Review Paper: Three Level Password Authentication

Mrs. S. A. Tatugade, Lecturer, Comp. Engg. Dept, R.M.P. Ambav, India.

sandhyatatugade@gmail.com

Mr. A. A. Tatugade, Asst. Prof. EXTC. R.M.C.E.T. Ambav, India.

tatugadeaa@rmcet.com

Mr. H. R. Kulkarni, Asst. Prof. Comp. Engg. Dept. B.V.I.T. Palus. India.

kulhrushi@gmail.com

ABSTRACT : To provide good security is main issue as web development came into existence. From many years text-based passwords are used in many areas these passwords are not enough to counter many problems. Secrete information can easily hacked by hackers as the passwords are not enough secure. Therefore, there is need of something more secure. Therefore, this technique tries to increase security by involving the different levels and is more user friendly. In this Three Level Password Authentication approach involving text-based password at level 1, pattern lock based Authentication at level 2, and automated generated one-time password (received through an automated SMS to the authentic user) at level 3. Using this technique pattern set in the system authentication plays a crucial role, is named as 3 Level Security that can be employed in any fields and organization for storing confidential documents, and this paper ensures the security through three levels like, in first level through text-based password, in second level through Pattern Lock based Authentication and finally through One Time Password.

Keywords - Authentication, hackers, Password, Pattern Lock, 3-level security, secure.

I. INTRODUCTION

Now a day's every client is depending upon computer. In many fields like organizations, medical, financial, banking, etc. and sometime these fields require strong security for secure than confidential data and provide confidentially to data because if they lost the data, they can lose money as well as information which is very important for them and important for attacker so that's why computer security is exists [4].

Computer security identify user and define the access level for these authenticated users and gives them access to the system and keeps unauthorized persons away from system access, so just authorized person get access to the security systems. For identification of user the commonly uses user is and password and then if user ID and password is correct user get access, but sometime this type of security is not enough for some situation where strong security is needed. So, requirement of strong security is needed, but some time on the user ID and password system, there password can be easily guessed by the attacker. In authentication person password and user ID is needed. So, to make the system secure some different idea should be implemented, and the newly implementation must be user friendly so in current paper proposed system will provide strong security with consideration of many approaches.

Three Level password security system where users must complete three levels of authentication for getting access for particular data or webpage. There users have to complete first level which is depending upon text-based authentication, username and password is correct then he will go to the second page where he has to complete second pattern type security level here user have to draw a pattern like android operating system, on desktop screen using mouse and then if pattern is correct then user will get OTP in his e-mail.

Attackers attack the user accounts and if get user name and password is easy. But in second level to draw pattern is difficult to guess pattern and can't access any data in user account.

1.1 PURPOSE

In the current state there are many authentication schemes and most of these suffer from many weaknesses. Some of them are based on the physical and behavioral properties of the user, and some others are based on knowledge of the user such as textual and graphical passwords. Furthermore, there are more authentication schemes that are based on tokens, such as smart cards i.e. based on what you have. Among the various authentication schemes, the most commonly used schemes are textual password and token-based schemes, or the combination of both. However, both these authentication schemes are vulnerable to certain

attacks. This paper represents a 3-level password authentication scheme, which is a multifactor authentication system. To be authenticated, this project plans to present a 3-level password system by combining the features of the existing authentication schemes. The three different levels used in the three-level password authentication scheme are text-based password, Pattern Lock based Authentication and One Time Password (OTP) [1].

II. CURRENT WORKING SYSTEM

Current working system based on text based password authentication and this authentication system have some drawbacks like text based password is some time guessable to attacker because many time people uses some personal information like birthdate, vehicles registration number, mobile number, name etc. as password and so this attacker can get access to data using this personal information like date of birth, mobile no, pet name or other type of personal information and using some technique. There is also another drawback of this system which is if attacker uses the dictionary attack to know the password, in most case the password will be in attackers hand system will get compromised.

III. CHARACTERISTIC OF PROPOSED SYSTEM

- Provides strong security from both attackers and hackers.
- The system is user friendly and has simply interfaced.
- Protects system unalterable to attacks [3].
- This system is used only for security purpose in applications where providing security is needed.

FLOW CHART OF PROPOSED SYSTEM

In fig 1.1 shows the flow chart in which first of all user must fill information for registration the information saved in database for future use. User login may be successful or unsuccessful depending upon criteria matches.

IV. REGISTRATION PROCESS

In the system the registration process is carried out by Text-based authentication, and pattern lock with user's choice afterwards OTP is generated [1]. In registration process security impose in text-based password by using the combination of one capital letter one special symbol and one numeric value. In pattern lock user should give any kind of pattern according to user's choice. After these two levels the registration system randomly generate one-time password and this generated random code is valid for only that registration phase. If the registration is

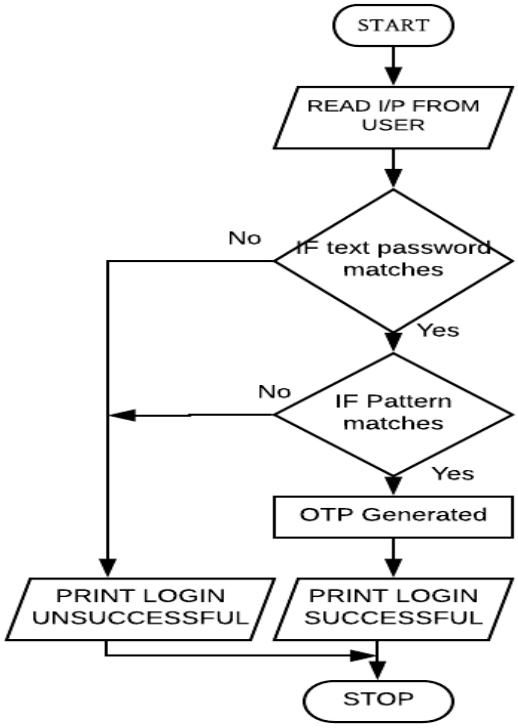

FIG. 1.1 FLOW CHART

successful, all related data of user is saved in database.

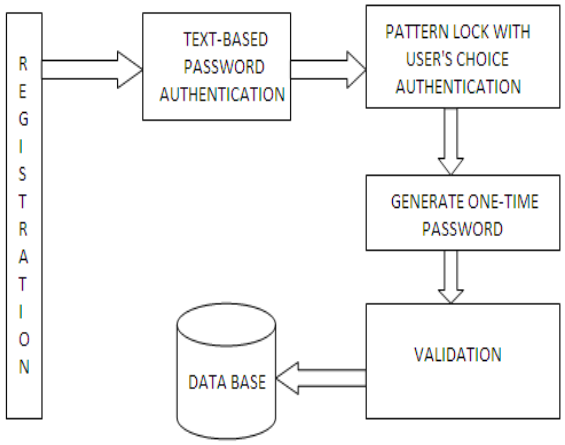

FIG1.2 REGISTRATION PROCESS

In fig 1.2 Registration process user will be register in database by using following steps. First user must give strong text-based password without using common personal information like birthdate, mobile number etc. user must register with mobile number so that it can be used to get one-time password. After that user must choose pattern which user want to register. The pattern given by user is compared each time when user want to login system. After completing these two levels system generate one-time password and the one-time password is valid only for that respective registration. If the registration is successful, then only the data is saved to the database and message of successful registration is display.

V. THREE-LEVEL AUTHENTICATION PROCESS

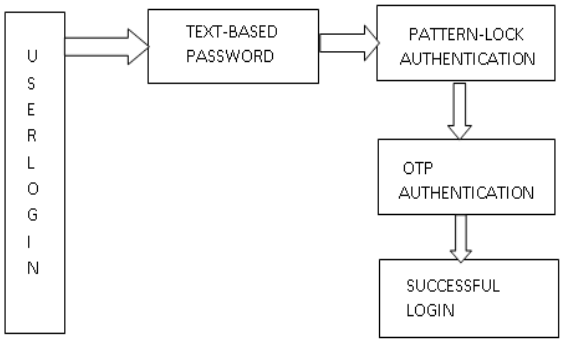

FIG 1.3 AUTHENTICATION PROCESS

In above Fig. 1.3 shows flow of authentication process [2]. When user want to login the system then login is based on following options. When user need to login the system, user must give the text-based password first. The text-based password must match with previous given password. This is nothing but first level. After completing first level user enter second level. Here user must draw pattern. If the pattern matches, then only user can enter into next level. Pattern given while registration process is already saved into database, if current pattern is match with previous pattern (pattern given by user at registration phase) then user complete its second level of authentication. After completing this second level, the random password generated at the registration time is send on users mobile. If user fails any one stage from these three then the user can not be able to successful login.

Thus, at three different level the security has been imposed by

- At level 1 text-based password user can use special symbols as well as numbers [4].
- At level 2 user will be ask for pattern levels, so that user can choose the different unique pattern.
- After completing 2 levels the system will generate one-time numeric password which is valid for user login.

SYSTEM REQUIREMENTS OF PROPOSED SYSTEM

Operating System: Windows 8.1

Front end: NetBeans 8.2 with JDK 8

Database: MySQL

MAIN MODULES OF SYSTEM

1. First module is registration module which performs registering the details like name, e-mail, address, mobile no, collage name, state, country, area code, username, password which is used to login and storing data.
2. Second module is login form is login the administrator and as well as client which is registered admin.
3. Third module is pattern lock is checking the pattern is valid or not.
4. Forth module is One Time Password is generated and send clients registered mobile number.

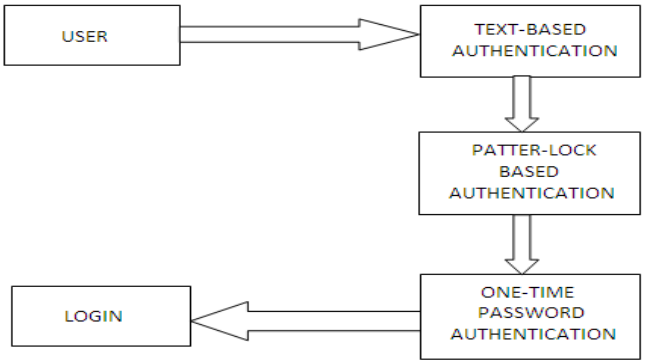

Fig 1.4 SYSTEM ARCHITECTURE

In this phase 3- Level Authentication System, user provides user name and text-based password for first level password authentication process. After completing first level i.e. user enter correct username and password user enter in second level. In second level user should enter pattern and this pattern should match with already saved pattern (user selected in registration phase) in database then user enter in next level. In third level random code generated by system will send to users mobile (mobile number also registered in registration phase). If any one level from these three levels is mismatched, then user will not authenticate for application or system.

This paper proposed the security system fig 1.4 shows the system architecture.

VI. CONCLUSION

The three-level security approach applied on the above system, makes it highly secure. This system will help to oppose attack at the client side. 3-Level security system is a time-consuming approach, as the user must traverse through the three levels of security. And will need to refer to his mobile number for the one-time automated generated password. This system will be a benefit in areas where high security is the main issue, as an example we can take a case of a firm where this system will be accessible only to some higher designation holding people, who need to store and maintain their crucial and confidential data secure. In future not only, we will add more features but also make our system customizable.

VI. ACKNOWLEDGEMENT

The authors would like to thank all the authors mentioned in the references as well as all other authors for their earlier work on this topic.

REFERENCES

[1] Security Analysis and Implementation of 3- Level Security System Using Image Based Authentication, Author: Surabhi Anand, Priya Jain, Nitin and Ravi Rastogi.

[3] Implementation of Security System Using 3-Level Authentication by 1Nagesh.D Kamble, 2J.Dharani © 2014 IJEDR | Volume 2, Issue 2 | ISSN: 2321-9939 pg. no1528 to 1532.

[3] S3PAS: A Scalable Shoulder - Surfing Resistant Textual Graphical Password Authentication Scheme, Author: Huanyu Zhao and Xiaolin Li.

[4] http://data.conferenceworld.in/ESM/P220-228.pdf

[5] http://en.wikipedia.org/wiki/Hue

[6] http://en.wikipedia.org/wiki/Color_vision