A Novel Authentication Mechanism with Efficient Mathematic Based Technique

Balajee R. M.[1,*], Suresh Kallam[2], M. K. Jayanthi Kannan[3]

[1]Research Scholar, School of Computer Science and Engineering, Faculty of Engineering and Technology, JAIN (Deemed to be University), Bangalore – 562112, ORCID: 0000-0003-2928-9509, India

[2]School of Computer Science and Engineering, Faculty of Engineering and Technology, JAIN (Deemed to be University), Bangalore – 562112, ORCID: 0000-0002-8698-2644, India

[3]School of Computing Science and Engineering, VIT Bhopal University, Bhopal-Indore Highway, Kothrikalan, Sehore, Madhya Pradesh – 466114, ORCID: 0000-0001-8238-9731, India

Email: balajee.rm@gmail.com; sureshkallam@gmail.com; dr.mkjayanthikannan@gmail.com

Abstract

The security of any device or data on it is greatly dependent on the authentication and session handling. Using an MFA-based OTP method, the most popular web apps, such as communication mail, social media platforms, and financial transactions, manage spoofing attempts and attempt to keep them to a minimum. There is statistical evidence that indicates that between April 2020 and March 2022, this well-known OTP mechanism lost 1434.75 crore rupees, further weakening its hold on security. This unusual situation is driving research toward authentication methods that rely solely on itself without external aid. In order to improve security, self-dependent authentication methods (passwords, combinations of image clicks, etc.) have not been streamlined or made sufficiently dynamic. By comparing state-of-the-art methods, the suggested work, Mathematic Based Technique (MBT), will enhance the dynamic behaviour of passwords and optimize to give greater security. In the event of an eavesdropping assault, the Mathematic Based Technique (MBT) will make it difficult for hackers to pull the efforts to crack the password with the probability with permutation value is equal to O (78^{10}). Mathematical proof of the result is provided, and it is compared to the six best state-of-the-art mechanisms which are now in use, those are Picasso Pass (PP) which uses layered mechanism, Dynamic Password Protocol (DPP) which uses date and time in it, Dynamic Pattern Image (DPI) which resembles mobile pattern authentication, Dynamic Array Pin (DAP) which uses area based pin or a pre-defined pin, and Bag of Password (BP) which uses image.

Keywords: Self dependent Authentication; Probability with Permutation; CBP-Challenge Based Password; DPI-Dynamic Pattern Image; DPP-Dynamic Password Protocol; DAP-Dynamic Array Pin; PP-Picasso Pass and BP-Bag of Password; MBT-Mathematic Based Technique

1. Introduction

The system's session handling and authentication are crucial components to consider while evaluating the security. Before session handling is involved, the authentication is the vital one to consider, which allows a user to access system resources. On the way of enhancing the authentication process, which can only permit the associated user to access available and authorized resources and it becomes the main goal of the research. Certain authentication mechanisms have a visually appealing design that makes it much easier for users to remember and recall their required passwords to enter for logging in. Examples of these mechanisms also include few which are based on color combinations [10], spin wheels [12], unlocking with patterns [8], behavior based approaches [4]. The most widely used and popular authentication in today's world is the method having 2 steps and we called it as Multi Factor Authentication (MFA) and it mostly associated with OTP's. This also accomplished with the use of email

DOI: https://doi.org/10.54216/JCIM.150107
Received: January 30, 2024 Revised: April 27, 2024 Accepted: July 24, 2024

authentication from a network and mail provider, also with periodic change of text provider from authenticator software like Microsoft Authenticator. All these mechanism's relying on the third-party applications or telecommunication providers, which is the problem to consider. This technique greatly increases the likelihood of a data leak. The Times of India survey evidence stating the fact about a whooping loss of approximately Rs. 5,000 crore [15] in an Indian sub-continent region which also best describes the likelihood of a data leak in the existing mechanism. This clearly communicates the idea that MFA is popular but not concrete mechanism, it survives since there isn't a best suitable replacing method which can effectively offer authentication in order to provide better authentication security in self-dependent technique.

In addressing the self-dependent authentication, there are some methods which are in the filed and few are to be listed. The conventional and traditional password authentication technique is slowly and gradually changing towards a attractive way with a graphical things in it to provide the authentication procedure a more modern appearance and feel. Thus, a few graphical implementation techniques are pattern based unlock [8], spin wheel [12], and color-based authentication [10]. When things about the enhancement of authentication security with the consider of mentioned strategies, the first thing is that which comes to mind is that they are concentrating on improving the graphical ability and providing attractive end user's experience which is in contrast with our goal of providing better authentication security. When utilizing or thinking about the additional hardware based authentication techniques like MFA (two step or multi step), the techniques with the likes of behavior-based authentication [11] might be coming in picture. Using this technique, the actions of the individual will be studied and recorded. If the algorithm anticipates any odd actions which seems to be not a normal one, then the login may be restricted. The problem with this technique is that, on occasion, an actual user's differentiated login activity may also be restricted because of a change in environment or behavior.

There are some other technique which tries to replace the MFA with OTP and those eager market technique which try to efficiently replace are biometric based authentication, computer vision and RFID based authentication. These authentication techniques are aid to bring unique way in the process of authentication. Also few more authentication techniques which gained faith in market and likes of face recognition and finger print recognition. The background behind these techniques are the uniqueness of the source of input with once finger print or once face which cannot be duplicated with other persons. At the same time, these are disadvantages on these techniques, even though it had uniqueness in the input resource and those are coming up in the way of additional hardware in use. If the face need to be scanned, there is a need of camera and finger print required the finger print scanner. These devices need to be there, where you need to authenticate. Think about today's world, people used to move around and try to login in various devices as per the requirement or need. All these places and systems should be associated with the additional hardware to do the authentication which is practically impossible or making the scenario to be rare to get suited for flexible authentication. This exactly says about the issue and the need of self-dependent authentication which provides the flexibility in authentication and as the name resembles, it is self-dependent and no need of any additional hardware for the authentication. At the same time, there is an issue in considering the self dependent authentication and that is about the reliability of authentication with eavesdropping attack. Every time someone considers enhancing the security of self-dependent authentication, there may also be good consideration of changing the password dynamically. The password that is provided for login should be changed on each try with the new value and the user need to remember these things easily. This leads to certain queries here by the found or identified techniques and those are, (i) The type of tip that can be given to the user to help them remember the password?, (ii) The method by which dynamicity will be included into the password?, (iii) The number of passwords the user can recall?, (iv) How likely is it that someone will hack the password?, (v) How much the method is enhancing the self-dependent authentication process?.

2. Literature Survey

Some excellent state-of-the-art protocols currently in use, such as Picasso Pass (PP) which uses layered mechanism, Dynamic Password Protocol (DPP) which uses date and time in it, Dynamic Pattern Image (DPI) which resembles mobile pattern authentication, Dynamic Array Pin (DAP) which uses area based pin or a pre-defined pin, and Bag of Password (BP) which uses image can be used to answer problems partially regarding dynamic password changes. The current time will be incorporated into the text which act as a password as an optional feature by using the technique Dynamic Password based Protocol [2] method. The timing can be adjusted to any position or slot of the password, although there are two hour and two minute digits cumulatively leads to four numbers or slot filling on the password. The known application value (current time) to introduce dynamicity is the problem here. At the same time, it is also known to others and will become easy to crack it. Only issue to the hackers is to identify the slot belongs to time filling on the password.

DOI: https://doi.org/10.54216/JCIM.150107
Received: January 30, 2024 Revised: April 27, 2024 Accepted: July 24, 2024

In order to use the Dynamic Array based Pin which uses area based pin or a pre-defined pin [5], the user must register themselves during the registration step with a fixed set of integers. There will be a show or display of two randomly generated or changed of sequence ordered rows of numbers during the login step. Every number between 0 and 9 will be present in both rows to match each other. In order to determine the current position of pass code text which will be used as password, the user must found the consecutive Level 0 - Registering User digits in the second row and obtain the match of corresponding upper row numbers or digits. Have those selected digits or integers, lastly, finish the pass code with those selected values and submit it into the website as a password. The problem here is that the numbers or the integers are fixed during the registration process which will not change and limited to the maximum of 10 digits for the number if integer selection.

During the login procedure, the Challenge Based Password (CP) which uses substitution of Mathematicematical symbols [9] approach will generate random numbers during login phase. Four fixed calculation types and one among those should be chosen by the user during the registration stage which need to the applied over the random number on the login stage. The computation by applying the selected Mathematic symbol result between each digit in the pass string will create the password text. The final password text that needs to be typed is the result which formed on this process. The last three methods on the specified four will have mechanism of appending the initial bit to either slot of pass string, but the issue here is to consider the bits in the same position for the pass string. Thus, the mechanism is still insufficient to generate further dynamicity.

The Picasso Pass (which uses layered approach) (PP) [3] is an intriguing five-layered dynamic password scheme; the main problem is that only one of the five layer is having dynamicity on it and which will be selected during the registration process. This device for logging in should have a 4*4 grind to display the things. The color as one layer, shape as one layer, theme as one layer, alphabet as one layer, and location as one layer and those are the five levels that are integrated in the grid as one after the other to show the user during login stage. The user must press the registered or chosen one (during registration stage) among the data present in five levels on five consecutive times. The 4*4 grid will be randomly sequenced the order of show which will make user to press different item on each time, but the issue is the user will press the same place on the screen which will be easily cracked by the hacker. Every time it displays a picture with several layer combinations, the user simply needs to select the original layer. For instance, the first iteration square must be selected, but the display will have an alphabet and a red square on it. Another alternative is to draw a blue circle with some shape on it. Another alternative has a yellow triangle with a few points inside of it. The user will reject all other disruptions and choose the precise square. The user must choose from five iterations in a similar manner to create the right combination. The problem here is that to choose the same place on every iteration over the five times is easy to crack.

Every time the Dynamic Pattern Image (resembles mobile pattern drawing) [6] method is used with a dynamic pattern were four nodes and three edges should be drawn by the user. When registering, the user must enter a four-digit number and register himself on the authentication process. When logging in, the misarranged sequence will be displayed or shown in a three-by-three matrix to the end user which will allowing the end user to create a pattern by matching the numbers which are provided in the registration stage. When a user requests to logging in, the pattern must get matched by the corresponding numbers which are entered during the registration process. The problem in this case is that the four-digit number is fixed, and the user may also see the number's sequence. Only thing is, it look like user entering different pattern but actually becomes easy to crack by seeing the display numbers. This method will not hold up in the event that the hacker launches an eavesdropping attack.

The bag of passwords (image based authentication) technique [4, 1], which uses image on its process of authentication which also requires the user to provide a new password each time when they logging in to the system. Here, the problem is to remembering number of passwords which will become difficult because of the numerous count and every time one of it need to be applied by the user when attempting to log in. The more passwords a person can remember, the more secure the system's authentication will be and the more complex the things to user. To facilitate and make the remembering process easier to the end user, the user will always see the photos linked to the password entry which will act a hint to the password and which makes the user to recall the password easily to a particular level. The images that are kept in the database will be shown or displayed to the user according that password will be expected back from the user. To maintain security in this case, the photos that are kept in the database are the encrypted one and again getting back to the user after decryption. Table 1 is a collection of the comparative authentication security survey results and it is shown.

DOI: https://doi.org/10.54216/JCIM.150107
Received: January 30, 2024 Revised: April 27, 2024 Accepted: July 24, 2024

Table 1: Issues and Features of Various Authentication Categories and Methodologies Available

Authentication Categorization	**Authentication Methodology**	**Issues in Proposed System**	**Features in Proposed System**
Hardware additionally required for login	Computer vision which can use RFID for its process of authentication. It can be scanned for authenticate the user [16]	Dependent on the excess hardware which is required to do the authentication.	Another hardware which took physical things which can be scanned from the end user (may be face scan through camera, barcode scan or QR code scan) and also which is also unique by its way.
	The user can use the finger print for the authentication which may provide the uniqueness [7]		Another hardware which took physical figure print from the end user and also which is also unique.
Attractive and graphical representation	This resembles the mobile pattern drawing to unlock the web pages [8]	When the eavesdropping attack comes in, it is exposed for the hacker to get listening in and makes the password as breakable one to the hacker.	User friendly way to represent the pass combination for authentication.
	The wheel should be spined and left in the proper position to match the character which is provided on the Level 0 - Registering User [12]		
	The password can be filled as color combination selection from the available one which should match the same in registration stage [10]	The password is filled with color combination so it is be restricted to select within 10 colors which is only within the easy possible differentiation can be done by the end user. Remarkably, it is also similar to the standard password way of logging in.	
Multi Factor Authentication	One time password is sent by the application through telecommunication provider [15]	It relies completely on the third-party app, the strength of the telecommunication network provider in that region and occasionally also depends on a mobile device to log in to a third-party app. These temporary text which sent may be that offers an instant pass link, code to execute on a click or pin to verify, etc.	The required pass pin for the login is created as random one and communicates back to the end user through mobile telecommunication.
	Microsoft authenticator like authenticator software's will provide or generate periodic change of text which can be used any time with in 30 sec or 1 min for the login purpose [14]		The required pass pin for the login is created as random one and communicates back to the end user through authenticator app and those pass pin is valid up to 30 seconds or 1 minute.
	Email based login link or One time password is sent by the application through email to the user for login process [15]		The required pass pin for the login is created as random one or the required pass link is created and communicates back to the end user through mail.

DOI: https://doi.org/10.54216/JCIM.150107
Received: January 30, 2024 Revised: April 27, 2024 Accepted: July 24, 2024

Behavior tracking based authentication	The user's behavior will be tracked and based on that deviation during login is absorbed. In this way authentication will be crosschecked on every login attempt [11]	When the actual user tries to login the system from a different location or from a different environment which is in forceful need, then the may wrongly predict the actual user as the fack user due to change of behavior and tries to potentially block the actual user as well.	The behavior tracking system will be hard to notice and its presence is hidden from user. This will not add any additional burden to the user while logging in.
Dynamic Approach for Password Entry during Login	Bag of Password (BP) which uses image as a hint of password [4, 1]	Due to limitations of number if images and location layer items which can be used to induce the dynamicity, it will restrict the number of iterations to a smaller level and in tern which is needed to break the password with eavesdropping considerations.	Dynamic behavior of password is improving due to change of password every time and it can with satnd against eaves dropping attack.
	Picasso Pass (PP) which uses number of levels for authentication [3]		Dynamic behavior of password is improving due to the proposed mechanism which had five levels in it.
	DAP (Dynamic Array Pin) which uses area based pin or fixed integers [5]	The total number of digits are limited to 0-9 and due to the nature of mechanism proposed, there can only be ten random values at a time for the display and scrolling which introduces limited dynamicity.	Dynamic behavior of password is improving due to selection of integers in registration stage and applying it on the login stage which holds scrolling nature for the pass string selection.
	Dynamic Pattern Image (DPI) which resembles like mobile pattern drawing but dynamic [6]	It cannot survive with eaves dropping attack consideration, especially when hackers listening in.	Every time when the end user draws the pattern to login, it appears to be different due to change of number positions in the grid displayed on the screen.
	Dynamic Password Protocol (DPP) which uses date and time on the password text [2]	The dynamic part of password is restricted to only four slots which are inducing the dynamic behavior over the login and this is not sufficient.	When the time keeps on changing, it changes the pass string also, since the time value is induced in the pass string.
	Challenge Based Password (CBP) which uses Mathematicematical operators for authentication process [9]	The selection of technique and operators (out of 4) will result in restricted dynamic behavior and reduced resistance to the attack as eavesdropping.	Due to operator selection during the registration stage, the displayed number will be modified by the operator and a new pass string will be applied for login purpose.

3. Proposed Mechanism – Mathematic Based Technique (MBT)

The Mathematic Based Technique had its core work with 4 processing levels. The levels are,

1. Level 0 – Registering User
2. Level 1 – Input Parameter Value Selection
3. Level 2 - Hidden Calculations

DOI: https://doi.org/10.54216/JCIM.150107
Received: January 30, 2024 Revised: April 27, 2024 Accepted: July 24, 2024

4. Level 3 - Password Entry

The level 1, 2, 3, three core levels of MBT will be associated with the ruleset based on the end user established at Level 0-Registering User.

3.1 Level 0 - Registering User

The end user must establish a pattern of entering the password on each try in Level 0-Registering User. The end user must first determine the number of slots (anywhere between max of 10 and min of 6).

The first step is for the user to select one, two, or three input variable names. These are not the values of the variables—just their names. Every user will have the same variable name, which will be named "IP_1" for the first user, "IP_2" for the second, and "IP_3" for the third. Here, IP is the Input Parameter.

Next, using the straightforward mathematically based concealed expression or formula, the user must decide and record the core part formula and choose slot for the core response (either min two or max three positions). Constant values are not restricted to use with the formula or expression and it is based on user preference. The following three factors should be taken care and to be accounted while determining the core part of expression or formula solution/response for filling the core slot.

(i) The answer/response value will always be positive, if in case negative then convert it as positive. Replacing only the sign negative to positive is enough.
(ii) Adding zero before the answer is the strategy to make up for any fixed core positions, if the actual answer digits are not sufficient to fill number of digits in the response.
(iii) Count the answer digits from left to right in relation to the number of core positions, if the fixed core positions are lesser than the number of answer digits, and discard the remaining answer digits which are excess on further right side.

The end-user must now establish a pattern for populating the password's with non-core positions. When providing a password in the non-core positions, you can calculate an expression or formula value that is suggested to be less complicated than the core part expression or formula (i.e., core answer can be done with + 1 or – 1, for instance). The end user can now use all specific input parameters (IP_1, IP_2, IP_3) as per the requirement and the solution to the core expression or formula, also known as $CORE_{RES}$, to fill in the remaining positions of non-core positions. In this case, the $CORE_{RES}$ is merely a Core expression or formula's solution. The non-core positions should likewise have one to three position as per the requirement chosen by the end user and the non-core positions corresponding

The proposed approach can be fine-tuned with further three more steps, in which the mandate one is the last and the initial two is the optional choices to select by the end user.

1. Choosing the Character Replacement
2. Choosing the Moment of Position
3. Input Selection and Creating Line Pattern

3.1.1 Choosing the Character Replacement

In the name of character replacement, one flexible option that the end user can opt for it, if required. In this, the end user can select any special character as per the wish from the set of alphabet (A–Z or a–z) which may be upper case or lower case for the replacement in relation to the numbers/character in a certain position (which may be a core position or a non-core position). The replacement character can also be chosen from the "simple character list" provided here "$,%,!,@,#,^, ,(,), &,*{,},<,>,[,],,,". Every digit from 0 to 9 must have its match associated with single character provided by the end-user in this stage. A replacement character match for the digits are allowed to have duplicates of character in it, it depends on the user wish only. In order to make the password as user-friendly and avoid the programmatically issues, there are few ignored characters which are not listed here. This is to ensure the password simplicity while entering and make the user experience flaw free.

As a last step in this, there should be the end-user process of choosing the position for the replacement (it is restricted to 1 position) with the chosen replacement character and as expected on the login phase, the original number should be replaced with this chosen replacement character to get the correct password for authentication.

Example: Matching Replacement Character with Digits and Selecting Position for the Replacement

Choosing replacement character for the digits from zero to nine is displayed in the table 2.

DOI: https://doi.org/10.54216/JCIM.150107
Received: January 30, 2024 Revised: April 27, 2024 Accepted: July 24, 2024

Table 2: Matching End-User Replacement Character with Digit

Actual Number	Chosen Replacement Character	Selected In
ZERO	z	Lower Case
ONE	z	Lower Case
TWO	Z	Upper Case
THREE	$	Simple Character List
FOUR	$	Simple Character List
FIVE	$	Simple Character List
SIX	X	Upper Case
SEVEN	x	Lower Case
EIGHT	Y	Upper Case
NINE	y	Lower Case

3.1.2 Choosing the Moment of Position

On the level 0 – registering the end user process they has an option to select the moving positions only if they required it. While selecting the moving positions, they need to select one direction as either right side or left side and then the number of steps or push that the current position will take on the password must be decided. To keep things clean and simple, it is essential about the step count with respect to the position should be limited to one or two only. In the end as an additional and optional one, now it is about to select the frequency of position movement and it should be selected as a periodic manner such as daily movement, weekly movement or else monthly movement. if not, another way of position movement selection can be done by the means of login status with the success count. Again on the way of keeping the authentication procedure clean and simple, the success count of login iteration can be chosen as either one or two. For the setup made with success iteration count or with the duration frequency, the entire slot will now be going in the selected direction as left side or right side. When the motion, the moving position comes to an edge, the further movement will be in a closed path. The path is virtually connected on left most edge with the right most edge as a rounded one.

3.1.3 Input Selection and Creating Line Pattern

In this phase, the end user need to draw a line drawing (for example, normally we will be saying this as pattern to unlock in a mobile devices) as shown figure 1 and it will be used to pick the input parameter values on the later stage during login attempt. The line drawing by the end-user should consider the following rule set, (i) The line drawing by the end user should be in the rule set of data structures tree format with out any looping in it, (ii) The pattern drawing should be having continuous flow in it (for an example, it is drawn with out taking the hand) and will not have any branches from any of the node or parallel edges will not be made from an any node and (iii) The tree format of data structure will have edges and nodes in it. On the final point of time (finish the drawing) the min count of connecting lines (edge) is said to be CL_{MIN} which have value as > or = to the count of end-user chosen input parameters IP_{COUNT}.

The input parameter values in future login will be chosen from the node positions which are drawn currently by the end-user in the line drawing. The values and sequence of input parameter will follow the line sequence from left to right and from the top to bottom approach (for an example, our normal writing order of text in a paper). In a 3 x 3 board, when the line drawing involved node count exceeding the IP_{COUNT} then IP_1 is assigned with first involved node on the line drawing and IP_2 with the second involved node on the line drawing and similarly IP_3 with the third involved node on the line drawing. On the first iteration, the required input parameters will take initial three involved node positions and corresponding number in a 3 x 3 board. Later, for the second iteration, it will move one position forward in a flow (for example, the IP_1 value will be considered with the second involved node on the line drawing and further all input values will be pushed one step forward in a line drawing). This will continue for every count of login success iterations.

DOI: https://doi.org/10.54216/JCIM.150107
Received: January 30, 2024 Revised: April 27, 2024 Accepted: July 24, 2024

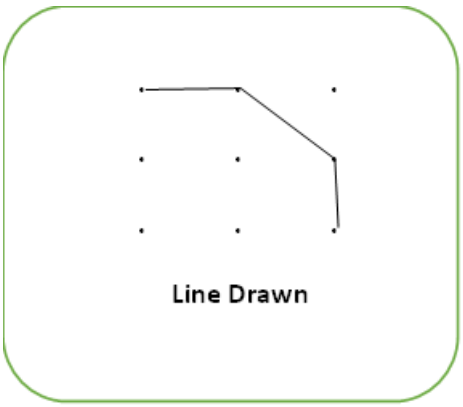
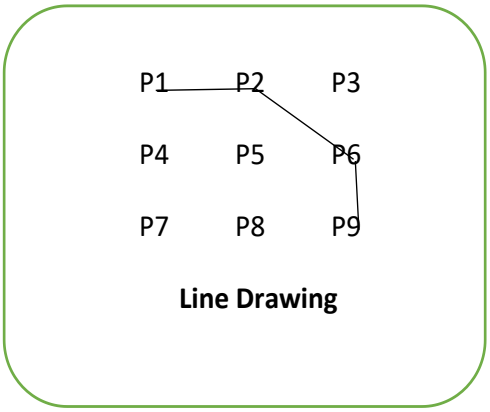


Figure 1. Line Drawn – Level 0 - Registering User

3.2 Level 1 - Input Parameter Value Selection

Example: Assuming five successful iteration of login completed already and going for the sixth one,



Considered Positions of Value Nodes

Iteration 1 : IP_1 = P1, IP_2 = P2, IP_3 = P6

Iteration 2 : IP_1 = P6, IP_2 = P9, IP_3 = P1

Iteration 3 : IP_1 = P1, IP_2 = P2, IP_3 = P6

Iteration 4 : IP_1 = P6, IP_2 = P9, IP_3 = P1

Iteration 5 : IP_1 = P1, IP_2 = P2, IP_3 = P6

Iteration 6 : IP_1 = P6, IP_2 = P9, IP_3 = P1

Figure 2. Input Parameter Value Selection – Part 1

The end user need to apply, Level 0 - Registering User rule for the selection of value node positions with respect to input parameters and successful login count as depicted in figure 2.

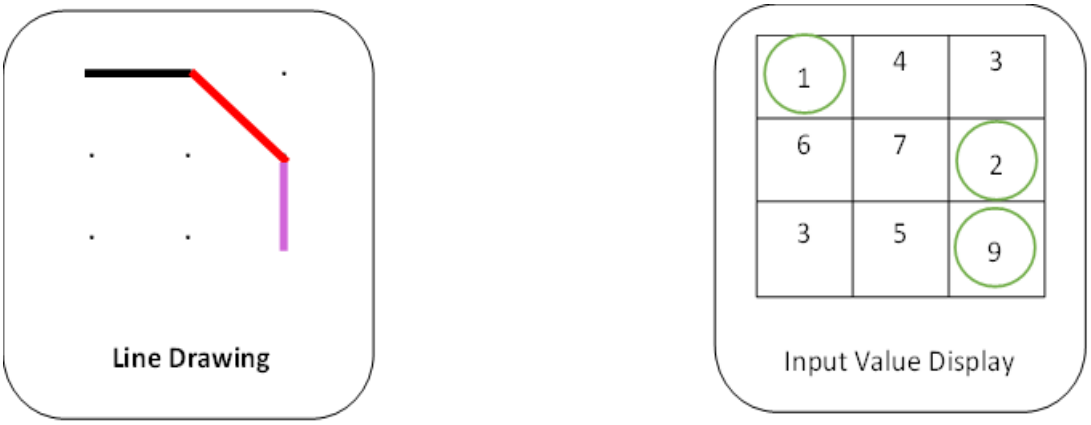


Figure 3. Input Parameter Value Selection – Part 2

Now the end user need to choose value node positions for the input parameters on the 6th successful iteration as shown in figure 2 and figure 3.

6th Iteration: IP_1 = P6 (2), IP_2 = P9 (9), IP_3 = P1 (1)

DOI: https://doi.org/10.54216/JCIM.150107
Received: January 30, 2024 Revised: April 27, 2024 Accepted: July 24, 2024

3.3 Level 2 - Hidden Calculations

Now the end user need to apply the formula which he or she already registered and know. The formula for th core slot is taken and applied with the input parameter value which is selected from the figure 2. Similarly, after attaining the solution for the core part, the non-core part expression or formula is taken and applied with the respective values for the non-core part solution. At the end of this stage, the password with solution for all slots will be ready. Then after, we need to substitute the replacement character if it is opted and further there should be position moving, similarly, if it is already opted by the end user during level 0 – registering user.

Example: Considering the period as a second week and applying the calculation as shown in table 3.

Table 3 provides the step-by-step instructions for arriving at the final password using the chosen input data for the second week of login.

Table 3: Password Arrival with Input Parameters and Formulas – Second Week

Involved Process	Metrics and Expressions	Password Arrival
Step 1: Workout of Core Section	Input Parameters: $IP_1 = 2$, $IP_2 = 9$ and $IP_3 = 1$ Expression: $IP_1 - IP_2 + IP_3 + 500 = 2 – 9 + 1 + 500 = 494$	_ _ _ 4 9 4 _
Step 2: Workout of Core Section – Part 1	Input Parameters: $IP_1 = 2$, $IP_2 = 9$, $IP_3 = 1$ and $CORE_{RES} = 494$ Expression: $CORE_{RES} + 1 = 495$	4 9 5 4 9 4 _
Step 3: Workout of Core Section – Part 2	Input Parameters: $IP_1 = 2$, $IP_2 = 9$, $IP_3 = 1$ and $CORE_{RES} = 494$ Expression: $CORE_{RES} – 1 = 493$	4 9 5 4 9 4 4
Step 4: Character Replacement	Input: 0 – z, 1, - z, 2 – Z, 3 – $, 4 – $, 5 - $, 6 - X, 7 - x, 8 - Y, 9 - y	4 9 5 4 9 4 $
Step 5: Movement of Position	Input 1st Week Slot: _ _ _ _ _ _ _	$ 4 9 5 4 9 4

3.4 Level 3 - Password Entry

The password is calculated in the level 2 - hidden calculations. The calculated password is also applied with the replacement character and position movement as opted. Then the final password is applied over the page og login. If the system calculated value as per the rules provided and your password is matched, then login success or else login fail. **Example:** Password entry

Calculated Password: $ 4 9 5 4 9 4

4. Research Parameters and Result

4.1 Mathematic Based Proof Parameters

Table 4 shows the mathematic formula which are present now for the calculation of permutations and combinations. The formula will be chosen as per the requirements and the requirements here are about to allow redundancy in position values and also the position or place value matters in the final solution framed. The said requirements are get suited with one formula from permutation and that is selected for our mathematic calculation. The comparison and the selection details with metric considered are shown in table 4.

DOI: https://doi.org/10.54216/JCIM.150107
Received: January 30, 2024 Revised: April 27, 2024 Accepted: July 24, 2024

Table 4: Mathematic Based Technique – Suitable Formula Selection

Is the position or place of value considered	Is the Redundancy Permitted	Permutation Formula (PF) or Combination Formula (CF)	Actual Mathematic Formula	Status of Selection for Proposed MBT
Considered	Not Permitted	PF	$n_{p_r} = \frac{n!}{(n-r)!}$	Not Selected
Considered	Permitted	PF	$n_{p_r} = n^r$	Selected
Not Considered	Not Permitted	CF	$n_{c_r} = \frac{n!}{r!\,(n-r)!}$	Not Selected
Not Considered	Permitted	CF	$n + r - 1_{c_r} = \frac{(n+r-1)!}{r!\,(n-1)!}$	Not Selected

The permutation formula is selected from the table 4 and further the considered scenario for proposed technique is given below,

Scenario 1: Without Considering Eaves Dropping Attack

- Iterations to Crack Password – CPI-WOED

Scenario 2: Considering Eaves Dropping Attack

- Iterations to Crack Password on Best Case – CPI-WED$_{(\text{BEST CASE})}$
- Iterations to Crack Password on Worst Case – CPI-WED$_{(\text{WORST CASE})}$

4.2 Mathematical Proof and Calculated Values for the Proposed Mechanism

In this mathematical proof section, all methods are scaled to max of 10 position slots and max character considerations on these methods are limited to specified 17 special characters in this article, all alphabets with case sensitiveness and also all decimal digits. The existing technique is subjected to max values as specified here and as per the applicability on those techniques as well. As per the table 4, the permutation formula selected and the got results are shown in table 5. The example shows the taken available position filling slot for the password as "9", but as per the technique, the max is restricted to "10" slots. Both values are shown below.

Table 5: Proposed MBT's Comparative Result

Metric	DPP	CBP	DAP	DPI	BP	PP	MBT$_{\text{Example}}$	MBT$_{\text{Max}}$
CPI-WED$_{(\text{WORST CASE})}$	2	7	1	1	1	5^5	78^9 (One Password Entry)	78^{10} (One Password Entry)
CPI-WED$_{(\text{BEST CASE})}$	10^{10}	7	10!	1	100	5^5	78^9 (One Password Entry)	78^{10} (One Password Entry)
CPI-WOED	62^{10}	10^{10}	10^{10}	9!-5!	52^{10}	60^5	78^9 (One Password Entry)	78^{10} (One Password Entry)

DOI: https://doi.org/10.54216/JCIM.150107
Received: January 30, 2024 Revised: April 27, 2024 Accepted: July 24, 2024

The proposed MBT's comparison result as a graph is given below in figure 4.

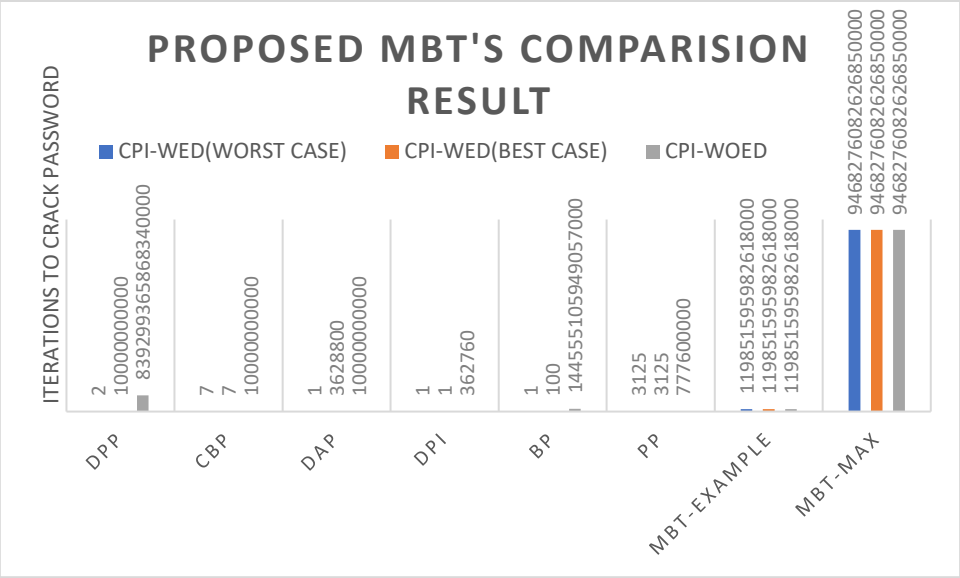


Figure 4. Proposed MBT's comparison Result for Iterations Required to Crack Password

Unlike other existing measures, the MBT is not subjected to random things which can turn the results abruptly. So, as per the MBT, the best case and worst case leads to same calculated value, since no randomness inducing possibility is there. Even the consideration of eavesdropping and non-consideration of eavesdropping does not make any change in MBT (but in existing techniques, changes will be there). The obtained results of proposed MBT is compared with the all possible existing technique results with best possibility on considering all characters to the max.

5. Conclusion

There are 13 core techniques in total surveyed with respect to authentication technique and its security improvement process. In the security improvement process, the focused area of research is narrow down to self-dependent authentication mechanism (does not relie on any additional devices or third party network support). In this process of improving the self-dependent authentication technique, there are some good existing techniques surveyed. In the mentioned 13 research articles, there are 6 self-dependent way of authentication with dynamic password change is found as the existing best fit and the same is taken for the comparison of proposed work. Those six best existing state of the art techniques including PP which uses layered mechanism, DPP which uses date and time in it, CBP which uses selected operators on its authentication process, DPI which resembles mobile pattern authentication, DAP which uses area based pin or a pre-defined pin, and BP which uses image. These techniques are compared with the Math-Based-Technique (MBT) in two ways. The MBT-Example and the MBT-Max both are compared with the six existing best techniques. There is also a primary concern which divides the comparison in two major parts and that primary concern is the consideration of eaves dropping attack which is a depreciator of self-dependent authentication technique. Further in clear research focus of considering eaves dropping attack, the research is conducted with the best case and worst case scenarios on all the methods taken for comparison. The measured value of 78^{10} is the achieved best result from the proposed MBT technique and it says, that much attempts required by the hacker to crack the password in every single iteration which is almost impossible. The probability to crack the pass string is inverse of 78^{10} (i.e., $1 / 78^{10}$) for the hackers.

References

[1] Balajee, R. M., et.al., "Authentication Improvization by the Image with Random Choice Approach." International Computation and Information Tech., ICICIT 2021. 2022. 61-71.

[2] Channabasava, H., et.al.,. Improving Authentication with DPP. Proceedings, Smart Computng Conference, 2019, Vol. 2, pp. 597-611.

[3] van Eekelen, et.al., "Dynamic password with graphical schemas", The Hague University of Appled Sciences. 2014.

DOI: https://doi.org/10.54216/JCIM.150107
Received: January 30, 2024 Revised: April 27, 2024 Accepted: July 24, 2024

[4] MK, J. K. (2021, July). Bag of Password Tech for Authentication and Analysis with Python, Java and PHP Languages. International Confrence in Communication Systems pp. 1030-1037. 2019.

[5] Boudour, R., et.al.,. DAP: A NFC payment security technique. Journal of Informtion Security: 6(29), 325-338, 2020.

[6] Sherubha, "Graph Based Event Measurement for Analyzing Distributed Anomalies in Sensor Networks", Sådhanå(Springer), 45:212, https://doi.org/10.1007/s12046-020-01451-w

[7] Piyush K. Pareek, Pixel Level Image Fusion in Moving objection Detection and Tracking with Machine Learning ",Fusion: Practice and Applications, Volume 2 , Issue 1 , PP: 42-60, 2020

[8] Shivam Grover, Kshitij Sidana, Vanita Jain, "Egocentric Performance Capture: A Review", Fusion: Practice and Applications, Volume 2, Issue 2 , PP: 64-73, 2020.

[9] Abdel Nasser H. Zaied, Mahmoud Ismail and Salwa El- Sayed, A Survey on Meta-heuristic Algorithms for Global Optimization Problems, Journal of Intelligent Systems and Internet of Things,Volume 1 , Issue 1 , PP: 48-60, 2020

[10] Mahmoud H.Alnamoly, Ahmed M. Alzohairy, Ibrahim M. El-Henawy, "A survey on gel images analysis software tools, Journal of Intelligent Systems and Internet of Things,Volume 1 , Issue 1 , PP: 40-47, 2021.

[11] A. Roy, et al., (2020) "Anasysing Behaviour with Fuzzy over EndUser Authentication Security." Journal of Discrete Mathematics, pp. 211 – 219, 2(21).

[12] M. Kameswara, et.al., (2018) "Graphical way with spin wheel authentication.", IJET, Vol. 7, Issue. 2, pp. 872-891.

[13] P Kumari, L S, et.al., "Authentication with lagrange interpolation by considering email". In proceedings of International Conference on Data Engg. and Tech, 2k18, pp. 142-153.

[14] Jessica B, et al., "Two Factor Factirization based Authentication Mechanism:An Analysis Over." in Digital Investigation 35, pp. 301-320.2013.

[15] M Amador, et al., "Vulnerabilities Findings over Banking with implementation of OTP and SMS Mechanismr." Wireless Networks pp. 1-14, 2022.

[16] Mudra H, et.al., "An Article on RFID Security Protocols with IoT", Electronics. 2023, 13(11): pp. 75-89.

[17] Sathya Preiya, V., and V. D. Ambeth Kumar. (2023). Deep Learning-Based Classification and Feature Extraction for Predicting Pathogenesis of Foot Ulcers in Patients with Diabetes. Diagnostics 13(12), 1983.

[18] Balakrishnan, Chitra, and V. D. Ambeth Kumar. (2023). IoT-Enabled Classification of Echocardiogram Images for Cardiovascular Disease Risk Prediction with Pre-Trained Recurrent Convolutional Neural Networks. Diagnostics 13(4), 775

[19] Hemamalini, Selvamani, and Visvam Devadoss Ambeth Kumar. (2022). Outlier Based Skimpy Regularization Fuzzy Clustering Algorithm for Diabetic Retinopathy Image Segmentation. Symmetry, 14(12), 2512.

[20] Ambeth Kumar, V.D. Ramakrishnan,M. (2013). Temple and Maternity Ward Security using FPRS. Journal of Electrical Engineering & Technology, 8(3), 633-637.

[21] Kumar, V.D.A., Sharmila, S., Kumar, A. et al. (2023). A novel solution for finding postpartum haemorrhage using fuzzy neural techniques. Neural Comput & Applic. 35(33), 23683–23696

[22] Kumar, V.D.A., Ruphitha, S.V., Kumar, A. et al. An effective method for predicting postpartum haemorrhage using deep learning techniques. Multimed Tools Appl (2022). https://doi.org/10.1007/s11042-021-11622-4.

DOI: https://doi.org/10.54216/JCIM.150107
Received: January 30, 2024 Revised: April 27, 2024 Accepted: July 24, 2024