PROTECTION USING THREE DIMENSIONAL PASSWORD

DR DINESH KUMAR RANGARAJAN,

Professor,

Department of Computer Science and Engineering,

DR ARUN PRASATH RAVEENDARAN,

Professor,

Department of Electronics and Communications Engineering,

Siddhartha Institute of Technology and Sciences,
Narapally, Hyderabad, Telangana – 500 088.

ABSTRACT

Authentication procedure includes providing security to any system. Text, biometrics, and other methods can be used for authentication. To ensure security, this The form of textual password commonly uses an encryption technique. Each method has its own set of downsides and limits. A new authentication approach has been developed to solve the issues. The 3D Password approach is a multi-factor and multi-factor authentication technique with a multi-factor and multi-factor authentication strategy. The virtual environment that houses the user interface that looks to be a real-time environment but is not is the most significant aspect of 3D Password. Because it is difficult to hack and easy to use, a 3D password is more secure than conventional authentication schemes. The advantage of the 3D password is that it combines existing system authentication with enhanced user security. This study focuses on how to develop three-dimensional passwords as well as design suggestions for three-dimensional passwords. The 3D password is used to circumvent existing authentication techniques' limits and weaknesses. The 3D Password is a multi-featured, multi-factor authentication solution that integrates the advantages of existing authentication methods in a single virtual 3D environment. The notion of the new authentication mechanism, how it works, and how it can be used will be the emphasis of this talk.

I. INTRODUCTION

Various authentication systems or algorithms provide authentication, which is one of the most critical security services. Authentication must be set up on any system to ensure that only authorised personnel may use or operate the system and the data it contains. There are a variety of authentication techniques to choose from, some of which are efficient and secure but

have drawbacks. Many authentication systems have been introduced in the past, such as gr There are four main types of authentication.

Knowledge Base: "Knowledge based" refers to what you already know. The finest example of this authentication scheme is a textual password. The best illustration of a knowledge base strategy is a textual password.

Token-Based Authentication: You can utilise token-based authentication with any ATM or swipe card. Any graphical password or face identification strategy is a recognition base technique.Biometrics Base: One example of a biometrics base authentication mechanism is a thumb or finger impression.aphical passwords, text passwords, biometric authentication, and so on.

Recall Base: Nowadays, system security is a big concern. The Scheme Textual is an example of a Scheme that is built on recollection. The user enters a password to safeguard the system. To some extent, a Strong Textual Password can help secure a system. However, it is tough to recall.

Recognition Base: In the Recognition Base system, the user must identify and recognise his or her own password, which he or she created. Shoulder surfing attacks are a risk with graphical passwords. The recognition strategy also includes a biometrics-based authentication technique. Fingerprints, palm prints, face recognition, voice recognition, retina recantation, and other biometrics are examples of authentication methods. Biometrics is the science of capturing and replaying biometric data. An attack, as well as a hill climbing attack, can be launched. There is a danger of fraud, loss, and theft with token-based authentication.

II. RELATED SURVEY

Authentication of any system entails providing that system with security. Textual, biometric, and other authentication approaches are available. To ensure security, this form of textual password usually uses an encryption method. Each of these methods has its own set of limits and disadvantages. To address these issues, a new authentication mechanism called as 3D Password has been developed. It is a multi-factor and multi-factor authentication technique. (2015, Abhilash Sukla)

Alphanumerical usernames and passwords are the most used computer authentication technique. This approach has been found to have a number of disadvantages. Users, for example, tend to choose passwords that are easy to guess. Easily deduced. If, on the other hand, a password is forgotten, It's difficult to guess, and then it's difficult to recall. To Some researchers have proposed solutions to this problem.created authentication methods that rely on images as a source of information passwords. We perform a thorough investigation in this study.(Ying Zu 2015)

III. METHODOLOGY

Textual, biometric, and other authentication methods are available. To ensure security, this form of textual password usually uses an encryption method. Each of these methods has its own set of limits and disadvantages. These passwords aren't 100% secure or effective, and they contain certain flaws. Because it incorporates the benefits of earlier existing authentication methods into a single platform authentication scheme, the proposed authentication system is a multi-factor and multi-password secure authentication technique. The proposed system creates a 3D virtual world in which the user can interact with a variety of virtual objects or items. In this 3D virtual environment, the user can browse and interact with a variety of virtual things. A set of actions and interactions with moving virtual objects in a 3D virtual environment are used to build the user's 3D Password. The proposed system can combine previously established schemes such as textual passwords, graphical passwords, biometrics, and even token-based methods in an unified 3D virtual environment. The authentication system that will be included in the user's 3D Password will reflect the user's demands and preferences. Textual and graphical passwords may be included in a 3D Password by a user who is good at memorising and recalling passwords. Individuals who have difficulty memorising and recalling passwords may also want to include biometrics or smart cards in their 3D Password. As a result, the user will be able to select and determine how the ideal and desired 3D Password should be implemented.

IV. RESULTS AND DISCUSSION

The user first authenticates with a simple textual password in 3D password, which implies the user supplies a username and a password. This authentication is verified, and if successful, the user is transported to a 3D virtual environment, where a computer with a keyboard appears on the screen. On that screen, the user must input a password (textual), which is saved in the form of encrypted coordinates in a simple text file (x1, y1, z1). After successful authentication, the user is automatically redirected to an art gallery, where he or she can select numerous points in the gallery or take action in the environment, such as turning on/off switches or doing other actions.

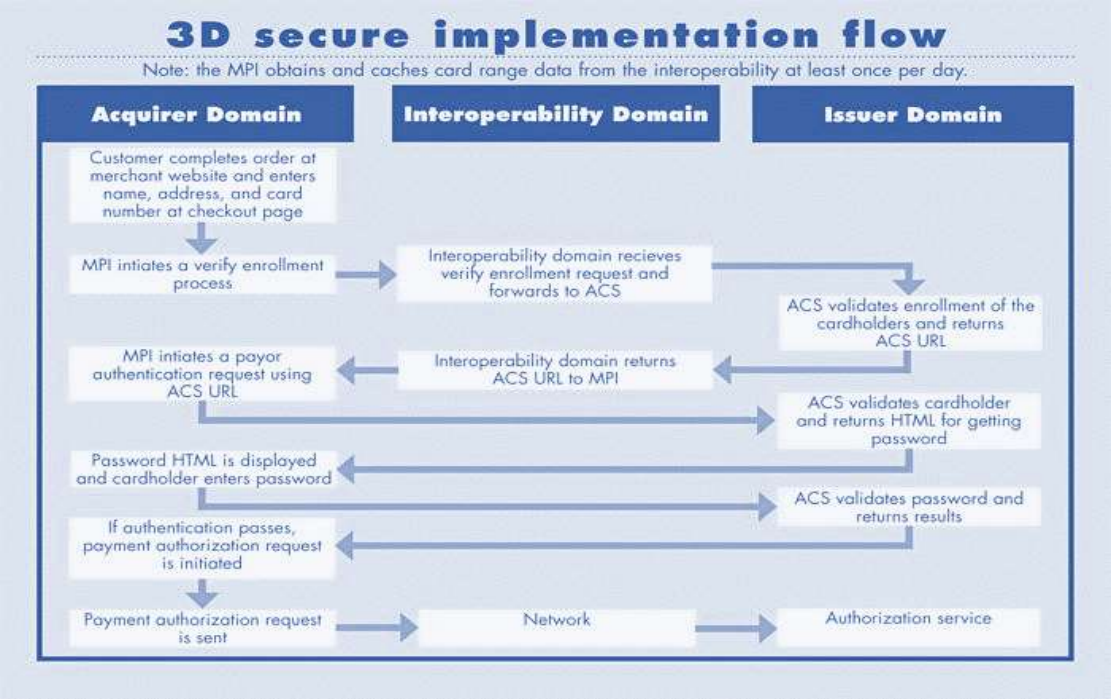

FIGURE 1. FLOW CHART OF SECURITY USING 3D PASSWORD

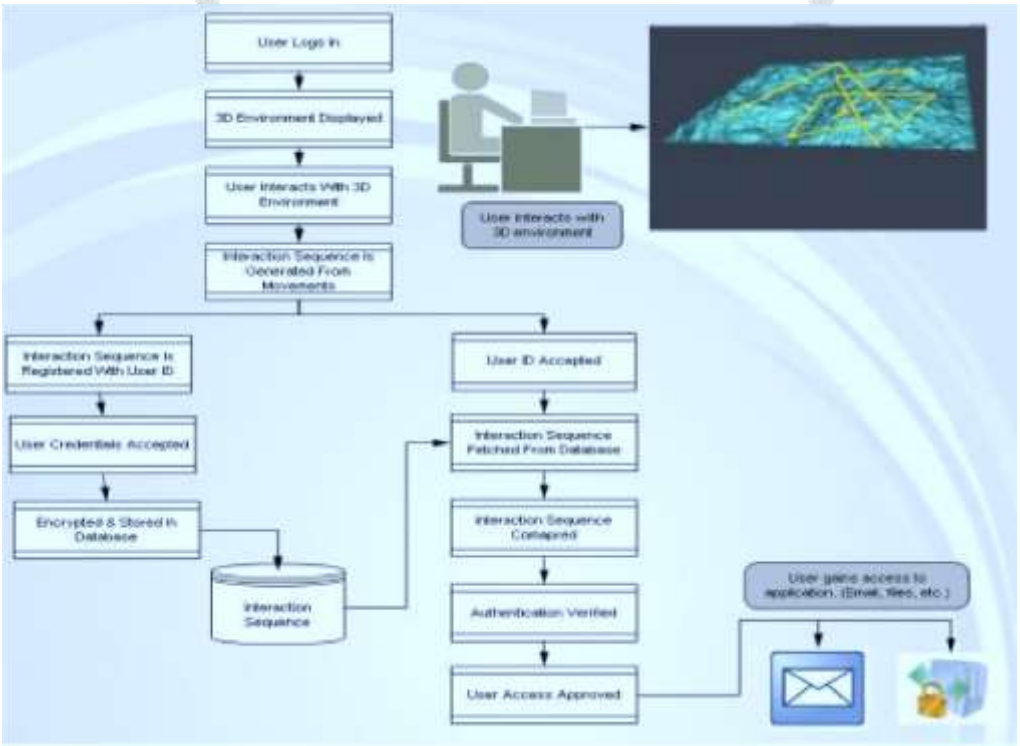

FIGURE 2. ARCHITECTURE OF SECURITY USING 3D PASSWORD

The sequence of positions in which the user clicked (i.e. selected items) is saved in encrypted form in a text file. In this technique, the password for that specific user is set. We utilised the 3d Quick hull algorithm, which is based on the convex hull algorithm from the design and analysis of algorithms, to choose points. When the user logs in again, this password will be used for authentication. For authentication to be successful, the user must do the tasks in the same order as the file. If authentication is successful, the authorised user is granted access**.**

ANALYSIS OF SECURITY

To grasp and comprehend how safe an authentication technique is, all conceivable attack methods must be considered. It's crucial to know whether the suggested authentication mechanism is resistant to such attacks. Furthermore, if the suggested authentication mechanism is not immune to such assaults, we must devise countermeasures to prevent them. This section explains how to defend against such attacks.

Attack with Harshness

Because of the following factors, the attack is extremely difficult.

1. The time it takes to log in can range from 20 seconds to 2 minutes, making it extremely time consuming.
2. Attack Costs: An attacker must fabricate all biometric information if a 3D Virtual Environment has biometric objects.

Attack that has been well-researched

The attacker attempts to discover the most likely distribution of 3D passwords. To carry out such an attack, the attacker must first learn about the most likely 3D password distributions. This is quite challenging because the attacker must research all of the current authentication mechanisms utilised in the 3D environment. It necessitates an examination of the user's object selection for the 3D password. Furthermore, a well-studied assault is difficult to execute because the attacker must perform a bespoke attack for each 3D Virtual environment design. This environment contains a unique set of items and sorts of object responses not seen in any other 3D virtual environment.

Attack on the Shoulders

An attacker records the user's 3D password using a camera or attempts to observe the genuine user while the 3D password is being entered. This is the most effective method of attacking 3D passwords and several other graphical passwords. The user's 3D password, on the other hand, may incorporate biometric data or textual passwords that are not visible from behind. As a result, we presume that the 3D password should be entered in a secure location that is not vulnerable to a shoulder surfing assault.

Timing of the Attack

The attacker watches how long it takes a valid user to log in correctly using 3D Password, which gives an indicator of the length of the 3-D Password. This assault is doomed since it only offers the attacker hints

V. CONCLUSION

Textual and token-based passwords are now used for authentication, which are subject to a variety of attacks. The 3D Password is a multi-featured, multi-factor authentication solution that integrates the advantages of existing authentication methods in a single virtual 3D environment. The three-dimensional password is a cutting-edge authentication mechanism that is still in its infancy. The user experience of the 3-D password will be enhanced and improved by creating various sorts of 3-D virtual settings, deciding on password spaces, and analysing user feedback and experiences from such settings. The 3D password represents the user's authentication preferences and demands, making 3D password usage straightforward. Other authentication systems are less safe and trustworthy than the 3D Password technique. We can make any system more secure by utilising 3d Password, and it will be advantageous for apps used in the commercial world, the government sector, and personal use.

REFERENCES

1. Alsulaiman, F.A.; El Saddik, A., "Three -for Secure" IEEE Transactions on Instrumentation and measurement, vol.57, no.9, pp 1929 - 1938.Sept. 2008.
2. Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod "Secure Authentication with 3D Password" International Journal of Engineering Science and Innovative Technology (IJESIT)
3. Duhan Pooja, Gupta Shilpi, Sangwan Sujata, & Gulati Vinita "SECURED AUTHENTICATION: 3D PASSWORD" International Journal of Engineering and Management Studies.
4. S. Ranjitha "Secure Authentication with 3D Password" IFET College of Engineering
5. Anuradha Srivastava "3-D PASSWORD – A more secured authentication" Slideshare.net
6. "3D PASSWORD – Seminar" http://www.seminarsonly.com/computer%20science/3Dpassword.php
7. http://www.ijesit.com/Volume%202/Issue%202/IJESIT2 0130 2_16.pdf
8. 3D Password: Minimal Utilization of Space and Vast Security Coupled with Biometrics for Secure Authentication