# Enhance Security Methods for Identifying Users without their Login Ids

Pallavi M. Ingale
PG Student
Department of Computer Engineering
SSBT's College of Engineering & Technology,
Bambhori, Jalgaon

Girish Kumar Patnaik
Professor and Head
Department of Computer Engineering
SSBT's College of Engineering & Technology,
Bambhori, Jalgaon

## ABSTRACT

Authentication to a computer system is divided in to two mechanisms, identification and verification. For identification the login IDs have been used and for verification password can be used. The existing password based system can be augmented by strengthening the identification process. Instead of a login ID identification process utilizes personal secret data to identify a user uniquely. The identification process asks the user to choose a correct login ID among multiple choices of partially obscured IDs. Since, identification process does not accept a login ID during the authentication process. For gaining an access to the computing system a stolen or cracked password cannot be used, unless a correct identification material is provided by attacker. Hence in this paper, the three step verification process is provided to enhance the security. The security will be provided using user authentication and device authentication by an authentication methods.

## Keywords

Cybersecurity, Authentication, Identification, Password.

## 1. INTRODUCTION

Internet Security is a process to create a rules and actions to protect against attacks over the internet. Internet Security is a catch all term for covering security for transactions made over the internet. Internet security encompasses overall authentication and protection of data sent via internet. To allow access only legitimate users, computer systems employ an authentication mechanism. Identification and verification are two parts of the authentication procedure. The authentication procedure is composed of two parts, identification and verification. The identification is for answering the question and the verification is for answering. Traditionally the identification is performed with a username and the verification is performed with a password. Authentication is a process in which a system verifies the identity of a user who wishes to access it. The user who wishes access to a resource, the access control is based on identity of the user and authentication is essential to effective security.

Authentication is the process of verifying a rights of identity. Example is When John Doe going to a bank to make a withdrawal, john tells the bank teller he is John Doe a claim of identity. The bank teller asks to show a photo ID, so john hands the teller his driver's license. The bank teller checks the license to make sure it has John Doe printed on license and compares the photograph on the license against the person claiming to be John Doe. If the photo and name match with the person, then the teller has authenticated that John Doe is who he claimed to be. Similarly by entering the correct password, the user is providing proof that they are the person belongs to the username. There are three types of techniques for do this. The first type of authentication is accepting evidence of identity given by a credible person who has proof on the said identity. The second type of authentication is comparing the attributes of the object itself to what is notable about objects of that origin. The third type of authentication relies on documentation or other external assertion.

The identification is accomplish with a username or login ID and the verification is performed with a password. The plain text passwords are transformed into hash values with a one-way hash function in a password based system and stored in a password hash file. A new hash value is generated from the newly entered password during the verification process and compared with the stored hash value in the password hash file. If the hash values match, access is permitted. The password verification process is the heart of the most authentication systems. There are a number of ways to obtain other users password for illegal access. The Plain text passwords can be captured from the network, by malware or by key logging software. When the plain text password is not accessible, the attackers can try password guessing attack where they try possible values for the victim user. In shoulder surfing attack the attacker uses observation techniques such as looking over someone's shoulder to get information. Due to this reason advance security methods play an important role to authenticate the user.

To overcome the challenge of shoulder surfing attacks, the contributions in the proposed system is involvement of advance security methods in the process of user identification. By using advance security methods the security in the system will be increased.

Rest of the paper is organized as follows: Section 2 gives an overview of the related work; Section 3 presents the proposed approach; Section 4 presents the result & discussion and Section 5 concludes the proposed approach.

## 2. RELATED WORK

In the past, there was lot of research done on the authentication methods. The login IDs have been used for identification and passwords for verification. Many schemes have been proposed to enhance both parts, but they may require specialized devices or they may not be always reliable. This password verification process is the backbone of the most authentication systems. Certain disadvantages of regular password appear like stolen the password, forgetting the password and weak password. Therefore a large requirement to have a strong authentication method is needed to secure the system as possible. Structure of literature survey as authentication methods is shown in Figure 1.

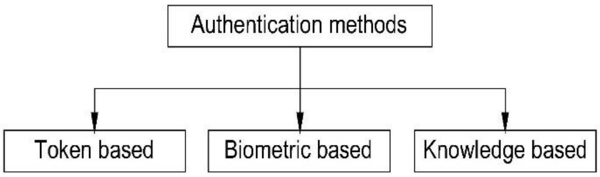

**Fig 1: Authentication Techniques.**

## 2.1 Token based technique

The token is used in addition to or in place of a password to prove that the customer is who they claim to be. The token acts like an electronic key to access something. Tokens can contain chips with functions varying from very simple to very complex, including multiple authentication methods. The simplest security tokens do not need any connection to a computer. The tokens have a physical display, the authenticating user simply enters the displayed number to log in. Other tokens connect to the computer using wireless techniques, such as Bluetooth. These tokens transfer a key sequence to the local client or to a nearby access point. Alternatively, another form of token that has been widely available for many years is a mobile device which communicates using an out-of-band channel.

Boneau et al., in [1], presents comprehensive approach leads to key insights about the difficulty of replacing passwords. The two decades of proposals to replace text passwords for general purpose user authentication on the web using a broad set of twenty five usability, deploy ability and security benefits that an ideal scheme might provide. The comprehensive approach leads to key insights about the difficulty of replacing passwords. Many academic proposals have failed to gain traction because researchers rarely consider a wide range of real world constraints. The framework provides an evaluation methodology and benchmark for web authentication proposals.

Schclar et al., in [2], presents a novel approach for user authentication based on the keystroke dynamics of the password entry is introduced. Also the cluster representatives (CR) and Inner cluster representatives (ICR) strategies introduced to select the representatives. A common problem in user authentication is the acquisition of data. Hence the approach selects representative users, a dataset with a large enough number of users was required.

## 2.2 Biometric based technique

Many different aspects of human physiology, chemistry or behaviour can be used for biometric authentication. The selection of a particular biometric for use in a specific application involves a weighting of several factors. The identification of seven such factors to be used when assessing the suitability of any trait for use in biometric authentication.

Zhang et al., in [4], proposed Three-dimensional (3-D) palm print to be a significant biometrics for personal authentication. Three dimensional palm prints are harder to counterfeit than 2-D palm prints and more robust to variations in illumination and serious scrabbling on the palm surface. Three novel global features of 3-D palm prints which describe shape information and can be used for coarse matching and indexing to improve the efficiency of palm-print recognition, particularly in very large databases. The three proposed shape features are maximum depth of palm centre, horizontal cross-sectional area of different levels, and radial line length from the centroid to the boundary of 3-D palm-print horizontal cross section of different levels.

Yun et al., in [5], proposed a biometric user identification method based on users gait. The obtainable features from users gait divided into two categories: walking pattern and stepping pattern (dynamic footprints), and considers an approach of identifying user with dynamic footprints. A software module is developed to extract dynamic Footprints from the samples acquired, and PCA (Principal Component Analysis) and neural network technique are employed to identify the user with extracted features.

Gomathi and Nasira, in [6], presents A Survey on Biometrics based Key Authentication using Neural Network. In this paper, the two issues to be considered for user authentication system are recognition of the authorized user and rejection of the impostor. So a better classifier is necessary to perform this task. Some of the widely used classifier is based on fuzzy logic, neural network, etc. Among those, neural network can be efficient in classification. This survey provides various biometrics based authentication system based on neural network.

## 2.3 Knowledge based technique

Knowledge Based Authentication (KBA) is a method of authentication that relies on user specific knowledge to prove the identity of an end user and grant access to secure information on the web. This method typically requires the end user to answer a set of challenge questions in order to validate the user to his or her account. For knowledge based authentication there is a significant weight placed on requesting the right knowledge from the end user. Information that only he or she could possibly know, in order to validate their identity.

Towhidi et al., in [7], proposed the Knowledge Based Authentication Attacks. In this paper, the attacks pattern of textual and graphical password describes according to CAPEC standard, describing their effects on both conventional and image password. The image password is classified into three categories: Recognition Based, Pure Recall Based and Cued Recall Based. Finally reviews the common attacks of knowledge base authentication and the reflection in textual and graphical password is presented.

Golhar and Adane, in [8], presents Graphical Knowledge Based Authentication Mechanism. The use of Inclusive Exclusive principle can be applied to find the minimum or maximum number of images required to form the image sequence. CBIR operates on a totally different principle, retrieving or searching stored images from a collection by comparing features automatically extracted from the images themselves. Maximum or minimum number of images and their sequences can be determined by using mathematical concept using Inclusion Exclusion Principle.

Chiasson et al., in [9], proposed an integrated evaluation of the Persuasive Cued Click Points graphical password scheme including usability and security evaluations and implementation considerations. In this paper, use persuasion to influence user choice in click-based graphical passwords. Hence more difficult to guess click-points.

Daniel et al., in [10], presents Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique. A comprehensive study of the graphical password schemes is performed. The graphical password schemes can be compared and categorized into two groups, recognition-based scheme and recall-based scheme.

Also several usability and security features for research continuity in this area are listed.

Alternative methods to replace or fortify the password based authentication system have been developed and some are widely used at this time. When two methods from two different categories are combined, it is considered two-factor authentication.

# 3. PROPOSED SOLUTION

The proposed approach describes the solution to authenticate the user by providing more security in the system. An existing system consist drawback of single step verification i.e. less security level is exist in the existing system. The proposed solution overcomes this drawback by providing more security in the system using three step verification. The three step verification process includes three methods namely colour based method, hybrid method and pattern matching method. The verification process also include one-time password process to enhance security in the system.

## 3.1 Proposed System Architecture

Architecture is a system that unifies its components or elements into a coherent and functional blocks. Figure 2 shows architecture of the proposed system. User does registration and make selection of algorithm. Authentication phase contains three algorithms. Proposed system mainly consists of THREE algorithms Colour Based Algorithm, Hybrid Algorithm and Pattern Matching algorithm.

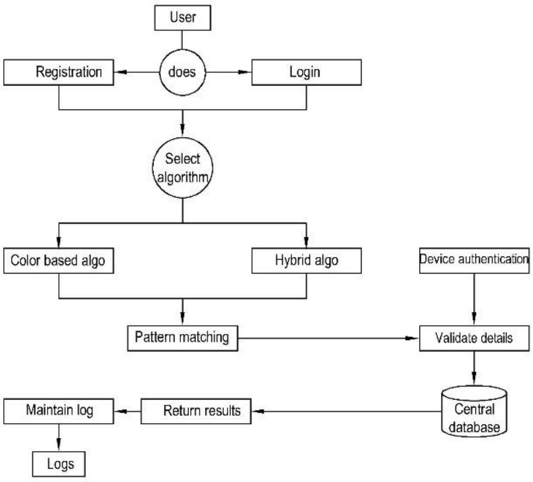

**Fig 2: Architecture of Proposed System**

### *3.1.1 Colour based Algorithm*

In colour based algorithm there is two phases namely registration and authentication phase. During registration phase, the user gives sequence to colours which is even and these sequence can be stored in database.

Let, C[8] be an array of randomly ordered 8 predefined colours.

Let, IP[k] is randomly chosen colours from c[8].

- Where k is even and 1<k≤8

In authentication phase, the interface is displayed. The interface corresponds to array of randomly ordered 8 predefined colours and 8×8 number grid in which numbers from 1 to 8 are placed randomly. Both these grid and array changes for each session.

Let, C[8] be an array of randomly ordered 8 predefined colours.

Let, M[8][8] is a randomly generated grid and for every i, 1≤i≤8 and

M[i][j] is random no between 1 to 8.

- Where, 1≤j≤8

The logic elaborate in this scheme is that the index assign to the first colour represents a row and the index assign the second colour represents a column of the 8×8 number grid. The number in the intersection cell of selected row and column of the grid is the part of session password. This procedure is repeated again for the remaining colour sequence.

Let, Mk[rk][ck] is the input from the grid.

-Where 1≤k≤4

And rk and ck are row and column respectively in the grid.

In both the cases, if the password entered by the user in registration phase is match with password entered in authentication phase, then he is permitted to face the pattern authentication. Otherwise, the user is require to re-enter the session password according to sequence of colours.

Let, Compare row and column sequence with IP[k].

Hence,

M[rk] = IP[k],

M[ck] = IP[k+1]

-Where k is odd no. and 1≤k≤8.

### *3.1.2 Hybrid Algorithm*

In hybrid algorithm there is two phases namely registration and authentication phase. During registration phase, the user give their secret password. The minimum length of the secret pass is at least 6 digits and it will be contain even number of characters.

Let, User submits secret password IP[k].

Let, N is the length of password which is even.

-Where IP[k]≥6

In authentication phase, an interface correspond to 6×6 grid is displayed. The grid contains both alphabets and numbers which are in between 0 to 9 and a to z, placed at random and the interface changes every time.

Let, M[6][6] is a randomly generated grid and M[i][j] is a random characters between 0 to 9 and a to z respectively.

The idea involved in the hybrid authentication scheme is that: Firstly, the user has to consider the secret pass in terms of pairs. The first letter in the pair is used to select the row and the second letter in the pair is used to select the column in the 6×6 grid. The intersection cell letter of the selected row and column generates the character which is a part of the session password. In this way, the idea is repeated for all other pairs in the secret password.

Let, Mk[rk][ck] is input from the grid,

-Where 1≤k≤3

And rk and ck are row and column respectively in the grid.

Let, M[R] = [rk][cn]

-Where, $0 \leq k \leq 5$ and n is selected cell value.

Let, M[C] = [rn][ck]

-Where, $0 \leq k \leq 5$ and n is selected cell value.

Let, Mk = M[R] + M[C]

Thus, the password inputted by the user in authentication phase is match with password in registration phase i.e. the session password is now verified by the server to authenticate the user.

Let, Compare value of row and column with IP[k]

Hence,

M[R] = IP[k],

M[C] = IP[k+1]

-Where k is odd no. and $1 \leq k \leq N$

### *3.1.3 Pattern Matching Algorithm*

In pattern matching algorithm the 3×3 grid is displayed. The values in between 1 to 9 is displayed.

Let,

M[3][3] is a grid and M[i][j] is a values between 1 to 9.

-Where $0 \leq i < 3$ and $0 \leq j < 3$

The user has to draw a sequence, as draw-a-secret which are joining the dots, i.e. user give input from the grid.

Let, M[ip][jp] is the input from the grid.

-Where $1 \leq p \leq 9$

And

ip, jp are the row and column respectively, in the grid.

For normal registered user, if the sequence drawn in registration phase matches with the sequence drawn during the authentication phase, then the user is given the permission to access the next step verification. If the draw-a-secret is wrong, then a message sequence does not match is indicated to the user.

Let, Seq = seq+M[ip][jp];

-Where seq is sequence of selected pattern.

## 3.2 Design

The design includes proposed solution to increase more security in the system using three step verification. The design of proposed system is divided into three phases that are colour based design, hybrid design and pattern design.

### *3.2.1 Colour based Design*

The colour based design is a authentication method use to enhance security in the system. In this design, the interface corresponds to 8×8 number grid in which numbers from 1 to 8 are placed randomly. The array of randomly ordered 8 predefined colours are displayed. Both these grid and array changes for every session. The interface grid can be implemented using vector. The 8×8 values can be generated in vector. The algorithm for colour based registration is shown in algorithm 1.

**Algorithm 1 Colour based Registration Algorithm**

```
Require: iseq (Input Sequence)
1: Generate random colour sequence
   Random r = new random ();
   i = r.nextInt (8);
   Arr[i] = Random.nextInt (8);
2: Each colour is given a value
   Col[i] = [0-8];
3: Select colour and click on that colour, these sequence is
stored as iseq.
```

The Vector class implements a augmented array of objects. Like an array, it contains components that can be accessed using an integer index. However, the size of a Vector can augment or shrink as needed to accommodate adding items after the Vector has been created.

```
Vector v = new vector ();
For (int i=0; i≤v.size; i=i+8)
v.add (arr[i]);
```

The algorithm for colour based authentication is shown in algorithm 2.

**Algorithm 2 Colour based Authentication Algorithm**

```
Require: db (Database), True (Homepage), False (Error page),
Iseq (Input Sequence)
1: Generate random colour sequence
   Random r = new random ();
   i = r.nextInt (8);
   Arr[i] = Random.nextInt (8);
2: Generate 8×8 values in vector
   Vector v = new vector ();
   For ( int i=0; i≤v.size; i=i+8 )
   v.add (arr[i]);
3: Each colour is given a value
   Col[i] = [0-8];
4: Select odd colour for row and even colour for column, click
   on intersection cell.
   Col [i0] = row[i];
   Col [0i] = column[i];
5: Match the sequence with input sequence
6: if (seq == iseq) then
7: True
8: end if
9: if (seq ≠ iseq) then
10: False
```

### *3.2.2 Hybrid Design*

The hybrid design is session password authentication method. In hybrid design the grid is of size 6×6 and it involve the alphabets and numbers. These are randomly distribute on the grid and the interface changes every time. During registration user can submits its secret password. According to secret password user can select row of first number in secret password and select column of second number in secret password. In this design the grid will be implemented using vector. The grid consist of a to z alphabets and 0 to 9 numbers respectively. The algorithm for hybrid registration is shown in algorithm 3.

**Algorithm 3 Hybrid Registration Algorithm**

```
Require: db (Database)
1.  User submits the secret password of even number.
2.  Store the password in db.
```

The class collection made up of exclusively of static methods that operate on or return collections. Class collection contains polymorphic algorithms that operate on collections, “wrappers", which return a new collection backed by a specified collection, and a few other odds and ends. The algorithm for Hybrid authentication is shown in algorithm 4.

**Algorithm 4 Hybrid Authentication Algorithm**

```
Require: db (Database), True (Homepage), False (Error page)
1: Generate 6×6 grid values using vector, value contains 0-9
    and a-z.
     for (v.add (val[i] )
2: Shuffle vector,
    Collection. Shuffle (v)
3: Generate grid 6×6 using vector
    Vector v = new vector ();
    String val = new string ()
    for (int i=0; i<v.size; i=i+6)
    Mat[ij] = val[i]
4: Select odd number for row and even number for column,
    click intersection cell.
5: Split complete sequence to get all pairs
    String seq1 = seq.split()
6: Split pairs to get rows and column
    String colseq = seq1.split ()
7: Split each seq to get values of rows and columns
    String rowseq = colseq.split ()
8: Match each character with corresponding character of row
    and column.
    For ( int i=0; i < seq.len; i++ )
    Char c = (char)(seq.charAt(i))
9: if c = rowseq[i] then
10: True
11: end if
12: if c ≠ rowseq[i] then
13: False
14: end if
```

### 3.2.3 Pattern Matching Design

In pattern matching design, the 3×3 grid is dispayed. During the first phase that is Registration phase, first the user has to select his username and a textual password. Then objects are displayed shown to the user to select from them as his graphical password in the form of draw a secret. The algorithm for pattern matching registration is shown in algorithm 5.

**Algorithm 5 Pattern Matching Registration Algorithm**

```
Require: db (Database)
1: Generate 3×3 grid values using vector
    Vector v = new vector ();
    for (int i=1; i≤9; i++)
    v.add (i);
2: Each cell is given a value
    for (int i=0; i<9; i++)
    Cell[i] = v [i+1];
3: User selects cell value sequence
    Seq+ = cell[i];
4: Store value sequence in db.
```

After selecting the user has to draw those selected objects on a touch sensitive screen. During the second phase that is Authentication phase, the user has to give his username and textual password and then submit his graphical password by drawing it in the same way during the registration phase. If the user has to draw correctly the user is authenticated and only then user can permissible to access the account. The algorithm for pattern matching authentication is shown in algorithm 6.

**Algorithm 6 Pattern Matching Authentication Algorithm**

```
Require: db (Database), True (Homepage), False (Error page)
1: Generate 3×3 grid values using vector
    Vector v = new vector ();
     for (int i=1; i≤9; i++)
     v.add (i);
2: Each cell is given a value
    for (int i=0; i<9; i++)
    Cell[i] = v[i+1];
3: User selects cell value sequence
    Seq+ = cell[i];
4: Match values from database
5: if cell[i] = cell [db] then
6: True
7: end if
8: if cell[i] ≠ cell [db] then
9: False
10: end if
```

## 4. RESULT AND DISCUSSION

Evaluation of the proposed approach versus existing approach is carried out in the result and discussion section. Result section represents the experimental results of the proposed approach as well as the existing approach. Evaluation of the both the approaches is carried out in the discussion section on the basis of obtained results. In some cases various parameters i.e. performance metrics are used to evaluate the system, in order to decide which one is the best.

### 4.1 Result

Experimental result present the effectiveness of proposed system, in which involvement of authentication methods is proved better by carrying out experiments. Results are carried out using java. In proposed system Time consumed by each algorithm at different steps and also total time and average time for complete algorithm execution is considered. The results are taken by executing the algorithms with all combinations and average of 10 iterations are taken into consideration. Below Results show verification and validation time required by each algorithm at each step.

The time consumed as:

**Table 1: Time Comparison of Authentication Methods**

| | Text pass | Colour | Hybrid | Pattern | OTP | Encrypt |
|---|---|---|---|---|---|---|
| User1 | 0.02 | 0.033 | | 0.12 | 15 | 0.05 |
| User2 | 0.01 | | 0.042 | 0.17 | 10 | 0.059 |
| User3 | 0.01 | 0.25 | | 0.16 | 20 | 0.55 |
| User4 | 0.02 | | 0.05 | 0.15 | 30 | 0.59 |
| User5 | 0.02 | 0.19 | | 0.11 | 25 | 0.39 |
| Avg. time | 0.016 | 0.157 | 0.46 | 0142 | 20 | 0.3278 |

Table 1 shows time comparison of authentication methods. All values provided are in seconds. The proposed approach was evaluated by an experimental results in which included 5 users. The users are various technical and non-technical backgrounds, of different ages ranging from twenty to forty years. The primary experimental objective was to evaluate the recognition success rate of the proposed method dependent on the size of target group population and also in comparison to traditional algorithm.

Every participant accomplish ten repetitions of all three selected algorithms, so that 15 steps per user were recorded in total. The test was not evaluated sequentially but rather over a longer period of time (15mins) and with pauses in order to provide additional variability and to obtain more realistic study results. The users were seated while performing the test, but were not influenced in any other way. User time consumed is expressed as a time required performing all algorithm steps.

Figure 3 shows the graph of impact of time comparison in which graph can be generated from time comparison of authentication methods.

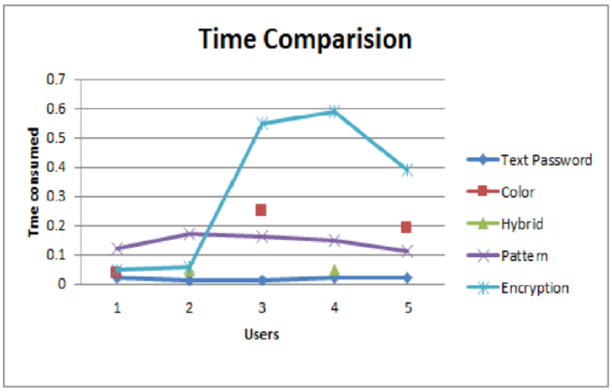

**Fig 3: Impact of Time Comparison**

The proposed approach is providing higher level of security to web based applications. While implementing combination of various algorithms are used. All combinations of algorithms are executed to get complete idea of performance of system. Performance is evaluated in terms of time consumed by all algorithms to get intermediate or final results. The OTP (one time password) completely depends on the network carrier for receiving sms. Figure 4 shows impact of OTP in which graph is depends on network carrier.

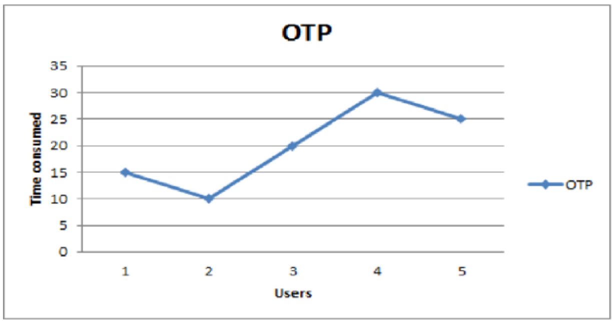

**Fig 4: Impact of One Time Password**

Performance Metric used in prediction is time utilized by all algorithm steps. The proposed algorithms are designed in such a way that any combination of algorithms can be selected to obtain better output.

### 4.2 Discussion

The purpose of the discussion section is to state interpretations and opinions, explain the implications of findings in the experimental evaluation. Main function of discussion section is to answer the questions posed in the Introduction, explain how the results support the answers and, how the answers fit in with existing knowledge on the topic. The discussion section is important to know the detail advantage and need about proposed solution.

Results of experiment evaluate performance of proposed system at various levels and steps. Performance get reduce when there are more number of steps. As the steps in algorithms are changed time consumed will also change, eventually the above results will change accordingly. But as observed after working on various combinations with different number of users we get different results. All algorithms used at once may cause annoyance between users, so only some combinations of algorithms can only be used.

## 5. CONCLUSION

The Proposed security methods provide more security than existing system. The three step verification process is provided in proposed approach to enhance the security. Thus experiments shows combining multiple algorithms for security purpose can increase the level of security and also reduces time for processing. Experiments results shows the time consume by all algorithms are different and can be reduced by combining it with other algorithms.

In future, it would be a point of research to increase security by using better user interface or combine this algorithms with more famous algorithms to get better security and less time consumption.

## 6. REFERENCES

[1] Joseph Bonneau, cormac Herley, Paul C van Oorschot,and Frank Stajano, “The Quest to Replace Passwords: AFramework for Comparative Evaluation of Web Authentication Schemes", 2012, IEEE Symposium onSecurity and Privacy, pp. 553 – 567.

[2] Alon Schclar, Lior Rokach, Adi Abramson, and YuvalElovici, “User Authentication Based on RepresentativeUsers, IEEE Transactions on Systems, Man, And Cybernetics Part C: Applications and Reviews", Vol. 42,No. 6, November 2012, pp. 1669 - 1678.

[3] Nikos Komninos, Emmanouil Georgakakis, Christos“NAVI: Novel Authentication with Visual Information,IEEE Symposium on Computers and Communications",2012, pp. 588 - 595.

[4] Bob Zhang, Wei Li, Pei Qing, and David Zhang, “PalmPrint Classification by Global Features", IEEETransactions on Systems, Man, And Cybernetics: systemsVol. 43, No. 2, March 2013, pp. 370 378.

[5] Jaeseok Yun, Gregory Abowd, Woontack Woo, JehaRyu, “Biometric User Identification with Dynamic Footprint”, 2007, 2nd Intl Conference on Bio-InspiredComputing: Theories and Applications, pp. 225-230.

[6] P. M. Gomathi, Dr. G. M. Nasira , “A Survey on Biometrics based Key Authentication using Neural Network”, Double Blind Peer Reviewed InternationalResearch Journal, Volume 11 Issue 11 Version 1.0 July 2011.

[7] Farnaz Towhidi, Azizah Abdul Manaf, Salwani MohdDaud, Arash Habibi Lashkari, “The Knowledge BasedAuthentication Attacks", University Technology Malaysia (UTM), 2010, pp. 765 - 775.

[8] Priti C. Golhar, Dr. D.S. Adane, “Graphical KnowledgeBased Authentication Mechanism", ISSN, Volume 2,Issue 10, October 2012, pp. 48 - 54.

[9] Sonia Chiasson, Elizabeth Stobert, Alain Forget,Persuasive Cued Click-Points: Design, Implementation,and Evaluation of a Knowledge-Based AuthenticationMechanisms”, IEEE TRANSACTIONS ONDEPENDABLE AND SECURE COMPUTING, VOL. 9,No.2, MARCH/APRIL 2012, pp. 222 - 235.

[10] Muhammad Daniel Hafiz, Abdul Hanan Abdullah,Norafida Ithnin, “Towards Identifying Usability and Security Features of Graphical Password in KnowledgeBased Authentication Technique", 2008, IEEE.