International Journal of Electrical and Computer Engineering (IJECE)
Vol. 7, No. 1, February 2017, pp. 408~416
ISSN: 2088-8708, DOI: 10.11591/ijece.v7i1.pp408-416

Biometric Identification and Authentication Providence using Fingerprint for Cloud Data Access

A. Amali Mary Bastina[1], N. Rama[2]
[1]Department of Computer Science, Loyola College, Chennai 600034, India
[2]Post Graduate and Research Department of Computer Science, Presidency College, Chennai 600005, India

Article Info

Article history:

Received Jul 19, 2016
Revised Oct 22, 2016
Accepted Nov 6, 2016

Keyword:

Authentication
Biometrics
Entropy
Fingerprint
Mobile cloud computing

ABSTRACT

The raise in the recent security incidents of cloud computing and its challenges is to secure the data. To solve this problem, the integration of mobile with cloud computing, Mobile biometric authentication in cloud computing is presented in this paper. To enhance the security, the biometric authentication is being used, since the Mobile cloud computing is popular among the mobile user. This paper examines how the mobile cloud computing (MCC) is used in security issue with finger biometric authentication model. Through this fingerprint biometric, the secret code is generated by entropy value. This enables the person to request for accessing the data in the desk computer. When the person requests the access to the authorized user through Bluetooth in mobile, the Authorized user sends the permit access through fingerprint secret code. Finally this fingerprint is verified with the database in the Desk computer. If it is matched, then the computer can be accessed by the requested person.

Corresponding Author:

A. Amali Mary Bastina,
Department of Computer Science,
Loyola College,
Chennai 600034, India.
Email: amalimarybastina@gmail.com

1. INTRODUCTION

Sharing of configuration of computer resources is used by cloud computing, it is one of the computer technology that leverages cloud resources for "enabling ubiquitous, convenient, on-demand network access. That is, sharing the resources is from network servers, storage, applications and services. In cloud computing, the definition behind the "cloud" is proposed by Figure [9], it is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers.

Nowadays, the utilization of cloud resources under the mobile devices is a recent research approaches to envelope the network process easily it is called Mobile Cloud Computing Figure [14]. The aim of Mobile Cloud Computing is to enhance the mobile dives computing capability and conserve mobile resources such as battery, mobile internal and external storage capability and the vital function is to enhance the data safety to enrich the computing experience of mobile users Figure [4].

Biometric system is one of the pattern recognition techniques, the operation behind the biometric system it obtain through the biometric data from an individual person and extracting the feature set from the obtaining data, and comparing the obtaining feature set is compared to the storage data as template in the database Figure [1]. There are other several biometrics are also available in mobile computing such as DNA, Ear, Face, Fingerprint, Gait, hand and finger geometry, Iris, Keystroke, Odor, Palm print, retinal, signature and voice.

In this proposed theory, the cloud computing uses Fingerprint based biometric authentication. Here, the particular file which is requested can be accessed by the user through mobile finger authentication. When the requested user, needs to access the particular data in protective folder in computer, he process it through mobile cloud computing with the help of Bluetooth to get authenticated by the Authorized user.

The remainder of this paper is organized as follows: Section II deals with literature survey: An overview of MCC and finger print biometric recognition, Section III briefly discuss about proposed methodology, Section IV discuss the Experimental Results and Section V concludes the paper.

2. LITERATURE SURVEY

The energy conservation for the mobile device is presented in figure [11]. Here the author and her associates implemented the mobile energy conservation based on executing mobile application in their mobile devices which also means mobile execution or cloud execution. For this process, both the execution asymptotical analysis of the optimal scheduling is also provided.

Improvisation of quality of Really Simple Syndication (RSS) reading service for mobile users is described in figure [13]. There are two proposed algorithms: Cloud-assisted pre-fetching and cognitive pushing. Fetching of the multimedia content of the RSS for all mobile users are takenin first part, and in the second part, appropriate time is set for pushing the data to mobile users. These processes are well utilized through cloud computing technology.

In figure [10], the mobile cloud service is provided through optimal resource management tool that maximizes the benefit of the mobile cloud service provider which proposed one of the outlines for the resource allocation to the mobile application, formulate the optimal models though, this maximizes the service provider in the mobile application.

Energy efficient link for data Intensive application in mobile cloud computing is presented in figure [12], and also for data tolerant application. To optimize data tolerant and data Intensive system, throughout energy consumption is designed by using the discrete-time stochastic dynamic program. This reduces the average energy consumption for packet delivery and implements a scalable approximate dynamic programming.

The Security of the internet service is presented in figure [8] based on cloud mobile computing system. In this system, securing the internet is through Biometric authentication. The password is created through this method and it is stored as a template. Several techniques are used for this system such as large scale character recognition, algorithm such as k-nearest neighbor, and artificial neural network classifier.

In figure [10] represents the number of authentication techniques. The core designers Weirich and Sasse figure [5] reports the result of the series of user interviews about password behavior and is also based on phrase arguments to persuade the users who is introduced to adopt a better security behavior. Stanton figure [6] likewise researched on the users for the purpose of discovering the range of user security behavior in a wide variety of contexts, not just in password choice and its use.

In figure [2] proposed as an identity is based on the encryption and biometric authentication for secure the data in cloud computing. Several steps are presented to access the data that are setting the parameter, key distribution, create the template for features, finally processing the cloud data.

Accessing the cloud service is implemented in Figure [3], here increasing the security for accessing the data through biometric authentication. Here the researchers secure the data based on the combination of images and texts as a hybrid approach.

3. PROPOSED METHODOLOGY

Mobile cloud computing is the integration of the cloud computing and mobile devices, and is also applied by the cloud computing application in mobile application. Figure 1 shows proposed Methodology.

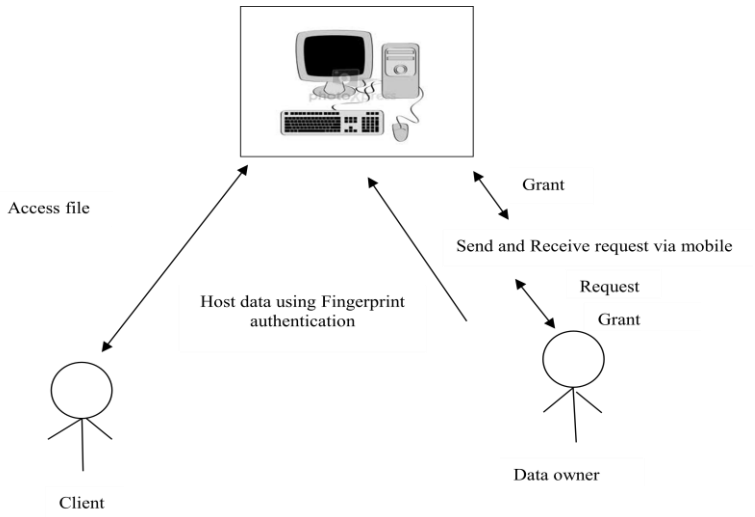

Figure 2. Proposed Methodology

3.1. Overview of Proposed Framework

The proposed model is used for the security purpose efficiently. In this model, the proposed biometric authentication for application execution on the cloud based mobile technology. First, we access a file in the PC. Secondly sending the request for accessing the file. For accessing the file secret code is needed. This secret code is developed using biometric recognition. In this research, fingerprint is used as biometric authentication is developed. The aim of the mobile cloud computing is to give a proxy for mobile clients connecting to Cloud services. This type of methods consists of three parts such as mobile service client, middleware and cloud services. Fingerprint biometric is mostly used in various authentication applications due to the advantage of its best balance among other authentication system and also costing of the fingerprint based biometric authentication system is very low compared to other authentication system. The main advantage of the fingerprint based authentication system is user friendly. From the fingerprint, we calculate the secret code developed by Maximum-Entropy Expectation-Maximization Algorithm. Request is been sent to the data owner, and the client receives the acknowledgement of accessing the PC through Bluetooth in his mobile.

3.2. Secret Code Developed by Maximum-Entropy Expectation-Maximization Algorithm

Expectation-Maximization (EM) algorithm offers an approximation of the pdf (Probability density function) by an iterative optimization under the maximum prospect of criterion.

Probability density function $P(x)$ can be approximated as the sum of KGaussian function

$$P(x) = \sum_{k=1}^{K} w_k G(x - D_k, Co_k) \quad (1)$$

Here, Gaussian function center is represented by D_k, where covariance matrix is indicated by Co_k, and each center weight is represented by w_k. The Gaussian function is given in below equation

$$(x - D_k, Co_k) = \frac{exp\left\{-\frac{(x - D_k)^T Co_k^{-1}}{2}(x - D_k)\right\}}{(2\pi)^{D/2Co_k|1/2}} \quad (2)$$

From the above two equation (1 & 2), we can observe that the logarithm of the possibility of function for the given Gaussian mixture parameters that has M observations can be written as

$$L_L(\theta_p) = \sum_{m=1}^{M} log \sum_{k=1}^{K} w_k G(x_m - D_k, Co_k) \quad (3)$$

Here x_m is the m^{th} sample and $\theta_p$is a set of parameters.

The entropy term is added in order to make the estimated density function smooth and not to have an impulse distribution.

$$H(\theta_p) = -log \sum_{i=1}^{K} \sum_{j=1}^{K} w_i w_j G(D_i - D_j, Co_i + Co_j) \tag{4}$$

Maximize the entropy value using augmented probable function L_{ME}; it is parameterizedby a positive scalar p_s, augmented probable function L_{ME} is given below:

$$L_{ME}(\theta_p, p_s) = L_L(\theta_p) + p_s H(\theta_p) \tag{5}$$

The expectation step of the EM algorithm can be separated into two terms, one is the expectation related with likelihood and the other is the expectation related with the entropy penalty.

$$p_L^t(k,m) = \frac{w_k G(x_m - \mathrm{D_k}, Co_k)}{\sum_{l=1}^{K} w_l G(x_m - \mathrm{D_l}, Co_l)} \tag{6}$$

$$p_E^t(k,l) = \frac{w_k w_l G(\mathrm{D_k} - \mathrm{D_l}, Co_k + Co_l)}{\sum_{mm=1}^{k} \sum_{m=1}^{K} w_{mm} w_m G(\mathrm{D_{mm}} - \mathrm{D_m}, Co_{mm} + Co_m)} \tag{7}$$

Here L denotes that this expectation is from the likelihood function, E denotes that this expectation is from the entropy penalty, and t denotes the number of iteration.

The lower bound function$\varphi_L^t(\theta_p)$ for the
Likelihood function is given by:

$$L_L(\theta_p) = \sum_{m=1}^{M} log \sum_{k=1}^{K} w_k G(x_m - \mathrm{D_k}, Co_k) \geq \sum_{m=1}^{N} \sum_{k=1}^{K} p_L^t(k,m) log \frac{w_k G(x_m - \mathrm{D_k}, Co_k)}{p_L^t(k,m)} = \varphi_L^t(\theta_p) \tag{8}$$

Lower bound functions $\varphi_E^t(\theta_p)$ for the entropy is given below:

$$\begin{aligned} H(\theta_p) &= \delta\left(\sum_{k=1}^{K} \sum_{l=1}^{K} w_k w_l G(\mathrm{D_k} - \mathrm{D_l}, Co_k + Co_l)\right) \\ &\geq \sum_{k=1}^{K} \sum_{l=1}^{K} p_E^t(k,l)\, \delta \frac{w_k w_l G(\mathrm{D_k} - \mathrm{D_l}, Co_k + Co_l)}{p_E^i(k,l)} \\ &\geq -\sum_{k=1}^{K} \sum_{l=1}^{K} p_E^t(k,l)\, log\left(\frac{w_k w_l G(\mathrm{D_k} - \mathrm{D_l}, Co_k + Co_l)}{p_E^i(k,l)}\right) = \varphi_E^t(\theta_p) \end{aligned} \tag{9}$$

In the above equation δindicated concave function
The combination of two lower bounds given another relationship is given below:

$$\varphi_{ME}^t(\theta_p, p_s) = \varphi_L^t(\theta_p) + p_s \varphi_E^t(\theta_p) \tag{10}$$

Since we have the lower bound function, the new estimates of the parameters are easily calculated by setting the derivatives of$\varphi^t(\theta_p, p_s)$with respect to each parameter to zero.

a) Mean
The mean vector is calculated by equation:

$$D_k^{t+1} = \left(\sum_{m=1}^{M} p_L^t(k,m) Co_k^{-1} - 2v \sum_{t=1,l\neq k}^{k} p_E^t(k,l)(Co_k + Co_t)^{-1} \right)^{-1} \times \left(\sum_{m=1}^{M} p_L^t(k,m) Co_k^{-1} x_m - 2v \sum_{l=1,t\neq k}^{K} p_E^t(k,l)(Co_k + Co_t)^{-1} m_l \right) \quad (11)$$

b) Weight:
Weight parameter is calculated by below equation:

$$w_k^{t+1} = \frac{\sum_{m=1}^{M} p_L^t(k,m) - 2v \sum_{l=1}^{K} p_E^t(k,l)}{N - 2v}$$

c) Covariance:
Covariance parameter is calculated using below equation:

$$\begin{aligned} \left\{ \varphi_{ME}^t(\theta_p, p_s) \right\}_{Co_k} &= \sum_{n=1}^{N} p_L^t(k,n) log \frac{w_k G(x_m - \mathrm{D_k}, Co_k)}{p_L^t(k,n)} \\ &- 2v \sum_{t=1,l\neq k}^{K} p_E^t(k,l) log \times \frac{w_k w_l G(\mathrm{D_k} - \mathrm{D_l}, Co_k + Co_l)}{p_E^t(k,l)} \\ &- 2v\, p_E^t(k,k) \frac{w_k w_k G(0,2Co_k)}{p_E^t(k,k)} \end{aligned} \quad (12)$$

Here $2logGG(\mathrm{D_k} - \mathrm{D_l}, Co_k + Co_l)$ is equal to

$$\begin{aligned} log\{G(\mathrm{D_k} - \mathrm{D_l}, Co_k + Co_l)\}^2 &= \left\{ \int_{-\infty}^{\infty} G(x - D_t) G(x - D_m, Co_m) dx \right\}^2 \\ &\leq \int_{-\infty}^{\infty} \{G(x - D_t, Co_t)\}^2 dx \int_{-\infty}^{\infty} \{G(x - \quad D_m, Co_m)\}^2 \, dx \\ &= G(0,2Co_l) G(0,2Co_m) \end{aligned} \quad (13)$$

Using the above equation with symmetry property of Gaussian, we introduce the lower bound for the covariance.

$$\begin{aligned} \left\{ \varphi_{Co_k}^t(\theta_p, p_s) \right\}_{Co_k} &\geq \sum_{m=1}^{M} p_L^t(k,m) log \frac{w_k G(x_m - D_k, Co_k)}{p_L^t(k,n)} \\ -v \sum_{l=1,l\neq k}^{K} p_E^t(k,l) log &\times \frac{(w_k w_l)^2 G(0,2Co_k) G(0,2Co_1)}{p_E^t(k,l)} \\ (-\, v p_E^t(k,k) log \frac{w_k^2(0,2Co_k)}{p_E^t(k,k)} &= \varphi_{Co_k}^t(\theta_p, p_s) \end{aligned} \quad (14)$$

Then new estimated covariance is obtained by new lower bound setting.

$$Co_k^{t+1} = \frac{\sum_{m=1}^{M} p_L^t(k,m)(x_m - D_k)\left((x_m - D_k)\right)^T}{\sum_{m=1}^{M} p_L^t(k,m) - v \sum_{t=1}^{K} p_E^t(k,l)} \quad (15)$$

This method to prove that this algorithm converges to a local maximum on bound is generated by the Cauchy–Schwartz inequality. This type of inequality is met with equality, when the covariance matrices of the different kernels are equal.

3.3. Advanced Encryption and Decryption Algorithm

Encryption and decryption is most important to secure the data in all security development. In this researches, the file has to be hidden is secured by these algorithm. Encryption and Decryption plays an important role in security. The created entropy value is used for decrypting the entropy file, if the entropy value is matched.

3.3.1. Advanced Encryption Standard (AES) Algorithm

There are two main important parts in AES algorithm, which are data procedures and key schedules. The data procedure is one of the important for encryption, it has four operations: (Inv) SubBytes, (Inv) ShiftRows, (Inv) MixColumns, and (Inv) AddRoundKey. AES operated in two fields, $GF(2)$ and $GF(2^8)$. In $GF(2)$ addition is denoted by $\oplus$, andmultiplication is denoted by $\otimes$. Similarly, the two symbols, $\oplus$ and $\otimes$, denote addition and multiplication in $GF(2^8)$. Each operation is explained below.

1) Subtypes:

In this operation, two calculations are involved that are $GF(2^8)$ inversion and affine transformation. For each byte s_i in the data block, this operation is assigned by

$$t_i = A_{s_i}{}^{-1} + 63 \quad (16)$$

In the above equation, s_i^{-1} is the inverse of the input byte, s_i indicates the i^{th} byte of the data block. A is a constant row vector for 8×8 circulant vector $[1\ 0\ 0\ 0\ 1\ 1\ 1\ 1]$over$GF(2)$, $A_{s_i}{}^{-1}$ denotes the matrix-vector multiplicationover GF (2).

2) Shift Rows:

Changing the byte position process is obtained through this operation. Assigning different offset for rotating each row and obtain the new state. For example

$$\begin{bmatrix} s_0 & s_4 & s_8 & s_{12} \\ s_1 & s_5 & s_9 & s_{13} \\ s_2 & s_6 & s_{10} & s_{14} \\ s_3 & s_7 & s_{11} & s_{15} \end{bmatrix} \xrightarrow{ShiftRows} \begin{bmatrix} s_0 & s_4 & s_8 & s_{12} \\ s_5 & s_9 & s_{13} & s_1 \\ s_{10} & s_{14} & s_2 & s_6 \\ s_{15} & s_3 & s_7 & s_{11} \end{bmatrix}$$

In the above matrix, first row is unchanged, the second row is left circular shifted by one, the third row is by two, and the last row is by three.

3) MixColumns:

In this operation, four new bytes are obtained by mixes every consecutive four byte of the state. For example

$$\begin{bmatrix} s_0 & s_4 & s_8 & s_{12} \\ s_1 & s_5 & s_9 & s_{13} \\ s_2 & s_6 & s_{10} & s_{14} \\ s_3 & s_7 & s_{11} & s_{15} \end{bmatrix} \xrightarrow{MixColumns} \begin{bmatrix} t_0 & t_4 & t_8 & t_{12} \\ t_1 & t_5 & t_9 & t_{13} \\ t_2 & t_6 & t_{10} & t_{14} \\ t_3 & t_7 & t_{11} & t_{15} \end{bmatrix}$$

Every consecutive four bytes are represented as $s_i, s_{i+1}, s_{i+2}\ and\ s_{i+3}$, in which i belongs to $\{0,4,8,12\}$. Then four bytes are transformed by

$$\begin{bmatrix} t_i \\ t_{i+1} \\ t_{i+2} \\ t_{i+3} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_i \\ s \\ s_{i+2} \\ s_{i+3} \end{bmatrix}$$

In the above matrix, each entry is belongs to$GF(2^8)$.

4) AddRoundKey and key Expansion:

AddRoundKey operation is simply an addition, in which each round have 128-bit round key and which is segmented in to 16 bytes k_i.

$t_i = s_i + k_i$, where
$0 \le i \le 15$ (17)

The key expansion expands a unique private key as a key stream of $(4r + 4)$ 32-bit words, where r is 10, 12, or 14. The private key is segmented into Nk words according to the key length, where NK is 4, 6, or 8 for a 128-bit, 192-bit, or 256-bitcipher key, respectively.

3.3.2. Advanced Decryption Standard Algorithm:

Corresponding to the transformations in the encryption, InvSubBytes, InvShiftRows, InvMixColumns, and AddRoundKey are the transformations used in the decryption.

1) InvSubBytes Transformation:

It is the inverse transformation ofSub Bytes.

2) InvShiftRows Transformation:

It is the inverse transformation of ShiftRows. Here the first is not changed; one byte is shift cyclically to the right for second row, two byte is shifted to right for third row. Finally four byte is shifted cyclically to the right for third row**.**

3) InvMixColumns Transformation:

It is the inverse transformation of InvMixColumns. It is transformed column by column on the state.

4) AddRoundKey:

AddRoundKey process is same as the Encryption, but this operation used in reverse order.

4. EXPERIMENTAL RESULTS

The proposed system is evaluated in JAVA platform. Here, two emerging trends are used that are cloud and mobile, these two trends are combined and challenging the security performance.

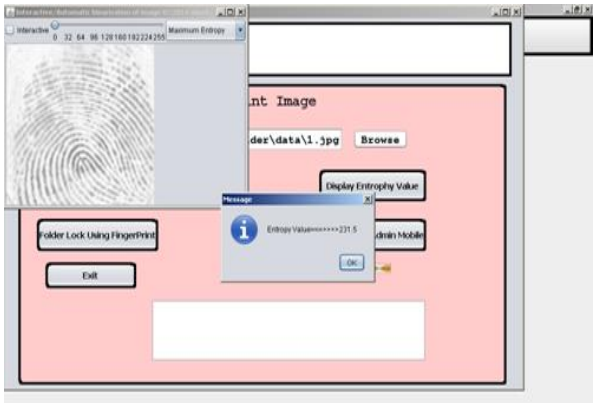

Figure 3. Entropy Value for user Fingerprint

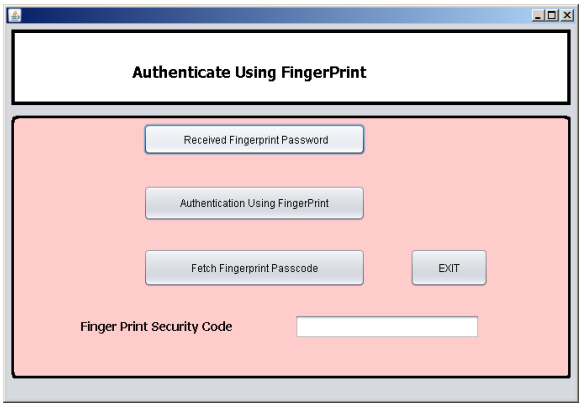

Figure 4. Authentication received by admin from client

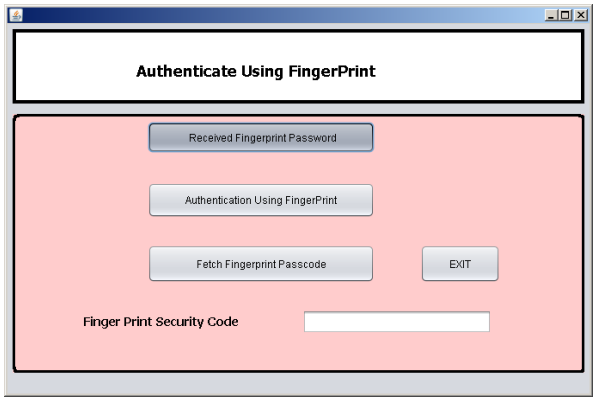

Figure 5. Authentication Received by Client from Admin

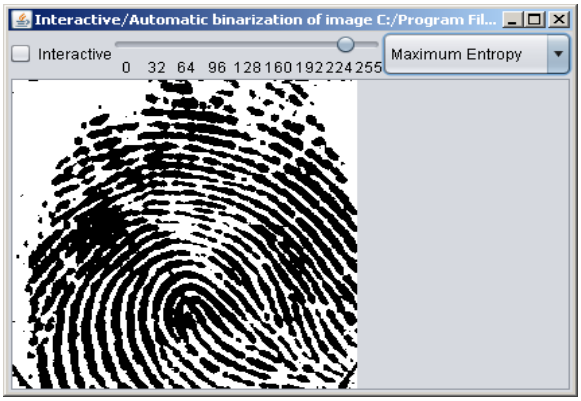

Figure 6. Maximum Entropy Value

Figure 7. Fingerprint Authentication

The proposed mobile cloud computing secured the security system through biometric authentication. In this process, the admin registers her/his details such as user name, password and phone number and logins the system with that specified password. Figure 2 gives the entropy value for admin fingerprint. The entropy value is calculated by Maximum-Entropy Expectation-Maximization Algorithm. Figure 3 & 4 illustrates the authentication between the client and admin through Bluetooth. The request is communicated by the client to access the PC is shown in Figure 3, acknowledgment is sent back by the admin is shown in Figure 4. Figure 5 & 6 illustrates the maximum entropy value and fingerprint matching to the database stored in the PC. Then the client accesses the specified folder through this entropy value.

5. CONCLUSION

Cloud computing promises the IT companies and provides increased flexibility. One of the key problems is information security. This research presented a controllable security scheme for a cloud storage owner to secure their data. Mobile cloud computing is presented with fingerprint biometric authentication with Maximum Entropy Expectation-Maximization Algorithm which uses to create the secret code. This paper offers cloud storage identify for accessing data or files from PC through anywhere by mobile using fingerprint recognition.

REFERENCES

[1] Jain AK, Ross A, Prabhakar S. "An introduction to biometric recognition". I*EEE Transactions on circuits and systems for video technology*. 2004 Jan; 14(1): 4-20
[2] Cheng H, Rong C, Tan Z, Zeng Q. "Identity based encryption and biometric authentication scheme for secure data access in cloud computing". *Chinese Journal of Electronics*. 2012 Apr; 21(2): 254-9
[3] Popescu DE, LoneaAM. "A hybrid text-image based authentication for cloud services". *International Journal of Computers Communications & Control.* 2013 Feb 18; 8(2): 263-74.
[4] Macedo DF, Dos Santos AL, Pujolle G. "From TCP/IP to convergent networks: challenges and taxonomy". *IEEE Communications Surveys & Tutorials.* 2008 Jan 1; 10(4): 40-55.
[5] Weirich D, Sasse MA. "Pretty good persuasion: a first step towards effective password security in the real world". In *Proceedings of the 2001 workshop on New security paradigms* 2001 Sep 10 (pp. 137-143). ACM.
[6] Stanton JM, Stam KR, Mastrangelo P, Jolton J. "Analysis of end user security behaviors*". Computers & Security*. 2005 Mar 31; 24(2): 124-33.
[7] O'Gorman L. "Comparing passwords, tokens, and biometrics for user authentication". *Proceedings of the IEEE*. 2003 Dec; 91(12): 2021-40.
[8] Omri F, Foufou S, Hamila R, Jarraya M. "Cloud-based mobile system for biometrics authentication". *InITS Telecommunications (ITST), 2013 13th International Conference on* 2013 Nov 5 (pp. 325-330). IEEE.
[9] Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I. "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility". *Future Generation computer systems*. 2009 Jun 30; 25(6): 599-616.
[10] Kaewpuang R, Niyato D, Wang P, Hossain E. "A framework for cooperative resource management in mobile cloud computing". *IEEE Journal on Selected Areas in Communications*. 2013 Dec; 31(12): 2685-700.
[11] Zhang W, Wen Y, Guan K, Kilper D, Luo H, Wu DO. "Energy-optimal mobile cloud computing under stochastic wireless channel". *IEEE Transactions on Wireless Communications*. 2013 Sep; 12(9): 4569-81.
[12] Xiang X, Lin C, Chen X. "Energy-efficient link selection and transmission scheduling in mobile cloud computing". *IEEE Wireless Communications Letters*. 2014 Apr; 3(2): 153-6.

[13] Wang X, Chen M. "Pre-Feed: cloud-based content pre-fetching of feed subscriptions for mobile users". *IEEE Systems Journa*l. 2014 Mar; 8(1): 202-7.
[14] Sanaei Z, Abolfazli S, Gani A, Buyya R. "Heterogeneity in mobile cloud computing: taxonomy and open challenges". IEEE Communications Surveys & Tutorials. 2014 Feb; 16(1): 369-92

BIOGRAPHY OF AUTHOR

Amali Mary Bastina. A Lecturer, Department of Computer Science, Loyola College, Chennai 600034. Email: amalimarybastina@gmail.com