IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Survey on Comprehensive Analysis on Various Techniques used in Authentication

[1]Mrs. M. Parvathi, [2]Mrs. P. Shobana

[1]Head of the Department, [2]Assistant Professor
[1] Computer Science Department
[1]Name Latha Mathavan Arts and Sciene College, Madurai, Tamilnadu, India

Abstract : Protection is compulsory needed for the private and non-private as well as for business, army and non-public organization. Usually all the users are using only text password and it is also an easy and famous method for generating for data protection. But these types of passwords can be easily hacked and also it can be easily guessed by others. To avoid the hacking we have to increase the level of protection using authentication at number of levels. We may consider three level of authentication for the retrieval. In this survey paper we analyzed various authentication techniques applied in three levels. It is somewhat risky for the hackers to hack all the three levels of password ti retrieve the data. While we applied three level protections it is discovered that the protection level to the data is more than the text password authentication.

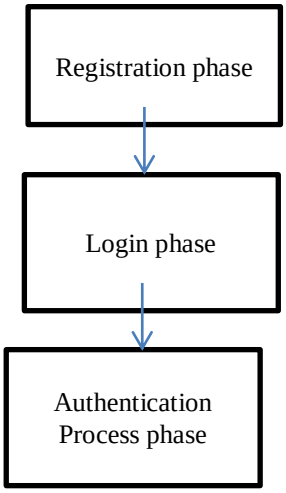
***IndexTerms* – Authentication techniques, Graphical password**

I. INTRODUCTION

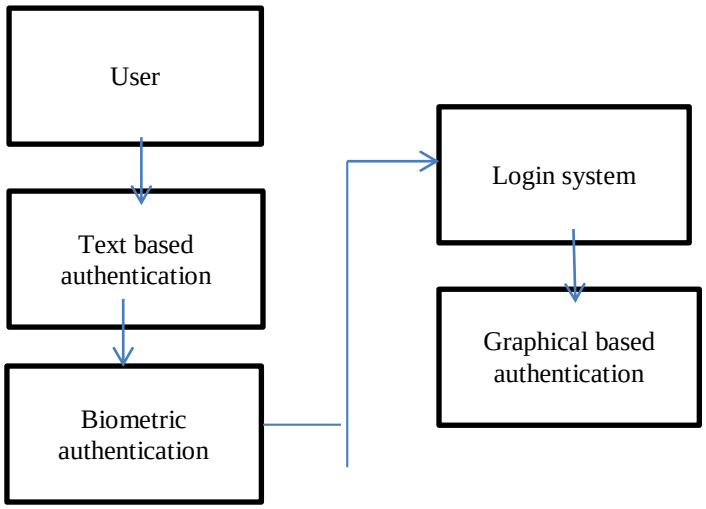
In this paper, data can be retrieved only when the user enter the correct password in all the three levels. There is various types of passwords used to protect the system. It have maximum security that nobody can guess all types of passwords. It contains three logins and in each login there are three different types of password system. Users have the right to set passwords as they wish. Here we will discuss about text password, a biometric password and graphical based password.at three level protection. There are minimum possibilities to hack the passwords. If a hacker hacked first level password, it is impossible to hack the second password. If so it is complicated to hack the third level password. When we are using various levels of authentication technique, we have to include new technology, innovative and non-predictable mechanisms to develop the authentication techniqes. There are three phases in the password generation. Registration phase, login phase and process phase

II. PROPOSED SYSTEM

PHASES



LEVEL OF AUTHENTICATION



A. Registration Phase

User need to login first and need to fill details in registration form.

Password Set-up

1. While registering, the user has to generate all the three-level passwords as per mechanisms applied.
2. Following are the three levels for password set-up.
   a. *First Level:* The first level is a normal text-based password system.
   b. *Second Level:* The second level is a biometric password
   c. *Third Level:* The third level is a graphical-based password method.

B. Login Phase

After registrations, users can login and check all the three security levels. User has to remember all three passwords for future usage.

D. Authentication Process Phase

When the login to the first level and If it is incorrect user has to enter the password again. We may set number of trails to enter the correct password. If it exceeds three attempts then the user cannot login to the system. if it is correct then the second level password will be entered. In this also the biometric must be matched with the image already uploaded at the time of login. If it is incorrect the login will be cancelled. If correct user has to enter the third level password, it must also be correct, if not login will be cancelled.

III. METHODOLOGY

3.1 TEXT BASED AUTHENTICATION

In this authentication method alphanumeric password characters are represented by random decimal numbers which resist online security attacks such as shoulder surfing and key logger attacks. In the registration process password string is converted into a completely new string of symbols or characters before encryption. This strategy improves password security against offline attacks such as brute-force and dictionary attacks. In the proposed scheme passwords consist of alphanumeric characters therefore users are not required to remember any new kind of passwords such as used in graphical authentication. Hence password memorability burden has been minimized. However mean authentication time of the proposed scheme is higher than the textual password scheme due to the security measures taken for the online attacks.

3.2 BIOMETRIC AUTHENTICATION

Biometric authentication is a security process that relies on the unique biological characteristics of individuals to verify they are who they say they are. Biometric authentication systems compare physical or behavioral traits to stored, confirmed, authentic data in a database. Biometric authentication works by comparing two sets of data: the first one is preset by the owner of the device, while the second one belongs to a device visitor. If the two data are nearly identical, the device knows that "visitor" and "owner" are one and the same, and gives access to the person.

The important thing to note is that the match between the two data sets has to be **nearly identical** but not **exactly identical**. This is because it's close to impossible for 2 biometric data to match 100%. For instance, you might have a slightly sweaty finger or a tiny, tiny scar that changes the print pattern.

Designing the process so that it doesn't require an exact match greatly diminishes the chance of a false negative (the device doesn't recognize your fingerprint) but also increases the odds that a fake fingerprint might be considered genuine.

Applications of biometric systems

Biometric systems can be used in a large number of applications. For security reasons, biometrics can help make transactions, and everyday life is both safer and more practical. The following domains use biometric solutions to meet their respective needs:

- Legal applications:
  - Justice and law enforcement: Biometric technology and law enforcement have a very long history, and many very important innovations in identity management have emerged from this beneficial relationship. Today, the biometrics applied by the police force is truly multimodal. Fingerprint, face, and voice recognitions play a unique role in improving public safety and keeping track of the people we are looking for.
- Government applications:
  - Border control and airport: A key area of application for biometric technology is at the border. Biometric technology helps to automate the process of border crossing. Reliable and automated passenger screening initiatives and automated SAS help to facilitate international passenger travel experience while improving the efficiency of government agencies and keeping borders safer than ever before.
  - Healthcare: In the field of healthcare, biometrics introduces an enhanced model. Medical records are among the most valuable personal documents; doctors need to be able to access them quickly, and they need to be accurate. A lack of security and good accounting can make the difference between timely and accurate diagnosis and health fraud.
- Commercial applications:
  - Security: As connectivity continues to spread around the world, it is clear that old security methods are simply not strong enough to protect what is most important. Fortunately, biometric technology is more accessible than ever, ready to provide added security and convenience for everything that needs to be protected, from a car door to the phone's PIN.
  - Finance: Among the most popular applications of biometric technology, financial identification, verification, and authentication in commerce help make banking, purchasing, and account management safer and more convenient and responsible. In the financial area, biometric solutions help to ensure that a customer is the person he/she claims to be when accessing sensitive financial data by

entering his/her unique biometric characteristics and comparing them to a model stored in a device or on a secure server. Banking solutions and the payment technologies available today use a wide range of biometric modalities: fingerprints, iris, voice, face, fingerprint, palm veins, behavior, and other types of biometric recognition are all used alone or combined in a multifactorial manner as a system, to lock accounts and serve against fraud.

- Mobile: Mobile biometric solutions live at the intersection connectivity and identity. They integrate one or more biometric terms for authentication or identification purposes and take advantage of smartphones, tablets, other types of handhelds, wearable technology, and the Internet of things for versatile deployment capabilities. Thanks to the versatility brought by modern mobile technology, as well as the proliferation of mobile paradigms in the consumer, public, and private world, mobile biometrics is becoming more and more important.
- Eye movements tracking applications:

- Automotive industry: there is an established relationship between eye movement and attention. Thus, tracking the car driver's eye movements can be very helpful in measuring the degree of sleepiness, tiredness, or drowsiness. The sleepiness of the driver can be detected by analyzing either blink duration and amplitude or the level of gaze activity [3].
- Screen navigation: one of the most important applications for people with disabilities is screen navigation. Using cameras, the application can track a person's eye movements in order to scroll a web page, write text, or perform actions by clicking on buttons on a computer or mobile devices. Therefore, this kind of application is gaining more attention recently due the rapid development and the growing need of new means of screen navigation especially on mobile devices platforms.
- Aviation: the flight simulators track the pilot eye and head movement in order to analyze the pilot's behavior under realistic circumstances. This simulator is capable of evaluating a pilot's performance based on his eye movements combined with other information. It can be also used as an important training tool for new pilots in order to help them to look at the primary flight display (PFD) more regularly in order to monitor different airplane indicators.

3.3 GRAPHICAL BASED AUTHNTICATION

In a **graphical password authentication** system, the user has to select from images, in a specific order, presented to them in a graphical user interface (GUI). According to a study, the human brain has a greater capability of remembering what they see(pictures) rather than alphanumeric characters. Therefore, graphical passwords overcome the disadvantage of alphanumeric passwords. Graphical Password Authentication has **three major categories** based on the activity they use for authentication of the password:

- **Recognition based Authentication:** A user is given a set of images and he has to identify the image he selected during registration. For example, *Passfaces* is a graphical password scheme based on recognizing human faces. During password creation, users are given a large set of images to select from. To log in, users have to identify the pre-selected image from the several images presented to him.
- **Recall based Authentication:** A user is asked to reproduce something that he created or selected at the registration stage. For example, in the *Passpoint* scheme, a user can click any point in an image to create the password and a tolerance around each pixel is calculated. During authentication, the user has to select the points within the tolerance in the correct sequence to login.
- **Cued Recall:** Cued Click Points (CCP) is an alternative to the PassPoints technique. In CCP, users click one point on each image rather than five points on one image (unlike PassPoints). It offers cued-recall and instantly alerts the users if they make a mistake while entering their latest click-point.

IV CONCLUSION

There are so many authentication techniques to protect the data from hackers. If the user applies more levels of authentication security level also will be increased. Risky level to access the data will also be increased. The authentication should not be easily guessed one. The user must increases new techniques and mechanism to set the authentication password for the protection.

REFERENCES

[1] Pathik Nandi, Dr. Preeti Savant 2022.Graphical password authentication system. Journal for research in applied science and engineering ISSN : 2321-9653

[2] Shah Zaman Nizamani. Syed Raheel Hassan, Tariq Jamil Khanzada, Mohd Zalisham Jali 2017. A text based authentication scheme for improving security of textual password. The science and information organization , Volume 8 Issue 7

[3] Kavita Gupta 2018. Review paper on biometric authentication **international journal of engineering research & technology,** ISSN (Online) : 2278-0181

[4] Syed Wajid Shah, Salil S. Kanhere, Recent trends in user authentication -a survey, IEEE Access PP(99), DOI:10.1109/ACCESS.2019