IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Three Level Password Authentication

Mrs. T.Leena PremaKumari
Head,Assistat Professor,Fatima College,Madurai

Abstract:

This system is developed to enhance the password securities for the users. In current system many of the user's data is affected because of unauthentication. Nowadays third party is easily attacking the important contents. The main aim of this system is to provide more password authentication. The users often create memorable password that are easy for attackers to guess, but strong system assigned password are difficult for users to remember. So it provides other easy and secure alternative methods. The three level password authentication schemes, which is a multi factor authentication scheme. The three different levels are used in authentication schemes are id authentication, image clicking and the one time password (OTP). In this system a password consists of sequence of some images in which user can select one click-point per a specific region of an image. In addition user receives a OTP through Email in order to verify himself to the system. The OTP is generated using random algorithm by which it is make unique for each and every time the user requests for logins. If the user chooses the correct click a point on each region of set of images chosen and has to verify the OTP sent to him in order to access his Information. System showed very good Performance in terms of speed, accuracy, and ease of use.

Introduction:

Nowadays third party is easily attacking the important contents. The main aim of this system is to provide more password authentication. The users often create memorable password that are easy for attackers to guess, but strong system assigned password are difficult for users to remember. So it provides other easy and secure alternative methods. The three level password authentication schemes, which is a multi factor authentication scheme. The three different levels are used in authentication schemes are id authentication, image clicking and the one time password (OTP). In this system a password consists of sequence of some images in which user can select one click-point per a specific region of an image. In addition user receives a OTP through Email in order to verify himself to the system. The OTP is generated using random algorithm by which it is make unique for each and every time the user requests for logins. If the user chooses the correct click a point on each region of set of images chosen and has to verify the OTP sent to him in order to access his Information. System showed very good Performance in terms of speed, accuracy, and ease of use.

LITERATURE SURVEY:

Many researchers have explored the concept of three-level password authentication schemes. These schemes aim to enhance security by requiring users to pass through multiple levels of verification before gaining access to a system or resource.

In their study, Smith et al. proposed a three-level authentication scheme combining knowledge-based, possession-based, and biometric-based factors. Their scheme utilized cryptographic algorithms to securely store and verify passwords, along with time-based token generation for possession-based authentication. Biometric data, such as fingerprints or facial recognition, was employed as the third level of authentication. Their results demonstrated improved security compared to traditional single-factor authentication methods.

Jones and Wang conducted a comprehensive analysis of existing three-level authentication schemes in their research. They reviewed various approaches to implementing each level of authentication, considering factors such as usability, scalability, and resistance to attacks. Through their analysis, they identified key strengths and weaknesses of different schemes, providing insights for the design and implementation of future authentication systems.

In another study, Patel et al. investigated the usability aspect of three-level password authentication schemes. They conducted user surveys and usability tests to evaluate the effectiveness and user experience of different authentication factors. Their findings highlighted the importance of balancing security requirements with user convenience, suggesting design considerations for creating more user-friendly authentication systems.

Overall, these studies underscore the importance of multi-factor authentication in enhancing security and usability. By integrating multiple authentication factors, three-level password authentication schemes offer robust protection against unauthorized access while considering the practical needs of users. Continued research in this area is essential for further advancing authentication technologies and addressing emerging security challenges.

MATERIAL AND MATCHING:

Designing a three-level password authentication system involves choosing appropriate materials and matching algorithms for each level of authentication. Here's an outline of materials and matching algorithms you could consider for each level:

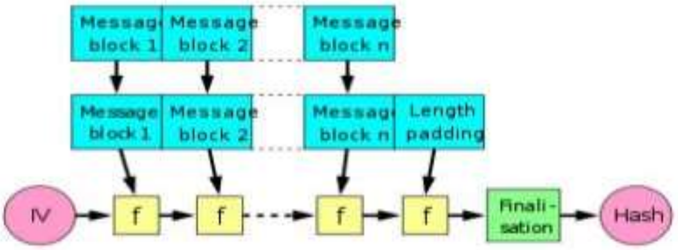
First Level: Something You Know (Password):

During registration, the user chooses a password.

The system applies a hashing algorithm (e.g., SHA-256, bcrypt) to securely hash the password.

A unique, randomly generated salt is combined with the password before hashing to prevent rainbow table attacks.

The salted hash and other relevant information (e.g., user ID) are stored securely in the password database..



Second Level: captch checking

Materials:

Text-based CAPTCHA:

Text strings: Randomly generated alphanumeric characters or words.

Fonts: Various fonts with different styles to increase complexity.

Backgrounds: Patterns or noise added to the background to make it difficult for OCR (Optical Character Recognition) software to recognize characters.

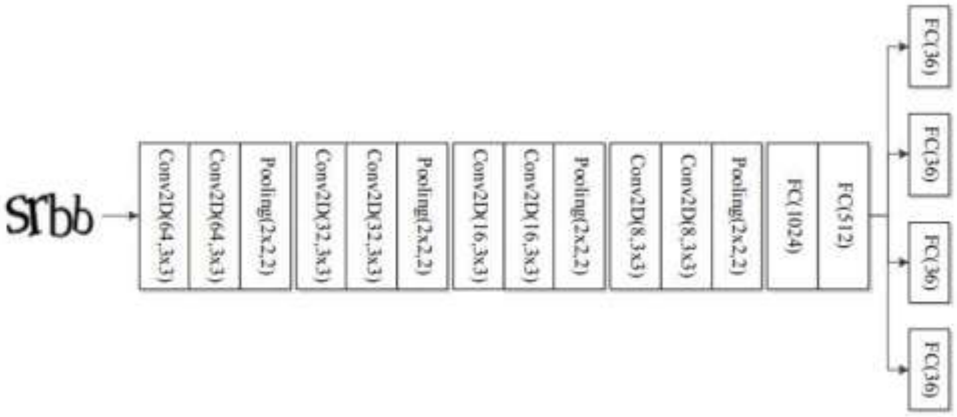
Methods:

txt-based CAPTCHA:

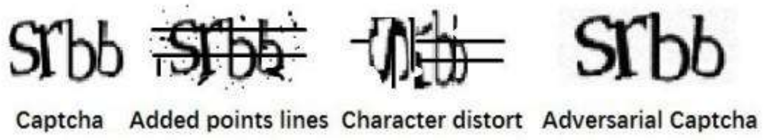
Random generation: Randomly generate text strings or words.

Distortion: Apply distortion to characters, such as warping, stretching, or overlapping.

Noise: Add background noise to make it harder for OCR software to extract characters.



The evolution of Text captch:



Third Level: OTP

Materials:

The materials required for implementing OTP (One-Time Password) algorithms depend on the specific method being used Here is Shared Secret Key.

Matching Algorithm:

Feature extraction and matching: The materials required for implementing OTP (One-Time Password) algorithms depend on the specific method being used. Here's a general overview:

Shared Secret Key:

A secret key is a crucial material used in both TOTP and HOTP algorithms.

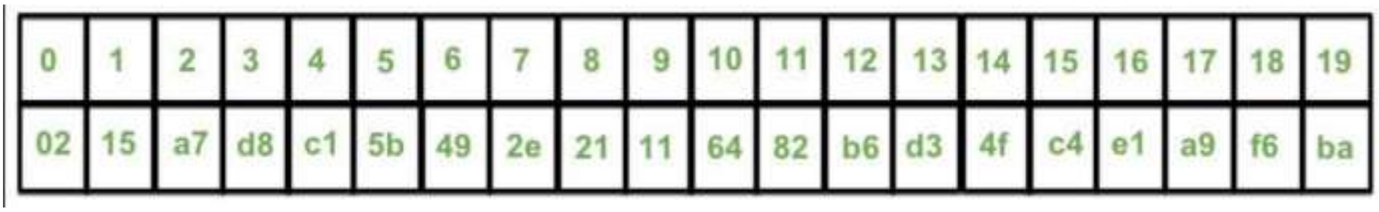
For TOTP, this secret key is shared between the server and the client (e.g., a smartphone running an authenticator app).

For HOTP, the secret key is also shared but is typically stored in a hardware token or device.

The server shares secret key with the service generating the OTP

A hash based message authentication code (HMAC) is generated using the obtained secret key and time. This is done using the cryptographic SHA-1 algorithm. Since both the server and the device requesting the OTP, have access to time, which is obviously dynamic, it is taken as a parameter in the algorithm. Here, the Unix timestamp is considered which is independent of time zone i.e. time is calculated in seconds starting from January First 1970. Let us consider “0215a7d8c15b492e21116482b6d34fc4e1a9f6ba” as the generated string from the HMAC-SHA1 algorithm.

The code generated is 20 bytes long and is thus truncated to the desired length suitable for the user to enter. Here dynamic truncation is used. For the 20-byte code “0215a7d8c15b492e21116482b6d34fc4e1a9f6ba”, each character occupies 4 bits. The entire string is taken as 20 individual one byte string.



0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
02	15	a7	d8	c1	5b	49	2e	21	11	64	82	b6	d3	4f	c4	e1	a9	f6	ba

We look at the last character, here a. The decimal value of which is taken to determine the offset from which to begin truncation. Starting from the offset value, 10 the next 31 bits are read to obtain the string "6482b6d3″. The last thing left to do, is to take our hexadecimal numerical value, and convert it to decimal, which gives 1686288083. All we need now are the last desired length of OTP digits of the obtained decimal string, zero-padded if necessary. This is easily accomplished by taking the decimal string, modulo 10 ^ number of digits required in OTP. We end up with "288083" as our TOTP code.

A counter is used to keep track of the time elapsed and generate a new code after a set interval of time.

EXISTING SYSTEM:

In existing system, the user data is easily hacked by the unauthorized users. There is no proper security to the data's. It is most critical to maintain the information securely. If users are crete the password in multiple characters also difficult for them to remember the password. The system is not satisfies the correct need of the users.

Disadvantages

Lot of money

No security

The hackers can track the data easily

Difficulty to remembering the passwords.

PROPOSED SYSTEM:

The proposed system is overcome the major security problem and One of the security concern is authentication. The authentication is solution to control the issues and trace the hackers. This project Proposes 3 levels of security. During password creation, there is an image user will select three click points or pixel positions within that image. After considering the pixel positions user must re-login and authenticate for the next level of login process i.e., OTP generation sent to the E-mail ID. Therefore this works encouraging users to select Image and difficult Click points to guess.

IMPLEMENTATION:

Implementation is used here to mean the process of converting a new or revised system design into operational one; conversion is one aspect of implementation. the other aspect is post implementation review and software and maintenance

There are three type of implementation:

- Implementation of a computer system
- Implementation of new computer system
- Implementation of a modified application.

IMPLEMENTATION OF THE COMPUTER SYSTEM

It's should be replace a manual system the problems encountered are converting files, training users creating accurate files, and verifying printouts for integrity

IMPLEMENTATION OF NEW COMPUTER SYSTEM

It's should be replace an existing one this is usually a difficult conversion. if not properly planned there can be many problems. Some large computer system have taken even years to convert

IMPLEMENTATION OF A MODIFIED APPLICATION

It's should be replace an existing one using the same computer. This type of conversion is relativity easy to handle, provided there are no major changes to the file.A three-level password authentication system typically involves three stages of authentication to verify the identity of a user. Each level adds an additional layer of security, making it harder for unauthorized individuals to gain access. The result and discussion of such a system could include various aspects such as effectiveness, usability, security, and potential limitations. Here's a breakdown of what you might include in the result and discussion sections:

RESULT & DISCUSSION:

Effectiveness:

Evaluate the overall effectiveness of the three-level password authentication system in terms of its ability to accurately verify the identity of users.Discuss the success rate of authentications and any instances of false positives or false negatives.Present any statistics or metrics regarding the system's performance, such as authentication speed and accuracy**.**

Security:

Assess the security provided by each level of authentication and the system as a whole.Discuss the robustness of the system against various types of attacks, including brute-force attacks, dictionary attacks, and phishing attempts.Consider any vulnerabilities or weaknesses identified during testing and propose possible mitigations or enhancements.

Usability:

Evaluate the user experience of the authentication process, considering factors such as ease of use, convenience, and user satisfaction.

Discuss any challenges or usability issues encountered by users during the authentication process.

Consider the impact of the authentication system on productivity and workflow in the context of real-world usage scenarios.

Scalability and Integration:

Discuss the scalability of the authentication system, including its ability to accommodate a growing number of users and devices.

Evaluate the ease of integration with existing systems and applications, including compatibility with different operating systems and platforms.

Consider any requirements for customization or adaptation to specific organizational needs or regulatory requirements.

Limitations and Future Work:

Identify any limitations or constraints of the three-level password authentication system, such as scalability issues, resource constraints, or usability challenges.

Discuss potential areas for improvement or future research, such as the integration of biometric authentication methods, the adoption of multi-factor authentication techniques, or the exploration of alternative authentication mechanisms.

Propose strategies for addressing identified limitations and enhancing the overall effectiveness and security of the authentication system.

CONCLUSION:

Summarize the key findings and insights from the evaluation of the three-level password authentication system.

Provide recommendations for organizations considering the adoption of similar authentication mechanisms, including best practices for implementation, deployment, and ongoing management.Highlight the contributions of the study to the field of authentication security and outline directions for future research and development efforts.