*International Journal of Applied and Advanced Scientific Research (IJAASR)*
*Impact Factor: 5.655, ISSN (Online): 2456 - 3080*
*(www.dvpublication.com) Volume 3, Issue 1, 2018*

# A COMPARATIVE STUDY ON FINGERPRINT HASH CODE, OTP AND PASSWORD BASED MULTIFACTOR AUTHENTICATION MODEL WITH AN IDEAL SYSTEM AND EXISTING SYSTEMS

**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 Comparative Study on Fingerprint Hash Code, OTP and Password Based Multifactor Authentication Model With an Ideal System and Existing Systems”, International Journal of Applied and Advanced Scientific Research, Volume 3, Issue 1, Page Number 18-32, 2018.

**Abstract:**

Authentication is the process to validate the user identity and to grant some resources or services to the user. Authentication process uses many factors like password, biometrics, or One Time Password. Multifactor authentication model always gives higher security than single-factor authentication model. 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. Fingerprint Hash code acts as a 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. In this paper based on focus group interaction, first, we define an Ideal Authentication System. The Ideal Authentication System used in this study consists of different components like Ideal Security, Ideal User-Friendly, Ideal Input, Ideal Process, and Ideal Performance Evaluation Matrices. In this paper, we also compare new Multifactor Authentication Model based on Fingerprint Hash code, OTP, and Password with existing authentication systems. The traditional user-id, password-based internet/mobile banking system, Apple iPhone X face recognition system, HDFC OTP Checkout for online transactions and Indian Aadhaar card registration process are the different existing systems used in this study to compare with the new model.

**Key Words:** Authentication, Multifactor Authentication Model, Fingerprint Hash Code, OTP & Ideal Authentication System.

## 1. Introduction:

By definition, authentication is using one or multiple mechanisms to show that who you declare or 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. Three worldwide referred authentication process are (1) Token supported authentication, (2) Biometric supported authentication, and (3) Knowledge supported authentication.

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 [1-2]. 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.

One time password can be generated in two forms. (1) Time-synchronized OTP: In time-synchronized OTPs the person has to enter the password within a time frame or within a stipulated time, in other words, OTP having lifespan only for few amount of time after that time it will get expired and another OTP will be generated. (2) Counter-synchronized OTP: In Counter-synchronized OTP, instead of regenerating OTP after the stipulated time, a counter variable is coordinated or synchronized between client device and server.

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 a difference in Hash code [11-14]. 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.

A service model or system called ideal system, when that must have the following characteristics [15]:

- ✓ An ideal model / system should capable of incorporating changes in services, or inclusion / deletion / updating of new / old services without affecting its overall framework or performance.
- ✓ Postulation made in the model / system should be minimal.
- ✓ The service should be accessible all time 24×7 basis, around the year 365 days.
- ✓ The user interface should be simple, user-friendly and highly explanatory.
- ✓ The response time should be very good.
- ✓ The error rate should be zero or nullified.
- ✓ Security should be very high or unauthorized access or use data by the unregistered user should be prevented.

In this paper, we discuss an ideal Multifactor Authentication System which is finest in terms of all its characteristics or fulfils every aspects or need of all its stakeholders. Multifactor Authentication Model is an advanced technology to protect user and user credentials from an intruder in the highly secured way. The paper is discussed in six sections. Section 1 describes introductory theory about fingerprint biometrics, Hash code, and Ideal system. Section 2 explains about an Ideal system. Section 3 describes Ideal Authentication Model. Section 4 describes Multifactor Authentication Model based on Fingerprint Hash code, OTP, and Password. Section 5 makes a comparison of new Multifactor Authentication Model with different existing Authentication systems. Section 6 concludes the paper with findings of the comparative study.

## 2. An Ideal System:

It is well known that we can improve the performance of any system by comparing it with a hypothetical, predicted system of that kind called Ideal system [15]. The word Ideal system refers to the system which has utmost characteristics, which cannot be improved further. It is what our mind tells ultimate and which reached the pinnacle of success in the respective field, which can be compared to all other systems of similar type, which lacks in some qualities [16]. The less-efficient system can be converted into the ideal system with the aid of research and continuous innovation in that field. Many objects we can consider as ideals like an ideal gas, ideal fluid, ideal engine, ideal switch, ideal voltage source, ideal current source, ideal semiconductor and ideal communication technology and all of these are considered as standards to improve the quality and performance of similar type. Recently many ideal systems are studied, which includes ideal technology system [15], ideal business system [16], ideal education system [17-20], ideal strategy [21], ideal energy source [22], ideal library system [23], ideal banking system [24-25], and ideal mobile banking system [29]. The ideal system of any kind can be placed in mind, while improving the characteristics of practical devices/ systems and reach ideal system or considered to be a pinnacle of success [15-29].

## 3. Ideal Authentication System:

Ideal Authentication System is a system which has properties like highly user-friendly, ubiquitous services, always available, very cheaper and 100% efficient in all aspects. An ideal or error-free biometric system should make an accurate and correct decision on every test sample regardless of any performance degrading factors like variation or differences in inter-class, similarities in intra-class, different representation for enrolled and sample data, and extreme noise and low sample data quality. Some of the ideal systems with respect to Authentication System are listed in Table 1.

Table 1: List of Ideal components with respect to Authentication System

| S.No | Ideal System Components | Definition of Ideal Systems/Components |
|---|---|---|
| 1 | Ideal Speed | The time is taken by the Automatic Verification or Authentication System to authenticate the registered user |
| 2 | Ideal Data Transfer Rate | Any amount of data can be transferred from source to destination without any delay or within null unit of time duration (In client Server Model) |
| 3 | Ideal Signalling efficiency | The quality of the signal is 100% efficient in all aspects. |
| 4 | Ideal Security | 100% protection of Registered user means no intruder can able to break the system anyway. |
| 5 | Ideal Availability | Service can be available any part of the world anytime. |
| 6 | Ideal Bandwidth | The volume of Information per unit of time that a system can handle is unlimited or uncountable. |
| 7 | Ideal False Acceptance Rate | The percentage of system incorrectly classifies the input pattern to an unregistered user is zero. |
| 8 | Ideal False Rejection Rate | The probability that the Authentication framework unable to identify a match between the authentic people is always zero. |
| 9 | Ideal Equal Error Rate | Acceptance and rejection mistakes are identical in the system and which is equal to zero. |

| | | |
|---|---|---|
| 10 | Ideal Failure to Enroll Rate | The unsuccessful attempt made to enroll in database or template of an Automatic Fingerprint Identification System by the input is zero. |
| 11 | Ideal Accuracy Rate | Because of False Rejection Rate and False Acceptance Rate is zero, the accuracy of the system becomes high. |

As shown in Figure 1, we have proposed an Ideal Authentication Model, which consists of different components like Ideal Security, Ideal User-Friendly, Ideal Input, Ideal Process, and Ideal Performance Evaluation Matrices.

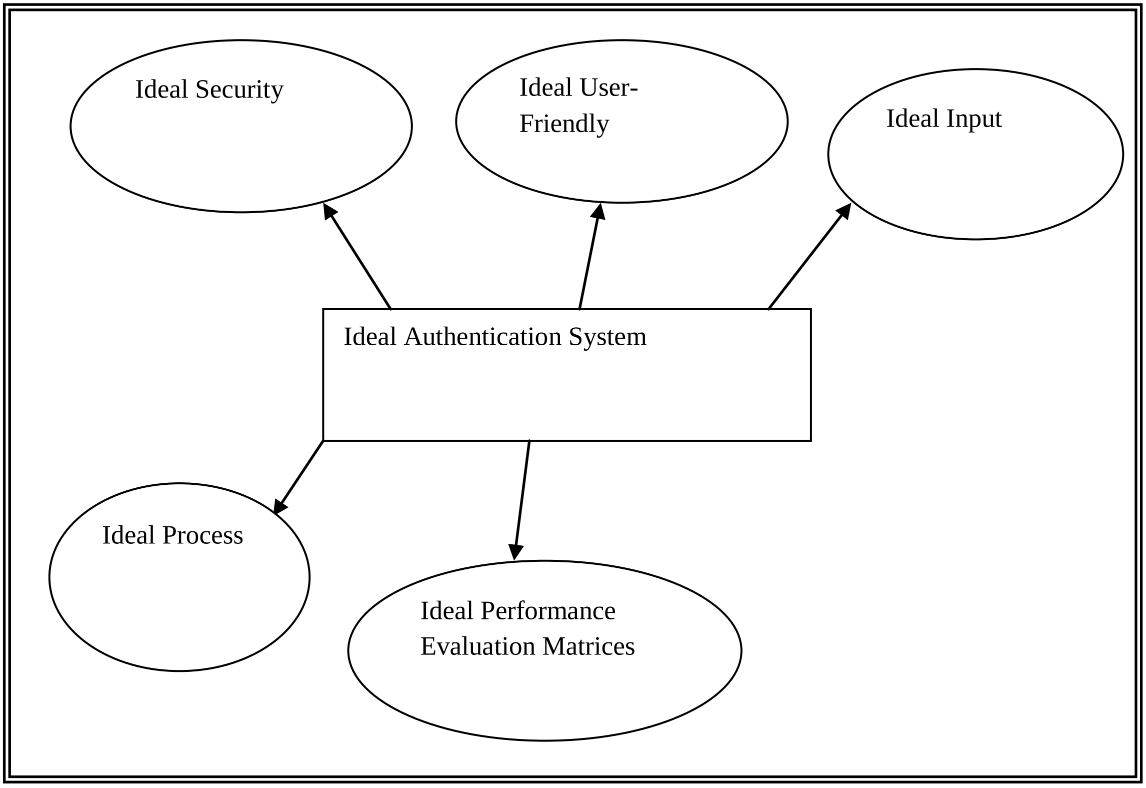
Ideal Security
Ideal User-Friendly
Ideal Input
Ideal Authentication System
Ideal Process
Ideal Performance Evaluation Matrices

Figure 1: Ideal Authentication System Model

**3.1 Ideal Security:** In Ideal Authentication System, Ideal Security refers a system, which is impossible for an intruder to break the system or impossible for the unregistered user to access the system. Ideal Security model improves or makes the system robust by maintaining security mechanism at various levels like user level, network level, template or database level. Security can be enhanced to maximum or optimal level by the use of multifactor authentication model. Table 2 shows Ideal security various components technologies and benefits.

Table 2: Description of various characteristics of Ideal Security

| S.No | Characteristics | Descriptions |
|---|---|---|
| 1 | High User level Security | Minimum data is remembered by the user for the authentication process. To realize this use Physiological or Behavioral biometrics |
| 2 | High Network level Security | Difficult to get original data or information.<br>Decrypting of the message by the unknown user becomes impossible. |
| 3 | Ideal Template level or Database level security | Non revertible template or impossible to get actual information. |
| 4 | Multifactor Authentication Security | Use more than one factor for authentication like Biometrics, One Time Password (OTP), and Password. |

**3.2 Ideal User-Friendly:** The goal of the ideal user-friendly component is that user should able to get access to the system effortless or easily without remembering anything or very minimum amount of data. Ideal user-friendly system should have some characteristics, which are listed in Table 3 to call itself as Ideal.

Table 3: Description of various characteristics of Ideal User-Friendly

| S.No | Characteristics | Description |
|---|---|---|
| 1 | High Response Time | User should get Authenticated as early as possible or with least amount of time |
| 2 | High Access Time | User should get access to the system with least amount of time |
| 3 | Automatic Process | User should able to get authenticated automatically without entering |

| | | |
|---|---|---|
| | | anything on the screen or just by standing infront of the system |
| 4 | High speed | The execution time for authentication should be very minimum |
| 5 | High Availability | Anytime, Anywhere, Anyplace or simply ubiquitously available |
| 6 | Effort free | The user should able to work with the system effortless or freely. |

**3.3 Ideal Input:** Ideal Input ensures that registered user should able to get access to the system or authenticated with very less or no input. In an Ideal Authentication system, the Ideal input having different characteristics, which are listed out in Table 4.

Table 4: Description of various characteristics of Ideal Input [Source: Aithal, P. S. & Pai T, Vaikunta [26])

| S.No | Characteristics | Description |
|---|---|---|
| 1 | Minimum possessions | Users will be carrying only one data or no data along with them to get authenticated |
| 2 | Minimum input | The number of data or instruction to the system is as minimum as possible |
| 3 | Input Selectivity | Select input data rather than remembering and entering |
| 4 | Ubiquitous Data | Anytime, Anywhere, and Anyplace able to input or feed data |
| 5 | Reliability | The input should not have any imperfections. It should not fail during execution |
| 6 | Usability | The input should have infinite usability for various applications. |
| 7 | Efficiency | The provided input should have 100% efficiency with an intention to get accurate results. |
| 8 | Input Security | The input should be protected from intruder |
| 9 | Short execution time | The input provided to the system should execute with a minimum amount of time. |

**3.4 Ideal Process:** In an Ideal Authentication system, Ideal process refers user should able to complete authentication process without any fault, fast and completely. The different characteristics, of the Ideal process, are listed out in Table 5.

Table 5: Description of various characteristics of Ideal Process

| S.No | Characteristics | Description |
|---|---|---|
| 1 | High Atomicity | The Authentication process should complete fast without any errors or should not abort in between if it has started. |
| 2 | Ideal Consistency | After the authentication process system should end up with the consistent state. |
| 3 | Maximum Isolation | The intermediate state of Authentication process should be invisible to other users. |
| 4 | High Availability | Anytime, Anywhere, Anyplace or simply ubiquitously available |
| 5 | Effort free | Authentication process should be effortless. |
| 6 | High durability | After a transaction completes, the changes made should persist even in the case of unexpected system failure.<br>If user credentials like password or biometric are changed, it should persist, if that process completes just before the failure. |

**3.5 Ideal Performance Evaluation Matrices:** In Ideal Authentication System, Ideal Performance Evaluation Matrices refers all the performance evaluation matrices normally used for the authentication system. This component is having scope in the biometrics-based authentication system. The different characteristics, of Ideal Performance Evaluation Matrices, are listed out in Table 6.

Table 6: Description of various characteristics of Ideal Performance Evaluation Matrices

| S.No | Characteristics | Description |
|---|---|---|
| 1 | Ideal False Acceptance Rate | The percentage of system incorrectly classifies the input pattern to an unregistered user is zero. |
| 2 | Ideal False Rejection Rate | The probability that the Authentication framework unable to identify a match between the authentic people is always zero. |
| 3 | Ideal Equal Error Rate | Acceptance and rejection mistakes are identical in the system and which is equal to zero. |
| 4 | Ideal Failure to Enroll Rate | The unsuccessful attempt made to enroll in database or template of an Automatic Fingerprint Identification System by the input is zero. |
| 5 | Ideal Accuracy Rate | Because of False Rejection Rate and False Acceptance Rate is zero, the accuracy of the system becomes high. |
| 6 | Ideal Execution time | Automatic Verification or Authentication process should complete as early as possible for the registered user. |

### 4. 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, and converted into Hash code.

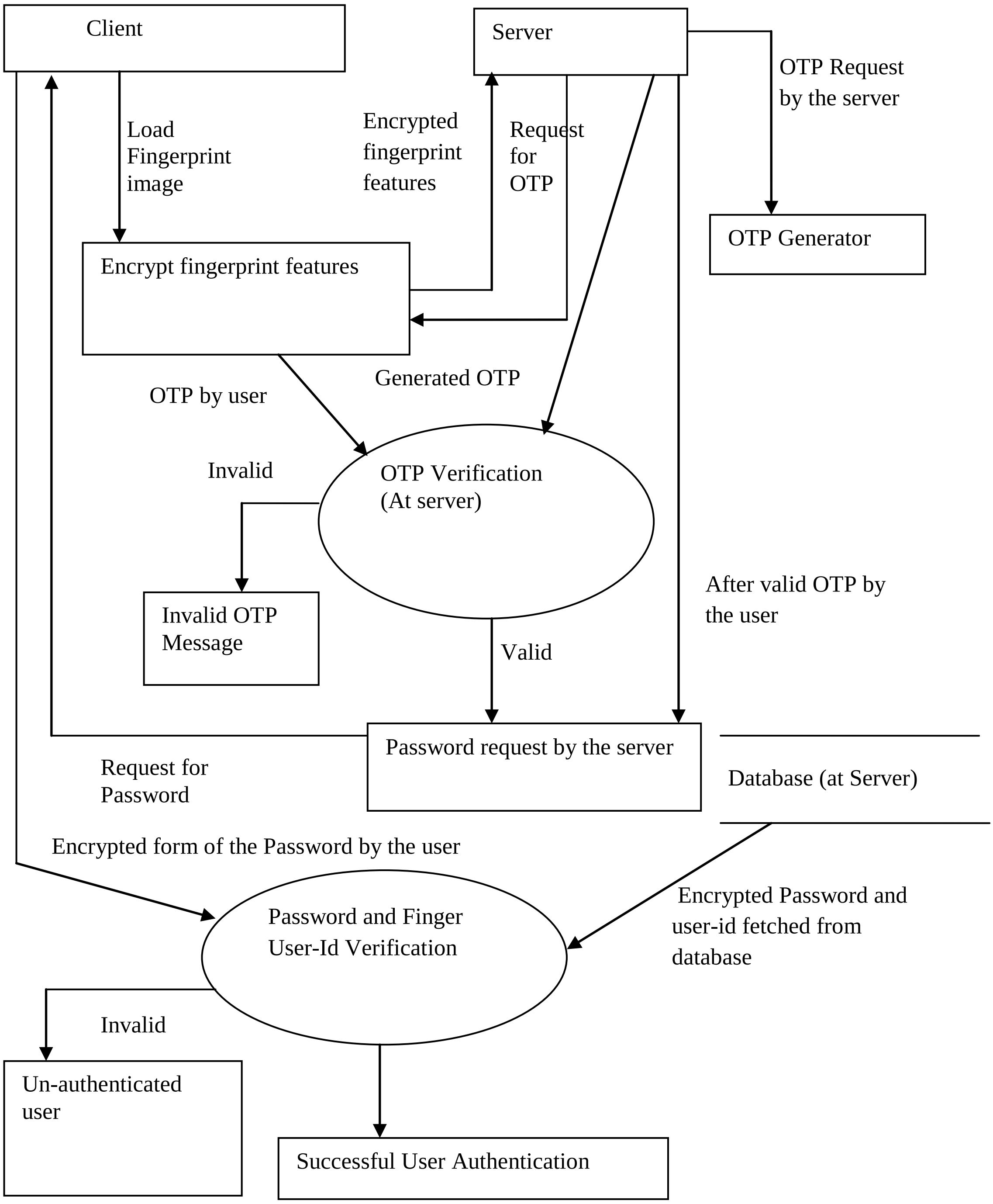
Client
Server
OTP Request by the server
Load Fingerprint image
Encrypted fingerprint features
Request for OTP
OTP Generator
Encrypt fingerprint features
Generated OTP
OTP by user
Invalid
OTP Verification (At server)
Invalid OTP Message
After valid OTP by the user
Valid
Password request by the server
Database (at Server)
Request for Password
Encrypted form of the Password by the user
Password and Finger User-Id Verification
Encrypted Password and user-id fetched from database
Invalid
Un-authenticated user
Successful User Authentication

Figure 2: Dataflow Diagram of Proposed Multifactor Authentication

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.

**4.1 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 the 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.

## 5. Comparison of New Multifactor Authentication Model with existing Systems:

Here we compare Multifactor Authentication Model based on Fingerprint Hash code, OTP, and Password with different existing systems of the same kind or slightly different systems or any system which makes use of biometric or password or username or OTP for authentication. The different system considered in this study are the traditional user-d, password-based internet/mobile banking system, Apple iPhone X face recognition system, HDFC OTP Checkout for online transactions, and Indian Aadhaar card registration process. These comparisons help to understand where this model stands in terms of its features compare to the existing systems.

The new model is compared with all the existing models under four constructs as Advantages, Benefits, Constraints, and Disadvantages [30-42]. Table 7, Table 8, Table 9, and Table 10 shows Advantages, Benefits, Constraints, and disadvantages comparative study of new Multifactor Authentication Model with traditional username and password based Internet/Mobile Banking System respectively.

Table 7: Advantages comparative study of new Multifactor Authentication Model v/s traditional user-id and password based Internet/Mobile Banking System.

Table 7: Advantages comparative study of new Multifactor Authentication Model v/s traditional user-id and password based Internet/Mobile Banking System.

| S.No | New Multifactor Authentication Model | Traditional user-id and password based Internet/Mobile Banking System |
|---|---|---|
| 1 | The Nonreversible Fingerprint Hash code is used in network level<br>Highly secured encrypted user-id and password are used in network level Fingerprint Hash code is used in network level | Highly secured encrypted user-id and password are used in network level |
| 2 | Fingerprint Hash-id is used for identification purpose which is in Hash or encrypted form | User-id is used for identification purpose which is in Hash or encrypted form |
| 3 | Easily revocable Fingerprint Hash-id and password which is in Hash or encrypted form | Easily revocable user-id and password which is in Hash or encrypted form |

| | | |
|---|---|---|
| 4 | High template protection is ensured | High user-id and password protection is ensured in database level |
| 5 | The system having ability to authenticate with one knowledgebase input (Hash-id by selection, OTP is entered by viewing and Password by knowledge base entry) | The system having ability to authenticate with two knowledgebase input (user-id by selection, OTP is entered by viewing and Password by knowledge base entry) |
| 6 | Depending on the device and network Provides ubiquitous authentication | Depending on the device and network Provides ubiquitous authentication |
| 7 | Interactive and explorative user interface | Interactive and explorative user interface |
| 8 | One knowledge base parameter input | Two knowledge base parameter inputs |
| 9 | Simple User authentication from customer point of view | Simple User authentication from customer point of view but user-id also remembered along with password |
| 10 | Reduced error in inputting due to one selection type input. | Input error little more due to lack of selection input. |
| 11 | Due to Hash code user, personal data or input are secured. | Due to encrypted data user personal data or input are secured. |
| 12 | Due to RDBMS transaction property atomicity, consistency, and isolation properties are ensured. | Due to RDBMS transaction property atomicity, consistency, and isolation properties are ensured. |
| 13 | Changed Password and Biometric-id durable for a long time. | Changed Password and User-id durable for a long time. |
| 14 | All the fingerprint performance evaluation matrices like False Acceptance Rate, False Rejection Rate, Equal Error Rate, Failure to Enroll Rate, and Accuracy Rate gives good accuracy or matching rate. | User-id and Password give highest accuracy rate. |
| 15 | Lifespan or validity of OTP is very less, say 2 minutes. | OTP used for financial transaction having more validity. |

Table 8: Benefits comparative study of new Multifactor Authentication Model v/s traditional user-id and password based Internet/Mobile Banking System.

| **S.No** | **New Multifactor Authentication Model** | **Traditional user-id and password based Internet/Mobile Banking System** |
|---|---|---|
| 1 | Security in all aspects of network and template, Simple and easy way to input, reduced execution time can become influence parameters for Increased customer faith and also can attract new customers. | Security in all aspects of network and database and reduced execution time increased customer faith and also attracted new customers. But due to password attacks, users require advanced way of authentication like biometrics. |
| 2 | Cryptographically encrypted one hash code and password only stored in the database, which makes database memory utilization very less and efficient. | Cryptographically encrypted user-id and password only stored in database, which makes database memory utilization very less and efficient. |
| 3 | Both fingerprint-id and passwords are protected by OTP means OTP is first entry type input. | OTP is used only for financial transactions. |
| 4 | Ubiquitous authentication with one knowledge base input. | Ubiquitous authentication with two knowledge base inputs. |
| 5 | Authentication failure is very rare or practically zero compare to any other biometrics-based authentication. | An authentication failure occurs when user-id, password or both becomes wrong. |
| 6 | Revocability can be done easily if password or Finger-id is compromised. In most of the fingerprint-based authentication system, revocability of fingerprint is not so easy. | Revocability is done easily if the password is compromised. |
| 7 | Due to RDBMS transaction property, at the time of system failure. | Due to RDBMS transaction property, ensures a safe state at the time of system failure. |
| 8 | The simple, Navigational, and explorative user interface, the speed of authentication, and Effort free input and process can have | The simple, Navigational, and explorative user interface, the speed of authentication, and Effort free input already enhanced user trust, happiness, |

| | | |
|---|---|---|
| | chances to enhance user trust, happiness, and satisfaction. | and satisfaction. But the user needs still more security for their data and transactions. |

Table 9: Constraints comparative study of new Multifactor Authentication Model v/s traditional user-id and password based Internet/Mobile Banking System.

| S.No | New Multifactor Authentication Model | Traditional user-id and password based Internet / Mobile Banking System |
|---|---|---|
| 1 | Good Network architecture, network availability, and Network availability of mobile service provider's are essential for smooth working. | Good Network architecture, network availability, and Network availability of mobile service provider's are essential for smooth working. |
| 2 | Good RDBMS management and disaster recovery techniques are essential. | Good RDBMS management and disaster recovery techniques are essential. |
| 3 | Requires high configuration system and efficient algorithms for fingerprint Hash code creation and for encryption. | Requires high configuration system and efficient algorithms for user-id and password encryption. |
| 4 | Requires navigational and explorative user interface. | Requires navigational and explorative user interface, and Input should be selective rather than entry type. |
| 5 | While selecting fingerprint features for Hash code, unique features should be selected for collision-free Hash code and for effective user identification. | Unique user-id is selected for collusion free user-id and for effective user identification. |

Table 10: Disadvantages comparative study of new Multifactor Authentication Model v/s traditional user-id and password based Internet/Mobile Banking System.

| S.No | New Multifactor Authentication Model | Traditional user-id and password based Internet/Mobile Banking System |
|---|---|---|
| 1 | Network cost for OTP | Network cost for OTP in financial transactions. |
| 2 | Network and server Failures will shut down the Authentication process | Network and server Failures will shut down the Authentication process |
| 3 | Complex backend design of user interface | Complex backend design of user interface |
| 4 | Negligence of the user in selection of input and Lack of concentration of the user increases the non-matching rate in authentication process. | The negligence of the user in entering the input and Lack of concentration of the user increases the non-matching rate in authentication process. |
| 5 | Requirement of continuous availability of the server increases cost | Requirement of continuous availability of the server increases cost |

Table 11, Table 12, Table 13, and Table 14 shows Advantages, Benefits, Constraints, and disadvantages [30-42] comparative study of new Multifactor Authentication Model with Apple iPhone X facial recognition system. Here the comparison is not more useful because the Apple iPhone X facial recognition used for mobile locking and not for secured transaction or authentication.

Table 11: Advantages comparative study of new Multifactor Authentication Model v/s Apple iPhone X facial Recognition System

| S.No | New Multifactor Authentication Model | Apple iPhone X Facial Recognition System |
|---|---|---|
| 1 | Nonreversible Fingerprint Hash code is used in network level | Face recognition image are stored on the mobile phone. Authentication is done locally. |
| 2 | Fingerprint Hash code alone is not used for the purpose of authentication. Authentication is done with the aid of Fingerprint Hash code, OTP, and Password. | Face of the user image alone is used for authentication/recognition purpose. |
| 3 | Hashed fingerprint gives more security | The unhashed Face image is an easy target for Hackers. |
| 4 | Multiple inputs are necessary for authentication or matching, which includes Fingerprint Hash code, OTP, and Password | Only face image of the user is needed for Authentication/Matching/Verification purpose. |
| 5 | At least one knowledge base input is required (password) | None of the Knowledgebase input is used for Authentication/Matching/Verification purpose. |
| 6 | System is not easily mimicable | The system is easily mimicable. |

Table 12: Benefits comparative study of new Multifactor Authentication Model v/s Apple iPhone X facial Recognition System

| S.No | New Multifactor Authentication Model | Apple iPhone X facial recognition system |
|---|---|---|
| 1 | Security in all aspects of network and template, Simple and easy way to input, reduced execution time can become influence parameters for Increased customer faith and also can attract new customers | Not implemented in large scale due to security failure in its infant stage only. |
| 2 | Cryptographically encrypted one hash code and password only stored in the database, which makes database memory utilization very less and efficient. | Not used in Client-Server architecture. |
| 3 | Both fingerprint-id and passwords are protected by OTP means OTP is first entry type input. | OTP is not used in verification or matching process. |
| 4 | Ubiquitous authentication with one knowledge base input. | Ubiquitous matching with no knowledge base inputs. |
| 5 | Authentication failure is very rare or practically zero compare to any other biometrics-based authentication. | Authentication/matching failure occurs when face image is hacked by the intruder |

Table 13: Constraints comparative study of new Multifactor Authentication Model v/s Apple iPhone X facial Recognition System

| .S.No | New Multifactor Authentication Model | Apple iPhone X facial Recognition System |
|---|---|---|
| 1 | Good Network architecture, network availability, and Network availability of mobile service provider’s are essential for smooth working. | Not used in network, used in local system |
| 2 | Good RDBMS management and disaster recovery techniques are essential. | Not used in client-server architecture |
| 3 | Requires high configuration system and efficient algorithms for fingerprint Hash code creation and for encryption. | Requires high configuration system and efficient algorithms for processing of facial features from face image |
| 4 | Requires navigational and explorative user interface. | Not having much scope for interface because no entry type input required. Input is captured through a mobile camera. |
| 5 | Provides good security architecture through multifactor authentication model. | Good security architecture is essential |

Table 14: disadvantages comparative study of new Multifactor Authentication Model v/s Apple iPhone X facial Recognition System

| S.No | New Multifactor Authentication Model | Apple iPhone X facial Recognition System |
|---|---|---|
| 1 | Network cost for OTP | Not suitable for network feature comparison. |
| 2 | Network and server Failures will shut down the Authentication process | The client-server architecture is not implemented. |
| 3 | Complex backend design of user interface | User interface having not much scope due to lack of manual input. |
| 4 | Negligence of the user in selection of input and Lack of concentration of the user increases the non-matching rate in the authentication process. | Negligence of the user in storing face image in unsecured places causes security failure. |

Table 15, Table 16, Table 17, and Table 18 shows Advantages, Benefits, Constraints, and disadvantages [30-42] comparative study of new Multifactor Authentication Model with HDFC OTP Checkout for online transactions.

Table 15: Advantages comparative study of new Multifactor Authentication Model v/s HDFC OTP Checkout for online transactions

| S.No | New Multifactor Authentication Model | HDFC OTP Checkout for online transactions |
|---|---|---|
| 1 | Nonreversible Fingerprint Hash code is used in network level. | Highly secured encrypted OTP is used in network level |
| 2 | The system having ability to authenticate with one knowledgebase input (Hash-id by selection, OTP is entered by viewing and | The system having the ability to authenticate without knowledgebase input. |

| | | |
|---|---|---|
| | Password by knowledge base entry) | |
| 3 | Depending on the device and network Provides ubiquitous authentication | Depending on the device and network Provides ubiquitous authentication |
| 4 | Interactive and explorative user interface | Interactive and explorative user interface |
| 5 | One knowledge base parameter input | No knowledge base parameter inputs |
| 6 | Simple User authentication from customer point of view | Simple User authentication from customer point of view |
| 7 | Reduced error in inputting due to one selection type input. | More Reduced error in inputting due to lack of selection or entry types input. |
| 8 | Due to Hash code user, personal data or input are secured. | Due to encrypted data user personal data or input are secured. |
| 9 | Lifespan or validity of OTP is very less, say 2 minutes. | OTP used for financial transaction having less validity. |

Table 16: Benefits comparative study of new Multifactor Authentication Model v/s HDFC OTP Checkout for online transactions

| **S.No** | **New Multifactor Authentication Model** | **HDFC OTP Checkout for online transactions** |
|---|---|---|
| 1 | Security in all aspects of network and template, Simple and easy way to input, reduced execution time can become influence parameters for Increased customer faith and also can attract new customers | Security in all aspects of network and database and reduced execution time increased customer faith and also attracted new customers. When the mobile phone is stolen users requires advanced way of authentication like biometrics. |
| 2 | Cryptographically encrypted one hash code and password only stored in the database, which makes database memory utilization very less and efficient. | Cryptographically encrypted user-id and password only stored in the database, which makes database memory utilization very less and efficient. |
| 3 | Both fingerprint-id and passwords are protected by OTP means OTP is first entry type input. | Only OTP is used for authentication/transaction purpose. |
| 4 | Ubiquitous authentication with one knowledge base input. | Ubiquitous authentication with OTP |
| 5 | Authentication failure is very rare or practically zero compare to any other biometrics-based authentication | An authentication failure occurs when OTP is wrong, which very rare or uncommon. |
| 6 | The simple, Navigational, and explorative user interface, the speed of authentication, and Effort free input and process can have chances to enhance user trust, happiness, and satisfaction. | The simple, Navigational, and explorative user interface, the speed of authentication, and lack of manual input already enhanced user trust, happiness, and satisfaction. But the user needs still more security for their data and transactions. |

Table 17: Constraints comparative study of new Multifactor Authentication Model v/s HDFC OTP Checkout for online transactions

| **S.No** | **New Multifactor Authentication Model** | **HDFC OTP Checkout for Online Transactions** |
|---|---|---|
| 1 | Good Network architecture, network availability, and Network availability of mobile service provider's are essential for smooth working. | Good Network architecture, network availability, and Network availability of mobile service provider's are essential for smooth working. |
| 2 | Good RDBMS management and disaster recovery techniques are essential. | Good RDBMS management and disaster recovery techniques are essential. |
| 3 | Requires high configuration system and efficient algorithms for fingerprint Hash code creation and for encryption. | Requires high configuration system and efficient algorithms for OTP encryption. |
| 4 | Requires navigational and explorative user interface. | Requires simple interface due to lack of knowledgebase input. |
| 5 | While selecting fingerprint features for Hash code, unique features should be selected for collision-free Hash code and for effective user identification. | Unique user-id is selected for collision-free user-id and for effective user identification but verification is done only through OTP. |

Table 18: Disadvantages comparative study of new Multifactor Authentication Model v/s HDFC OTP Checkout for online transactions

| S.No | New Multifactor Authentication Model | HDFC OTP Checkout for Online Transactions |
|---|---|---|
| 1 | Network cost for OTP | Network cost for OTP |
| 2 | Network and server Failures will shut down the Authentication process | Network and server Failures will shut down the Authentication process |
| 3 | Complex backend design of user interface | Simple backend design of user interface |
| 4 | Negligence of the user in selection of input and Lack of concentration of the user increases the non-matching rate in the authentication process. | No manual input, which reduces error in input. |
| 5 | Requirement of continuous availability of the server increases cost | Requirement of continuous availability of the server increases cost |

Table 19, Table 20, Table 21, and Table 22 shows Advantages, Benefits, Constraints, and disadvantages [42-51] comparative study of new Multifactor Authentication Model with Indian Aadhaar card registration process.

Table 19: Advantages comparative study of new Multifactor Authentication Model v/s Indian Aadhaar card registration process

| S.No | New Multifactor Authentication Model | Indian Aadhaar card registration process |
|---|---|---|
| 1 | Nonreversible Fingerprint Hash code is used in network level | Highly secured encrypted OTP is used in network level |
| 2 | The system having the ability to authenticate without knowledgebase input (Hash-id by selection, OTP is entered by viewing and Password by knowledge base entry) | The system having ability to authenticate without knowledgebase input. |
| 4 | Interactive and explorative user interface | Interactive and explorative user interface |
| 5 | One knowledge base parameter input | No knowledge base parameter inputs |
| 6 | Simple User authentication from customer point of view | Simple User authentication from customer point of view |
| 7 | Reduced error in inputting due to one selection type input. | More Reduced error in inputting due to lack of selection or entry types input. |
| 8 | Due to Hash code user, personal data or input are secured. | Due to encrypted data user personal data or input are secured. |
| 9 | Lifespan or validity of OTP is very less, say 2 minutes. | OTP used for financial transaction having little bit more validity. |
| 10 | Fingerprint thumb capturing will not fail frequently for kids. | Registration process involving fingerprint thumb image captures requires many attempts for kids. |

Table 20: Benefits comparative study of new Multifactor Authentication Model v/s Indian Aadhaar card registration process

| S.No | New Multifactor Authentication Model | Indian Aadhaar card registration process |
|---|---|---|
| 1 | Security in all aspects of network and template, Simple and easy way to input, reduced execution time can become influence parameters for Increased customer faith and also can attract new customers | Not having scope for authentication. Its one-time registration for a single user. |
| 2 | Cryptographically encrypted one hash code and password only stored in the database, which makes database memory utilization very less and efficient. | Cryptographically encrypted user-id and biometric only stored in the database, which makes database memory utilization more but efficient. |
| 3 | Both fingerprint-id and passwords are protected by OTP means OTP is first entry type input. | Both fingerprint template and OTP makes authentication/transaction process. |
| 5 | Authentication failure is very rare or practically zero compare to any other biometrics-based authentication. | An authentication failure occurs when thumb minutiae details vary with a dry finger or cold weather, or finger damage or cut. |
| 6 | The simple, Navigational, and explorative user interface, the speed of authentication, and Effort free input and process can have chances to enhance user trust, happiness, and satisfaction. | Simple, Navigational, and explorative user interface, speed of registration, and lack of manual input already enhanced user trust, happiness, and satisfaction. |

Table 21: Constraints comparative study of new Multifactor Authentication Model v/s Indian Aadhaar card registration process

| S.No | New Multifactor Authentication Model | Indian Aadhaar card registration process |
|---|---|---|
| 1 | Good Network architecture, network availability, and Network availability of mobile service provider's are essential for smooth working. | Good Network architecture, network availability, and Network availability of mobile service provider's are essential for smooth working. |
| 2 | Good RDBMS management and disaster recovery techniques are essential. | Good RDBMS management and disaster recovery techniques are essential. |
| 3 | Requires high configuration system and efficient algorithms for fingerprint Hash code creation and for encryption. | Requires high configuration system and efficient algorithms for OTP encryption. |
| 4 | Requires navigational and explorative user interface. | Requires simple interface due to lack of knowledgebase input. |
| 5 | While selecting fingerprint features for Hash code, unique features should be selected for collision-free Hash code and for effective user identification. | Unique user-id is selected for collision-free user-id and for effective user identification but verification is done only through OTP. |

Table 22: Disadvantages comparative study of new Multifactor Authentication Model v/s Indian Aadhaar card registration process

| S.No | New Multifactor Authentication Model | Indian Aadhaar card registration process |
|---|---|---|
| 1 | Network cost for OTP | Network cost for OTP |
| 2 | Network and server Failures will shut down the Authentication process | Network and server Failures will shut down the registration process |
| 3 | Complex backend design of user interface | Complex backend design of user interface |
| 4 | Negligence of the user in selection of input and Lack of concentration of the user increases the non-matching rate in the authentication process. | No manual entry type input, which reduces error in input. |
| 5 | Requirement of continuous availability of the server increases cost | Requirement of continuous availability of the server increases cost |
| 6 | The quality of the fingerprint capturing or sensing technology does not affect the system | The quality of the fingerprint capturing or sensing technology affects the system |

## 6. Conclusion:

In this paper initially, we have discussed an ideal system characteristic with respect to Ideal Authentication System. Ideal Authentication system consists of different components, which includes Ideal Security, Ideal User-Friendly, Ideal Input, Ideal Process, and Ideal Performance Evaluation Matrices. We have compared Fingerprint Hash code, OTP and Password-based Authentication Model with existing systems, which includes, the traditional user-id, password-based internet/mobile banking system, Apple iPhone X face recognition system, HDFC OTP Checkout for online transactions and Indian Aadhaar card registration process. Some of the important findings of the comparative study are mentioned below.

- ✓ One time captured static fingerprint image are not vulnerable to climate or weather condition changes compared to any other biometric-based authentication system like Indian Aadhaar Card registration process.
- ✓ The new multifactor Authentication model requires less knowledgebase input compared to traditional user-id and password based Internet/Mobile banking authentication [52-55].
- ✓ If the user takes care and ensures user-level security through external devices like USB drive or Private cloud drive, we can eliminate password factor from authentication process.
- ✓ The new Multifactor Authentication model produces good performance evaluation matrices, which includes False Acceptance Rate, False Rejection Rate, Equal Error Rate, Failure to Enroll Rate, and Accuracy Rate for Fingerprint Hash code compare to any other Hash code based matching systems.

## 7. 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. Krishna Prasad, K. & Aithal, P. S. (2018). A Study on Multifactor Authentication Model Using Fingerprint Hash Code, Password and OTP. International Journal of Advanced Trends in Engineering and Technology, 3(1), 1-11. DOI: http://doi.org/10.5281/zenodo.1135255.
12. Krishna Prasad, K. & Aithal, P. S. (2018). A Study on Fingerprint Hash Code Generation Based on MD5 Algorithm and Freeman Chain Code. International Journal of Computational Research and Development. 3(1), 13-22. DOI: http://doi.org/10.5281/zenodo.1144555.
13. Tulyakov, S., Farooq, F., Mansukhani, P., & Govindaraju, V. (2007). Symmetric hash functions for secure fingerprint biometric systems. Pattern Recognition Letters, 28(16), 2427-2436.
14. Das, P. P., Chakrabarti, P. P., & Chatterji, B. N. (1987). Distance functions in digital geometry. Information Sciences, 42(2), 113-136.
15. Aithal, P. S., & Shubhrajyotsna Aithal, (2015). Ideal Technology Concept & its Realization Opportunity using Nanotechnology, International Journal of Application or Innovation in Engineering & Management (IJAIEM), 4(2), 153 - 164. DOI: http://doi.org/10.5281/zenodo.61591.
16. Aithal, P. S. (2015). Concept of Ideal Business & Its Realization Using E-Business Model, International Journal of Science and Research (IJSR), 4(3), 1267 - 1274. DOI: http://doi.org/10.5281 /zenodo.61648.
17. Aithal, P. S., & Shubhrajyotsna Aithal, (2016). Impact of On-line Education on Higher Education System. International Journal of Engineering Research and Modern Education (IJERME), 1(I), 225-235. DOI: http://doi.org/10.5281/zenodo.161113.
18. Aithal, P. S., & Shubhrajyotsna Aithal (2015). An Innovative Education Model to realize Ideal Education System. International Journal of Scientific Research and Management (IJSRM), 3(3), 2464-2469. DOI: http://doi.org/10.5281/zenodo.61654.
19. Aithal, P. S., & Shubhrajyotsna Aithal, (2014). Ideal education system and its realization through online education model using mobile devices. Proceedings of IISRO Multi Conference 2014, Bangkok, 140 – 146. ISBN No. 978-81-927104-33-13.
20. Aithal, P. S., (2016). Review on Various Ideal System Models Used to Improve the Characteristics of Practical Systems. International Journal of Applied and Advanced Scientific Research, 1(1), 47-56. DOI: http://doi.org/10.5281/zenodo.159749.
21. Aithal, P. S. (2016). The concept of Ideal Strategy & its realization using White Ocean Mixed Strategy, International Journal of Management Sciences and Business Research (IJMSBR), 5(4), 171-179. DOI: http://doi.org/10.5281/zenodo.161108.
22. Sridhar Acharya, P. and Aithal, P. S., (2016). Concepts of Ideal Electric Energy System for production, distribution and utilization. International Journal of Management, IT and Engineering (IJMIE), 6(1), 367-379. DOI: http://doi.org/10.5281/zenodo.161143.
23. Aithal, P. S., (2016). Smart Library Model for Future Generations. International Journal of Engineering Research and Modern Education (IJERME), 1(1), 693-703. DOI: http://doi.org/10.5281/zenodo. 160904.

24. Aithal, P. S. (2016). Ideal Banking Concept and Characteristics. International Research Journal of Management, IT and Social Sciences (IRJMIS), 3(11), 46-55. DOI: http://dx.doi.org/10.21744/irjmis.v3i11.311.
25. Aithal, P. S. (2016). A Comparison of Ideal Banking Model with Mobile Banking System. International Journal of Current Research and Modern Education (IJCRME), 1(2), 206-224. DOI: http://dx.doi.org/10.5281/ZENODO.198708.
26. Aithal, P. S., & Vaikuth Pai, T., (2016). Concept of Ideal Software and its Realization Scenarios. International Journal of Scientific Research and Modern Education (IJSRME), 1(1), 826-837. DOI: http://doi.org/10.5281/zenodo.160908.
27. Shubrajyotsna Aithal, & Aithal, P. S., Bhat, G. K. (2016). Characteristics of Ideal Optical Limiter and Realization Scenarios using Nonlinear Organic Materials – A Review. International Journal of Advanced Trends in Engineering and Technology (IJATET), 1(1), 73-84. DOI: http://doi.org/10.5281/zenodo.240254.
28. Aithal, P. S., Suresh Kumar P. M. (2017). Ideal Analysis for Decision Making in Critical Situations through Six Thinking Hats Method. International Journal of Applied Engineering and Management Letters (IJAEML), 1(2), 1-9. DOI: http://dx.doi.org/10.5281/zenodo.838378.
29. Krishna Prasad, K., & Aithal, P.S. (2017). A Customized and Ideal Mobile Banking Technology Using 5G Technology. International Journal of Management, Technology and Social Science (IJMTS), 2(1), 25-37. DOI: http://dx.doi.org/10.5281/zenodo.820860.
30. Aithal, P. S., Shailashree, V. T., Suresh Kumar, P. M. (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.
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., & Suresh Kumar, P. M. (2015). Application of ABCD Analysis Model for Black Ocean Strategy. International Journal of Applied Research (IJAR), 1(10), 331-337. DOI: http://doi.org/ 10.5281/zenodo.163424.
33. Aithal, P. S., Shailashree, V. T., & Suresh Kumar P. M., (2016). ABCD analysis of Stage Model in Higher Education. International Journal of Management, IT and Engineering (IJMIE), 6(1), 11-24. DOI: http://doi.org/10.5 281/zenodo.154233.
34. Aithal, P. S., Shailashree, V. T., & Suresh Kumar, P. M. (2016). Analysis of NAAC Accreditation System using ABCD framework. International Journal of Management, IT and Engineering (IJMIE), 6(1), 30-44. DOI: http://doi.org/10. 5281/zenodo.154272.
35. Aithal, P. S., Shailashree, V. T., & Suresh Kumar, P. M. (2016). Application of ABCD Analysis Framework on Private University System in India. International Journal of Management Sciences and Business Research (IJMSBR), 5(4), 159-170. DOI: http://doi.org/10.5281/zenodo.161111.
36. 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.
37. Aithal, S., & 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://dx.doi.org/10. 21013/jas.v4.n3.p1.
38. Aithal, P. S., Shailashree, V. T. & Suresh 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.
39. Varun Shenoy, & Aithal P. S., (2016). ABCD Analysis of On-line Campus Placement Model, IRA-International Journal of Management & Social Sciences, 5(2), 227-244. DOI: http://dx.doi.org/10.21013/jmss .v5.n2.p3.
40. 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.
41. Aithal, P. S., Shailashree V. T & Suresh 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/10.528 1/zenodo.62022.
42. Aithal, P. S. & Suresh Kumar, P. M. (2016). Opportunities and Challenges for Private Universities in India. International Journal of Management, IT and Engineering (IJMIE), 6(1), 88-113. DOI: http://doi.org/10.5281/zenodo. 161157.

43. Padmanabha Shenoy, & Aithal, P. S., (2016). A Study on History of Paper and possible Paper Free World. International Journal of Management, IT and Engineering (IJMIE), 6(1), 337-355. DOI: http://doi.org/10.5281/zenodo. 161141.
44. 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.
45. Aithal P. S. & Shubhrajyotsna Aithal (2016). Impact of On-line Education on Higher Education System. International Journal of Engineering Research and Modern Education (IJERME), 1(1), 225-235. DOI: http://doi.org/ 10.5281/zenodo.161113.
46. 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.
47. 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.
48. Prithi Rao, and Aithal, P.S. (2016). Green Education Concepts & Strategies in Higher Education Model, International Journal of Scientific Research and Modern Education (IJSRME), 1(1), 793-802. DOI: http://doi.org/ 10.5281/zenodo.160877.
49. Aithal, P. S. & Shubhrajyotsna Aithal (2016). Ekalavya Model of Higher Education – an Innovation of IBM’s Big Data University. International Journal of Current Research and Modern Education (IJCRME), 1(2), 190-205. DOI: http://dx.doi.org/10.5281/zenodo.198704.
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.
51. 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.
52. Kumar, D., & Ryu, Y. (2009). A brief introduction of biometrics and fingerprint payment technology. International Journal of advanced science and Technology, 4, 25-38.
53. 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.
54. 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.