International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Novel Authentication Mechanism with Efficient Math Based Approach

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

Submitted: 27/01/2024 **Revised**: 05/03/2024 **Accepted**: 13/03/2024

Abstract: The authentication and session handling plays a vital role on the security of any device or data present on that. The top web applications including the communication mail, social information sharing platforms, financial transactions are controlling the spoofing attacks and try to kept it in minimal by using the MFA based OTP mechanism. This well known OTP mechanism is also start to lose its grip over the security with the statistical proof of losing 1434.75 crore rupees between April 2020 to March 2022. This abnormal scenario is pushing the research to focus on self relaying way of authentication without any additional support. The issue of self relaying authentication (likes of password, combination of image clicks, etc..) is not been optimized and not been enough dynamic to provide better security. The proposed work, Math Based Approach (MBA) will improve the dynamic behaviour of password and optimize to provide better security by comparing the state of the art techniques. The Math Based Approach (MBA) will bring the attempts required to break the password in presence of eaves dropping attack with the permutation value equal to O (7810). The result is proved by a mathematical way and which is compared with 6 best existing state-of-the-art mechanisms like Challenge Based Password (CBP), Dynamic Password Protocol (DPP), Dynamic Pattern Image (DPI), Dynamic Array Pin (DAP), PicassoPass (PP) and Bag of Password (BP).

Keywords: *Self Relying Authentication, Multi Factor Authentication (MFA), Permutation, Math Based Approach (MBA), Challenge Based Password (CBP), Dynamic Password Protocol (DPP), Dynamic Pattern Image (DPI), Dynamic Array Pin (DAP), PicassoPass (PP) and Bag of Password (BP).*

1. Introduction

The research here is only focusing on the self relying authentication mechanism like entering the password, since due to the reason, the trending mechanisms like MFA [11, 18, 19, 26] leads to an loop hole for cracking the system as per the survey result with the statistical proof of losing 1434.75 crore rupees between April 2020 to March 2022 [22]. This in the region of India.

The self relying mechanism is the one which can able to go on as self dependent on the authentication process (like filling the password). This self relying mechanism will not required any third party support or external device support on filling the password. In a best understanding way, we can say, the OTP mechanism required third part support and so it is not a self relying mechanism and also we can say some examples of being not a self relying authentication mechanism as iris scanning authentication, finger print scanning based authentication, face recognition authentication, etc., since these authentication mechanism requires the additional device to authenticate.

The biggest challenge of self relying authentication mechanism like password based one is about the eaves dropping attack. The eaves dropping attack is nothing but a scenario where the hackers will see the password entering in the system, may be standing near by or from a remote location. There is demand to prove the betterment of self relying authentication mechanism with the consideration of eaves dropping attack.

When focusing only on the self relying mechanism, the existing mechanism is not proven very good against the eavesdropping attack which is a known killer of self relying authentication mechanism. The research is focused to improve the number of attempts required to break the password with and with out the presence of eavesdropping attack. The focus is on target of achieving the improvement in result of the proposed mechanism with the comparison of existing best state of the art techniques (six) like Challenge Based Password (CBP), Dynamic Password Protocol (DPP), Dynamic Pattern Image (DPI), Dynamic Array Pin (DAP), PicassoPass (PP) and Bag of Password (BP) with the consideration of both scenarios with respect to eaves dropping attack. The result will be proved in the mathematical derivations. To prove it in mathematical way, the permutation and combination formulas will be analysed and suitable formula will be chosen and it will be used to calculate the values required to break the password. In other

[1] * *Research Scholar, School of Computer Science and Engineering, Faculty of Engineering and Technology, JAIN (Deemed to be University), Bangalore – 562112, India. ORCID: 0000-0003-2928-9509, Email ID: balajee.rm@gmail.com*
[2] *School of Computer Science and Engineering, Faculty of Engineering and Technology, JAIN (Deemed to be University), Bangalore – 562112, India. ORCID: 0000-0002-8698-2644, Email ID: sureshkallam@gmail.com*
[3] *School of Computing Science and Engineering, VIT Bhopal University, Bhopal-Indore Highway, Kothrikalan, Sehore, Madhya Pradesh – 466114, India. ORCID: 0000-0001-8238-9731, Email ID: dr.mkjayanthikannan@gmail.com*
** Corresponding Author Email: balajee.rm@gmail.com*

terms it can be said as the calculation made to find the possibility of hacker to break the password.

Finally, the narrow down approach for the research is going to be the protection of application in web and standalone against the authentication based attack with the consideration of self relying authentication mechanism with and with out eaves dropping attack by the efficient and novel state of the art self relying proposed authentication technique called Math Based Approach (MBA).

2. Literature Survey

When considering the security of the system, the authentication and session handling plays an important role. The authentication is the first step which led the user of the system to access the resources and then the session handling comes into the picture. The research is on the focus of improving the authentication mechanism which can allow only the corresponding user to access the system resources. Some authentication mechanisms are very attractive with graphical way, this attractiveness is on the way of remembering the password easily to do the login and few such are based on color combination based authentication [16], spin wheel based authentication [15], pattern unlock [14] in combination with behavior approach and the innovative bag of password approach [1].

The authentication mechanism as of now trending in todays world is with the Multi Factor Authentication (MFA) with the support if Mobile OTP from Network, Email Authentication, OTP from Authenticator Software like Microsoft Authenticator. The issue with this mechanism is about the dependency with the third part app or network provider. The data leak is highly possible on this approach and the best fact that describing the data leak in this approach is the proof of losing around thousand five hundred crore [22] in a country like India according to Time of India survey. This strongly conveys the message that MFA is in trend because of the fact that there is no proper alternate mechanism which can efficiently provide authentication to counter MFA.

The biometric based authentication, CV and RFID based authentication is coming up with the uniqueness in authentication mechanism like once face or one figure print can not be matched with others. The issue here is about the additional device usage. Where ever we are going, all the places needs the same device to unlock the web page. This makes it complicate and the objective of the research here is to have self relying authentication mechanism which will reduce the dependency over the devices for authentication process.

The behavior based authentication [13] can be as used as a support with other authentication mechanism like MFA or device based authentication. The individuals behavior will be analyzed in this technique and if the algorithm predicts any abnormal behavior then the login can be restricted. The issue here is about some times the actual user may also be restricted from login due some change of location or environment where he or she actually be in.

The regular password authentication mechanism is slowly transforming with graphical way so that it will provide the refreshing look and feel on authentication process. In such a way, color based authentication [16], spin wheel based authentication [15] and pattern lock [14] are few technique of graphical implementation. When we think about in what way it is increasing the security then the answer straight away is these technique is not focusing on improving the security and in other way these techniques are focusing on refreshing look and feel experience of end user.

When every there is a thinking about improving the self relying authentication security, there come a thought of dynamic password change. In every attempt the entering password for login should be changed. The issue here is listed as,

(i) How many passwords the user can remember
(ii) What kind of hint can be provide to user for remembering the password
(iii) How many hints the user can remember
(iv) In what way, dynamicity will be induced in the password
(v) How much the technique is improving the self relying authentication mechanism
(vi) What is possibility of attacker to hack the password

On the way of addressing the questions on dynamic password change, there are some good existing state of the art protocols namely Challenge Based Password (CBP), Dynamic Password Protocol (DPP), Dynamic Pattern Image (DPI), Dynamic Array Pin (DAP), PicassoPass (PP) and Bag of Password (BP).

The Challenge Based Password [8] technique will provide random numbers during login process and there will be four types of fixed calculations can be applied over the random number. The answer of the calculations can be added with every digit if pass string. The resultant is the final password which need to be entered. The other 3 ways are adding first bit in either string, adding last bit in either string and adding same position bits in either string. In this way still the mechanism is not good enough to induce more dynamicity.

The Dynamic Password Protocol [7] technique will bring in the current timing in to the password as a optional one. The timing can be made in any position but total of four digit includes two hour digits and two minutes digits. The issue here is the known applying value (current time) to bring in the dynamicity.

The Dynamic Pattern Image [9] mechanism will have pattern drawing each time, the pattern is dynamic with 4

nodes and 3 edges. The user needs to provide 4 digit number during registration phase and during login phase the mis-ordered sequence will be displayed in 3*3 matrix to draw the pattern. The end user requestion the login needs to draw the patter to match the numbers provided in registration phase. The issue here is the 4 digit number is fixed and the sequence of number is also shown to end user. This technique will not with stand with the consideration of eaves dropping attack against the hacker.

The Dynamic Array Pin [5] mechanism needs user to register with fixed set of numbers during registration phase. During login phase, there will be display of two row of numbers, both the row of numbers are random generated. All numbers from 0-9 will be there in both the rows. The user need to find the number digits of registration phase sequential in second row and corresponding upper row numbers should be taken as the current position pass code. Then finally, fill the completed pass code to enter in the web page. Here the issue is during registration phase the numbers are fixed and that to 10 digits only.

The PicassoPass (PP) [4] is the interesting dynamic password mechanism with five layers, the issue here is only one all five data is fixed in registration phase. There is a 4*4 grind in this mechanism for login. In the grid there is 5 layers combined and those are color, shape, theme, alphabet and location. Five times the user have to press the registered data. Each time it will show multiple layer combination in picture, the user only know which is the original one need to choose. For example, the forst iteration square need to be chosen, but the display will have square in red color and alphabet in it. In another option, circle in blue color and some shape it it. In another option triangle in yellow color and some location in it. The user will select the exact square and reject other disturbances. Similarly five iterations, the user need to select for making correct combination. In this the issue is, in each iteration one among the five is correct in that way in 5.

The image based authentication like bag of password technique [1, 3] in which the user will enter different password every time during the login. Here, the remembrance of password will become a challenging task, since many password the user need to remember to enter during the login attempt. How many password, the user is remembering that much the authentication security of the system will improve. To make it easier, the images associated with the password entry will be shown to the user on every attempt, these images will be stored in the database. In that scenario, the images which are are stored in the database are encrypted [2, 6] for ensure the security.

The survey done on the authentication security in comparative basis is been listed in table 1.

Table 1: Existing Authentication Techniques and its Challenges

Categorization	Methodology	Features	Challenges
MFA [22]	Mobile OTP from Network [24]	Generates random pin and Sends in message	Depends on third party application, network strength and some times with the device like mobile which already have it as logged in to third part application which provides immediate pass link, code, pin, etc.
	Email Authentication [21]	Generates and sends authentication link or pass code in mail	
	OTP from Authenticator Software like Microsoft Authenticator [25]	Always ready with new random pin for every 30 seconds in authenticator application.	
Additional Device based Authentication	Biometric Authentication [10,12,17]	Physical data required to do authentication.	Additional devices required for authentication and dependent on the device.
	CV and RFID based Authentication [20, 23]	Face, Iris and Barcode based authentication	
Supportive Authentication	Behavioral Authentication [13]	We would not notice it easily util, it notified	The actual user may also got blocked by the system
Graphical Way	Color based Authentication [16]	Easier to remember the password	Very similar to generic password method
	Spin wheel Authentication [15]		Exposed to eavesdropping and it can be broken
	Pattern unlock [14]		
Dynamic Password Change	Bag of Password [1, 3]	Improves security a lot by dynamic approach and brings in graphical way for easier remembrance	The number of attempts required to break with eavesdropping considerations can be improved.

	PicassoPass [4]	Improves dynamic ability with 5 layers	
	DAP (Dynamic Array Pin) [5]	Scrolling of array introduces dynamic behavior and easier to use	The scrolling and dynamicity is limited to 10 random values
	Dynamic Pattern Image [9]	The dynamicity is achieved by mapping pattern to numbers	It is not withstand against eavesdropping attack
	Dynamic Password Protocol [7]	Introducing the time in the password	Only limited to 4 slots in dynamic behaviour
	Challenge Based Password [8]	Introducing operators in the password with random string	The operators and the method chosen (out of 4) will lead to lesser resistance against eavesdropping.

3. Proposed Mechanism – Math Based Approach (MBA)

The Math Based Approach had its core processing on four layers. The layers are,

(i) Registration Phase
(ii) Input Layer (virtual input selection in non physical way)
(iii) Hidden Layer (Simple Math Formula or Expression)
(iv) Password Filling Layer

These MBA's last 3 core layer will work on the basis of the end user's pattern rule got set during the registration phase.

3.1 Registration Phase

In the registration phase, the end user need to set the pattern of entering the password on each attempt. Initially, the number of slots need to be fixed by the end user (6 to 10 to make it simple and secure).

Example: User fixing 8 slots

_ _ _ _ _ _ _ _

Then the input variable names need to be chosen by the end user as either 1 or 2 or 3 variables. These are only variables names and not the values. The name of the variable is going to be same for all the user and named the first one as 'V_A', second one as 'V_B' and third one as 'V_C'.

Example: 2 Variables

V_A and V_B

Then the user need to fix the core formula and slot for core answer (2 slots to 3 slots) from the simple math based hidden formula/expression. The formula/expression can also include constant values as per user interest. The core formula/expression answer for the core slot will be taken with following three considerations. (i) The final value (answer) will be converted to positive one. (ii) If fixed core slots are less than the answer digit counts, add zero before the answer to compensate the extra core slots. (iii) If fixed core slots are more than the answer digits counts then consider the answer digits from left to right with respect to number of core slots and leave the remaining.

Example: Simple formula/expression and 3 slots

Core Formula / Expression: $V_A + V_B$ -1000.

Core Slot (Red Marked One): _ _ _ _ _ _ _ _

Now, the user need to set pattern of filling non core slots of the password. When filling the non core slot of the password, it can be some expression value which is recommendable to be simpler than the core formula/expression (for an example, it can be core answer + 1 or – 1 or adding the core answer's particular part + 1, etc.). Now for filling the remaining slots, the end user can able to use selected variables and answer of the core formula/expression which is said as CF_{ANS}. Here the CF_{ANS} is nothing but a Core Formula Answer. The non core slots should also be 2 to 3 slots and same considerations in core slot answer will be applied on the non core slot answers to get filled.

Example: 2 Non Core Slot Sets

Set 1 – Non Core Formula / Expression: CF_{ANS} + 100

Set 1 – Non Core Slot (Green Marked One): _ _ _ _ _ _ _ _

Set 2 – Non Core Formula / Expression: CF_{ANS} - 10

Set 2 – Non Core Slot (Violet Marked One): _ _ _ _ _ _ _ _

The end user further more can optionally go for two more options and the third one is mandatory

(i) Opting for the Substitution
(ii) Opting for the Slot Moving
(iii) Mandatory Drawing Pattern of Input Selection

3.1.1 Opting for the Substitution

The first optional value added metric is given to end user in the name of substitution. Here, the end user can choose the alphabet (A-Z or a-z) or any special character from the list of "!,@,#,$,%,^,&,*,(,),{,},[,], ,<,>" for the substation with respect to numbers in a particular slot (this may be core slot

or non core slot). They have to provide one character for each number from 0 to 9. The character may repeat as well (like same character for all or few numbers from 0 to 9). The few special characters are avoided on the basis of programmatic comparison reason to check with the existing password during authentication process and also to make this as user friendly one. Finally, the end user will fix the slots for the substitution (only one) of selected alphabet characters or special characters, in which the actual number will be replaced with the character mapped.

Example: Setting Characters and Choosing Slot for Substitution. Setting character for the numbers from 0 to 9 is shown in the table 2.

Table 2: Character Mapping for Numbers

Number	Selected Character	Chosen From
0	A	Capital Alphabet
1	A	Capital Alphabet
2	A	Small Alphabet
3	A	Small Alphabet
4	A	Small Alphabet
5	@	Special Character Set
6	@	Special Character Set
7	@	Special Character Set
8	@	Special Character Set
9	@	Special Character Set

Substitution slot (highlighted one): _ _ _ _ _ _ _

3.1.2 Opting for the Slot Moving

If the end user is interested then they can opt for the moving slots. Initially the direction of movement should be selected as right or left then the step count of movement need to be chosen. The step count had been restricted to 1 or 2 for maintaining the simplicity. Finally, the frequency of the movement should be chosen as periodic one like day, week or month wise or else the moving frequency will be chosen as per the successful attempt count for every countable iteration. The successful login attempt count to choose will be provided as 1 or 2 to maintain the simplicity in authentication process. Now, the entire slot will be moving towards that direction for fixed iteration or time period. The movement is in a cyclic manner means that the moving of right end slot will come to left side of the password in a round manner.

Example: Setting up the step count and frequency of movement

Step count: 1

Frequency of Movement: Weekly movement

3.1.3 Mandatory Drawing Pattern of Input Selection

The user can draw the pattern like in mobile phone login and use it for the input selection on the dynamic way and the example is shown in fig. 1. The pattern will be drawn on the 3x3 matrix. The lines are edges and the connecting points are nodes. The pattern is drawn under the considerations, (i) The pattern is not allowed to have any closed path in it and (ii) The minimum number of edges in the pattern (E_{MIN}) should be greater than or equal to the number of selected variable count V_{COUNT}.

After the pattern is drawn, as per the users number of variable name selection, that many number of nodes will be selected as value holding nodes in each iterations. The same values will be substituted for the variables correspondingly (first position node value to first variable V_A and second position node value to second variable V_B and finally third position node value to the last variable V_C). Initially, the first three node in the pattern (first node is the left most and top most one in the pattern) will be taken as value node and then further every successful iteration, the last value node of the previous successful iteration will be taken as the first value node of the current iteration and then edge sequentially further value nodes will be taken.

Example: Drawing Pattern with 2 Considerations (no cycle and $E_{MIN} >= V_{COUNT}$)

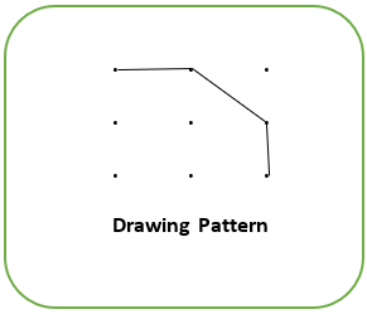


Fig. 1: Drawing Pattern – User Registration Phase

If the pattern comes to the end node, then it will be connected back to the first node in the pattern for the node value selection in a cyclic manner. During the process of system auto connecting the last node and first node of the pattern, If there are connecting points in between, then those are ignored.

3.1.4 Algorithm of MBA Registration Phase (MBA-RP)

Step 1: Initiate the registration process by filling the basic details required for authentication

(Name, User Name, Address, E-Mail ID, Contact Info).

Step 2: Fix the number of slots for password entry anywhere between 6 slots to 10 slots.

Step 3: Select the number of input variable ranging from 1 to 3 and it will be named as "V_A, V_B & V_C" correspondingly. The total count of variable will be stored in V_{COUNT}.

V_{COUNT} = {1 | 2 | 3}

Step 4: Fix the core formula/expression (can use selected variables and constant values) and core slot positions (2 or 3 slots) in a sequential manner for core formula answer entry with following considerations.

a. If core answer is negative then convert to same number positive value

b. If fixed core slots are less than the answer digit counts, add zero before the answer to compensate the extra core slots.

c. If fixed core slots are more than the answer digits counts then consider the answer digits from left to right with respect to number of core slots and leave the remaining.

Step 5: Set pattern of filling (fix slots from 2 to 3 for a non core slot set and fix formula/expression for each non core slot set) non core slots by secondary expressions using variable "V_A, V_B & V_C" which ever selected. These variable can be combined with the answer of core formula CF_{ANS}. The step 4 considerations will be applied for the non core slot answers too.

Step 6: If the user is opting for substitution, then proceed with MBA-RP-SUB algorithm.

If the user is not opting for the substitution then go to step 7.

Step 7: If the user is opting for slot moving, then proceed with MBA-RP-SM algorithm.

If the user is not opting for the slot moving then go to step 8.

Step 8: The user should go for drawing pattern of input selection, so proceed with MBA-RP-DP algorithm.

Step 9: Finish the registration process

3.1.4.1 Algorithm of MBA-RP-SUB

Step 1: Select the substitution character between A-Z, a-z and from the special characters "!,@,#,$,%,^,&,*,(,),{,},[,], ,<,>" against the number 0-9 with the rules.

a. Assign alphabet characters or special characters for all the numbers

b. The alphabet characters or special characters can be repeated against the numbers.

Step 2: Select the slot where the substitution need to be done (only one).

Step 3: Finish the MBA-RP-SUB process and go to step 7 of MBA-RP algorithm.

3.1.4.2 Algorithm of MBA-RP-SM

Step 1: Select the direction of movement as "Left" or "Right" over the slots.

Step 2: Select the step count of movement as 1 or 2.

Step 3: Select the frequency of movement as 3.a or 3.b

a. Select the frequency based on the count of successful login attempts. The successful login attempt count to choose will be provided as 1 or 2.

b. Select the frequency based on time period as day, week or month.

Step 4: The movement when it is in cyclic manner of the moving slot, the right most slot consider the left most slot as the next slot.

Step 5: Finish the MBA-RP-SM process and go to step 8 of MBA-RP algorithm.

3.1.4.3 Algorithm of MBA-RP-DP

Step 1: Initiate the drawing pattern by showing the 3x3 grid with points (nodes).

Step 2: Draw the pattern on the grid by drafting the lines (edges) over the points (nodes) with the rules,

a. The pattern is not allowed to have cycle (closed path) in it while drawing.

b. The minimum number of edges in the pattern (E_{MIN}) should be greater than or equal to the number of selected variable count $V_{COUNT.}$

If E_{MIN} >= V_{COUNT}, then valid or else invalid pattern.

Step 3: Selected number of variables in the set of "V_A, V_B & V_C" will be assigned with the

sequential position nodes in the drawn pattern as per the algorithm MBA-RP-DP-VN (Math Based Password – Registration Phase – Draw Pattern – Value Node), from where the values for the variables will be picked during login (3x3 grid will be shown with numbers to end users during login process).

Step 4: Finish the MBA-RP-DP process and go to step 8 of MBA-RP algorithm.

3.1.4.3.1 Algorithm of MBA-RP-DP-VN

Step 1: The pattern will be rendered from top most and left most edge of the drawn pattern.

Step 2: If assigning position nodes for the first login attempt (only successful login will count), then the first V_{COUNT} nodes in the drafting sequence will be a assigned as the position nodes for the variables "V_A, V_B & V_C" correspondingly and then go to step 5.

Step 3: If the end user already successfully logged in at least once, then the last attempt's last position node will be takes as the first position node for the current attempt.

Step 4: Assign V_{COUNT} position nodes by including the current first position node with the rules,

a. If $N_R >= V_{COUNT}$, then assign the position nodes in drafting sequence.

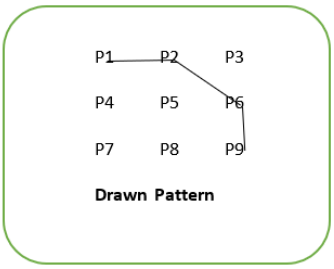
b. Else, consider the last node's next node as the first node and apply the drafting sequence to assign the position nodes.

where N_R is the sequentially remaining nodes count over the drawn pattern including current first position node.

Step 5: Finish the MBA-RP-DP-VN process and go to step 4 of MBA-RP-DP algorithm.

3.2 Input Layer (virtual input selection in non physical way)

Example: Considering 5 Successful login attempts made already



Considered Positions
First Attempt _: V_A = P1, V_B = P2
Second Attempt _: V_A = P2, V_B = P6
Third Attempt _: V_A = P6, V_B = P9
Fourth Attempt _: V_A = P9, V_B = P1
Fifth Attempt _: V_A = P1, V_B = P2
Sixth Attempt _: V_A = P2, V_B = P6

Fig. 2: User Input Selection – Login Page – Part 1

The input will be displayed to the end user in 3x3 matrix box. The user have to pick 1 or 2 or 3 variable values form the box as per the end user's registration phase rule and the example is shown in fig. 2.

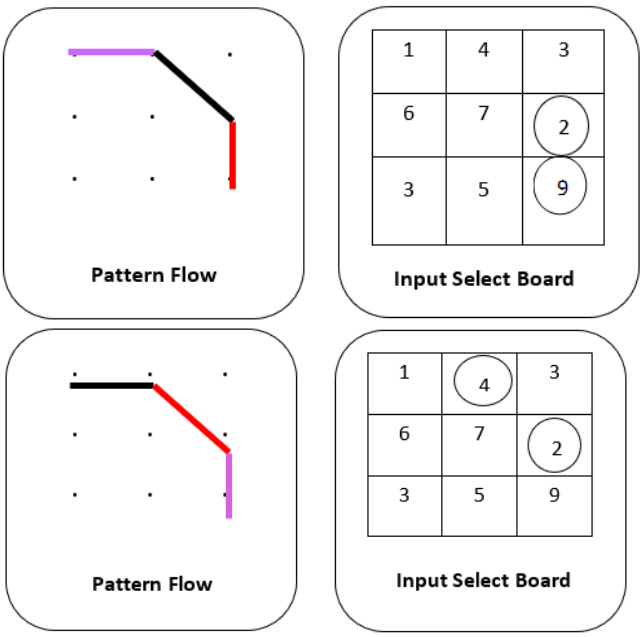


Fig. 3: User Input Selection – Login Page – Part 2

Sixth attempt choosing values (black indicated old, red indicated current and purple indicates future) are depicted in fig. 3.

Sixth Attempt: VA = P2 = 4, VB = P6 = 2

3.3 Hidden Layer (Simple Math Formula or Expression)

The user have calculate the math based password for the core slots and then calculate the password for the non core slots with simple expressions. The calculated password need to be modified as per the options opted (substitution and slot moving).

Example: Working on formula / expression with substitution and slot moving for 2nd week

The step by step process of arriving formula with the selected input values for the 2nd week of login is provided in the table 3.

Table 3: Arriving Password from Selected Input – Week 2

Step Wise Process	Input Values and Formula	Arriving Password
Step 1: Core Part	Input Values: V_A = 4, V_B = 2 Formula: V_A + V_B -1000	_ _ _ 9 9 4 _ _
Step 2: Set 1 – Non Core Part	Input Values: V_A = 4, V_B = 2, CF_{ANS} = 994	1 0 9 9 9 4 _ _

	Formula: CF_{ANS} + 100	
Step 3: Set 2 – Non Core Part	Input Values: V_A = 4, V_B = 2, CF_{ANS} = 994 Formula: CF_{ANS} – 10	1 0 9 9 9 4 9 8
Step 4: Optional Substitution	Input: 0 – A, 1, - A, 2 – a, 3 – a, 4 – a, 5 - @, 6 - @, 7 - @, 8 - @, 9 - @	1 0 9 9 9 4 9 @
Step 5: Optional Slot Moving	Input 1st Week Slot: _ _ _ _ _ _ _ _	@ 1 0 9 9 9 4 9

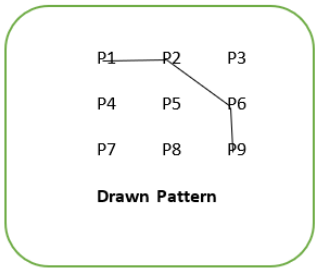
3.4 Password Filling Layer

The final password after modification with respect to the options opted during the registration phase, will be applied on the web page for the authentication with corresponding user name. It will be cross checked by the server generated password value for the corresponding user name with current input and formula/expression as per the registration phase rule. If the entered password got matched with the server generated password for the respective username then the authentication for using the web resources is success or else, it is failed.

Example: Filling Password

Current Password: @ 1 0 9 9 9 4 9

Additional Example: Seventh Iteration on Third Week



Considered Positions
First Attempt _: V_A = P1, V_B = P2
Second Attempt _: V_A = P2, V_B = P6
Third Attempt _: V_A = P6, V_B = P9
Fourth Attempt _: V_A = P9, V_B = P1
Fifth Attempt _: V_A = P1, V_B = P2
Sixth Attempt _: V_A = P2, V_B = P6
Seventh Attempt: V_A = P6, V_B = P9

Fig. 4: User Input Selection – Login Page – Part 3

Seventh attempt choosing values (black indicated old, red indicated current and purple indicates future) is depicted in fig.4 and fig. 5.

Fig. 5: User Input Selection – Login Page – Part 4

Sixth Attempt: V_A = P2 = 2, V_B = P6 = 9

Working on formula / expression with substitution and slot moving for 3rd week is shown in table 4.

Table 4: Arriving Password from Selected Input – Week 3

Step Wise Process	Input Values and Formula	Arriving Password
Step 1: Core Part	Input Values: V_A = 2, V_B = 9 Formula: V_A + V_B -1000	_ _ _ 9 8 9 _ _
Step 2: Set 1 – Non Core Part	Input Values: V_A = 2, V_B = 9, CF_{ANS} = 989 Formula: CF_{ANS} + 100	1 8 9 9 8 9 _ _
Step 3: Set 2 – Non Core Part	Input Values: V_A = 2, V_B = 9, CF_{ANS} = 989 Formula: CF_{ANS} – 10	1 8 9 9 8 9 9 7
Step 4: Optional Substitution	Input: 0 – A, 1, - A, 2 – a, 3 – a, 4 – a, 5 - @, 6 - @, 7 - @, 8 - @, 9 - @	1 8 9 9 8 9 9 @
Step 5: Optional Slot Moving	Input 2nd Week Slot: _ _ _ _ _ _ _ _	9 @ 1 8 9 9 8 9

Previous Password: @ 1 0 9 9 9 4 9

Current Password : 9 @ 1 8 9 9 8 9

4. Research Parameters and Result

The available formula based on the scenario is been provided in the table 5. The requirement for the proposed and existing approach is element position matters and repetition of elements is allowed. In such case the permutation formula is chosen accordingly

.

Table 5: Available Formulas and Selection Over that

Element Position Matters	Allowing Repetition of Elements	Permutation / Combination	Formula	Status of Chosen for the MBA Comparison
Yes	No	Permutation	$n_{p_r} = \frac{n!}{(n-r)!}$	NO
Yes	Yes	Permutation	$n_{p_r} = n^r$	YES

No	No	Combination	$n_{c_r} = \frac{n!}{r!\,(n-r)!}$	NO
No	Yes	Combination	$n+r-1_{c_r} = \frac{(n+r-1)!}{r!\,(n-1)!}$	NO

Table 6: Proposed Result of Math Based Approach (MBA)

Measure	CBP	DPI	DPP	DAP	PP	BP	MBA
ATK-ED$_{AT-BR}$ (Worst Case)	7	1	2	1	5^5	1	78^{10} (Single Iteration)
ATK-ED$_{AT-BR}$ (Best Case)	7	1	10^{10}	10!	5^5	100	78^{10} (Single Iteration)
ATK-WOED$_{AT-BR}$	10^{10}	9!-5!	62^{10}	10^{10}	60^5	52^{10}	78^{10} (Single Iteration)

The formulas are chosen and now the parameters as chosen as given,

(i) Attempt required to break the password with eavesdropping attack -> ATK-EDAT-BR
(ii) Attempt required to break the password without eavesdropping attack -> ATK-WOEDAT-BR
(iii) The ATK-EDAT-BR is considered in both best scenario and worst scenario for algorithm to perform and the measures are calculated.

These 3 parameters (including best case and worst case of number of attempt required to break the password with eaves dropping attack) will be taken for the existing 6 techniques and 1 proposed technique, so (6+1)*3=21 parameters.

4.2 Achieved Result on the Compared Techniques over the Considered Research Parameters

The result of Math Based Approach is shown in the table 6. All methods are restricted to maximum of 10 slots with usage of A-Z, a-z, 17 specified special characters and 0-9.

Formula Considered: $n_{p_r} = n^r$

r (No. of Slots) = 10

n (Total Available Options) = |A-Z| + |a-z| + |17 specified special characters| + |0-9|

n (Total Available Options) = 26 + 26 + 17 + 9

n (Total Available Options) = 78

Possibility to Break the Password on Every Single Iteration is $1 / n_{p_r} = 1 / 78^{10}$

Since the proposed mechanism MBA technique will behave in a same manner on both the scenarios, the result of the proposed technique is also going to be the same.

Scenario 1 -> Consideration of Eaves Dropping Attack,

Scenario 2 -> Consideration with out Eaves Dropping Attack

The comparison of all existing methods taken with the proposed technique with respect to following measures is shown in the table 6.

No. of attempts to break with eaves dropping attack (Best Case) -> ATK-ED$_{AT-BR}$ (Best Case),

No. of attempts to break with eaves dropping attack (Worst Case) -> ATK-ED$_{AT-BR}$ (Worst Case),

No. of attempts to break with out eaves dropping attack -> ATK-WOED$_{AT-BR}$

The mechanism of 6 best existing state-of-the-art technique includes Challenge Based Password (CBP), Dynamic Password Protocol (DPP), Dynamic Pattern Image (DPI), Dynamic Array Pin (DAP), PicassoPass (PP) and Bag of Password (BP) had been discussed in literature survey.

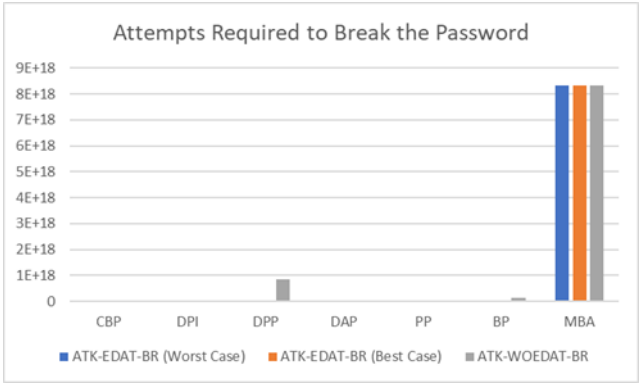


Fig. 6. Comparison Result Over Number of Attempts Required to Break the Password

The result in table 6 clearly shows that the proposed technique Math Based Approach (MBA) is out beaten the existing state of the art technique in authentication mechanism for improving the number of attempts required to break the password with and without consideration of

eaves dropping attack with the value of 78^{10}. The fig. 6 shows about the comparison result of proposed method and existing state of the art technique for the measure of number of attempts required to break the password in different scenario.

When considering the number of attempts required to break the password without eaves dropping attack, most of the techniques are performing almost well but not at the level of proposed technique. The second best after the proposed is Dynamic Password Protocol Approach which is with the value of 62^{10} which is far below the proposed measure of 78^{10}.

5. Conclusion

In view of improving authentication security with and with out consideration of eaves dropping attack is the challenging one. There are existing techniques which can bring in betterment in security in an efficient way. Such 13 core techniques are taken and examined. Finally the research narrow down is made with the inner field if improving authentication security named "dynamic password change" with six best existing state of the art techniques including DAP (Dynamic Array Pin), DPP (Dynamic Password Protocol), PP (Picassopass), CBP (Challenge Based Password), BP (Bag of Password) and (DMI) Dynamic Pattern Image. In this DMI is not with stand against eaves dropping attack, other 5 techniques are proven to a certain level to with stand against the eaves dropping attack. The proposed technique clearly out beaten all the existing state of the art best techniques with the measure of attempt required to break the password on both consideration of eaves dropping and non consideration of eaves dropping attack with the value of 78^{10}. In all the 3 measures number of attempts required to break the password without eaves dropping attack, number of attempts required to break the password with eaves dropping attack(best case), number of attempts required to break the password with eaves dropping attack(worst case), the proposed one is betting the existing with the value of 78^{10} which is way higher than the corresponding second best values of 62^{10} (Dynamic Password Protocol), 10^{10} (Dynamic Password Protocol), 5^{5} (PicassoPass). The proposed mechanism Math Based Approach (MBA) result also shows, the possibility for hacker to break the password in single attempt is $1 / 78^{10}$. This is highly impossible to do it so for the eave droppers or hackers.

Author contributions

Balajee R M : Conceptualization, Methodology, Software, Field study, Data curation, Writing-Original draft preparation, Reviewing and Editing, Software, Validation. **Suresh Kallam:** Investigation, Writing-Reviewing and Editing. **M K Jayanthi Kannan:** Investigation, Writing-Reviewing and Editing.

Conflicts of interest

No conflicts of interest from authors

References

[1] Balajee RM, MK JK. Performance Analysis of Bag of Password Authentication using Python, Java and PHP Implementation. In2021 6th International Conference on Communication and Electronics Systems (ICCES) 2021 Jul 8 (pp. 1032-1039). IEEE.

[2] R.M. Balajee, H. Mohapatra, K. Venkatesh, A comparative study on efficient cloud security, services, simulators, load balancing, resource scheduling and storage mechanisms. IOP Conf. Ser. Mater. Sci. Eng. 1070(1), 012053 (2021)

[3] Balajee RM, Jayanthi Kannan MK, Murali Mohan V. Image-Based Authentication Security Improvement by Randomized Selection Approach. InInventive Computation and Information Technologies 2022 (pp. 61-71). Springer, Singapore.

[4] Van Eekelen W, van den Elst J, Khan VJ. Dynamic layering graphical elements for graphical password schemes. Creating the Difference. 2014 Apr 3;65.

[5] Chabbi S, Boudour R, Semchedine F, Chefrour D. Dynamic array PIN: A novel approach to secure NFC electronic payment between ATM and smartphone. Information Security Journal: A Global Perspective. 2020 Nov 1;29(6):327-40.

[6] L. Voleti, R.M. Balajee, S.K. Vallepu, K. Bayoju, D. Srinivas, A secure image steganography using improved LSB technique and Vigenere cipher algorithm, in 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS) (IEEE, 2021 Mar 25), pp. 1005–1010

[7] Channabasava H, Kanthimathi S. Dynamic password protocol for user authentication. InIntelligent Computing-Proceedings of the Computing Conference 2019 Jul 16 (pp. 597-611). Springer, Cham.

[8] Fatima R, Siddiqui N, Sarosh Umar M, Khan MH. A novel text-based user authentication scheme using pseudo-dynamic password. InInformation and Communication Technology for Competitive Strategies 2019 (pp. 177-186). Springer, Singapore.

[9] Alalayah KM. Pattern Image based Dynamic Framework for Security in Web Application. International Journal. 2021 Mar;10(2).

[10] M.K. Rao, S.G. Santhi, M.A. Hussain, Multi factor user authentication mechanism using internet of things, in Proceedings of the Third International Conference on Advanced Informatics for Computing Research, 2019 Jun 15, pp. 1–5

[11] K.R. Ramya, B.M. Josephine, K.D. Praveen, M.B. Maruthi, C.S. Kumar, An efficient and secured biometric authentication for IoT. Int. J. Emerging Trends Eng. Res. 7(11), 604–609 (2019)

[12] S. Nalajala, B. Moukthika, M. Kaivalya, K. Samyuktha, N.L. Pratap, Data Security in cloud computing using three-factor authentication, in International Conference on Communication, Computing and Electronics Systems (Springer, Singapore, 2020), pp. 343–354

[13] A. Roy, S. Razia, N. Parveen, A.S. Rao, S.R. Nayak, R.C. Poonia, Fuzzy rule based intelligent system for user authentication based on user behaviour. J. Discr. Math. Sci. Cryptogr. 23(2), 409–417 (2020)

[14] G.K. Chaitanya, K. Raja Sekhar, Verification of pattern unlock and gait behavioural authentication through a machine learning approach. Int. J. Intell. Unmanned Syst. 2021

[15] M.K. Rao, S.G. Santhi, M.A. Hussain, Spin wheel based graphical password authentication resistant to peeping attack. Int. J. Eng. Technol. 7(2.7), 984–987 (2018)

[16] P. Saranya, S. Sharavanan, R. Vijai, R.M. Balajee, Authentication scheme for session passwords using color and image. Int. J. Smart Sensing Intell. Syst. 15, 10 (2017)

[17] A. Tarannum, Z.U. Rahman, L.K. Rao, T. Srinivasulu, A. Lay-Ekuakille, An efficient multimodal biometric sensing and authentication framework for distributed applications. IEEE Sens. J. 20(24), 15014–15025 (2020)

[18] Monisha, K., Rajasekhara Babu, M. (2019). A Novel Framework for Healthcare Monitoring System Through Cyber-Physical System. In: Internet of Things and Personalized Healthcare Systems. Springer Briefs in Applied Sciences and Technology(). Springer, Singapore, (pp. 21–36).

[19] S. Komatineni, G. Lingala, Secured E-voting system using two-factor biometric authentication, in 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC) (IEEE, 2020 Mar 11), pp. 245–248

[20] K. Neeraja, P.R. Rao, D.S. Maloji, D.M. Hussain, Implementation of security system for bank using open CV and RFID. Int. J. Eng. Technol. 7(2–7), 187 (2018)

[21] P.L. Kumari, G.S. Sekhar, Key exchange and E-mail authentication using lagrange interpolation, in Data Engineering and Communication Technology (Springer, Singapore, 2020), pp. 253–264

[22] https://timesofindia.indiatimes.com/business/india-business/over-9-lakh-incidents-of-phishing-otp-compromise-reported-in-last-two-years-42-indians-have-experienced-financial-fraud/articleshow/93361388.cms, News, Times of India Web Page, Referred on 2023 Aug 22.

[23] Marco KM. Facial Recognition Authentication Adds an Extra Layer of Security to Mobile Banking Systems. Journal of Applied Technology and Innovation (e-ISSN: 2600-7304). 2023;7(1):33.

[24] Aparicio A, Martínez-González MM, Cardeñoso-Payo V. App-based detection of vulnerable implementations of OTP SMS APIs in the banking sector. Wireless Networks. 2023 Jul 22:1-4.

[25] Berrios J, Mosher E, Benzo S, Grajeda C, Baggili I. Factorizing 2FA: Forensic analysis of two-factor authentication applications. Forensic Science International: Digital Investigation. 2023 Jul 1;45:301569.

[26] Suresh, K., RajasekharaBabu, M., & Patan, R. (2016, October). EEIoT: Energy efficient mechanism to leverage the Internet of Things (IoT). In 2016 International Conference on Emerging Technological Trends (ICETT) (pp. 1-4). IEEE.