key encryption AES algorithm is being used.

4. Proposed Protocol

Enrollment phase (when the first time during registration)

- Collect biometric sample from user in client side.
- Extract features from sample as template.
- Get public key from cloud authentication server.
- Encrypt the template using public key.
- Forward the encrypted biometric to server side.
- Decrypt the template using private key in server end.
- Once again encrypt the template using symmetric encryption scheme.
- Store the encrypted template in the cloud authentication database.

Login phase (Each time during login)

- Collect biometric sample from user in client side.
- Extract features from sample as template.
- Get public key from cloud authentication server.
- Encrypt the template using public key.
- Forward the encrypted biometric to server side.
- Decrypt the template using private key in server end.
- Collect the symmetric encrypted template from the cloud database.
- Perform decryption using symmetric encryption algorithm.
- Do the comparison with the plain biometric samples.

5. Algorithms used

- Minutiae extraction algorithm[20].
- RSA Algorithm[21].
- AES[22].

5.1 Minutiae Extraction Algorithm

Step 1: In Client end collect multiple samples of biometric of User.
Step 2: Feature vector Xi is computed from the given sample.
Step 3: Find the central core of the finger print.
Step 4: Find the x and y coordinate values of each feature vector.
Step 5: The distance from each feature vector value from core has been calculated.
Step 6: (x,y) and distance D is combinely called as minutiae.

5.2 RSA Algorithm

5.2.1. Key Generation

Step 1: Choose two prime no's p & q
Step 2: Calculate n = pq
Step 3: Calculate m = (p-1)(q-1)
Step 4: Choose any number e<m specified that it is co-prime to m, i.e gcd(e,m) = 1
Step 5: Calculate d such way that de mod m = 1, i.e. d = e^{-1} mod m
Step 6: The public key is {e,n) The private key is {d,n}

Figure 5. Finger print image with its features.

5.2.2 Encryption

Plaintext = M, M<n
Ciphertext = C
$C = M^e \bmod n$

5.2.3 Decryption

Ciphertext = C
Plaintext = M
$M = C^d \bmod n$

5.3 Advanced Encryption Standard (AES)

AES relies on a design principle referred to as a substitution-permutation network, combination of each substitution and permutation, and is quick in each software system and hardware. In contrast to its forerunner DES, AES doesn't use a Feistel network. AES could be a variant of Rijndael that includes a fixedblock size of 128 bits, and a key size of 128, 192, or 256 bits. Against this, the Rijndael specification as such is nominal with block and key sizes which will be any multiple of 32 bits, each with a minimum of 128 and a most of 256 bits.

AES operates on a 4×4 column-major order matrix of bytes, termed the state, though some versions of Rijndael have a bigger block size and have extra columns within the state. Most AES calculations are exhausted a special finite field.

The key size used for an AES cipher specifies the amount of repetitions of transformation rounds that convert the input, referred to as the plaintext, into the ultimate output, known as the ciphertext. The amount of cycles of repetition are as follows:

- 10 rounds for 128-bit keys.
- 12 rounds for 192-bit keys.
- 14 rounds for 256-bit keys.

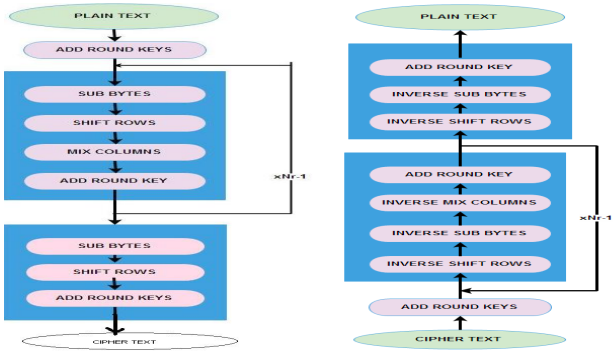

Figure 6. AES Encryption and Decryption.

Each round consists of many process steps, each containing four similar however completely different stages, together with one that depends on the cryptography key itself. A collection of reverse rounds are applied to remodel cipher text back to the initial plaintext using identical encoding key.

6. Conclusion

The methods used in the proposal for the authentication in cloud is the novel idea for better and enhanced security of the cloud consumers valuable information. In each and every level security has been maintained to the core. This will be the ultimate method for enhanced authentication system in cloud environment. Two types of encryption in two ends of authentication will increase the security of biometric template and that will be very much useful in providing secure authentication .In our proposal we have used finger print has biometric sample but in future it can be extended to some other biometrics also.

7. Future Work

The proposed protocol for authentication will increase the reliability of the adoption of cloud computing to our computing environment. In future we are going to do the implementation of the same above said model for better authentication which improves the security, which improves the trust among the cloud environment. And then instead of finger print as biometric sample we can try some other biometrics like iris, face etc.

8. References

1. Kadam Y. Security Issues in Cloud Computing A Transparent View. International Journal of Computer Science Emerging Technology. 2011; 316–22.
2. Vouk MA. Cloud Computing – Issues, Research and Implementations. Journal of Computing and Information Technology. 2008; 235–46.
3. Cloud computing. 2013. Available from: http://en.wikipedia.org/cloud_computing
4. Catteddu D, Hogben G. Cloud Computing:- Benefits, risks and recommendations for information security. Web Application Security. 2009; 7–17.
5. Sabahi F. Cloud Computing Security Threats and Responses. 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN).

6. Choi1 JH, Lee SH, Kim MK. Integrated user authentication method using BAC (Brokerage Authentication Center) in Multi-clouds. Indian Journal of Science and Technology. 2015; 8(25):1–7.
7. Lee S, Ong I, Lim HT, Lee HJ. Two factor authentication for Cloud computing. International Journal of KIMICS. 2010; 427–32.
8. Jain AK, Ross A, Prabhakar S. An introduction to biometric recognition. IEEE Trans Circuits Systems. Video Technology. 2004; 4–20.
9. Ratha NK, Connell JH, Bolle RM. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal. 2001; 614–34.
10. NIST SP 500-292. Cloud Computing Reference Architecture: An Overview. National Institute of Standards and Technology. 2011; 3–4.
11. CSA Top threats working group. The notorious nine-2013. CSA(cloud security alliance). 2013; 8–21.
12. Lee JY. A study on the use of secure data in cloud storage for collaboration. Indian Journal of Science and Technology. 2015; 33–6.
13. Gorman LO, Labs A, Ridge B. Comparing Passwords, Tokens, and Biometrics for User Authentication. Proceedings of the IEEE. 2003; 21–40.
14. Jain AK, Nandakumar K, Nagar A. Biometric template security. EURASIP Journal of Advances in Signal Processing. 2008; 1–17.
15. Israeli biometric data hacked. 2013. Available from: http://www.natlawreview.com/article/israeli-biometric-data-hacked
16. British biometric passport hacked. 2013. Available from: http://www.theinquirer.net/inquirer/news/1009515/british-biometricpassport-
17. Upmanyu M, Namboodiri AM, Srinanthan K, Jawahar CV. Blind authentication: A secure crypto biometric verification protocol. IEEE Transactions on Information Forensics and Security. 2010; 255.
18. Rajanbabu DT, Raj C. Multilevel encryption and decryption tool for secure administrator login over the network. Indian Journal of Science and Technology. 2014; 8–14.
19. Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM. 1978; 120–6.
20. Kavinhariharasudhan S et al. Double encryption based secure biometric authentication system. International Journal of Engineering Trends and Technology. 2012; 64–70.
21. RSA Algorithm. 2013. Available from: https://simple.wikipedia.org/wiki/RSA_(algorithm)
22. AES. 2013. Available from: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard