International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 4 ǁ 2022 ǁ PP. 32-38

Three-Layer Defence in Authentication Mechanism

[1] Siddhesh Deepak Patil, [2] Dr. Umarani Chellapandy
[1] *Student, School of Computer Science and Information Technology*
[2] *Associate Professor, School of Computer Science and Information Technology*
Jain Deemed-to-be University, Bangalore, Karnataka

ABSTRACT
Information security is the basic requirement for the current digital world, as we are used to send and receive data on the internet, authentications is the basic security measures which has to be followed by every individual to keep account safe from the hackers. This paper content the information related to three step authentication process, the primary component of this system is user id and password, secondary component of this system is one-time password system, the last component is email-id image verification. It also has log-in time face capture as well as logbook which captures the login entries like time and date. It has virus shortcut remover and it also checks weather the antivirus is working in real time or not.
Keywords: Authentication, Information Security, One-Time password, Antivirus, Password.

Date of Submission: 10-04-2022 Date of acceptance: 26-04-2022

I. Introduction

Three-step authentication is mainly used to add security to the login process of a particular application in which a user has to verify his identity three times to make sure his identity or its data is safe. This application can majorly be utilized in banking sector, bitcoin trading centre, security application…, etc. As of now we are using two step authentication which uses user-id password and one-time password which is not sufficient enough for security as hackers can easily bypass one-time password. Additionally, this paper contains information about a virus shortcut remover that will help to remove a certain shortcut file that is considered a virus and will also check if it's an antivirus that is functioning properly or not.

II. Literature Review

In [1], Ewe Syta. has different authentication methods that can be used, they are Knowledge-based (Numeric, Alpha-numeric, Graphical password), Possession-based (Token) and Biometric-based (Fingerprint, Facial recognition, Iris recognition, Hand geometry). It has explained an approach that users taken-based authentication which is cost effective, easy to use and secure. It has some security issues like RFID technology's nature is contactless, dues to this anyone can read the passive tags if they are on the same frequency. In [2], Fujii H. has expressed view on two-step authentication using SMS or Voice call to prevent phishing attack. It has descried about two different methods, two-authentication using SMS and voiceprint response (SV-2FA) and SV-2FA/Certificate Provisioning by using net banking model. In [3], G. E Blonder. Has proposed graphical password technique for first time, it suggest the technique that the user is required to point one or more predetermined position on the image, which he selects during registration time for every login. As compared to 4-digit PIN which has the combination of 10,000 possible but in graphical password using three taps its correct order there can be over 13.6 million possible combinations. In [5], Rane, in this new approach, images are shown to users during login phase. The user chooses several images in order to select a password. After this, the user selects one image and clicks to draw the secret. When logging in, the user draws the secret that was in the registration phase. Sequence of clicks is not required. In [6], Nagesh, this paper is a unique and esoteric study about using patterns as passwords and developing an extremely secure system employing 3 levels of security (Text Password, Pattern-Lock, and One-Time automated generated password).

Problem Statement

As security is crucial part nowadays everyone is neglecting this and they reducing the number of authentication layers used in the application which gives the user a major disadvantage to the user he may end up losing his data and access to his devices to the hacker. To overcome this problem, we have proposed a system with three-layer authentication which provides more security to user.

Proposed System
In this proposed system, we are using three-layer authentication approach to provide security to user's data. Three layers are properly described below as well as the other features of the system.,

Layer One: - In first layer of the system, the user has to enter their user-id and password which they had used during the time of registration, it is same as of the traditional method but with a different approach as this system has its own password matching algorithm which is unique in its own way, and we can enter the password in many different ways with certain keyword (i.e.., password), the user has only three chances to enter their password if they fail to do the application will terminate itself.

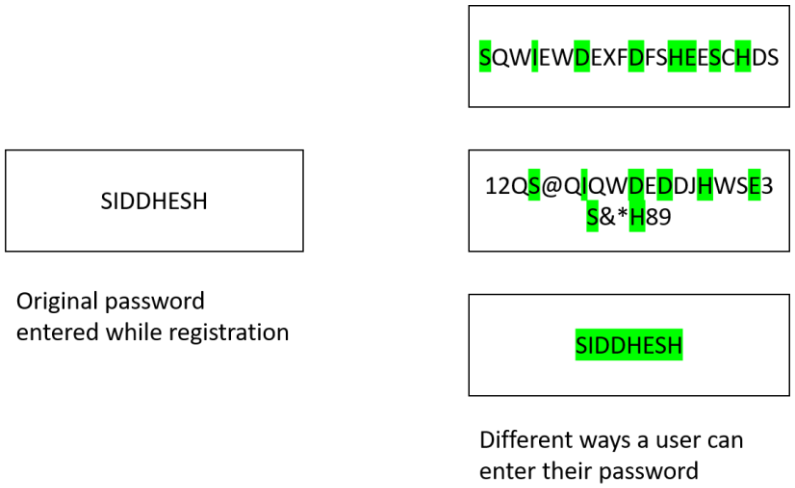

Fig.1 Different possible ways to enter the password

Layer Two: - The second layer consists of One-Time password which will be send to user's mobile number, which will be consists of 6-digit number which are randomly generated by the system. To send the one-time password we are making use of TextLocal API services, TextLocal is a SMS service provider which will be sending the OTP to the user, the user should enter that OTP in the system to pass the second layer.

Layer Three: - The final layer of this system will make use to email-id image verification, basically it means one image will be sent to the user's registered email-id they have to see that particular image and match it from six sets of images shown on the screen, it is a kind of OTP system but here its make use of images and the user has only three chances to pass this verification if they fail then the application will close and will capture the image of the user.

System Security: - Here it basically focuses on the Login, as this module is always hit first in most of the systems that have the login module. It basically checks for the intruders trying to access your system. It records the time of login for the user who enter correct usernames and passwords, but it captures a photograph of the intruders who fail to enter the password for three times.

Login Time Face Capture: - Here authenticated users can view a list of intruders who attempted to access the system, using the built-in web-cam images will be captured and showed in this section.

Log-Book Diary: - The log book will hold the user's login time of using this application and the entries can be seen here.

Virus Solutions: - Under this module the users can test their anti-virus and also remove the shortcut virus that may cause the higher usage of memory.

Test Your Anti-virus: - This unit injects non-harmful virus into the system and waits for the anti-virus to launch and if the anti-virus deletes the virus, then it means that the user's anti-virus is a real time else not real time.

Remove Shortcut Virus: - There is a risk that some crucial system files may be deleted when you run the shortcut remover on your system drive other the drives. This file basically scans all the files and folders of the triggered drive and deletes them as it is matched with the detection algorithm.

User Accounts Management: - A user account management module is designed to handle the basic operations of creating, editing and deleting users. Here the authorized users can only create the user. The management of the users can only be done in this section.

III. Results

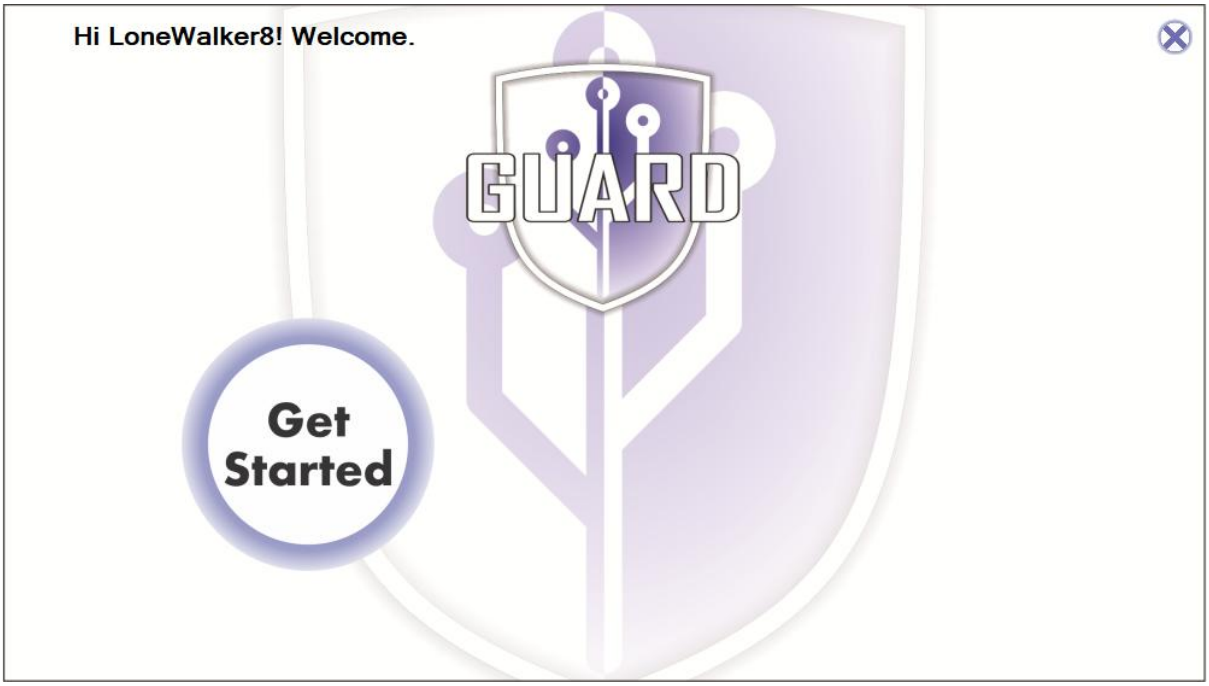

Fig.2 Home Screen of the system S

Fig.3 Login Screen (1st Step of Authentication)

Fig.4 Main Menu Screen

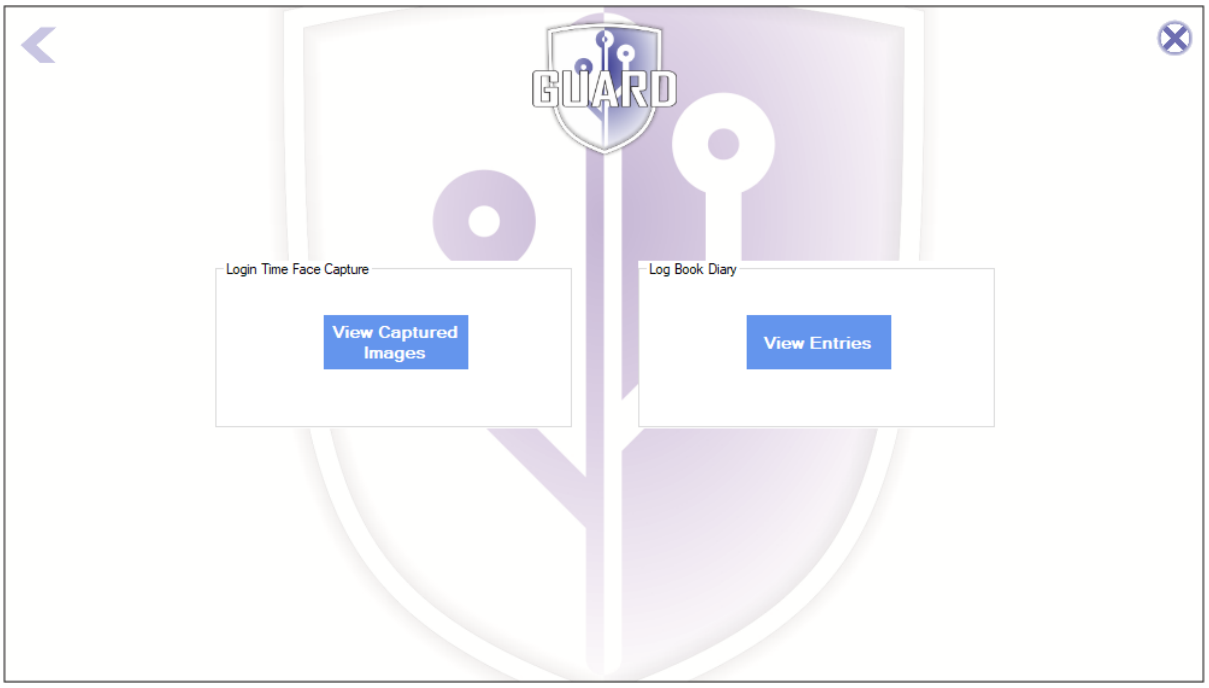

Fig.5 System Security Screen

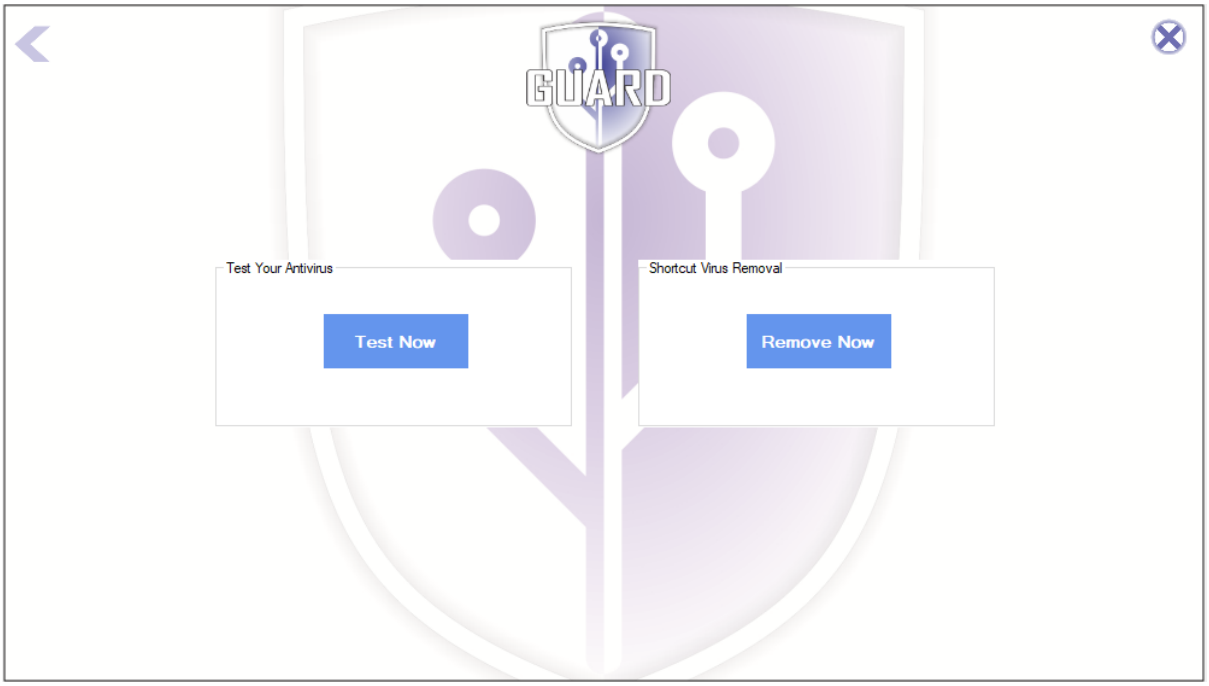

Fig.6 Virus Solution Screen

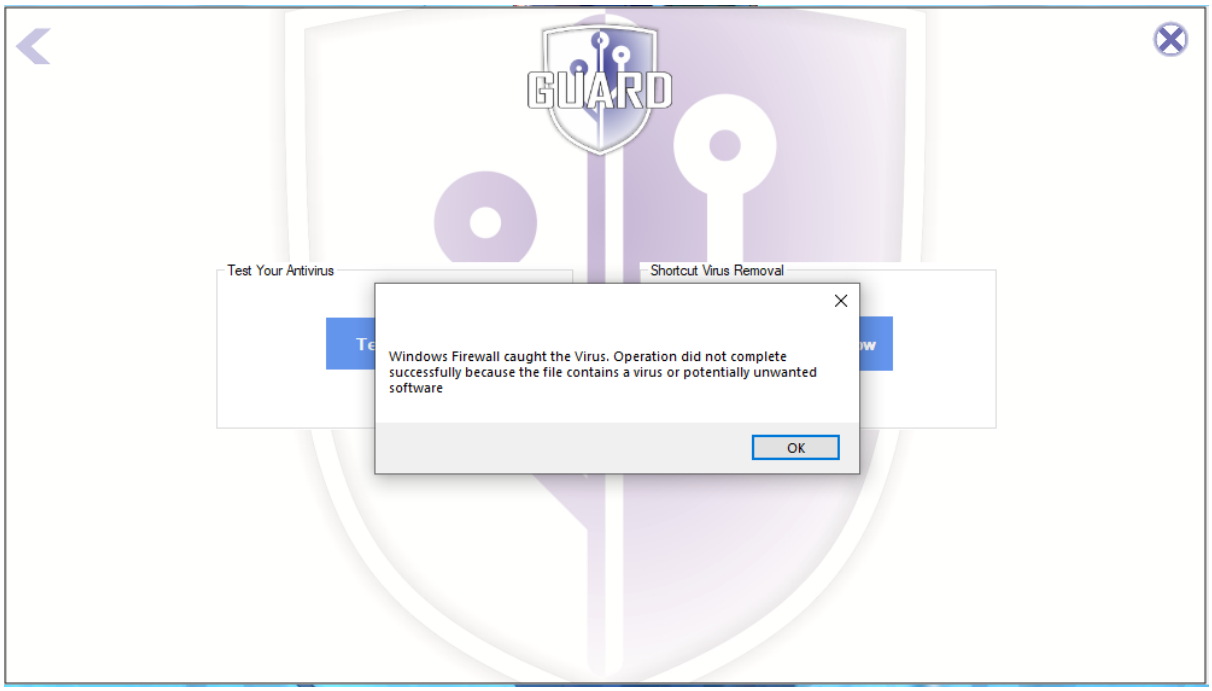

Fig.7 Testing Anti-Virus

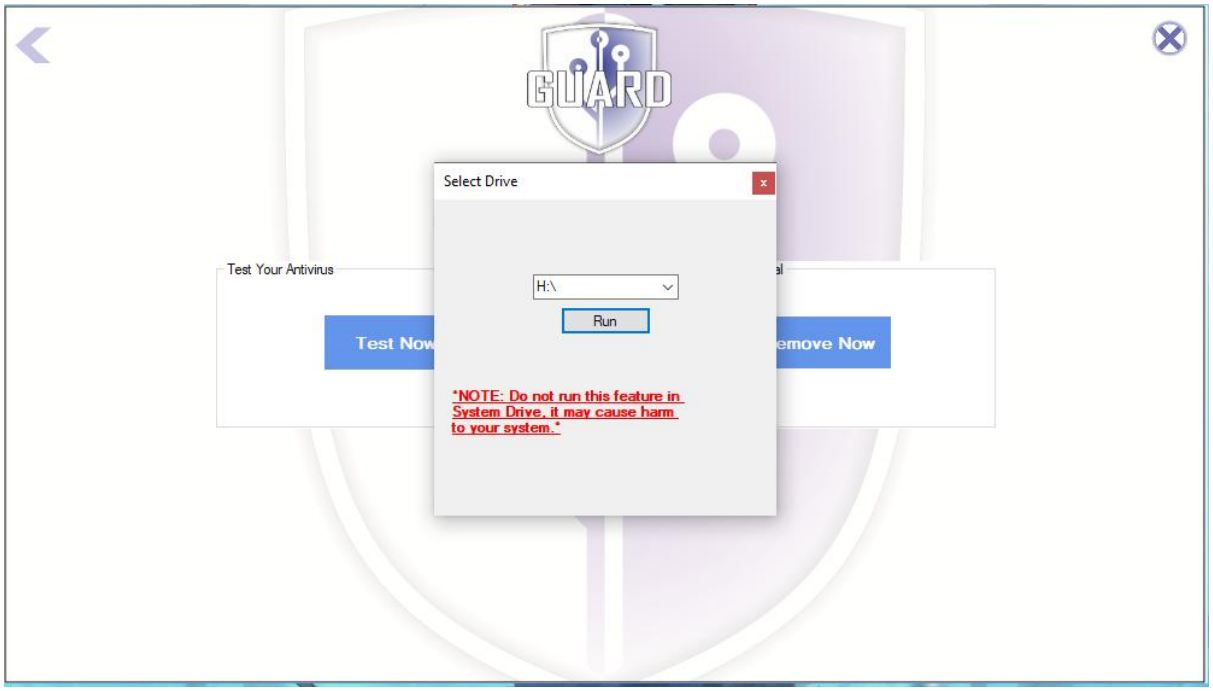

Fig.8 Virus Shortcut Remover

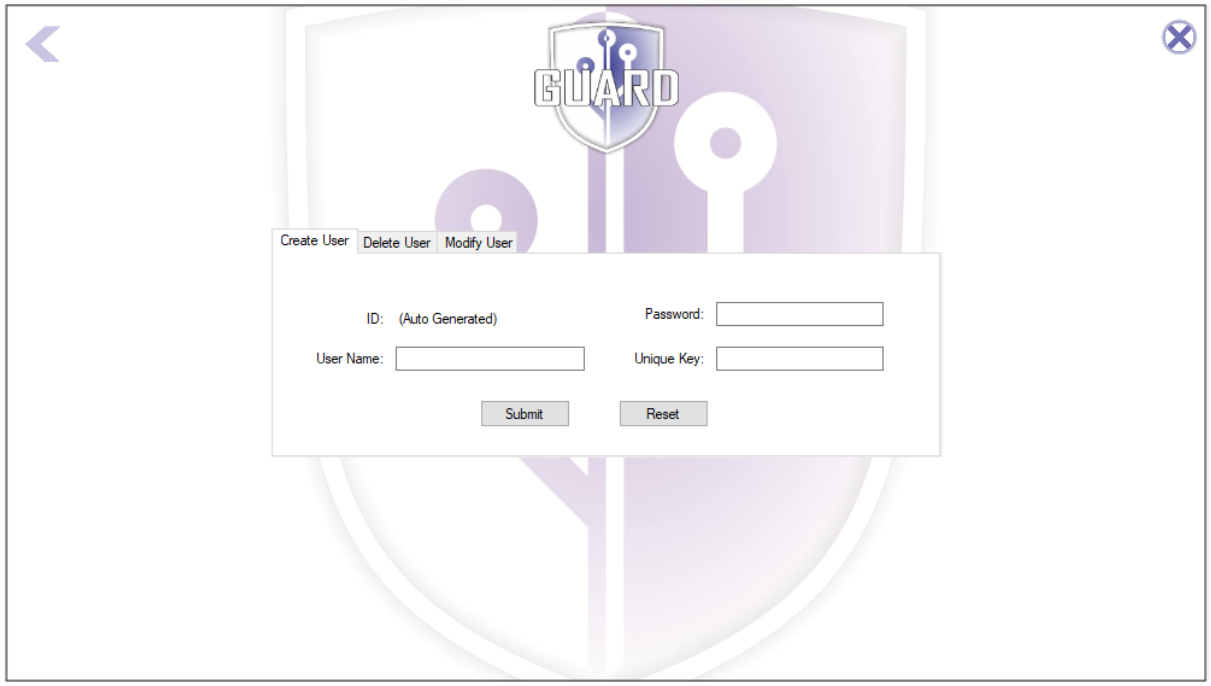

Fig.9 User Account

IV. Conclusion

In today's world, as the new technology is growing faster the two-factor authentication is not sufficient enough to keep our data safe from the hackers, as they can use tool like burp suite to bypass two-factor authentication and can easily take their data and use it. So, to avoid this three-factor authentication must be implemented in the system to keep themselves safe from the hackers. This paper examines one such idea to implement the three-factor authentication, which each layer is unique in its own way. It also has an anti-virus checker that tells you if the anti-virus is working or not in real-time programs claim your system is protected, but in fact it isn't. This system also captures the face of the user whenever they tries to login and will also note down the time and date during the login.

References

[1]. Syta, E., Kurkovsky, S., Casano, B. RFID-based authentication middleware for mobile devices. Proceedings 43rd Annual Hawaii International Conference on System Sciences (HICSS '10), January 2010
[2]. Fujii, H. and Tsuruoka, Y. SV-2FA: Two-Factor User Authentication with SMS and Voiceprint Challenge Response. Proceeding's 8th International Conference for Internet Technology and Secured Transactions (ICITST -2013), IEEE, 2013, pp. 283-287
[3]. G. E. Blonder, "Graphical Password," US5559961 A, Lucent Technologies, Inc. (Murray Hill, NJ), Sep. 1996.
[4]. Gehringer, Edward. (2002). Choosing passwords: Security and human factors. International Symposium on Technology and Society. 369 - 373. 10.1109/ISTAS.2002.1013839.
[5]. Rane, Pratibha & Shaikh, Nilam & Modak, Prarthana. (2016). Secure Authentication Using Click Draw Based Graphical Password Scheme. International Journal of Advanced Engineering Research and Science. 4. 1-4. 10.22161/ijaers.4.1.1.
[6]. Nagesh.D Kamble, J.Dharani. Implementation of Security System Using 3-Level Authentication