www.ijiarec.com

ISSN: 2348-2079 MAR-2015

International Journal of Intellectual Advancements and Research in Engineering Computations

# A FRAMEWORK TO CREDIT CARD ENDORSEMENT USING FINGERPRINT FOR AUTHENTICATION COMBINED WITH SSO PROTOCOL IN CLOUD

[1]Ms. V.Karunya, [2]Dr. S. Prabhadevi

## 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 enrolment 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. When working with credit card transaction SSO solutions allow users to sign on only once and have their identities automatically verified by each application or service they want to access afterwards. We build on proxy signature schemes to introduce the public key cryptographic approach to single sign-on frameworks, which represents an important milestone towards the construction of provably secure single sign-on application for online transaction.

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

## 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. In this paper, a new security model has been proposed that uses multiple finger prints combined with encryption and random numbers as authentication tools with SSO protocol.

## 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.

The term **"Biometrics"** has come to be associated with the automatic identification of a person based on a feature or characteristic. These may be based on either:

- A physiological characteristic such as a fingerprint or face.
- A behavioral characteristic such as a signature or voice.

**Author for Correspondence:**
[1]Final yr, ME(CSE), Nandha Engineering College, Erode, Tamilnadu, India. Email: Karunyavel07@gmail.com
[2]Prof/CSE, Nandha Engineering College, Erode, Tamilnadu, India. Email: s.prabhadevi@gmail.com

In this paper fingerprint is used for authentication for credit card transcation with additional extra feature for security.


Figure 1 : Fingerprint Extraction

## PROCESS FLOW

The initial process is the bank gets the fingerprint of the card holder to update and store in their cloud database along with the credit card account information, where this fingerprint image is used for matching with the original fingerprint of the card holder during the credit card usage. The feature of the fingerprint is directly stored in the database. The proposed method as shown in Fig. 1. integrates the fingerprint scanner and the credit card machine with the system of the vendor where the software is hosted. The credit card is swiped in the credit card machine and the card number is sent as input whereby the fingerprint scanner scans the fingerprint of the card holder and the image is sent as input to the system of the vendor. With the given number as input it is sent to the cloud database of the bank via the bank server, where the respected fingerprint image of the holder is retrieved and it is sent back to the server. Then in the vendor system, the holder is prompted to give his fingerprint in the scanner which is then sent to the server for comparison, if there is a match, the transaction is continued else it is rejected.

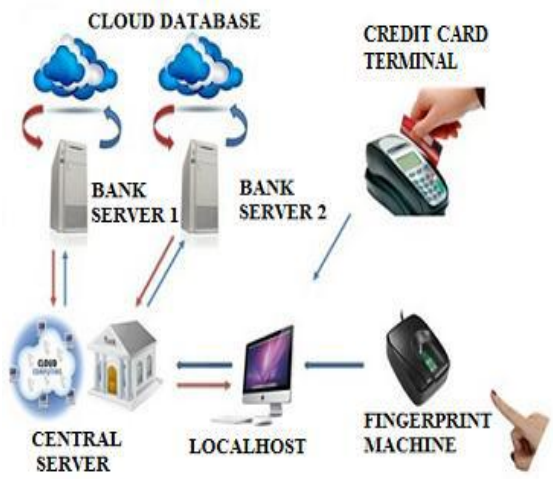


Figure 2: Flow diagram for user authentication

The traditional fingerprint recognition approaches are of two types: minutiae based methods and image based methods. The minutiae based methods use feature vectors extracted from the finger prints and stored as set of points in the multi dimensional plane. The feature vector may contain feature of minutia point such as their positions, orientations and types.

## SSO PROTOCOL

Single sign-on solutions allow users to sign on only once and have their identities automatically verified by each application or service they want to access afterwards. There are few practical and secure single sign-on models, even though it is of great importance to current distributed application environments. We build on proxy signature schemes to introduce the RSA public key cryptographic approach to single sign-on frameworks, which represents an important milestone towards the construction of provably secure single sign-on schemes. Our contribution is

two-fold, providing a framework that handles both session state across multiple services and granular access control. The intrinsic centralized access control functionality adds no additional cost to the single sign on protocol while providing an easy way to manage access policies and user rights revocation. Moreover, our approach significantly improves communication complexity by eliminating any communication between services

and identity providers during user identity and access permission verification.

Most of current application architectures require the user to memorize and utilize a different set of credentials (e.g username/password or tokens) for each application he/she wants to access. In a single sign-on platform, the user performs a single initial (or primary) sign-on to an identity provider trusted by the applications he wants to access. Later on, each time he wants to access an application, it automatically verifies that he is properly authenticated by the identity provider without requiring any direct user interaction. Single sign-on solutions eliminate the need for users to repeatedly prove their identities to different applications and hold different credentials for each applications. Furthermore, a well designed and implemented single sign-on solution significantly reduces authentication infrastructure and identity management complexity, consequently decreasing costs while increasing security.

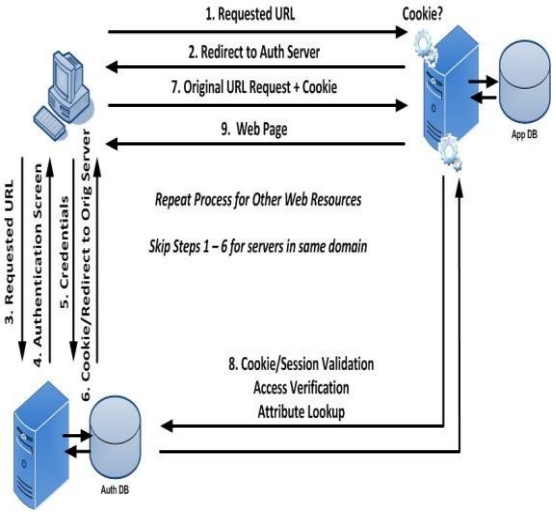


Figure 3 : Architecture of SSO PROTOCOL

## MECHANISM AND SOLUTION

### 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.

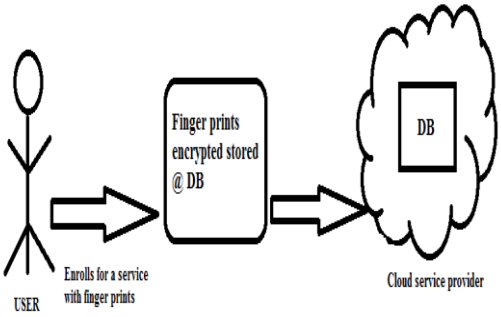


Figure 4 : Image Encryption model

A general approach in a biometric system is to store all captured biometric images in the Enrolment 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.

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

4.1.1. Enrollment phase

4.1.2. Access phase

4.1.3. Matching phase

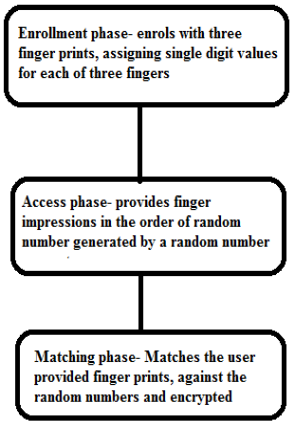


Figure 5: Three Phases of Image Encryption

## 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.

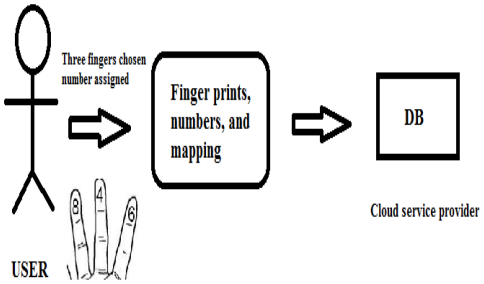


Figure 6: Architecture for Enrollment phase

## RSA ALGORITHM

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

## 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.

## 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 cipher text c corresponding to $c \equiv me \pmod{n}$. Step4: Cloud now sends message "M" in cipher text, or c, to user.

## DECRYPTION

Step1: User recovers m from c by using his private key exponent, d, by the computation $m \equiv cd \pmod{n}$.

Step2: Given m, User can recover the original message "M" by reversing the padding scheme. This procedure works since $c \equiv me \pmod{n}$, cd

≡(me)d (mod n), cd ≡ mde (mod n). By the symmetry property of mods we have that mde ≡ mde (mod n). Since de = 1 + kϕ(n), we can write mde ≡ m1 + kϕ(n) (mod n), mde ≡ m(mk)ϕ(n) (mod n), mde ≡ m (mod n). From Euler's Theorem and the Chinese Remainder Theorem, we can show that this is true for all m and the original message cd ≡ m (mod n), is obtained. Thus these are existing and proven algorithms that are employed in the proposed security model.

### 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.

### 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 20th second. The three digits constitute the numbers that are chosen by the user during Enrolment phase. User now provides the finger impressions in the order of the generated random number.

### 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.

### WORKING OF SSO

When input is given as three digit number and the fingerprint is stored in database as a image format. Both encryption and decryption is performed while processing the account for security purpose. In existing system when a user login into the account and perform a single transaction they will automatically logged out based on time interval which cause a inconvenient for accessing the account and become time consuming due to poor internet connection. But in proposed system using SSO protocol when a user enters a ID and Password it will stored in they cookie which will lead to redirect to the requested page without delay.

## CONCLUSION

In this paper using fingerprint and three digit inputs provides high secured which become a challenge for the hacker to break the code and also SSO protocol provides easier and low time for processing number of transaction in a single entry.

## REFERENCES

[1] Karthik Nandakumar, Student Member, IEEE, Anil K. Jain, Fellow, IEEE, and Sharath Pankanti, Senior Member, IEEE, “Fingerprint-Based Fuzzy Vault:Implementation and Performance”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 2, NO. 4, DECEMBER 2007.

[2] R.Cappelli, “Synthetic Fingerprint Generation,” Handbook of Fingerprint Recognition,Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, eds. New York: Springer, 2003.

[3] K.H.Davis,R.Biddulph,and S. Balashek, “Automatic recognition of spoken digits,” J. Acoust. Soc. Amer., vol. 24, no. 6, pp. 627–642, 1952.

[4] Dahl, M. Ranzato, A. Mohamed, and G. E. Hinton, “Phone recognition with the mean-covariance restricted Boltzmann machine,” in Advances in Neural Information Processing 23. Cambridge, MA: MIT Press, 2010.

[5] M. Bazen and S.H. Gerez, “Systematic methods for the computation of the directional fields and singular points of fingerprints,” IEEE Trans. Pattern Anal. Machine Intell., vol. 24, no. 7, pp. 905–919, July 2002.

[6] N. Otsu, "A threshold selection method from gray-level histograms," IEEE Trans. Syst., Man. Cybern., vol. SMC-9, pp. 62–66, 1979.

[7] M. Al-Alaoui, "A new weighted generalized inverse algorithm for pattern recognition", IEEE Transactions on Computers, vol. C-26, no. 10, October 1977.

[8] V. Digalakis, D. Rtischev, L. Neumeyer, and E. Sa, "Speaker adaptation using constrained estimation of Gaussian mixtures," IEEE Trans. Speech Audio Process., vol. 3, no. 5, pp. 357–366, Sep. 1995.

[9] McCallum, "Mallet: A machine learning for language toolkit," 2002, http://mallet.cs.umass.edu. A. Jules and M. Sudan, "A Fuzzy Vault Scheme," Proc. IEEE Int'l Symp. Information Theory, IEEE Press, 2002, p. 408.

[10] D. Balfanz et al., "The future of authentication",IEEE Security & Privacy, vol. 10, pp. 22-27, 2012.

[11] Phillips, A. Martin, C. Wilson, and M. Przybocki, "An introduction to evaluating biometric systems", IEEE Computer Society., Volume 33, No. 2, Feb. 2000, pp. 56–63.

[12] Anil K. Jain, Arun Ross and Salil Prabhakar: "An Introduction to Biometric Recognition" IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

[13] Jucheng Yang, Naixue Xiong, "A Fingerprint Recognition Scheme Based on Assembling Invariant Moments for Cloud Computing Communications." Jiangxi University of Finance and Economics, IEEE systems journal, vol. 5, no. 4, December 2011.

[14] A.Georghiades, P. Belhumeur, and D. Kriegman. From few to many: Illumination cone models for face recognition under variable lighting and pose. IEEE Transactions on Pattern Analysis and Machine Intelligence, 23(6):643–660, 2001. B. Miller, "Vital signs of identity," IEEE Spectrum, vol. 31, pp. 22–30, Feb. 1994.

[15] J. E. Siedlarz, "Iris: More detailed than a fingerprint," IEEE Spectrum, vol. 31, p. 27, Feb.1994.

[16] Jaliya Ekanayake, Student Member, IEEE, Thilina Gunarathne, Student Member, IEEE, and Judy Qiu "Cloud Technologies for Biometrics Applications "IEEE TRANSACTIONS ON PARALLEL AND DISTRI-BUTED SYSTEMS, VOL. 22, NO. 6, JUNE 2011

[17] Chang, K. I., K. W. Bowyer, and P. J. Flynn, "An evaluation of multi-modal 2D+3D face biometrics," IEEE Trans. on PAMI 27 (4), pp. 619-624, April 2005.

[18] Rabiner L., Juang B., "Fundamentals of Speech Recognition". PTR Prentice Hall, NJ, 1993.

[19] T. Sim, S. Baker, and M. Bsat. The CMU pose illumination and expression database. IEEE Transactions on Pattern Analysis and Machine Intelligence, 25(12):1615–1618, December 2003

[20] B. Moghaddam and A. Pentland. Probabilistic visual learning for object representation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(7):696–710, July 1997.

[21] B. Lee, H.K., Kim, K.: Strong proxy signature and its applications. In: Proc. Of the 2001 Symposium on Cryptography and Information Security (SCIS'01). vol. 2, pp. 603{608 (2001).

[22] Bellare, M., Fischlin, M., Goldwasser, S., Micali, S.: Identi_cation protocols secure against reset attacks. In: Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology. pp. 495{511. EUROCRYPT '01, Springer-Verlag, London, UK (2001).

[23] 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).