International Journal of Advanced Trends in Engineering and Technology (IJATET)
Impact Factor: 5.965, ISSN (Online): 2456 - 4664
(www.dvpublication.com) Volume 3, Issue 1, 2018

A STUDY ON MULTIFACTOR AUTHENTICATION MODEL USING FINGERPRINT HASH CODE, PASSWORD AND OTP

K. Krishna Prasad* & P. S. Aithal**
* Research Scholar, College of Computer and Information Science, Srinivas University, Mangaluru, Karnataka
** College of Computer and Information Science, Srinivas University, Mangaluru, Karnataka

Cite This Article: K. Krishna Prasad & P. S. Aithal, "A Study on Multifactor Authentication Model Using Fingerprint Hash Code, Password and OTP", International Journal of Advanced Trends in Engineering and Technology, Volume 3, Issue 1, Page Number 1-11, 2018.

Abstract:

By definition, Authentication is using one or multiple mechanisms to show that you are who you claim to be. As soon as the identity of the human or machine is demonstrated, then human or machine is authorized to grant some services. The modern research study reveals that fingerprint is not so secured like secured a password which consists of alphanumeric characters, number and special characters. Fingerprints are left at crime places, on materials or at the door which is usually class of latent fingerprints. We cannot keep fingerprint as secure like rigid passwords. Using some modern technology with copper and graphite spray it's easy to mimic fingerprint image. Fingerprints are a half-secret if passwords are leaked or hacked, it easily revocable using another password. But in a biometric security system, which uses only biometric features, is not easy to change fingerprint key or fingerprint are static biometric, which never change much throughout the lifespan. Fingerprints are left at car, door or anyplace where every person goes and places his finger. Fingerprint Hash code is not used for full security or authentication purpose but it can be combined with other security elements like password or OTP in order to enhance security. In this paper, a novel method for Authentication is proposed by making use of Fingerprint Hash Code, Password, and OTP. In this study, we make use of Euclidean Distance to generate fingerprint Hash Code. Fingerprint Hash code is generated using MD5 Hash Function. The Model is implemented using MATLAB2015a. This paper also analyzes novel Authentication model used in this study with the aid of ABCD analysis.

Key Words: Authentication, Fingerprint Hash Code, MD5 Hash Function, OTP, Euclidean Distance & Multifactor Authentication Model.

1. Introduction:

Authentication is a process of identifying the registered or already known user to provide some services and to protect user information from an intruder. Three worldwide referred authentication process are Token supported authentication, Biometric supported authentication, and Knowledge supported authentication [1-2]. Token supported authentication makes use of key cards, bank cards, and smart cards. Token supported authentication system sometimes uses knowledge supported techniques to improve security. Biometric supported authentication strategies, together with fingerprints, iris scan and facial reputation aren't yet extensively adopted. The essential flaws of this technique are that such systems can be costly, and the identification process may be slow and regularly unreliable. However, this form of technique presents the highest level of protection. Knowledge supported authentication is most commonly and widely used authentication technique and encompass both text-based and image-based passwords. The image-based techniques can be further subdivided into two classes: recognition-primarily based and recall based graphical techniques. The use of recognition based strategies, a person is provided with a set of images and the user is authenticated through recognizing and identifying the images, which is registered at the time of registration process. In recall based techniques it's essential that user has to reproduce something like a pattern, which is created or drawn at the time of registration process.

Automatic Fingerprint Identification System (AFIS) consists of different techniques like preprocessing, enhancement, segmentation, thinning, feature extraction, post-processing, minutiae orientation and alignment [3-10]. Fingerprint Hash code acts as the key, which can uniquely identify every person. So it can be replaceable with user-id or username and can work along with text-based or picture based or pattern based passwords. The fingerprint hash code is not constant with biometric sensors or readers. There are many types of research are carried out translation and rotation invariant fingerprint hash code generation but even small or pixel changes cause difference in Hash code [11]. Based on the different Methods of Fingerprint Hash code generation, it reveals that fingerprint hash code does not suit exclusively for authentication or security purpose. But it uniquely identifies an individual person or human being through a Hash code key.

In this study, we calculate Euclidean distance for a binary fingerprint image, which is a straight line distance from a pixel with value zero to the pixel with value non-zero, which is one in a binary image using Euclidean norm [10]. The Euclidean distance is calculated for all the pixels of the binary fingerprint image. The two points, k and l in two-dimensional Euclidean spaces and k with the coordinates (k1, k2), l with the coordinates (l1, l2). The line segment with the endpoints of k and l will form the hypotenuse of a right-angled

triangle. The space among factors k and l is defined as the square root of the sum of the squares of the differences among the corresponding coordinates of the points. In a two-dimensional Euclidean geometry Euclidean distance between two points k = (kx, ky) and l = (lx, ly) is given as follows [10].

$$d(k, l) = \sqrt{(lx - kx)^2 + (ly - ky)^2}$$

For example consider a 3×3 sized matrix with values as follows [10].

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

The Euclidean distance for each point is calculated as follows [10].

$$\begin{bmatrix} 1.4142 & 1.0000 & 1.4142 \\ 1.0000 & 0 & 1.0000 \\ 1.4142 & 1.0000 & 1.4142 \end{bmatrix}$$

The most natural or common matrix for finding distance matrix in the binary image is Euclidean distance [12-14]. Due to the lack of efficient algorithms in the field of Euclidean distance led to the development of many types of research in this field in order to define, elaborate and also to use some other methods to find the distance using other methods like the city block, chessboard or chamfer [14-16]. The Euclidean distance transform is global operation and the calculation of Euclidean distance is most common and simple operation and amount of calculation required is always directly proportional to the size of the entire image because this is calculated for every pixel.

This paper has nine sections. Section 1 describes introductory theory related to fingerprint, Hash code and Euclidean distance matrices. Section 2 explains about brief literature review of Multifactor Authentication Model developed by many researchers. This also covers brief theoretical aspects Biometrics, Password, One Time Password (OTP) and Token. Section 3 narrates Objective and methodologies of fingerprint Hash code generation using Euclidean distance. Section 4 describes algorithm of Fingerprint Hash code generation using Euclidean distance. This section also lists workflow of Fingerprint Hash code generation and MD5 Hash function procedure. Section 5 explains the Multifactor Authentication Model using Fingerprint Hash code along with dataflow diagram. Section 6 depicts how One Time Password can be generated. This section explains the OTP generation concept using algorithm. Section 7 explains Results and Discussions of Multifactor Authentication Model. Section 8 makes analysis of Multifactor Authentication Model used in this study using ABCD analysis. Section 9 concludes the paper.

2. Related Study:

Usually, in the literature, there is three universally recognized or accepted method of authentication, which is already known (for example password) or what is known, what you possess (For example token or ATM card), what you are throughout a lifetime or lifelong (For example Biometrics). Brainard et al., (2006) [17] proposed, one of the modern types of authentication is through somebody user knows, which is mainly based on the concept of confirmation. If more than one factor are used for authentication, which gives more security and is referred as Two-factor authentication. Two-factor authentication can be by combining any of the two factors which is mentioned above like password and One Time Password (OTP) or Password and Biometrics. Usually ATM makes use of two factor authentication model as ATM and Personal Identification Number (PIN).

Passwords alone are recognized to be one of the simplest goals of hackers. Therefore, most companies are looking for greater rigid strategies to defend or secure their clients and users. Biometrics are regarded to be very secure and are used in special organizations, however, they are not frequently used in online transactions or ATM, due to high cost required for hardware. As an alternative, banks and corporations are making use of tokens as a mean of two-factor authentication.

A security token is used for the purpose of authentication and to provide some services to the user and is usually physical device and sometimes also referred as the cryptographic token. Token usually comes in two forms which are software token and hardware token. Hardware tokens are small gadgets which are small and may be easily portable. Some of those tokens having hash or cryptographic keys or biometric data, at the same time as others display a PIN that changes with time. At any precise time a consumer or user desires to log-in, i.e. authenticate, he makes use of the PIN displayed at the token further to his regular account password. Software program tokens are programs that run on computers and offer a PIN that also changes with time. Such programs put in force a One Time Password (OTP).

OTP algorithms are very important in employing security of the underlying system because unauthorized user or intruder cannot able to guess or find the next password in the sequence. The collection must be random to the most feasible extent, unpredictable, and irreversible. Elements that can be utilized in OTP generation consist of names, time, seed, random numbers etc.

Bemmel, V., & Mian, S. (2009) US patent states that a biometric identification method is used at a point of sale counter with a system and a method is provided for authorizing payment through customer mobile phone [18]. Aloul, F. et al., (2009) [19] explains that two-factor authorization gives more security for mobile-

based financial transactions other than usual username and password, by utilization biometric identification mechanism. They develop One Time Password (OTP) which is valid for the only short duration of time which is generated based on IMEI number, IMSI number, username, hour, pin, minute etc and can be effectively used for online banking, ATM or mobile banking services. Jakobsson, M. et al., (2009) [20], introduced a new concept implicit authentication which is based on some actions carried out by the mobile user. They developed a model to implement implicit authentication and their preliminary investigation found that the approach is meaningful for usability or security purposes.

Angulo, J., & Wästlund, E. (2011) studied a lock pattern dynamics as a secure and user-friendly two-factor authentication method for giving security to user mobile phone's private and secret information. They modeled this on the Android mobile phone based on user lock pattern and used Random Forest machine learning classifier and achieved an average Equal Error Rate (EER) of approximately 10.39% [21]. Delac, K., & Grgic, M. (2004, June) [22] surveyed different biometric recognition methods and found that unimodal biometrics more vulnerable to attacks compare to multimodal biometrics. Biometric recognition system provides a consistent personal identification schema either to confirm or decide the distinctiveness of a person, which can be effectively used on any computer or mobile systems. Seo, H. et al., (2012) [23] proposes a very special method of biometrics for intelligent mobile devices for which existing physical and behavioral biometrics are unsuitable, by analyzing users input patterns. They found using an empirical method that the new method identifies the user with 100% efficiency.

De Marsico, et al., (2014) [24] suggested a new method of biometrics for mobile engagement, using face and iris recognition, multimodal biometrics referred as "FIRME" which is specially designed and embedded in mobile devices using the Android operating system. Both design and implementation of face and iris are considered as a separate module, whose flow of work separate and finally two modules are fused. They claim that this multimodal authentication can be effectively used to find the identity of the user. Kumar, D., & Ryu, Y. (2009) [25] surveyed biometric payment system used for various kinds of payment systems, in contrast to username and password no need of remembering anything. They also suggest in their study that when more and more customer uses the biometric system, cost of biometric reader will decrease and even small business firms also can use biometric systems [26-27].

Yoo, J. H. et al., (2007, December) [28] describes the design of an embedded biometric system that authenticates the person by using face-fingerprint or iris-fingerprint multimodal biometrics technology which is a new system compared to an existing embedded system that time. The existing embedded system had problems like low computational resource and memory space. They implemented the system and also found execution time and also found the equal error rate for face, iris, and fingerprint as 1.50%, 1.68%, and 4.53% respectively. Xi, K., & Hu, J. (2009, June) [29] proposed a new fingerprint fuzzy vault based on multiple or composite features which are effective, reliable, distortion tolerant and registration free. They modeled and tested their results on the public database and found that the new schema can improve verification performance considerably.

3. Objective of the Study:

Literature review reveals that there are already many studies are made on Multifactor Authentication Model. But this study focuses on Multifactor authentication model by making use of Fingerprint Hash code, Password, and OTP. Fingerprint alone not gives full security, in order to improve the security of the system fingerprint acts one factor along with OTP, password, or any other biometric psychological or behavioral traits. The main objectives of this study are given below.

- ✓ To propose an alternative approach for User Authentication using Multifactor, which includes, Fingerprint Hash code, Password and time synchronized One Time Password (OTP).
- ✓ To analyze the new model using ABCD analysis

Figure 1 explains the methodology used in this research work to generate Fingerprint Hash code. Here initially FVC ongoing 2002 benchmark dataset is considered for testing the hash code. The benchmark dataset image is binarised and Euclidean distance of the image is calculated for each pixel. The distinct values of the Euclidean distance matrices values are considered and 32-bit length hash code is generated. Distinct Euclidean distance value summation, mean value and standard deviation values are considered for generating Hash code.

4. Algorithm of Hash Code Generation Using Euclidean Distance:

This section explains step by step procedure to develop Hash code by making use of Euclidean distance matrix on a binary fingerprint image. The steps of the algorithm are explained below. The algorithm also shows the pseudo code [10].

Step 1: Input Grayscale fingerprint image
read (input_image)
Step 2: Convert input image into 256 × 256 sized two-dimensional image
resized_image = image_resize (input_image, [256, 256])
Step 3: Convert 256 × 256 sized grayscale image into binary image
binary_image = convert_to_binary(resized_image)

Step 4: Perform One's complement of the binary_image
Binary_image = One's complement(binary_image)
Step 5: Find the Euclidean distance of the image
euclidean_image = Euclidean_distance(binary_image)
Step 6: Find the distinct value of the Euclidean distance
distinct_eucllidean_value = distinct_value(euclidean_image)
Step 7: Find the distinct value summation
For i=1 to size(distinct_eucllidean_value)
euclidean_sum = distinct_eucllidean_value (i)
end for
Step 8: Find the mean of the distinct Euclidean value
euclidean_mean = mean(distinct_eucllidean_value)
Step 9: Find the standard deviation of the distinct Euclidean value
std_deviation = standard_deviation(distinct_eucllidean_value)
Step 10: Combine the value of Step-7, Step-8, and Step-9
combine_value = combine(euclidean_sum, euclidean_mean, std_deviation)
Step 11: Pass the value of Step-10 as parameter for MD5 Hash function
hash_value = MD5_DataHash(combine_value)

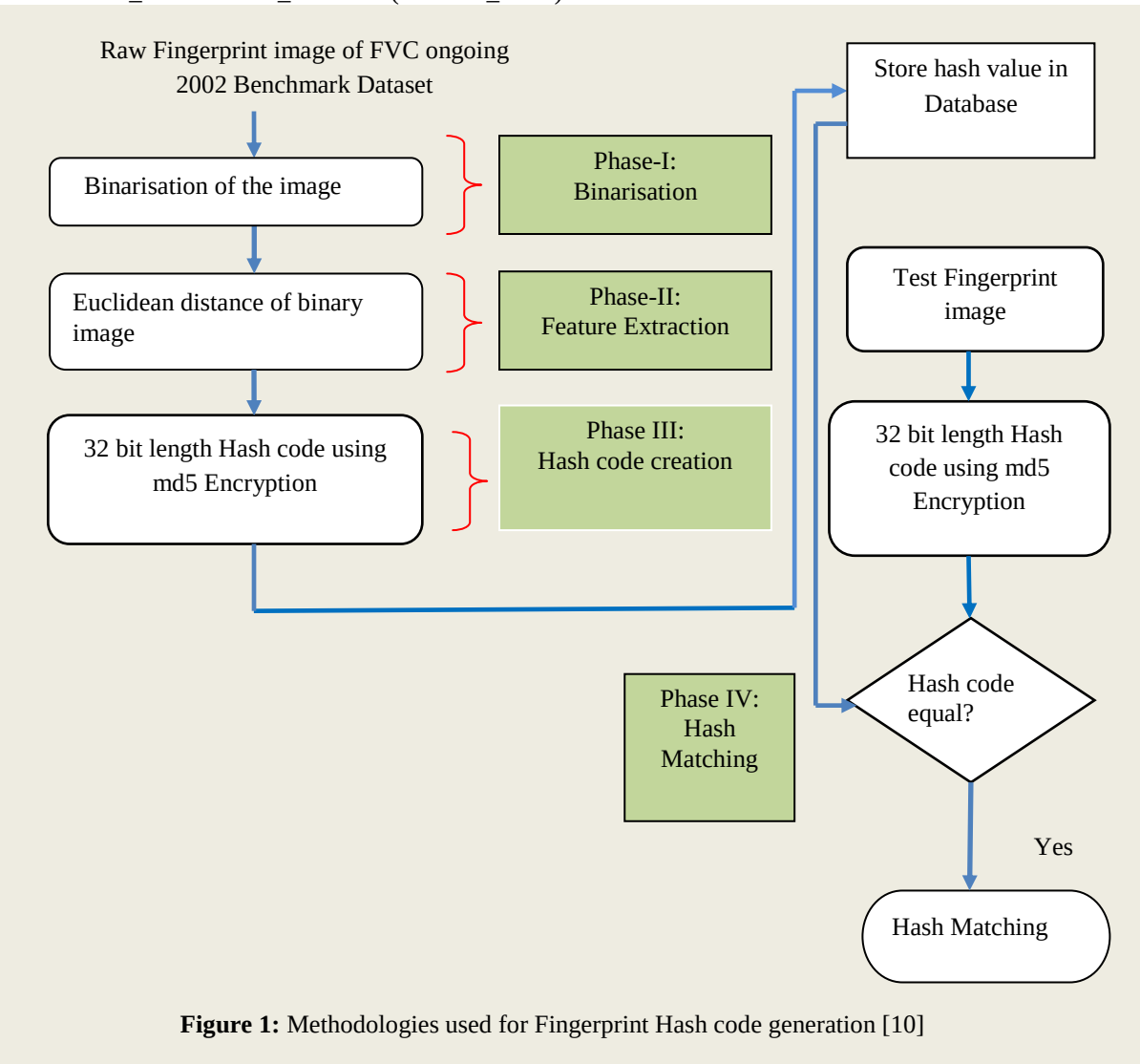

Figure 1: Methodologies used for Fingerprint Hash code generation [10]

The different process or work flow are listed below. With an intension to make the MD5 Hashcode more robust and to get the advantage of salting Euclidean distance sum, mean, and standard deviation are combined and passed to the MD5 algorithm [10].

- ✓ Converting input image to 256 × 256 sized grayscale image
- ✓ Converting to binary image
- ✓ Finding ones complement of binary image

- ✓ Finding Euclidean distance
- ✓ Finding distinct value of the Euclidean distance
- ✓ Finding the sum of the distinct Euclidean distance
- ✓ Finding the mean of the distinct Euclidean distance
- ✓ Finding the standard deviation of the distinct Euclidean distance
- ✓ Generating MD5 Hash code using combined sum, mean, and standard deviation of distinct Euclidean distance value

The process of the MD5 algorithm is disused below.

Input: Extracted Features
Output: Hash Code
Step-1: Attach the padded bits
Step-2: Append the length of the initial input to the result of the previous step-1
Step-3: Initialize MD buffer as A, B, C, D.
A four-word buffer (A, B, C, D) was used to evaluate the message digest. Here each of A, B, C, D is a 32- bit register
Step-4: Process message in 16-word blocks
Step-5: Finally, we get the 32-bit Hash code as output

5. Multifactor Authentication Model Using Fingerprint Hash Code, OTP, and Password:

Figure 2 shows Dataflow Diagram of Multifactor Authentication model used in this study. Initially on the client side using an interface user loads fingerprint image into the system. First, using Euclidean distance fingerprint image features are extracted, which is explained in Section 3 and 4. These features are encrypted and sent to the server. As soon as these features arrive at a server in encrypted form, the server receives that and request for One Time Password from OTP generator. OTP generator is a module or function, which is located at server machine. Time synchronized OTP is sent to the registered mobile phone user. Client system prompts a message to enter OTP, which is received to the registered mobile phone of the user. The user enters that OTP through the client interface and this OTP is compared with server generated OTP at the server side. If OTP is verified, server requests for the password, the user enters the password through a client-side interface and entered password reaches to the server. The server verifies the user entered a password with the already stored password in its database. Since database password is stored in encrypted format. The password which is stored in the database in encrypted form and finger user-id hash code is encrypted one again to enhance security.

So if an intruder gets stored hash codes from the database, still authentication cannot become successful. If both password and Fingerprint Hash code match them user is considered as an authenticated user. In other words authentication process successfully completes when OTP, Password, and Fingerprint Hash code matches. If anyone out of Fingerprint Hash code or Password does not matches user is considered an unauthorized user. If OTP not matches then the user is blocked from further steps in the authentication process. In this research study, this is not implemented as server and client in different machines. The model of this approach is implemented on the same machine using MATLAB 2015a.

6. One Time Password Generator:

In this research work, One Time Password Generator is responsible for generating OTP. This is a function located on the server. In this study, Time synchronized OTP is generated by combining some features. The time for which OTP is valid is administrative specific, for simplicity we consider in this work as 2 minutes. The algorithm for generating OTP is explained below.

Algorithm:

Step-1: Generate the Hash code for input fingerprint using MD5 Hash Function.
Step-2: Extract system Date and Time.
Step-3: Extract seconds separately.
Step-4: Consider only integer part of the seconds.
Step-5: A 4 × 4 sized matrices of the random number is generated.
Step-6: Date and Time are converted into string data type.
Step-7: Random matrix is concatenated with Date and Time string.
Step-8: Hash code of the input fingerprint image is concatenated with result of Step-7.
Step-9: Hash code is generated for combined string obtained from Step-8.
Step-10: A random number is generated between1 to 32.
Step-11: If the random number is in between 1 to 8 (including both) then extracts first 8 characters of the Hash code of size 32 characters generated in Step-8.
Step-12: If the random number is in between 9 to 16 (including both) then extract next 8 characters (from position 9 to 16) of the Hash code of size 32 characters generated in Step-8.
Step-13: If the random number is in between 17 to 24 (including both) then extract next 8 characters (from position 17 to 24) of the Hash code of size 32 characters generated in Step-8.

Step 14: If the random number is in between 24 to 32 (including both) then extract next 8 characters (from position 24 to 32) of the Hash code of size 32 characters generated in Step-8.

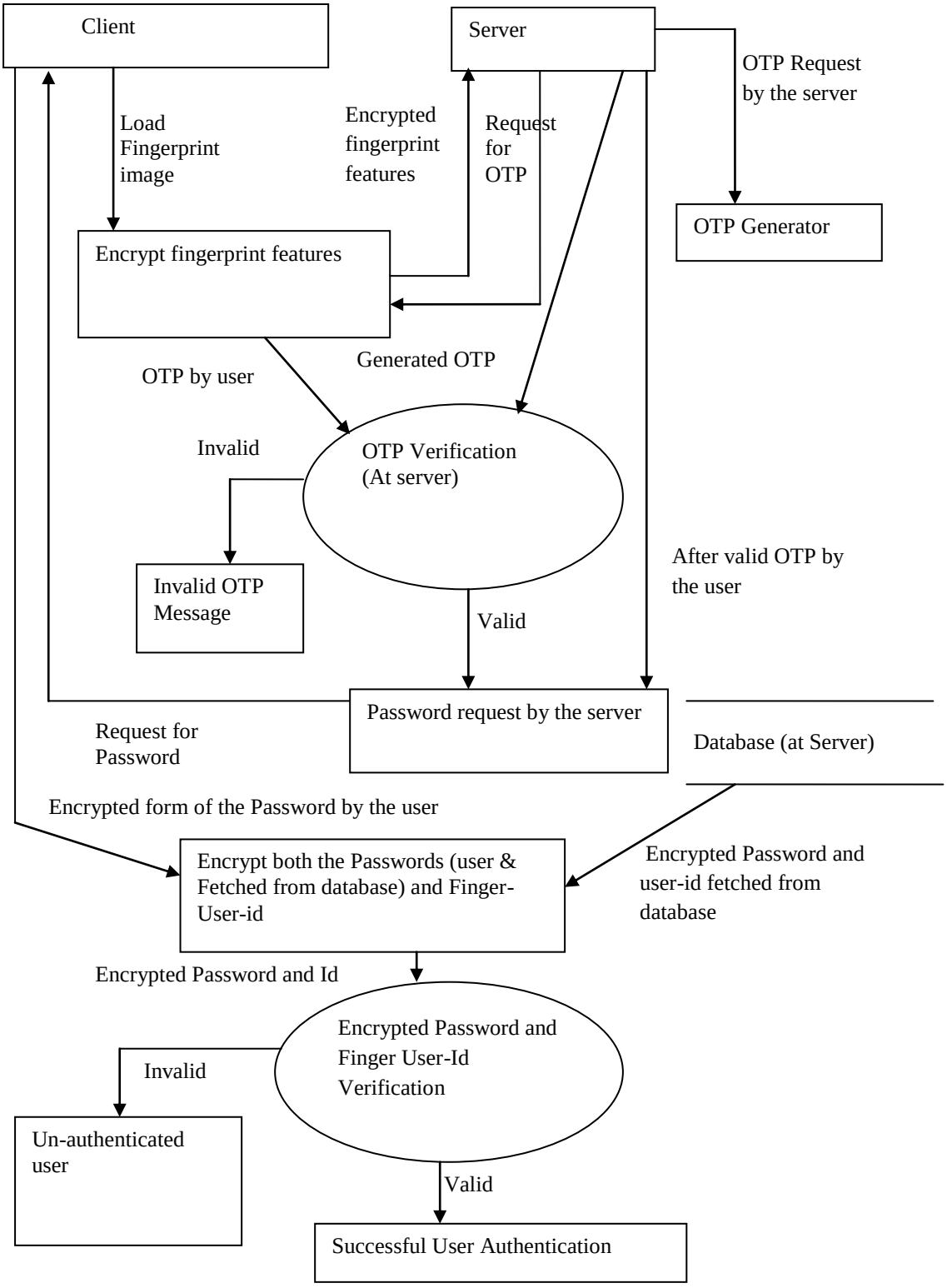

Figure 2**:** Dataflow Diagram of Proposed Multifactor Authentication

7. Results and Discussions:

In this research work, Multifactor Authentication model is not implemented as a client-server concept, but its model is implemented using MATLAB2015a. In order to extract the features of the fingerprint image,

Gabor filtering is utilized. Figure 3 shows screenshots of fingerprint feature extraction by utilizing segmentation process. This is treated as a client-side process. In client-side user fingerprint image is loaded into the system. Initially, an image is segmented and foreground region of the image is extracted from background region. Next fingerprint features are extracted. These features are converted into some double precision number using Gabor filtering. These values are encrypted and sent to the server for generating Hash code. Server-side processing includes Hash generation, OTP generation, OTP verification, Password Verification, and Fingerprint Hash verification. As soon as server receives fingerprint features in encrypted form, the server decrypts it and generates Hash code. This Hash code is used to generate OTP along with some other details. Figure 4 shows input dialog box for OTP.

As soon as Client receives the OTP, the user enters OTP through client interface and it is passed to the server back for verification, If OTP matches, server prompts a password for a client, and the user enters the password. Figure 5 shows the password message.

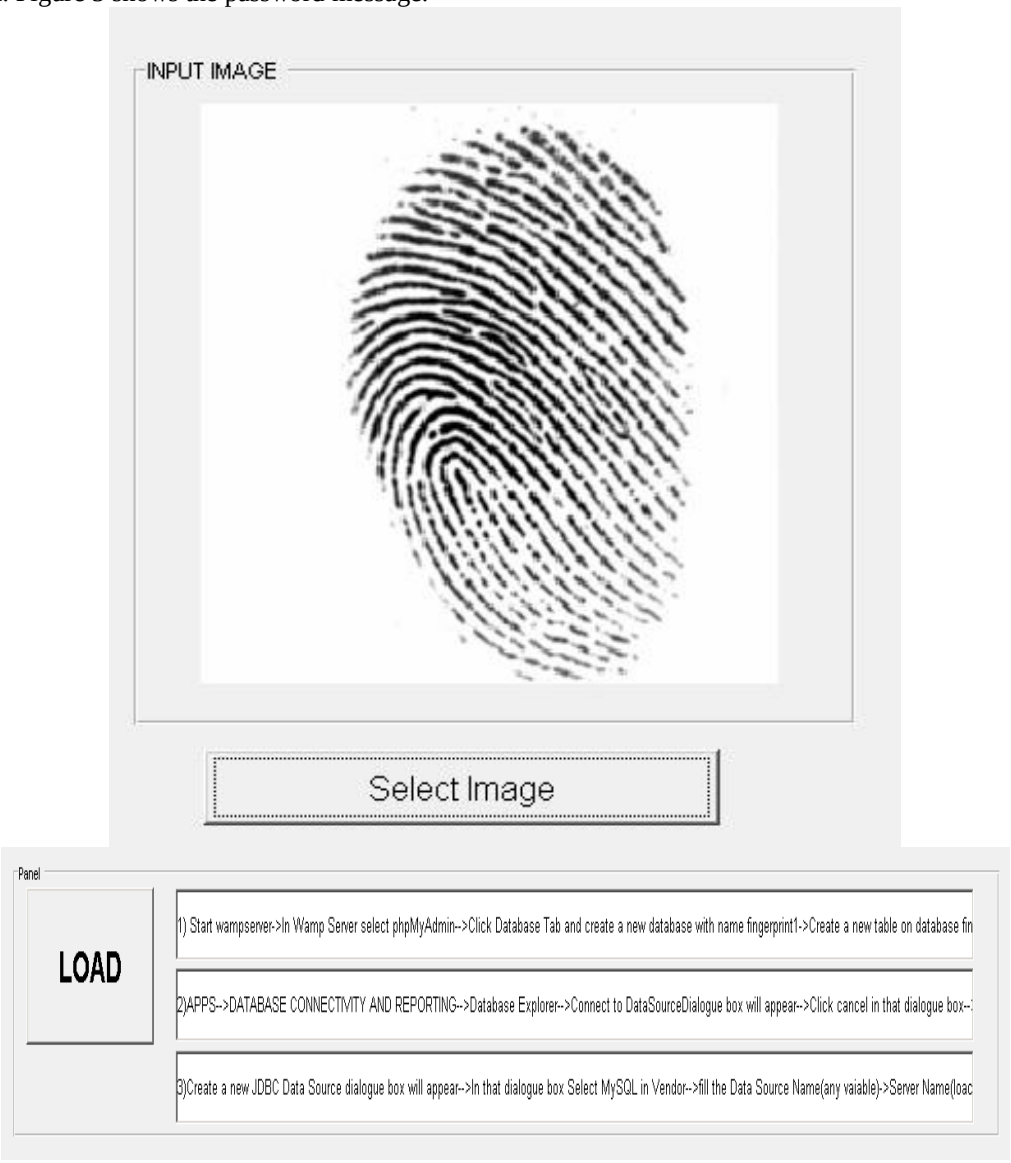

Figure 3: Screenshots of fingerprint feature extraction using segmentation Process (Client-side processing)

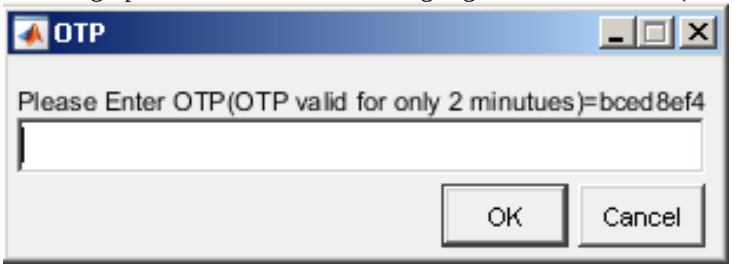

Figure 4: Screenshots of OTP with 2-Minutes of lifespan

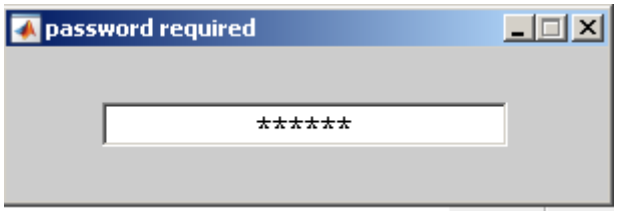

Figure 5: Screenshots of Password

Once user entered password reaches the server, the server verifies the password with database and if verification becomes a successful user is authenticated. Figure 6 shows the status of authentication.

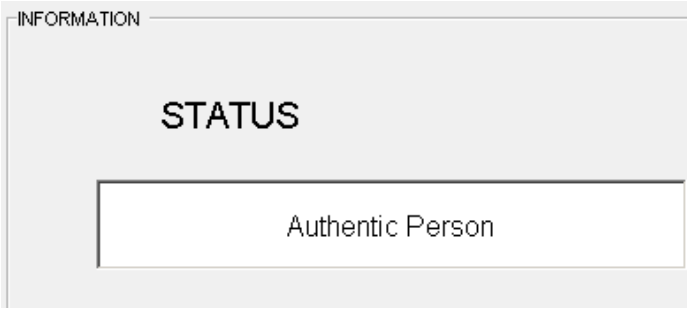

Figure 6: Screenshots of Status used in Multifactor Authentication Model

Table 1 shows screenshots of database values. Id represents the Hash value of the user fingerprint and hash column represents password. In the database, table password is stored in cryptographic Hash function. In the worst case, if an intruder hacks the database, he/she cannot understand password, because which is already stored in the Hash form in the database.

Table 1: Fingerprint-id and Password (hash) stored in Database

Id	hash
6b0cb74f5f8773667bf633a232b7ed12	63e7c5b52f995c466de97c7e1b13c45a
a0e5550770d0b6f72ca7f0afc1d0509a	46aa16250c809e993ccde5d5cababe12
2b4e687bf015532ba5ec6a0403d90935	2bc98e659d9627bca74ef482a953af5d
f1a14a44898a2eb2272aa76fe4ed8295	176f93ff4c5bb289decdfc2d9f8297a2
3b5a17d8092dbf0b23f71c2031dc2161	6ee1bca71a01ebba0f63fd076402f14f
4fbfe255d3610c804092653f9b4f61f6	5c98d6ca3f5d51048c98112cab8cb3b6
a542a749b79cfd482c4a45f4912f49ff	a843da9c81b63495736d1af10435227b
b8454d515e6f0a8893a5c97019e303ab	e2e638ac139b6da754e0a0e0533e65d7
c44837ccf2bf4903057c8b1678963fd5	1191e3745ad3aa05f405015cb4b88974
27f649b4d979e9b13ee5c412ab0d05a3	ebdd5c0b31050a546260fd849093f11d

8. ABCD Analysis of Multifactor Authentication Model:

Multifactor Authentication Model used in this research work can be analyzed using its predicted Advantages, Benefits, Constraints, and Disadvantages [30-50].

Advantages:

- ✓ Fingerprint Hash code used in Multifactor Authentication model acts as identity-key or index-key to uniquely identify individual persons.
- ✓ Fingerprint Hash code, combined with Password and OTP makes authentication process robust or highly secure.
- ✓ The fingerprint image is hashed through the double folded layer and salted enough.
- ✓ The modern study reveals that fingerprint images are not secret, not revocable but in this model, because fingerprint Hash code is used as index-key, securing of the fingerprint image is not essential.
- ✓ Changes in finger depending on weather condition or a cut or wound in finger does not affect the system performance in this model.
- ✓ Security details database table consist of only two fields as Fingerprint Hash-id and double folded encrypted password.
- ✓ The user Registered Mobile number is stored separately in another table. Fingerprint hash-id can be used to identify the user mobile number stored in the registration table.

Benefits:

- ✓ Multifactor Authentication Model can be effectively implemented in Internet banking and Mobile banking.
- ✓ This model does not require any fingerprint sensor device to capture user fingerprints. It uses a static image of the fingerprint.
- ✓ Cost and memory utilization is less compared to similar biometric fingerprint recognition systems

- ✓ Multifactor authentication model is effectively implemented in smart phones compared to any other platforms because smart phone already will be having one level of security through pattern lock or using password lock.
- ✓ In the worst case, if an intruder gets fingerprint image, it just acts as an identifier and not as security information. So intruder cannot break the system only with the fingerprint image.
- ✓ Even though fingerprint image cannot use solely in the authentication process, it can be protected in systems like laptop or desktop computer using login password.
- ✓ No need of remembering the User-id and Fingerprint Hash code just acts like email-id means even if public or intruder gets it, he/she cannot break the system.

Constraints:

- ✓ The user should remember the password and should not leak, or reveal to anyone, or write it on anywhere to protect it from the intruder or hacker.
- ✓ A password should be mixed with the number, alphanumeric characters or letters, Lower case and upper case letters, and special characters and the user should remember this.
- ✓ Lower mobile network coverage makes a denial to the system because of not getting the OTP in time.

Disadvantages:

- ✓ Biometric Fingerprint is less emphasized in verification or authentication process in Multifactor Authentication model.
- ✓ User cannot be verified or authenticated without remembering anything, at least password information user should carry along with him/her secretly
- ✓ Multifactor Authentication Model used in this study is not suitable for a system which does not utilize a mobile phone and computer like a biometric attendance system.
- ✓ Multifactor Authentication Model used in this study requires client-server architecture and not helpful for a standalone system.

9. Conclusion:

Authentication frameworks in light of multiple factors fingerprints have demonstrated to create low false acceptance rate and false rejection rate, alongside other favorable circumstances like simple and easy usage strategy. At the same time fingerprints are the half-secret if passwords are leaked or hacked, it easily revocable using another password. But in a biometric security system, which uses only biometric features, is not easy to change fingerprint key or fingerprint are static biometric, which never change much throughout the lifespan.

In this paper, we have discussed fingerprint Hash code generation using Euclidean distance. Fingerprint Hash code used in Multifactor Authentication model acts as identity-key or index-key to uniquely identify individual persons. Fingerprint Hash code, combined with Password and OTP makes authentication process robust or highly secure. The fingerprint image is hashed through the double folded layer and salted enough. Multifactor Authentication Model used in this study is not suitable for a system which does not utilize a mobile phone and computer like a biometric attendance system. Multifactor Authentication Model used in this study requires client-server architecture and not helpful for the standalone system.

10. References:

1. Parmar, H., Nainan, N., & Thaseen, S. (2012). Generation of secure one-time password based on image Authentication. Journal of Computer Science and Information Technology, 7, 195-206.
2. M'raihi, D., Bellare, M., Hoornaert, F., Naccache, D., & Ranen, O. (2005). Hotp: An hmac-based one-time password algorithm (No. RFC 4226).
3. Krishna Prasad, K. & Aithal, P.S. (2017). A Critical Study on Fingerprint Image Sensing and Acquisition Technology. International Journal of Case Studies in Business, IT and Education (IJCSBE), 1(2), 86-92. DOI: http://dx.doi.org/10.5281/zenodo.1130581.
4. Krishna Prasad, K. & Aithal, P.S. (2017). A Conceptual Study on Image Enhancement Techniques for Fingerprint Images. International Journal of Applied Engineering and Management Letters (IJAEML), 1(1), 63-72. DOI: http://dx.doi.org/10.5281/zenodo.831678.
5. Krishna Prasad, K. & Aithal, P.S. (2017). Literature Review on Fingerprint Level 1 and Level 2 Features Enhancement to Improve Quality of Image. International Journal of Management, Technology, and Social Sciences (IJMTS), 2(2), 8-19. DOI: http://dx.doi.org/10.5281/zenodo.835608.
6. Krishna Prasad, K. & Aithal, P.S. (2017). Fingerprint Image Segmentation: A Review of State of the Art Techniques. International Journal of Management, Technology, and Social Sciences (IJMTS), 2(2), 28-39. DOI: http://dx.doi.org/10.5281/zenodo.848191.
7. Krishna Prasad, K. & Aithal, P.S. (2017). A Novel Method to Contrast Dominating Gray Levels during Image contrast Adjustment using Modified Histogram Equalization. International Journal of Applied Engineering and Management Letters (IJAEML), 1(2), 27-39. DOI: http://dx.doi.org/10.5281/zenodo. 896653

8. Krishna Prasad, K. & Aithal, P.S. (2017).Two Dimensional Clipping Based Segmentation Algorithm for Grayscale Fingerprint Images. International Journal of Applied Engineering and Management Letters (IJAEML), 1(2), 51-65. DOI: http://dx.doi.org/10.5281/zenodo.1037627.
9. Krishna Prasad, K. & Aithal, P.S. (2017). A conceptual Study on Fingerprint Thinning Process based on Edge Prediction. International Journal of Applied Engineering and Management Letters (IJAEML), 1(2), 98-111. DOI: http://dx.doi.org/10.5281/zenodo.1067110
10. Krishna Prasad, K. & Aithal, P.S. (2017). A Study on Fingerprint Hash Code Generation Using Euclidean Distance for Identifying a User. International Journal of Management, Technology, and Social Sciences (IJMTS), 2(2), 116-126. DOI : http://doi.org/10.5281/zenodo.1133545
11. Tulyakov, S., Farooq, F., Mansukhani, P., & Govindaraju, V. (2007). Symmetric hash functions for secure fingerprint biometric systems. Pattern Recognition Letters, 28(16), 2427-2436.
12. Das, P. P., Chakrabarti, P. P., & Chatterji, B. N. (1987). Distance functions in digital geometry. Information Sciences, 42(2), 113-136.
13. Yamada, H. (1984). Complete Euclidean distance transformation by parallel operation. In Proc. of 7th Int. Conf. on Pattern Recognition, Montreal (Vol. 1, pp. 69-71).
14. Borgefors, G. (1986). Distance transformations in digital images. Computer vision, graphics, and image processing, 34(3), 344-371.
15. Danielsson, P. E. (1980). Euclidean distance mapping. Computer Graphics and image processing, 14(3), 227-248.
16. Yamashita, M., & Ibaraki, T. (1986). Distances defined by neighborhood sequences. Pattern Recognition, 19(3), 237-246.
17. Brainard, J., Juels, A., Rivest, R. L., Szydlo, M., & Yung, M. (2006, October). Fourth-factor authentication: somebody you know. In Proceedings of the 13th ACM conference on Computer and communications security (pp. 168-178). ACM.
18. Bemmel, V., & Mian, S. (2009). U.S. Patent No. 7,512,567. Washington, DC: U.S. Patent and Trademark Office.
19. Aloul, F. A., Zahidi, S., & El-Hajj, W. (2009, May). Two factor authentication using mobile phones. In AICCSA (pp. 641-644).
20. Jakobsson, M., Shi, E., Golle, P., & Chow, R. (2009, August). Implicit authentication for mobile devices. In Proceedings of the 4th USENIX conference on hot topics in security (pp. 9-9). USENIX Association.
21. Angulo, J., & Wästlund, E. (2011, September). Exploring touch-screen biometrics for user identification on smart phones. In IFIP Prime Life International Summer School on Privacy and Identity Management for Life (pp. 130-143). Springer Berlin Heidelberg.
22. Delac, K., & Grgic, M. (2004, June). A survey of biometric recognition methods. In Electronics in Marine, 2004. Proceedings Elmar 2004. 46th International Symposium (pp. 184-193). IEEE.
23. Seo, H., Kim, E., & Kim, H. K. (2012). A novel biometric identification based on a users input pattern analysis for intelligent mobile devices. International Journal of Advanced Robotic Systems, 9, 1-10.
24. De Marsico, M., Galdi, C., Nappi, M., & Riccio, D. (2014). FIRME: face and iris recognition for mobile engagement. Image and Vision Computing, 32(12), 1161-1172.
25. Kumar, D., & Ryu, Y. (2009). A brief introduction of biometrics and fingerprint payment technology. International Journal of advanced science and Technology, 4, 25-38.
26. Aithal, P. S. (2016). A Review on Advanced Security Solutions in Online Banking Models, International Journal of Scientific Research and Modern Education (IJSRME), 1(1), 421-429. DOI: http://doi.org/10.5281/zenodo.160971.
27. Aithal, P. S. (2015). Biometric Authenticated Security Solution to Online Financial Transactions. International Journal of Management, IT and Engineering (IJMIE), 5(7), 455-464, DOI: http://doi.org/10.5281/zenodo.268875.
28. Yoo, J. H., Ko, J. G., Chung, Y. S., Jung, S. U., Kim, K. H., Moon, K. Y., & Chung, K. (2007, December). Design of embedded multimodal biometric systems. In Signal-Image Technologies and Internet-Based System, 2007. SITIS'07. Third International IEEE Conference on (pp. 1058-1062). IEEE.
29. Xi, K., & Hu, J. (2009, June). Biometric mobile template protection: a composite feature based fingerprint fuzzy vault. In 2009 IEEE International Conference on Communications (pp. 1-5). IEEE.
30. Aithal, P. S., Shailashree, V. T., & Kumar, P. M. (2015). Application of ABCD Analysis Model for Black Ocean Strategy. International Journal of Applied Research, 1(10), 331-337. DOI: http://doi.org/10.5281/zenodo.163424.
31. Aithal, P. S. (2016). Study on ABCD analysis technique for business models, business strategies, operating concepts & business systems, International Journal in Management and Social Science, 4(1), 98-115. DOI: http://doi.org/10.5281/zenodo.161137.

32. Aithal, P. S., Shailashree, V. T., & Kumar, P. M. (2016). ABCD analysis of Stage Model in Higher Education. International Journal of Management, IT and Engineering, 6(1), 11-24. DOI: http://doi.org/10.5281/zenodo.154233.
33. Aithal, P. S., Shailashree, V. T, S., & Kumar, P. M. (2016). Analysis of ABC Model of Annual Research Productivity using ABCD Framework. International Journal of Current Research and Modern Education (IJCRME), 1(1), 846-858. DOI: http://doi.org/10.5281/zenodo.62022.
34. Aithal, P. S. (2017). ABCD Analysis of Recently Announced New Research Indices. International Journal of Management, Technology, and Social Sciences (IJMTS), 1(1), 65-76. DOI: http://doi.org/10.5281/zenodo.583644.
35. Varun Shenoy, & Aithal P. S., (2016). ABCD Analysis of On-line Campus Placement Model, IRA-International Journal of Management & Social Sciences (ISSN 2455-2267). Vol. 5, No. 2, pp. 227-244. DOI: http://dx.doi.org/10.21013/jmss.v5.n2.p3.
36. Aithal, P. S., and Shailashree, V. T., and Kumar, P. M. Suresh. (2016). Analysis of NAAC Accreditation System Using ABCD Framework. International Journal of Management, IT and Engineering, 6(1) 30-44. DOI: http://doi.org/10.5281/zenodo.154272.
37. Aithal, P. S., Shailashree, V. T., & Kumar, P. M. (2016). Application of ABCD Analysis Framework on Private University System in India. International Journal of Management Sciences and Business Research, 5(4), 159-170. DOI: http://doi.org/10.5281/zenodo.161111.
38. Aithal, P. S., Shailashree, V. T. & Suresh Kumar, P.M. (2016). The Study of New National Institutional Ranking System using ABCD Framework. International Journal of Current Research and Modern Education (IJCRME), 1(1), 389 – 402. DOI : http://doi.org/10.5281/zenodo.161077
39. Aithal, Shubhrajyotsna., & Aithal, P. S. (2016). ABCD analysis of Dye-doped Polymers for Photonic Applications. IRA-International Journal of Applied Sciences, 4(3), 358-378. DOI: http://doi.org/10.5281/zenodo.155103.
40. Architha Aithal, and Aithal, P. S., (2017). ABCD Analysis of Task Shifting – An optimum Alternative Solution to Professional Healthcare Personnel Shortage. International Journal of Health Sciences and Pharmacy (IJHSP), 1(2), 36-51. DOI: http://dx.doi.org/10.5281/zenodo.1038975.
41. Aithal, P. S., (2017). ABCD Analysis as Research Methodology in Company Case Studies. International Journal of Management, Technology, and Social Sciences (IJMTS), 2(2), 40-54. DOI: http://dx.doi.org/10.5281/zenodo.891621.
42. Aithal, P. S. (2017). Factor Analysis based on ABCD Framework on Recently Announced New Research Indices, International Journal of Management, Technology, and Social Sciences (IJMTS), 1(1), 82-94. DOI: http://dx.doi.org/10.5281/zenodo.584105.
43. Aithal, P. S., V.T. Shailashree, P. M. Suresh Kumar, (2015). A New ABCD Technique to Analyze Business Models & Concepts, International Journal of Management, IT and Engineering (IJMIE), 5(4), 409-423, DOI : http://doi.org/10.5281/zenodo.61652.
44. Aithal, P. S. & Suresh Kumar, P. M. (2016). CCE Approach through ABCD Analysis of 'Theory A' on Organizational Performance. International Journal of Current Research and Modern Education (IJCRME), 1(2), 169-185. DOI: http://dx.doi.org/10.5281/ZENODO.164704.
45. Aithal, P. S., Shailashree V. T. & Suresh Kumar P.M. (2016). Factors & Elemental Analysis of Six Thinking Hats Technique using ABCD Framework. International Journal of Advanced Trends in Engineering and Technology (IJATET), 1(1), 85-95. DOI: http://doi.org/10.5281/zenodo.240259.
46. Varun Shenoy & Aithal, P. S., (2017). Quantitative ABCD Analysis of IEDRA Model of Placement Determination. International Journal of Case Studies in Business, IT and Education (IJCSBE), 1(2), 103-113. DOI: http://dx.doi.org/10.5281/zenodo.1133691.
47. Aithal, P.S., (2015). Comparative Study on MBA Programmes in Private & Public Universities – A case study of MBA programme plan of Srinivas University. International Journal of Management Sciences and Business Research (IJMSBR), 4(12), 106-122. DOI: http://doi.org/10.5281/zenodo.163884.
48. Aithal P. S., and Suresh Kumar P. M., (2016). Analysis of Choice Based Credit System in Higher Education. International Journal of Engineering Research and Modern Education (IJERME), 1(1), 278-284. DOI: http://doi.org/10.5281/zenodo.161046.
49. Varun Shenoy and Aithal, P. S. (2016). Changing Approaches in Campus Placements - A new futuristic Model. International Journal of Scientific Research and Modern Education (IJSRME), 1(1), 766 – 776. DOI: http://doi.org/10.5281/zenodo.160966.
50. Aithal, P. S. & Shubhrajyotsna Aithal, (2016). A New Model for Commercialization of Nanotechnology Products and Services. International Journal of Computational Research and Development, 1(1), 84-93. DOI: http://doi.org/10.5281/zenodo.163536.