Securing Cloud Technology's Service Management using Cognitive and Biometric Approaches

P. Adlene Ebenezer, Amritesh Singh, Sakshi Singh, Ayush Sinha, Tarun Keshri

Abstract--- Cloud computing is an emerging technology that lets users to access the cloud server to store their data and access it on-demand, anywhere and at anytime. But it also has many security issues since the CSPs are not in the domain of trust. Thus, to guarantee the safety of data from untrusted sources many securing mechanisms are being adopted since the security of services in a cloud technology is a very important aspect, which cannot be ignored. If certain critical data falls in the wrong hands, it can wreak havoc. The existing systems apply cryptographic methods at a fine-grained access control and data sharing levels for the services of dynamic user groups in cloud, but it poses to be a challenging issue. In fine-grained access control each data item is given its own control policy. If an entity wants to access a data item it will have to provide its credentials to a third party policy enforcer, which is not the owner of the data. These access control policies and the entity credentials might reveal some critical information to the policy enforcer to which it is not entitled to know. In this paper we propose securing cloud technology services using biometric and cognitive methodologies for dynamic cloud user groups. Extraction of unique and different personal characteristics and behavioral patterns are used in management protocols. Cognitive security is based on application of AI technology of human thought process to find the most appropriate solution in a situation, and along with the users Biometric features like palm/finger prints, voice recognition, retina scan, facial recognition and with the addition of cryptographic methods to these an efficient and secure solution is developed.

Keywords--- Cloud Computing, Biometric, Security, Cognitive, Cryptography, Service Management.

I. INTRODUCTION

The application of perceptual, cognitive, and behavioral features can play an important role in advanced protocols dedicated to secure data management and remote-service provision. In many applications, to guarantee the highest level of security, it is necessary to use some procedures that can be dedicated to a particular user or a group of participants. To define such human oriented and secure management protocols, unique or characteristic personal features, including behavioral patterns as well as cognitive or visual perception abilities, can be considered. Unique personal and behavioral parameters can be extracted or evaluated by cognitive system that supports evaluating personal patterns and such biometric characteristics as the palm or finger movements, body motions, or specific gestures.

Apart from these personal characteristics evaluated by cognitive information systems, it is possible to create management procedures based on the perception abilities or the specific knowledge of a particular person. These protocols can be linked to the application of individual perception threshold, which is associated with the recognition, and interpretation of some specific visual data. Once the personal features are available, we can create secure procedures for data encryption, concealment, and transmission, as well as distributed-service management in fog and cloud environments. Such personally oriented technologies can also play an important role in future pervasive-computing technologies and even the Internet of Things. Different personal characteristics or motion patterns can be used in management protocols. The most important activity with regard to these types of personal features is the registration or extraction of unique or nonstandard personal characteristics, including motion and behavioral patterns. Cognitive-vision systems in connection with multimedia devices such as Leap Motion, Kinect, or motion capture sensors can be used for this extraction or evaluation. Among body movements, it is particularly worthwhile to consider the very specific natural gait, which can be characteristic for particular individuals, or simple exercises that can be performed by most people in different, personalized ways.

Among the last group of complex motion patterns, it is possible to consider only advanced movements observed in sports, gymnastics, or dances and possible for only a small group of persons with great physical skills. Here, it is possible to analyze longer motion sequences presenting special movements learned over a longer time that other performers would have difficulty quickly repeating. The personal features extracted should be stored in a personal-feature vector that can contain as much information as possible and describes biometric features or motion parameters, etc. For each application, it will be possible to select a small subset of such features that can be applied in a particular protocol.

Manuscript received June 10, 2019.

P. Adlene Ebenezer, Assistant Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology Chennai, T.N, India. (e-mail: adleneebenezer.p@rmp.srmuniv.ac.in)

Amritesh Singh, B.Tech (IV) Year Student, Department of Computer Science and Engineering, SRM Institute of Science and Technology Chennai, T.N, India. (e-mail: iamamritesh4@gmail.com)

Sakshi Singh, B.Tech (IV) Year Student, Department of Computer Science and Engineering, SRM Institute of Science and Technology Chennai, T.N, India. (e-mail: saksingh14@gmail.com)

Ayush Sinha, B.Tech (IV) Year Student, Department of Computer Science and Engineering, SRM Institute of Science and Technology Chennai, T.N, India. (e-mail: ayushsinha78@gmail.com)

Tarun Keshri, B.Tech (IV) Year Student, Department of Computer Science and Engineering, SRM Institute of Science and Technology Chennai, T.N, India. (e-mail: keshritarun767@gmail.com)

II. LITERATURE SURVEY

This section of Literature Survey is related to some important algorithms, modules and facts on the basis of analysis.

The author has introduced a biometric inspired homomorphic encryption algorithm for securing data transmission of files in cloud at hybrid level. Algorithm encrypts all the user data by providing unique one-time password and helps against phishing and shoulder surfing. [1]

The author proposed a Biometrics-as-a-Service (BaaS) framework to perform biometric matching in cloud devices for providing security and privacy to data. The author has used a Linux-based virtual machine environment for fake logging and data theft for cloud authentication. [2]

In this paper, the author introduced biometric authentication with compression and encryption of data. For providing security Advanced Encryption Standards algorithm is used generate the secret key with its feature extraction from fingerprint biometrics using algorithm named as Advanced Minutiae Base Algorithm. In the end the secret value is encrypted with generated biometric key using Advanced Encryption Standard (AES) Algorithm. [3]

In this paper, author has used multi model authentication using one biometric technique. He proposed a model based on Advanced Minutiae Base Algorithm (AMBA) and Advance Encryption Standard (AES) algorithm, which reduces the computational load on the cloud and securing identity of the person by disclosing or decrypting with the relevant / same secret key. [4]

The author discussed cognitive cryptography to secure data by splitting it among different groups of trustees. Most of the safety problems are associated with authentication and information protection with respect to cloud security alliance (CSA). [5]

TABLE I. **Literature Survey**

S. No	Title of paper	Author Name	Journal Name / Year of Publishing	Advantage	Dis-advantage
1.	Biometric Inspired Homomorphic Encryption Algorithm for Secured Cloud Computing	Yogesh Bala, Amita Malik	AISC, Vol. 652 2018	Encrypts the user information at run-time	Real test with distributed computing is not done
2.	Biometric Encryption in Cloud Computing: A Systematic Review	Mehreen Ansar, Muhammad Sheraz Arshad Malik, Mubeen Fatima, Sadaf Aslam, Anum Rasheed, Iqra Nazir	IJCSNS 2018	Execution and rendering micro payments to the corresponding developer	Need of Optimal matching algorithm selection is there
3.	AES block cipher implementations with AMBA-AHB interface	Paola Ceminari, Ariel Arelovich, Mart´ın Di Federico	IEEE, 2017	Usage of multi model authentication with one biometric technique	Use of scheme with more than one biometric technique is not there
4.	Multimodal biometric system: A review	Waleed Dahea, HS Fadewar	IJRAET Vol. 4, 2018	Using biometrics for the edge centric cloud	Generation of the secret key to enhance the security is required
5.	Cognitive Systems for Service Management in Cloud Computing	Urszula Ogiela, Makoto Takizawa, Lidia Ogiela	IEEE, 2018	Manage strategic information	Semantic interpretation of personal traits using non standard bio metric specifications is needed

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

System architecture

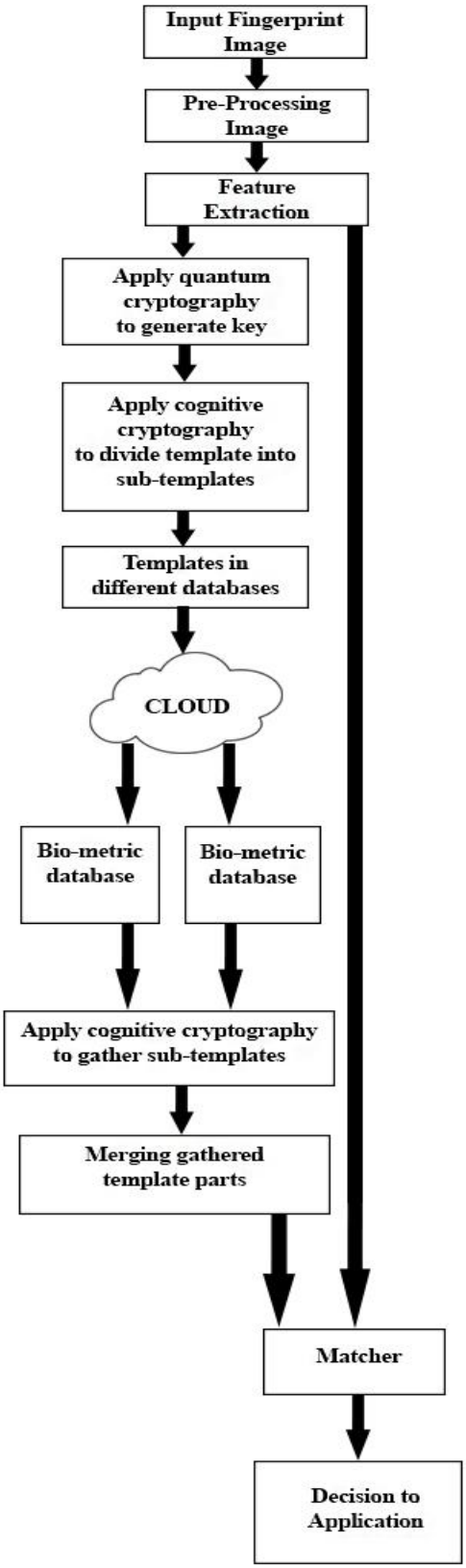

Fig. 1: Overview of System Architecture

III. MODULES

Pre-Processing Image

This module covers the biometric image pre-processing, which comprises of the following steps:

Conversion of RGB to gray-scale and Image Orientation: The input image is read from the graphics file. The image is resized using Bilinear interpolation to convert the image into a standard size. Let I(x, y) be a two dimensional gray-scale image. Fig. 2. refers the steps involved in the rotation process

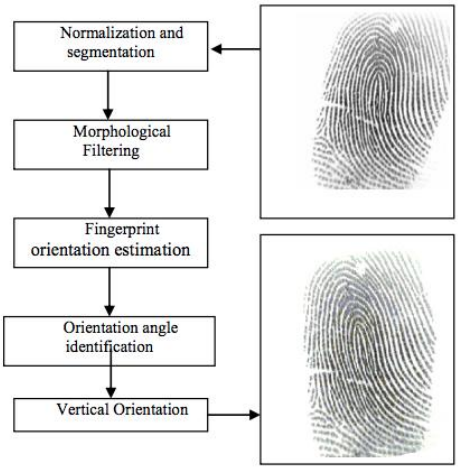

Fig. 2: Fingerprint rotation process

Normalization and Segmentation: The ridge region of input image is identified here. The image is segmented into blocks of size n x n and the standard deviation (STD) in each region is evaluated. If the standard deviation is greater than the threshold it is marked as part of the fingerprint. Then image is normalized to have zeroed mean, unit standard deviation before performing this step so that the threshold specified is relative to unit standard deviation. MASK image IM1 is obtained using equation (a), (b) and (c)

$$I(x,y)=I(x,y)-\text{mean}(I) \quad (a)$$

$$I(x,y)=I(x,y)/\text{STD}(I) \quad (b)$$

$$I_1(x,y)=RM+I(X,Y)*\text{SQRT}(RV) \quad (c)$$

Where, RM is the required mean and RV is the required variance.

Morphological Filtering: Morphological filtering is based on some mathematical morphology transformations. Here morphological closing is performed on the normalized and segmented gray-scale image I_{M1} to obtain the closed image, I_{M2}. The structuring element (SE) must be a single structuring object, rather than an array of objects. This fills the image regions and holes.

The dilation of a MASK image $I_{M1}(x, y)$ by a structuring element SE(m,n) is denoted by $I_{M2}(x, y)$.

$$I_{M2}(x,y)=D(I_{M1}, SE)(x,y)=\max\{I_{M1}(x-m, y-n)-SE(m,n)\} \quad (d)$$

Erosion of $I_{M2}(x, y)$ by a structuring element SE(m, n) is denoted by $I_{M3}(x, y)$

$$I_{M3}(x,y)=E(I_{M2}, SE)(x,y)=\min\{I_{M2}(x+m, y+n)-SE(m,n)\} \quad (e)$$

Orientation Estimation: Taking the MASK image as input, the orientation or the angle between the x-axis and the major axis of the ellipse bounding the MASK IM3 image that has the same second-moments as the region is calculated. Normalized second central moments of a pixel with unit length for the region 1/12 is calculated.

$$G_{XX} = \sum \frac{x^2}{N} + (1/12)$$

$$G_{YY} = \sum \frac{y^2}{N} + (1/12)$$

$$G_{XY} = \sum \frac{xy}{N} + (1/12)$$

If $G_{YY} = G_X$

$$Num = G_{YY} - G_{XX} + \sqrt{(G_{YY} - G_{XX})^2 + 4 \times G^2_{XY}}$$

$$Den = 2 \times G_{XY}$$

Else

$$Num = 2 \times G_{XY}$$

$$Den = G_{XX} - G_{YY} + \sqrt{(G_{XX} - G_{YY})^2 + 4 \times G^2_{XY}}$$

End

If $Num == 0 \& Den == 0$

Orientation =0

Else

$$Orientation = \frac{180}{\Pi} \times \tan^{-1} Num/Den$$

End.

If Orientation < 0

$$A = -(90 + Orientation)$$

Else

$$A = (90 - Orientation)$$

End

Core Detection: The proposed core detection algorithm is as follows.

- The thinned image obtained after filtering is transformed to a complement gray-scale image by replacing 0's with 255 and 1's with 0's.
- The local orientation of ridges is estimated and the region mask is applied. Because the orientation is calculated in radians it is now converted to degrees.
- For every 3x3 window the difference between the angles is obtained and the following conversion is made. Let D (k) is the angle of difference for the k^{th} element in the window k={1,2,3…8}.

If D (k) <= -pi/2

D (k) = D (k) + pi;

Else if abs (D (k)) < pi/2

D (k) = D (k);

Else

D (k) = pi ± D (k);

End

Obtain the sum of all difference values in the window.

- The core pixel is selected by considering all pixel locations, where the sum of all the differences is around 360, where a tolerance of ±3 is used. All candidate pixels close to each other are bridged together and only the centroid of this region is considered.
- Taking into consideration the thinned image around each core pixel, a 3x3 window and the pixels at each side of the window are taken as n1, n2, n3 and n4. The false core pixels are eliminated based on two conditions.

If (n1 & n3) > 0 & (n2 & n4) == 0

If (n2 & n4) > 0 & (n1 & n3) == 0

- On completion of detection of core point, region of interest is cropped from the image. For cropping of the region of interest, 'n' pixels around the core point are selected. Number of pixels around the core point 'n' is chosen to be 100-200 such that an adequate area around the core is considered

Feature Extraction

Biometrics is a combination of feature extractor, sensors and matching parts or modules, which implements recognition algorithms on particular biometric pattern. The sensor works by scanning the biometric trait and give output in digital form. The input fingerprint image is then converted to gray-scale from RGB, the blur effect is reduced, orientation is estimated and Ridge enhancement is done. The check and control is done to ensure that the output sample is reliable and safe for feature extraction and matching modules.

All this is done with the use of sensors to detect the biometric feature. Signal processing gives the clarity to the feature extracted. Matching the sample against a single stored template is called verification, and searching the sample against many stored templates in the database is called identification.

There are eight processing steps to the feature extraction process. These steps are: Pre-processing - The input image is made suitable for further processing by image enhancement techniques. Computation of Block Directions - Determination of primary ridge direction in each sub-region of an image is done.

Background / Foreground Segmentation - Identification of fingerprint area is done.

Extraction of Ridge- Extraction of ridge area within the foreground area is done. Removal of Blob- Elimination of non-elongated small structures is done. Thinning and Morphology- Here the ridges are thinned into one pixel wide skeletons.

Extraction of Minutia- Determine location and orientation of ridge bifurcations and ridge terminations. Block processing does the minutiae extraction process. Post-processing is performed on the minutiae extracted image to validate the minutiae. Post-processing -Elimination of extraneous minutia is performed.

Fig. 3: Input Image

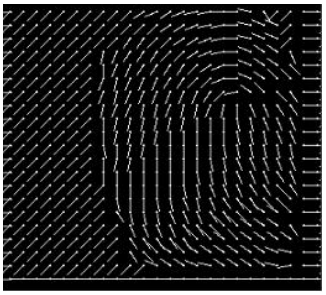

Fig. 4: Orientation Fields

Fig. 5: Ridges

Fig. 6: Thinned Image

Fig. 7: Minutia Features

Cryptographic Approach & Results

Here the hybrid of Cognitive and Quantum cryptographic approach is used.

Cognitive Cryptography: - The process is concerned with concealing data by distributing secret parts or shadows with the use of cognitive techniques. It is done by splitting and distributing the divided parts among selected groups of secret or concerned trustees for securing information. It's very innovative and useful tool for securing data.

Quantum Cryptography: - The Quantum Key Distribution is used for producing random key for communication between sender and a receiver. Key distribution assures no third party is involved. Quantum key Protocols communicate this key by using quantum channel.

Quantum key protocols or algorithms:

- BB84 :- In 1984 Charles Bennett and Gilles Brassard published the first QKD protocol. It is based on Heisenberg's Uncertainty Principle(HUP) and is simply known as the BB84 protocol after the authors names and the year in which it was published. It is one of the most prominent protocols and one could argue that all of the other HUP based protocols are essentially variants of the BB84 idea. The basic idea for all of these protocols is that Alice can transmit a random secret key to Bob by sending a string of photons where the secret key's bits are encoded by the polarization of photons. The HUP can be used to guarantee that an Eavesdropper cannot measure these photons and transmit them on to Bob without disturbing the photon's state in a detectable way thus revealing her presence.

Fig. 8. shows how a bit can be encoded in the polarization state of a photon in BB84. A binary is defined, 0 as a polarization of 0 degrees in the rectilinear bases or 45 degrees in the diagonal bases. Similarly the binary 1 can be 90 degrees in the rectilinear bases or 135 in diagonal bases. Thus a bit can be represented by polarizing the photon in either one of the bases.

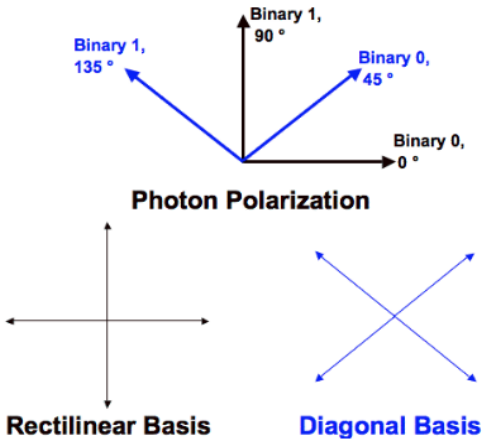

Fig. 8: BB84 encoding

In the first phase, Alice communicates with Bob over a quantum channel. Alice starts by choosing a random string of bits and for each bit, Alice randomly chooses a basis, rectilinear or diagonal, by which to encode the bit. She then transmits a photon for each bit with the corresponding polarization, as just described, to Bob. For every photon that Bob receives, he will measure the photon's polarization by a randomly chosen basis. If, for a particular photon, Bob had chosen the same basis as Alice, then in principle, Bob should measure the same polarization and thus he can correctly infer the bit that Alice intended to send. If he choses the wrong basis, his result, and thus the bit he will read, will be random.

In the second phase, Bob notifies Alice over any insecure channel what basis he used to measure each photon. Alice then reports back to Bob about whether he chose the correct basis for each photon. Now Alice and Bob discard the bits corresponding to the photons, which Bob measured with a different basis. Provided no errors have occurred or no one has manipulated the photons, Bob and Alice would now both have an identical string of bits, which is called a sifted key. Fig. 9. shows the bits Alice chose, the bases she encoded them in, the bases Bob used for measurement, and the resulting sifted key after Bob and Alice discarded their bits as just mentioned.

Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Fig. 9: Shifted Key

Before they finish, Alice and Bob agree on a random subset of the bits to compare to ensure consistency. If the bits are same, they are discarded and the remaining bits form the shared secret key. In the absence of noise or any other error, a disagreement in any of the bits would indicate the presence of an eavesdropper on the quantum channel.

This is because the eavesdropper, Eve, was attempting to determine the key, and she would have had no choice but to measure the photons sent by Alice before sending them to Bob. This is true since the no cloning theorem assures that she cannot replicate a particle of unknown state. Eve will not know what bases Alice used to encode the bit until after Alice and Bob discuss their measurements, and then Eve will be forced to guess. If she measures on the incorrect bases, the HUP ensures that the information encoded on the other bases is now lost. Thus when the photon will reach Bob, his measurement will now be random and he will read a bit incorrectly 50% of the time. Given that Eve will choose the measurement basis incorrectly on average of 50% of the time, 25% of Bob's measured bits will differ from Alice. If Eve has eavesdropped on all the bits then after n bit comparisons by Alice and Bob, they will reduce the probability so that Eve will go undetected to ¾^n. The chance at which an eavesdropper learned the secret is thus negligible if a sufficiently long sequence of the bits are compared.

- B92 :- In 1992, Charles Bennett proposed a simplified version of BB84 in his paper, "Quantum cryptography using any two non-orthogonal states". The only difference in B92 is that only two states are necessary rather than the possible 4 polarization states in BB84. As shown in Fig. 10. , 0 can be encoded as 0 degrees in the rectilinear basis and 1 can be encoded by 45 degrees in the diagonal basis. Like in the BB84, Alice transmits to Bob a string of photons encoded with randomly chosen bits but this time the bits Alice chooses decides which bases she must use. Bob will still randomly choose a basis to measure but if he chooses the wrong basis, he will not measure anything; a condition in quantum mechanics which is known as an erasure. Bob can simply tell Alice after each bit she sends whether or not he measured it correctly.

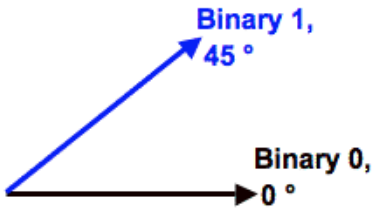

Fig. 10: B92-2 state encoding

Template Storage

Here the biometric template is stored in different cloud databases or different parts of the same database for future use. Cognitive Cryptography is again applied to gather the distributed parts of concerned database. In most of the large scale projects the biometric templates are captured on the client computer and then is sent to the server for storage on a central database. This will allow the users to gain access from multiple locations. Since all the biometric templates are stored only on the server, matching will happen only on the server itself. Thus it is important for the server to be accessible at all times in order for the system to function properly. The prefix "non" is not a word; it should be joined to the word it modifies, usually without a hyphen.

Merging, Pattern Matching & Decision Making

Here the gathered template parts are all merged together as one single template, this is called merging. Then it is closely matched to original template by using quantum secret key to avoid middleman attacks or data losses, this is called pattern matching. Decision-making is done by a computer program that decides whether the match is true or false and should the access be granted, and the result is given to the application. During the enrollment phase the biometric sample given by the user gets stored in the database, now when the user logs into his account that biometric template is compared with the template stored in the database and it gets a success on the basis of similarity points (P). P is the result of comparison between the extracted features and the features stored in the database.

If (P is low value) then there is Little similarity, and If (P is high value) then there is High similarity.

After that, the decision will be based on the similarity points (P), which is compared to a predefined threshold value (T).

If (P > T),
User is accepted
Else if (P < T),
User is rejected.

IV. CONCLUSION

This paper describes some possibilities of using behavioral and perceptional features in secure information management protocols executed in cloud and fog infrastructures. Personal characteristics can be extracted from motion sequences presenting unique movements, and can then be used in management procedures aimed at information sharing, encryption, and distribution. Besides simple body movements, security protocols can make use of visual abilities and perceptive skills. Perceptual or behavioral features can be extracted by cognitive-vision systems, which allow personal unique parameters to be evaluated in specific human actions. The main idea of applying the above features in cloud and fog service management processes stems from the secure authentication and verification procedures.

The universality of such protocols allows them to be used at different management levels, depending on the infrastructure and the available cloud resources. All simple processes can be realized at a lower level on personal workstations or at the middle level in the fog. They can be also performed at the highest level—in the cloud—using high-performance infrastructure. The low-level analysis is usually to secure procedures and the authorization aspects tied to particular services. At the high level, it is also possible to use personal, visual, or behavioral analyses dedicated to personal cryptographic solutions and verification procedures. Individuals with minor cognitive deficits may also expand the approach presented to allow its use. In such applications, it is necessary to source mainly personal features that do not change over time and are linked mainly to biometric patterns for security purposes.

It is allowed to use some independent features that can be acquired without specific physical skills and can change over time.

ACKNOWLEDGMENT

We thank Dr. T. R. Pachamuthu, Founder, Dr. R. Shivakumar, M.D., Ph.D., Chairman and Dr. V. Subbiah Bharathi, M.E., Ph.D., Dean, for their persistent endeavors towards education.

We extend our sincere thanks to Vice Principal - Admin and Head of the Department, Computer Science and Engineering, Dr. J. Jagadeesan, M.Tech., Ph.D., for the constant support.

It is indeed a pleasure to mention about Ms. P. Adlene Ebenezer, Assistant Professor, Computer Science and Engineering Department, project guide who has always been patient enough to solve the complexities of the project and relentlessly supported us throughout the project.

We thank all the teaching and non-teaching staff of Computer Science and Engineering department of SRM Institute of Science and Technology, Chennai, who provided us with the necessary resources for this project.

REFERENCES

1. Biometric Encryption in Cloud Computing: A Systematic Review, IJCSNS, Vol. 18, 2018
2. Cognitive and Biometric Approaches to Secure Service Management in Cloud-Based Technologies , IEEE, Cloud Computing 2018
3. An Efficient and Privacy - Preserving Biometric Identification Scheme in Cloud Computing, IEEE, 2018
4. Securing Mobile Cloud Computing using Biometric Authentication (SMCBA) , IEEE, 2014
5. Biometrics-as-a- Service: Cloud-Based Technology, Systems, and Applications, IEEE, 2018
6. https://researcher.watson.ibm.com/researcher/view_group_subpage.php?id=1922
7. Cognitive Systems for Service Management in Cloud Computing, IEEE, 2018
8. Secure sharing with cryptography in cloud computing, IEEE, 2013
9. Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in Cloud, IEEE, 2018
10. Cognitive cryptography techniques for intelligent information management, IJIM, 2018
11. https://ac.els-cdn.com/S1877050910003479/1-s2.0-S1877050910003479-main.pdf?_tid=2f4f2e19-4b3c-42c7-9dc1-fdb162d63315&acdnat=1552131611_0e01c2d7dc3319387f9f94607184145fhttp://www.touchngoid.com/store-fingerprint-template/
12. https://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/
13. https://www.bayometric.com/biometrics-secure-cloud-communication/
14. http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=97