# Novel Approach towards Authentication using Multi Level Password System

Bijoy Chhetri
Centre for Computers and Communication Technology, Chisopani, Sikkim, India

## ABSTRACT

The aim of this work is to design and develop authentication methods that is used to authorize user for access contents that are shared only when they have valid password. The system further thoroughly explores up to three levels of user authentication of user. Even though there are many varieties of folder protection system available, but several of them have failed due to key loggers and other threats that are promptly used by the intruders. The paper intends to create three level authentication system having three different kind of authorization. The pass key and process difficulty increase with each level. The project comprises of text password that is pass phrase, image-based password and color combination for the three levels respectively. This methodology is designed to ensure that there are negligible chances to crack password and even if intruder have cracked the first level or second level, it would be impossible to crack the third one. Many folder protection systems have proved to be more unfriendly and chance of losing data is more if password is forgotten so an attempt has been made to incorporate levels of protection to the contents so that only authorized user can access it.

## Keywords

Confidentiality, Authentication, Security, key, 3 level password.

## 1. INTRODUCTION

In this era of information technology and data science, the security parameters such as Confidentiality, Availability and Integrity has been compromised to various levels so much so that Industries are outsourcing their data to third party on agreement that their data should not be lost. In this case also the information security features have to be kept intact and no unauthorized person or system unless permitted should be able to access the contents. CIA model [5] is considered to be the key feature for the information security. The crucial components of security such as confidentiality, integrity and availability are addressed along with authentication to protect the data from unauthorized access. The existing model of CIA, as shown in the Fig 1 models the security aspects of network, network medium, media and data that transfers and stored in the media. Along with these three major pillars of security system, Authentication deal with the predefined credentials that are accessed from the media storage, matched with the who wants to access and only valid credentials will be granted access.

.

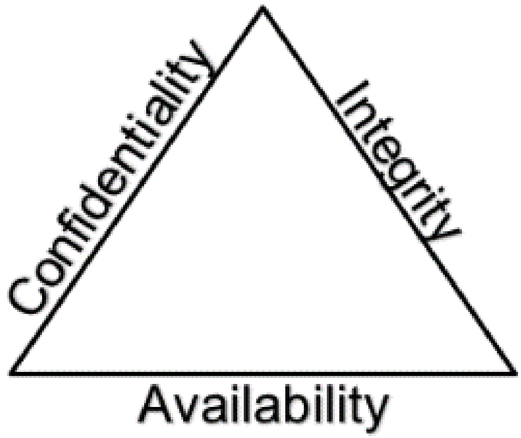

**Fig 1 Three Parameters of Security**

### 1.1 Confidentiality

One of the aspects of security, Confidentiality is maintaining a privacy. Data, media or medium of communication are meant to reach to the person who is intended to access but not to the wrong hands. The vulnerability of data rises with an unauthorized data. Thus, the feature of confidentiality is to prove that system implements a mechanism to forgo all unintended read and write while allowing only the intended access so that the message is seen to right person or system. Measures undertaken to ensure confidentiality is designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it. Access must be restricted to those authorized to view the data in question. It is common, as well, for data to be categorized according to the amount and type of damage that could be done should it fall into unintended hands. More or less stringent measures can then be implemented according to those categories.

### 1.2 Integrity

This measure of security is keeping alive with the consistency, accuracy, and trustworthiness of data over its period of communication and access. The originality of data should not be lost meaning to say that it should not have changed in transit so that receiver receives the same data sent by the sender. The core steps must be taken to ensure that the integrity of data is maintained by providing certain methods that are in place like file permissions, user access controls, version control etc. which is to prevent some of the erroneous changes or also to take control of accidental deletion by authorized users becoming a problem.

### 1.3 Availability

Availability is best termed as the reliability concept that any loss in data has to be recovered and also all the performing hardware when goes non-performing must repairs immediately when needed. The loss should not be the overhead to the entire transmission of data however it should maintain its originality in some form. This can be achieved by having efficient and effectively functioning operating system and performing environment that is free of any kind of software conflicts. It also becomes mandated that the system is kept up with the latest updates and upgrades so that it is kept current with all necessary security features added.

To enable all of the above discussed primary constraints of network security, we propose single protection System that uses a very easy and user-friendly interaction for the best and easy use. This system, built using C# language, is made for the windows application to protect the folder and give the perfect security to the folder.In order to make efficient use of this product, the authorized user must make a registration and provide text-based password. After having a text-based password, there is color combination password where registered user can set any color combination of any three-color given. Further, User can also make their own pattern by selecting different color combinations, in third case user have to enter picture password where the user can select any picture, then the picture, that is selected and is broken into different pieces then the user sets the picture password by clicking the different piece of image.

## 2. SURVEY OF AUTHENTICATION TECHNIQUES

Various authentication methods and methodologies are available in the research beds but for now few of the below mentioned has been highlighted here which are based on the scheme of Authentication that how does any user can be verified based on Token Based Authentication, Image or Biometric based and Password based (textual/Image) Authentication System [1-3].Token based System uses techniques to use tokens such as smart cards that are widely used by everyone. The method also uses combination of Textual Authentication to enhance the security of the system. Digits PIN is combined with the ATM card and other exchange cards that is an example of token-based Authentication. Biometric/ Image authentication techniques, to enumerate fingerprints, iris scan, and facial recognition, are nowadays fairly and widely adopted approaches [5-7]. However, the scheme may be little expensive and the processing of the data requires time making it bit slower and un reliable in terms of real time and time stamped consumption. But, this type is highest level of security which is reputable and cannot be shared or used for any unauthorized access to the contents.

Paper[9] presents a survey and a comparison of emerging techniques for image authentication. Methods are classified according to the service they provide, that is strict or selective authentication, tamper detection, localization and reconstruction capabilities and robustness against different desired image processing operations as mentioned in the paper.In order to to utilize the services provided by the cloud service providers one has to be an authorized customer, it is necessary to have strict authentication check[10].

Knowledge/ Textual Authentication which is simple, easy and widely used authentication technique.Two authentication techniques are based on text and colors proposed where they generate the session passwords and resistant to dictionary attack[12]. These methods actually amalgamate certain characters to form certain string and can be shared to be used by the authorized user. It can be of plain text or also of alphanumeric characters along with special symbols. Drawbacks associated with the textual passwords such as brute-force and dictionary attacks and same this problem held with graphical passwords which includes shoulder-surfing and are very expensive to implement. Two authentication techniques (pair-based authentication scheme and hybrid textual authentication scheme) for engendering the session passwords [13].It can also have mixture of picture-based and text based. The image based has separate categories of in terms of recognition and recall of the image used for graphical techniques. In recognition, scene of images is presented and it has to be identified by the user at the other end so as to identify the images that are selected during initial phase of making up of the password sequence. Once the sequence is made, the user is provided and asked to recall and reproduce the same pattern of images so that the actual sequence is revealed and the original image used as password is recalled using the recall methodologies.Although traditional alphanumeric passwords are used widely, they have problems such as being hard to remember, vulnerable to guessing, dictionary attack, key-logger, shoulder-surfing and social engineering [14].Various manual image based authentication was proposed like iris, finger print, face recognition however major problem of biometric as an authentication scheme is the high cost of additional devices needed for identification process [15].

## 3. Methodology

An attempt has been made to recover the password in three levels of work keeping in view all the authentication parameters that are existing and also by overcoming certain flaws of the schemes that was implemented. The methods used the combination of the three-scheme using textual, images and also the color combination which a human being has to remember while using this authentication key to open any private data that is kept secured with this methodology.

1. Authentication of user should be done after a user is registered.
2. Unauthorized user cannot access the folder.

3. Unauthorized user cannot rename and delete the folder.
4. Entering the wrong password should not get access to folder.

A windows-based application has been implemented to test the scheme of 3 level protection, by securing a private folder. The main advantage of this project is that it does not allow unauthorized access to folders, since it is a three levels of password authentication it will provide as much of security on folders containing document and other files.

The other advantages of that are fetched by project is as follows

1. It gives security to the folder.
2. The application is user friendly.
3. The application lets you secure the folder.
4. It will not give the access to delete the folder.
5. It will not give the access to rename the folder.

Based on the aforementioned requirements and proposed methodologies, the following scheme is proposed for the protection system.

## 3.1 Text Password.

For standard textual protection system AES (Advance Encryption Standard) [4,,5,8] is used. The encryption scheme is a symmetric encryption algorithm, formulated to use by hardware and software support system. This method supports 128-bit block length along with 128, 192, and 256 bits varied key length. AES is actually a substitution and permutation theory-based technique which combines both permutation and also combination to derives its feature using blocks and keys of varied sizes. In order to operate AES, a column matrix of 4 × 4 size known as state matrix is used which can be of larger block size and can also have additional column in the state. Various AES implementation is done using finite field of a particular function, for example, if there are 32 bytes b0, b1, b2, . . ., b30 these bytes are represented as matrix

{\displaystyle b_{0},b_{1},...,b_{15}}

| | | | |
|---|---|---|---|
| b0 | b2 | b3 … | b7 |
| b8 | b9 | b10 …. | b15 |
| b16 | b17 | b18 … | b23 |
| b24 | b25 | b26 … | b31 |

The AES cipher that is generated will also have number of repetition and transformation that are used to convert the input plain text and final cipher text is taken as appropriate password key pair

{\displaystyle

{\begin

{bmatrix}b_{0}&b_{4}&b_{8}&b_{12}

\\b_{1}&b_{5}&b_{9}&b_{13}

\\b_{2}&b_{6}&b_{10}&b_{14}

\\b_{3}&b_{7}&b_{11}&b_{15}

\end

{bmatrix}}}.

To illustrate the number of repetition that any standard AES can implement is 128-bit keys will have 10 cycles of repetition, 192-bit keys will have 12 cycles of repetition and similarly 14 cycles of repetition will take place for 256-bit keys.

Each repetition round can have several steps for processing containing similar or different stages which depends on the type of encryption key used to transform plain text to cipher text and similar set of reverse rounds are used to get back the original textual plain text from the cipher text using the same encryption key.

While implementing the 3 level of Authentication and Protection, the first level is to get the textual knowledge-based password as follows

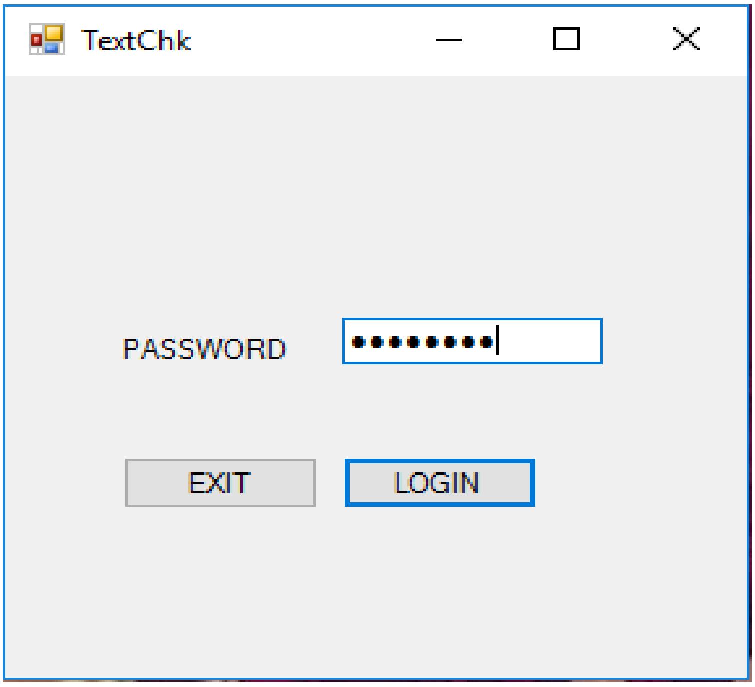

**Fig 2. Text password**

### 3.2 Color Combination.

There are three buttons with different colors (Red, Green, and Blue) and every button there is one fixed buffered numeric value. When the user clicks on button the buffered value will go to text box which concatenate with previous value in the text box.Its our Masking Algorithm.

Encryption Algorithm is based on Arithmetic operation. When the text box data has to be saved in database first encryption, algorithm encrypt the data using some arithmetic operation and the data will saved in the database. For the time of authentication, it first retrieves the data from the database and decrypt it using same arithmetic operation and compare both data if it is correct it moves on to next level of password.

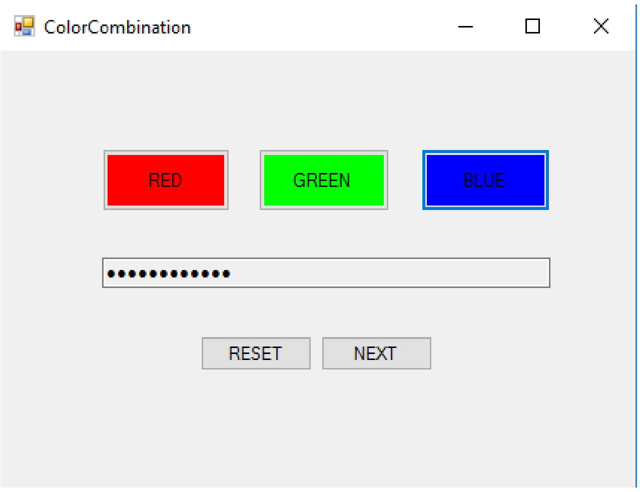

**Fig 3. Color Combination**

### 3.3. Picture Password.

Segmentation and re- sizing algorithm mainly focus on re- sizing the image into fixed sized and then segmenting that image into 100 invisible clickable buttons. Every button has a fixed buffered value which is masked from the user. The selected image will be re-sized into 500 x 295px of frame and every button have 51 x 31px.

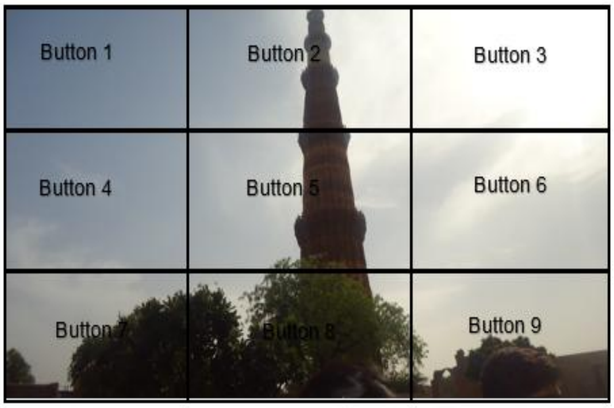

**Fig 4. re- sized and Segmented Image**

**Fig 5: Arranged Block to Obtain Original Image**

## 4.CONCLUSION AND FUTURE WORK

The proposed system enables the user to have a security for the windows folder by providing three levels password which is very difficult to access. This three level password authentication system can be use in many systems like personal computer, server systems that requires authentication before the access . This system totally denies the access to the folder to unauthorized person so anyone cannot delete the folder or anyone cannot rename the folder as they wish, for that the user has to strictly go through three level password authentication system.

This project will later be modified so that it can give different permissions to different users for the access of the folder and later the passwords can be modified which uses voice passwords. Due to this project all the user’s files within the folder and the folder is completely secure since no one can directly access the folder without going through the three-level password authentication.

While discussing the flaws of the project, it is always that there might be some kinds of situation were the project may not fit to the user requirements. Since it is a three-level password authentication system and it does not provide multiuser interface in the same system so the files or folders will only be accessed by the registered person.

The flaw of the project mainly focuses on its future scope, some of them are as follows:

1. The project can be further modified for authenticating different types of users to provide different permissions for them to access the folder.
2. The permissions like only to read the data within the folder, to copy the data from the folder or to modify the data of the folder.
3. Later it can also provide the authentication for the files.
4. It can also provide the authentication for the applications.
5. It can also be integrated with operating system to authenticate the users.

## 5.REFERENCES

[1] B. S. Thakare et al An Overview of Various Authentication Methods and Protocols, International Journal of Computer Applications (0975 – 8887) Volume 131 – No.9, December 2015.

[2] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, Senior Member, IEEE 2008 Three-Dimensional Password for More Secure Authentication.

[3] X. Suo, Y. Zhu, and G. S. Owen, ―Graphical passwords: A survey, In Proc. 21st Annu. Comput. Security Appl. Conf., Dec. 5–9, 2005, pp. 463–472 Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[4] R Kaur, EK Singh, Image encryption techniques: A selected review, Journal of Computer Engineering (IOSRJCE), 2013.

[5] Computer Security: Principles and practice. By W Stallings, L Brown, MD Bauer, AK Bhattacharjee

[6] Madhuri Yadav, Ravindra K. Purwar and Mamta Mittal, “Handwritten Hindi Character Recognition-A Review”, IET Image Processing, 2018.

[7] D. Jude Hemant, Daniela Elena Popescu, Mittal M., S Uma Maheshwari, “Analysis of wavelet, ridgelet, curvelet and bandelet transforms for QR code-based image steganography, 14th IEEE International Conference on Engineering of Modern Electric Systems (EMES) Romanian, 2017.

[8] V Agrawal, S Agrawal, R Deshmukh, Analysis and review of Encryption and Decryption for secure communication, IJSER, 2014

[9] Haouzia, A. & Noumeir, R. Multimed Tools Appl (2008) 39: 1. https://doi.org/10.1007/s11042-007-0154-3

[10] H. A. Dinesha and V. K. Agrawal, "Multi-level authentication technique for accessing cloud services," 2012 International Conference on Computing, Communication and Applications, Dindigul, Tamilnadu, 2012, pp. 1-4.
doi: 10.1109/ICCCA.2012.6179130

[11] Mada Alhaidary, Sk Md Mizanur Rahman, Mohammed Zakariah, M. Shamim Hossain, Atif Alamri, Md Sarwar M Haque, B. B. Gupta, "Vulnerability Analysis for the Authentication Protocols in Trusted Computing Platforms and a Proposed Enhancement of the OffPAD Protocol", Access IEEE, vol. 6, pp. 6071-6081, 2018

[12] Bin Hu, Qi Xie, Yang Li- Automatic verification of password based authentication protocols using smart card (2011)

[13] Priti Jadhao, Lalit Dole, Survey on Authentication Password Techniques, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013

[14] A.P. Sabzevar, A. Stavrou, Universal Multi-factor authentication using graphical passwords, in: IEEE International Conference on Signal Image Technology and Internet Based Systems, 2008, SITIS '08, Nov. 30 2008–Dec. 3 2008, pp. 625–632.

[15] Haichang Gao, Xiyang Liu, Sidong Wang, Honggang Liu, Ruyi Dai, Design and analysis of a graphical password scheme, in: 2009 Fourth International Conference on Innovative Computing, Information and Control, ICICIC, 7–9 Dec. 2009, pp. 675–678.