Volume 3, Issue 4, April 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Multiple Biometric Security in Cloud Computing

D.Pugazhenthi,
PG and Research Department of Computer Science,
Quaid-E-Millath College for Women, Chennai, India

B.Sree Vidya,
Research Scholar,
Bharathiyar University, Coimbatore, India

Abstract: Cloud computing is one of the emerging technologies, that takes network users to the next level. Cloud is a technology where resources are paid per usage rather than owned. One of the biggest challenges in this technology is Security. Though users use service provider's resources, there is a great level of reluctance from users' end because of significant security threats packed with this technology. Research in this core has provided a number of solutions to overcome these security barriers; each of these has its own pros and cons. This paper brings about a new model of a security system where in users are to provide multiple biometric finger prints during Enrollment for a service. These templates are stored at the cloud provider's end. The users are authenticated based on these finger print templates which have to be provided in the order of random numbers that are generated every time. Both finger prints templates and images provided every time are encrypted for enhanced security.

Key Words: cloud computing- biometrics- security- Finger prints – templates- encryption

I. INTRODUCTION

Cloud computing refers to an on-demand, self-service Internet infrastructure that enables users to access computing resources from anywhere and anytime. The services offered by a cloud can be categorized into Software as a Service, Platform as a Service, Infrastructure as a Service, and Storage as a Service and so on. Deployment of a cloud falls into three kinds, viz. public, private and community cloud. In a public cloud, resources are open to the general public over the Internet. A private cloud infrastructure is operated for a single organization. When the resources are shared among organizations with common concerns, then it becomes a community cloud. [1]. Multitenancy, massive scalability, elasticity are the basic characteristics of a cloud technology [2]. Cloud computations are operational on unfixed nodes in a network, leading to data loss and privacy issues. In this paper, a new security model has been proposed that uses multiple finger prints combined with encryption and random numbers as authentication tools.

II. Biometrics As Authentication Tool

Biometrics refers to the use of unique physiological characteristics to identify an individual. A number of biometric traits have been developed and are used to authenticate the person's identity. The idea is to use the special characteristics of a person to identify an individual.

Fig. 1 Sample Finger Print Impression

1. Finger Prints and other traits:

Biometric authentication uses human traits like finger prints, tongue impressions, iris and face recognitions that are unique to each individual and thus differentiating users. Combining biometric techniques and cloud computing for the purpose of a secure cloud computation has never been a new technology. Since the operations are carried out beyond trusted boundaries, cloud is more vulnerable to hacking and security breaches. When using biometrics as an authentication tool, a cloud user, during Enrollment for a service, registers with his unique traits (finger prints, tongue, face, iris etc.). These get stored as templates at the cloud service provider's end. Every time when an access is made, the

cloud user is prompted to provide his enrolled trait that is compared against the template and authenticated accordingly. Though these biometric traits are unique, problems arise when eavesdroppers gain access to these stored finger print templates.

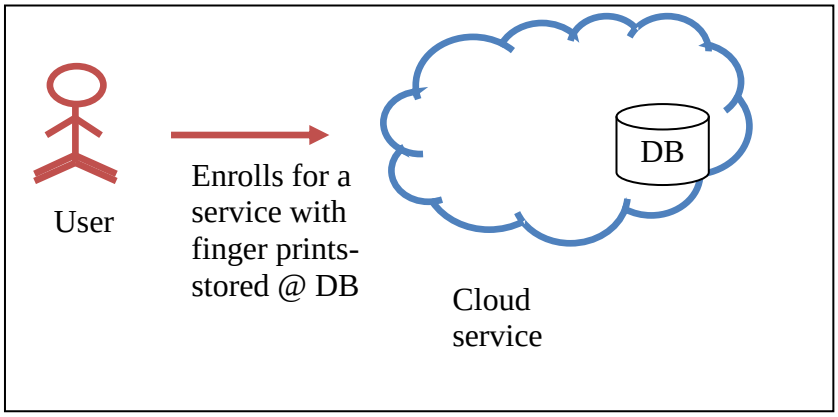

Fig.-2. User registering his biometric traits with the cloud service provider

2.2 Image Encryption

Encryption is the conversion of data into a form that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. For enhanced security, the biometric images from both user's end and service provider's end can be encrypted. By doing so, even if a hacker gains access to an image, he may not be able to decrypt it back to the original image, provided, the underlying encryption algorithm is very complex to decrypt. There are number of encryption algorithms that are used for the finger print images. One such algorithm is Elliptic encryption algorithm that is adopted in this paper.

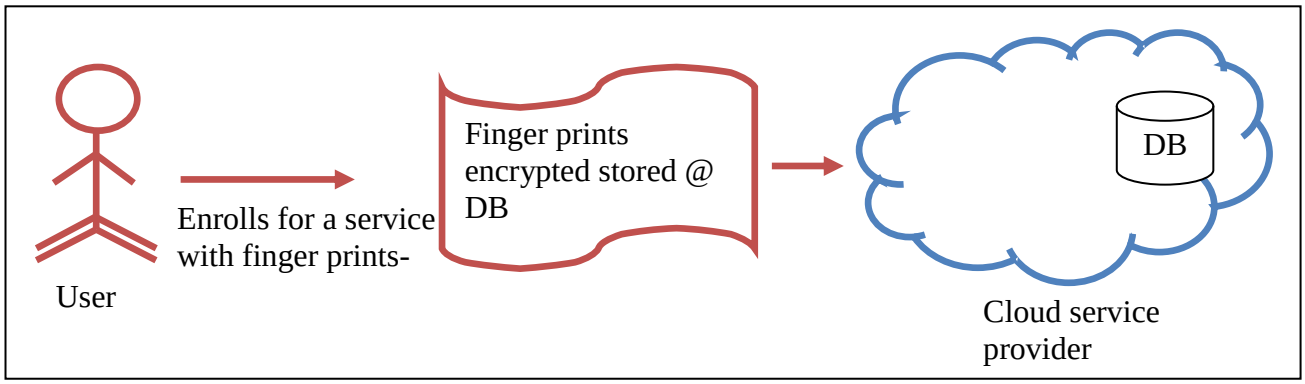

Fig.-3. Biometric traits are encrypted from user end and stored at the cloud.

III Security Issues In Cloud

A general approach in a biometric system is to store all captured biometric images in the Enrollment phase, and authentication is done using a matching process. This technique, undoubtedly suffers from security weaknesses [3]. Vulnerable storage may lead to an attacker stealing biometric templates and impersonating the legitimate user. The stolen biometric information may compromise other systems [4]. A cloud private matching algorithm is proposed in [5]. Two encrypted images are compared under double encrypted conditions, from the client and from cloud storage.

Several techniques have been proposed for biometric template protection. Among them, cancellable biometrics [6] is one such method. It satisfies a double goal: (a) unrecoverability of the original biometric data from the stored biometric template and (b) issue of a new biometric template when an existing template is compromised.

IV Proposed Schema

Multi finger security model is a technique where users, during registration can register with three finger templates of their choice and assign a single digit number for each of these three fingers. These recorded images are encrypted using Elliptical algorithm and stored at the service provider's end. The encryption algorithm is applied at three levels, viz.

- Finger print images
- Three single digit numbers
- Mapping of these number to the images

The new model can be evaluated at three phases namely

1. Enrollment phase
2. Access phase

3. Matching phase

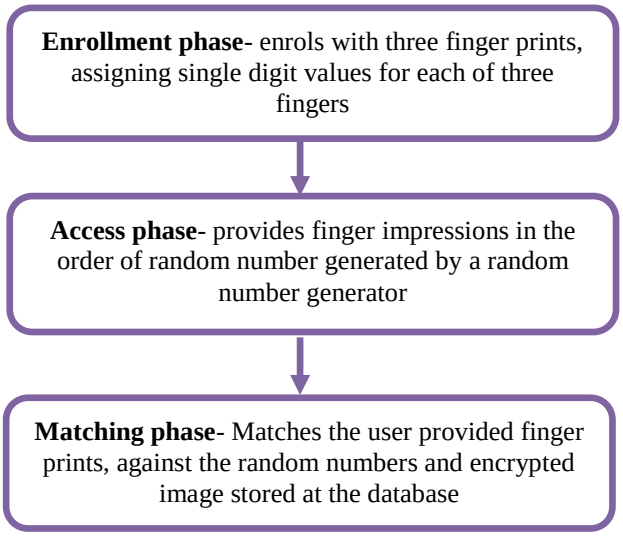

Fig.-4. Working model of the proposed schema

4.1 Enrollment phase:

When a user enrols for a service, he registers with three finger traits of his choice. The user then assigns three single digit numbers of his choice. All the three inputs, finger print images, three single digit numbers and mapping of numbers to fingers are all encrypted and stored at the service provider's end.

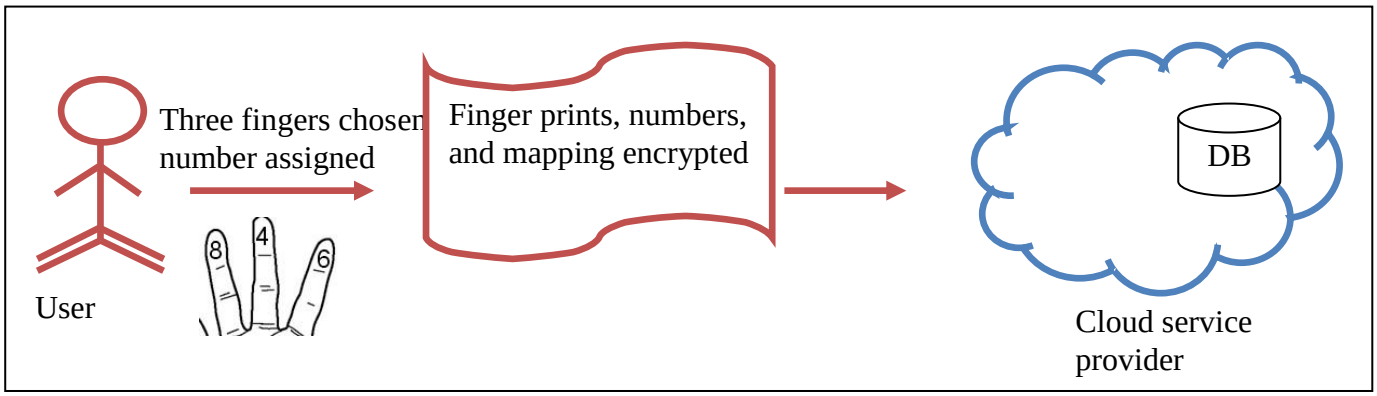

Fig.-5.Enrollment phase- user provides three finger prints assigning numbers to each

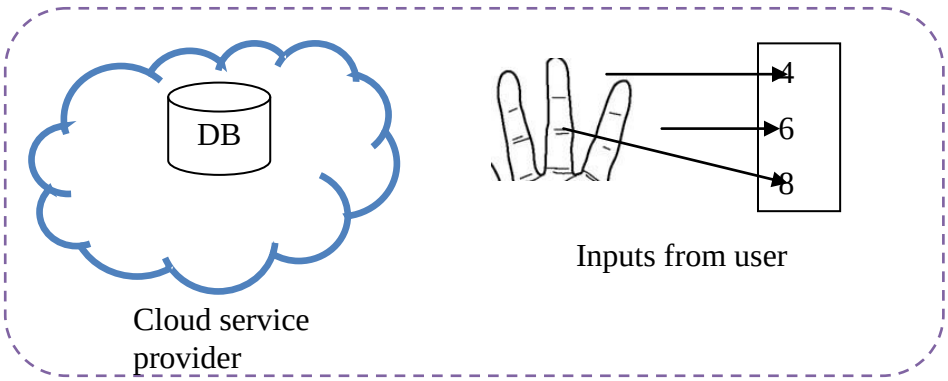

Fig.-6.Inputs given by the user stored at the cloud

4.2.1 Encrypting Biometric traits and user inputs:

Though security is provided by means of using three different inputs from the user, it can be made more efficient by using an encryption algorithm for the three inputs. The different algorithms adopted here are

- Elliptic curve algorithm for biometric images
- RSA algorithm for numbers and mappings

ELLIPTIC CURVE ALGORITHM

Elliptic Curve Cryptography (ECC) is the algorithm that is used for encrypting the biometric traits. Elliptic encryption is as follows [5].
Step1: User selects an Elliptic curve Ep(a,b), y2=x3+ax+b (modp), and get a point on the Elliptic curve as point G.
Step2: User selects a private key k, and generates public key K=KG
Step3: User sends Ep(a,b) and point K,G to B
Step4: When cloud receives the information, it will be encoded to be transmitted to the point M on Ep(a,b), and generates a random integer r(r<n)
Step5: Cloud calculates points C1= M+ rK; C2=r.
Step6: Cloud passes C1, C2 to User
Step7: After receiving the information, User calculates C1-kC2; the result is the point M. Because
C1-kC2=M+rrKk(rG)=M+rK-r(rkG)=M, then point M can be explicitly decoded.

RSA ALGORITHM
Three digit chosen numbers are encrypted using RSA algorithm. The RSA algorithm is as follows:

1. Key Generation
Step1: Choose two distinct prime numbers p and q.
Step2: Find n such that n = pq.
n will be used as the modulus for both the public and private keys.
Step3: Find the totient of n, $\phi(n)$
$\phi(n)=(p-1)(q-1)$.
Step4: Choose an e such that $1 < e < \phi(n)$, and such that e and $\phi(n)$ share no divisors other than 1 (e and $\phi(n)$ are relatively prime).
e is kept as the public key exponent.
Step5: Determine d (using modular arithmetic) which satisfies the congruence relation
$de \equiv 1 \pmod{\phi(n)}$.
In other words, pick d such that de - 1 can be evenly divided by (p-1)(q-1), the totient, or $\phi(n)$. This is often computed using the Extended Euclidean Algorithm, since e and $\phi(n)$ are relatively prime and d is to be the modular multiplicative inverse of e.
d is kept as the private key exponent.
The public key has modulus n and the public (or encryption) exponent e. The private key has modulus n and the private (or decryption) exponent d, which is kept secret.

2. Encryption
Step1: User transmits his/her public key (modulus n and exponent e) to Cloud, keeping his private key secret.
Step2: When Cloud sends a number "M" to user, it first converts M to an integer such that $0 < m < n$ by using agreed upon reversible protocol known as a padding scheme.
Step3: Cloud computes, with User's public key information, the ciphertext c corresponding to $c \equiv m^e \pmod{n}$.
Step4: Cloud now sends message "M" in ciphertext, or c, to user.

3. Decryption
Step1: User recovers m from c by using his private key exponent, d, by the computation
$m \equiv c^d \pmod{n}$.
Step2: Given m, User can recover the original message "M" by reversing the padding scheme. This procedure works since
$c \equiv m^e \pmod{n}$,
$c^d \equiv (m^e)^d \pmod{n}$,
$c^d \equiv m^{de} \pmod{n}$.
By the symmetry property of mods we have that
$m^{de} \equiv m^{de} \pmod{n}$.
Since $de = 1 + k\phi(n)$, we can write
$m^{de} \equiv m^{1 + k\phi(n)} \pmod{n}$,
$m^{de} \equiv m(m^k)^{\phi(n)} \pmod{n}$,
$m^{de} \equiv m \pmod{n}$.
From Euler's Theorem and the Chinese Remainder Theorem, we can show that this is true for all m and the original message
$c^d \equiv m \pmod{n}$, is obtained.
Thus these are existing and proven algorithms that are employed in the proposed security model.

4.2 Access phase:

When an access is made to the cloud, user provides finger impressions of these three registered finger prints. The order of the impressions is based on three digit random numbers generated.

4.2.1 Random Number Generation:

The proposed security model has an edge over other models that provide single finger print system. The reason is that, once an intruder gains access to a finger print template, he can claim to be an authenticated user. But in a multiple finger print system; even if an intruder manages to lacerate a stored template, still number tagged to each of the finger remains hidden. For authentication purpose, a Random Number Generator (RNG) is used. RNG generates a three digit random number (with repetition) every 20^{th} second. The three digits constitute the numbers that are chosen by the user during Enrollment phase. User now provides the finger impressions in the order of the generated random number.

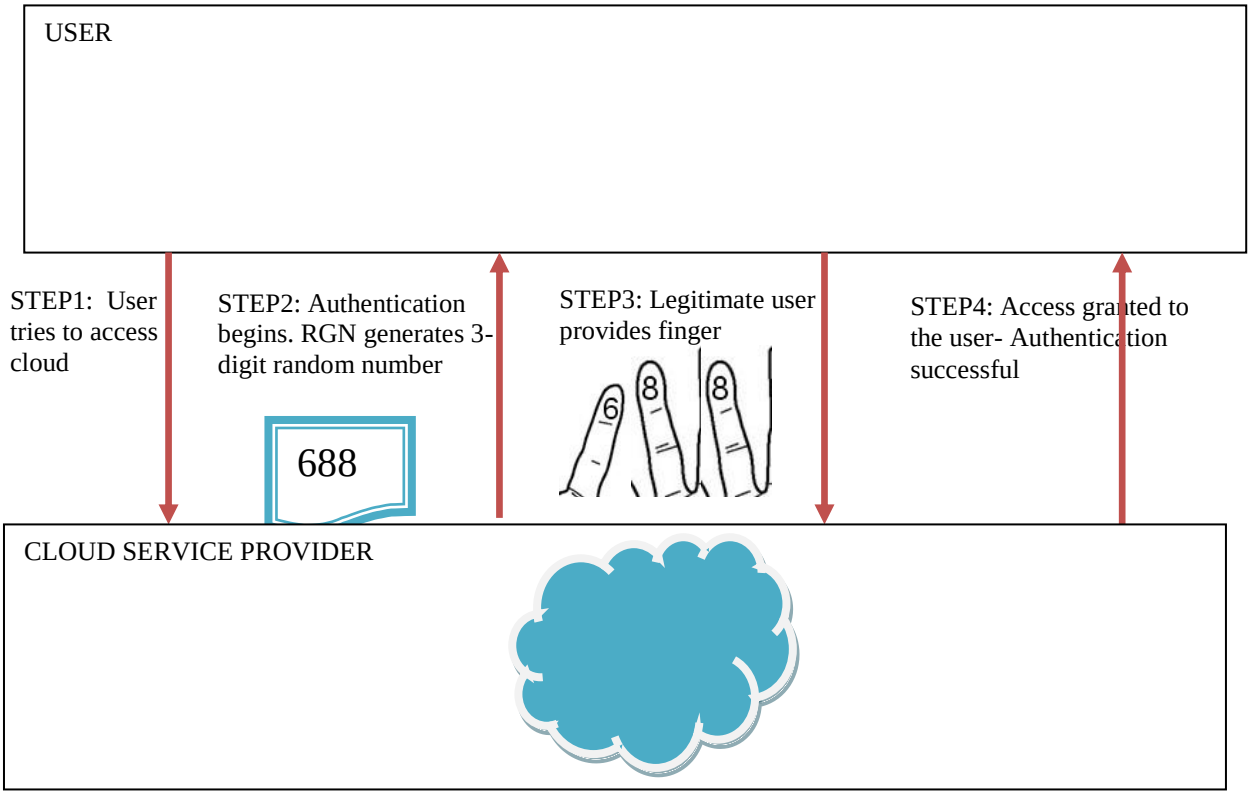

Fig.-7.Workings of the proposed security model for a legitimate user

4.2 Matching phase:

In this phase, a legitimate user is validated and an eavesdropper is invalidated. Even if the stored templates are hacked, the order of providing the impressions varies with the random number generated. Thus by means of trial and error, if a hacker tries with different permutations, access will be denied after three consecutive wrong attempts. The user has to re-set the numbering that was earlier assigned. This phase also includes a method of reassignment of a biometric template along with numbers and mappings when the existing one, assumed to be compromised after three consecutive wrong attempts.

V. Conclusion And Future Work:

Thus this research work brings about a new security model where three finger prints constitute an authentication. Though exiting efficient algorithms are used in this model, future work includes development of novel encryption algorithms that can make this model even more efficient.

REFERENCES

[1]. Alex Mu-Hsing Kuo, School of Health Information Science, University of Victoria, Victoria, Canada-*Opportunities and Challenges o f Cloud Computing to Improve Health Care Services*- Journal of Medical Internet Research

[2] Ravikiran Peelukhana, Shanthi Bala.P, Aghila.G, Department of Computer Science, Pondicherry University, Pudhucherri, India – *Securing Virtual Images Using Blind Authentication Protocol*- International Journal of Engineering science and Technology (IJEST)

[3] P.Tuylus, E.Verbitskiy, J.Goseling and D.Denteneer, *Privacy Protecting Biometric Authentication Systems, An Overview*, EUSIPCO 2004: XII European Signal Processing Conference

[4] - David Gonzalez Martnez, Francisco Javier Gonzalez Castano, Telematics Engineering Department, University of Vigo, Spain.-*Secure Crypto-Biometric System for Cloud Computing*

[5] *Tongue as a Biometric Visualizes New Prospects of Cloud Computing Security* – Sowmya, Suryavara, Shuchita Kapoor, Shweta Dhatterwal, Rohaila Naaz and Anand Sharma, Modi Institute of Technology and Science, Lakshmangarh, Rajasthan, India- 2011 International Conference on Information and Network Technology IPCSIT vol.4 (2011) IACSIT Press, Singapore

[6] N.K.Ratha, J.H.Connell and R.Bolle, *Enhancing Security and Privacy of Biometric Based Authentication Systems.* IBM Systems Journal, 40(3);614-634 2001

