iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** III **Month of publication:** March 2018

DOI: http://doi.org/10.22214/ijraset.2018.3021

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue II, March 2018- Available at www.ijraset.com

An Efficient Approach for Multilevel Authentication System for Banking Services

Ms. K. Usha Rani[1], Mrs. P. Rajeswari[2]
[1]*Mphil Scholar,* [2]*Assist.Professor,Department of Computer Science, Cauvery College for Women, Bharathidhasan University, Trichy, Tamil Nadu(India)*

Abstract: ***Increasing security has always been an issue since Internet and Web Development came into existence, text based passwords is not enough to counter such problems, which is also an anachronistic approach now. Therefore, this demands the need for something more secure along with being more user-friendly. Therefore, this system has to increase the security by involving a 3-level security approach, involving text based password at Level 1, Image Based Authentication at Level 2,slider based password authentication is implemented, at Level 3 password key such as 9 secret character's should be used. Thus an assiduous effort has been done for the Shoulder attack, Tempest attack, and Brute-force attack at client side, through the use of unique image set in the IBA System Authentication plays a crucial role in protecting resources against unauthorized and illegal use. Security at this level has been imposed by using Text based password (with special characters), which is a usual and now an anachronistic approach. At this level the security has been imposed using Image based authentication (IBA), where the user will be asked to select from the two difficulty levels. Both the levels will be having three unique Image grids, from where the user has to select three images, one from each grid. After the successful clearance of the above two levels, the 3-Level Security System will then generate a one-time numeric password that would be valid just for that login session. Any hacker if in the extreme case, suppose (although difficult) will cross through the above two mentioned security levels, will definitely not be able to cross the third security level.***

Keywords: Security, authentication, password, image grid, attacks

I. INTRODUCTION

Various graphical password schemes have been proposed as alternatives to text-based passwords. Research and experience have shown that text-based passwords are fraught with both usability and security problems that make them less than desirable solutions. Psychology studies have revealed that the human brain is better at recognizing and recalling images than text. Graphical passwords are intended to capitalize on this human characteristic in hopes that by reducing the memory burden on users, coupled with a larger full password space offered by images, more secure passwords can be produced and users will not resort to unsafe practices in order to cope. In this thesis, has propose a new click-based graphical password scheme called Cued Click Points (CCP). It can be viewed as a combination of Pass Points, Pass faces, and Story. A password consists of one click-point per image for a sequence of images. The next image displayed is based on the previous click-point so users receive immediate implicit feedback as to whether they are on the correct path when logging in. CCP offers both improved usability and security. Users could quickly create and re-enter their passwords. Another feature of CCP is the immediate implicit feedback telling the correct user whether their latest click-point was correctly entered. Authentication is an essential thing, which prevents unknown person in a computer based environment system.

Now a days, most frequently used method in the computer based system for authentication is text based authentication in which user create passwords by using characters, number and special characters. Earlier experiments has shown that text based passwords have struggled with usability and security issues. To mitigate these problems graphical passwords techniques have been introduced. In graphical based authentication, instead of text it uses images to create a password. Slider based authentication provides the set of count value which has used to set the pin number for ATM application. It is only used for secure process.

II. OBJECTIVE OF RESEARCH

A. Existing System

Security-sensitive environments protect their resources against unauthorized access by enforcing access control mechanisms. Text based passwords are not secure enough for such applications. User authentication can be improved by using both text passwords and structured images. The existing system is access control mechanism. It proposed Passwords which could be composed of several

points anywhere on an Image. They also proposed a scheme with three overlapping grids, allowing for login attempts that were approximately correct to be accepted.

1) *Drawbacks in the Existing Systems:* It seems obvious that some areas of an image are more attractive to users as click-points. If this phenomenon is too strong, the likelihood that attackers can guess a password significantly increases. If attackers learn which images are being used, they can select a set of likely hotspots through image processing tools or by observing a small set of users on the target image and then building an attack dictionary based on those points.

B. Proposed System

The proposed system consists of proficient multilevel authentication System is developed such as image based authentication, slider based authentication, passkey based authentication is implemented. A password authentication system should encourage strong passwords while maintaining memo ability. The authentication schemes allow user choice while influencing users toward stronger passwords. In our system, the task of selecting weak passwords (which are easy for attackers to predict) is more tedious, discouraging users from making such choices. In effect, this approach makes choosing a more secure password the path of least resistance. Rather than increasing the burden on users, it is easier to follow the system's suggestions for a secure password-a feature lacking in most schemes.

1) *Advantages Of Proposed System*

a) To increase the security of this system by increasing the number of levels used, the number of tolerance squares used.
b) User Registration increasing the number of levels used authentication.
c) Include encryption and decryption methods (AES algorithm).
d) Include Mail and Message Options
e) Include generate in pixel values randomly.

III. SCOPE OF THE RESEARCH

Authentication is an essential thing, which prevents unknown person in a computer based environment system. Now a days, most frequently used method in the computer based system for authentication is text based authentication in which user create passwords by using characters, number and special characters. Earlier experiments has shown that text based passwords have struggled with usability and security issues. To mitigate these problems graphical passwords techniques have been introduced. In graphical based authentication, instead of text it uses images to create a password. In slider based authentication the counter value will be provided .The pass key authentication has to pass a set of digits and characters as the password securing process. Thus in this thesis there are three levels of authentication will be used secure the application.

IV. RELATED WORK

Sonia Chiasson [2012] Persuasive Technology was first articulated by Fog as using technology to motivate and influence people to behave in a desired manner. An authentication system which applies Persuasive Technology should guide and encourage users to select stronger passwords, but not impose system-generated passwords. To be effective, the users must not ignore the persuasive elements and the resulting passwords must be memorable. As detailed below, PCCP accomplishes this by making the task of selecting a weak password more tedious and time consuming. The path of least resistance for users is to select a stronger password (not comprised entirely of known hotspots or following a predictable pattern). The formation of hotspots across users is minimized since click-points are more randomly distributed. PCCP's design follows Fogg's Principle of Reduction by making the desired task of choosing a strong password easiest and the Principle of Suggestion by embedding suggestions for a strong password directly within the process of choosing a password.

Yang Xiao [2012] discussed how to prevent users' passwords from being stolen by adversaries in online environments and automated teller machines. We propose differentiated virtual password mechanisms in which a user has the freedom to choose a virtual password scheme ranging from weak security to strong security, where a virtual password requires a small amount of human computing to secure users' passwords. The tradeoff is that the stronger the scheme, the more complex the scheme may be. Among the schemes, we have a default method (i.e., traditional password scheme), system recommended functions, user-specified functions, user-specified programs, and so on. A function/program is used to implement the virtual password concept with a tradeoff of security for complexity requiring a small amount of human computing. We further propose several functions to serve as system recommended functions and provide a security analysis. For user-specified functions, we adopt secret little functions in which security is enhanced by hiding secret functions/algorithms.

Ben Adida [2006] presented Lightweight Email Signatures (LES), a simple cryptographic architecture for authenticating email. LES is an extension of DKIM, the recent IETF effort to standardize domain-based email signatures. LES shares DKIM's ease of deployment: they both use the DNS to distribute a single public key for each domain. Importantly, LES supports common uses of email that DKIM jeopardizes: multiple email personality's firewalled ISPs, incoming-only email forwarding services, and other common uses that often require sending email via a third-party SMTP server. In addition, LES does not require DKIM's implied intra-domain mechanism for authenticating users when they send email. LES provides these features using identity-based signatures. Each domain authority generates a master key pair, publishes the public component in the DNS, and stores the private component securely. Using this private component, the authority delivers to each of its users, via email, an individual secret key whose identity string corresponds to the user's email address. A sender then signs messages using this individual secret key. A recipient verifies such a signature by querying the appropriate master public key from the DNS, computing the sender's public key, and verifying the signature accordingly. As an added bonus, the widespread availability of user-level public keys enables deniable authentication, such as ring signatures. Thus, LES provides email authentication with optional reputability. We built a LES prototype to determine its practicality. Basic user tests show that the system is relatively easy to use, and that cryptographic performance, even when using deniable authentication, is well within acceptable range.

Gaber [1997] Automated Teller Machines (ATMs), serve the easiest way for the bank and the users to transact money in the fastest way. It also brings more security threats by the hackers and the fraudulent. Shoulder-surfing using direct observation techniques, such as looking over someone's shoulder, to get passwords, PINs and other sensitive personal information is a problem that has been difficult to overcome. When a user enters information using a keyboard, mouse, touch screen or any traditional input device, a malicious observer may acquire the user's password credentials. In this paper, we discuss how to prevent shoulder-surfers and other fraudulent by hacking the passwords using various forms. We propose generating random passwords during each transaction with the original password as the reference. Thus the users' password serves as a black hole. By the results that we have obtained, this modified raditional system provides a better security than any other existing system.

Kalaikavitha [2013] In Online based applications most of them used static passwords. In that they follow multiple technics to secure their credentials. For examples: Multi level password authentications, hard codes, Session Passwords, bio- matric technics, and One Time Password. Every method has some advantages and disadvantages. Our proposed idea is to enhance the security level of One Time Password by Encrypting it and logging the user by forwarding the encrypted OTP with Password to the system. It increases the security level of the system. The impact of the Internet over the last few years has meant fundamental changes in the way we access business systems. The network security perimeter has crumbled at all levels while the number of users wanting network access has grown. The geographical location of users has also widened to a situation where they can be, not just in a different department or company branch office, but anywhere in the world. While there are enormous productivity benefits available from increased access, the security risks have greatly increased. The traditional method of securing system access was by authentication through the use of passwords.

Giuseppe [2005] Blaze, Bleumer, and Strauss (BBS) proposed an application called atomic proxy re-encryption, in which a semi-trusted proxy converts a cipher text for Alice into a cipher text for Bob without seeing the underlying plaintext. We predict that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks. Following recent work of Dodis and Ivan, we present new re-encryption schemes that realize a stronger notion of security, and we demonstrate the usefulness of proxy re-encryption as a method of adding access control to a secure file system. Performance measurements of our experimental file system demonstrate that proxy re-encryption can work effectively in practice.

Lee [2009] Internet of Things is a ubiquitous concept where physical objects are connected over the internet and are provided with unique identifiers to enable their self-identification to other devices and the ability to continuously generate data and transmit it over a network. Hence, the security of the network, data and sensor devices is a paramount concern in the IoT network as it grows very fast in terms of exchanged data and interconnected sensor nodes. This paper analyses the authentication and access control method using in the Internet of Things presented by Jing et al (Authentication and Access Control in the Internet of Things. In Proceedings of the 2012 32nd International Conference on Distributed Computing Systems Workshops, Macau, China, 18–21 June 2012, pp. 588–592). According to our analysis, Jing et al.'s protocol is costly in the message exchange and the security assessment is not strong enough for such a protocol. Therefore, we propose improvements to the protocol to fill the discovered weakness gaps. The protocol enhancements facilitate many services to the users such as user anonymity, mutual authentication, and secure session key establishment. Finally, the performance and security analysis show that the improved protocol possesses many advantages against popular attacks, and achieves better efficiency at low communication cost.

Sharma [2011] The provision of IP Multimedia Subsystem (IMS) introduces important advantages for users of 3G-WLAN access networks. In order to enjoy the benefits of a standardized IMS architecture, the user has to undergo authentication procedure with the access network, followed by an authentication procedure with the IMS layer. This multi-pass authentication procedure is essential for securing IMS from malicious users, resulting in added overhead and possible quality of service degradations. This approach is highly inefficient. The problem is further compounded when the user moves from one WLAN domain into another, which requires the authentication procedure to be repeated. To mitigate this problem, we present a lightweight, robust, and architecture-compatible IMS authentication protocol that implements a one-pass IMS procedure by promoting efficient key re-use for a mobile user. We further show how our protocol is extended to support IMS access over Long Term Evolution (LTE) - Heterogeneous network. IMS, an access network agnostic overlay, is adopted as a de facto standard for for delivering voice over LTE. We make use of Home Node B femtocells to perform the role of IMS proxy. To verify the feasibility of using our protocol in mobile networks, an abstract model of our protocol is derived.

Ningning [2011] Development of network of nodes connected with their trust values and the propagation of these trust values to far away nodes are basic operations of the modern day trustworthy networks. Trust can be exploited to mitigate the security threats in wireless network. Most of the existing trust propagation methods are based on flooding trust information, which puts a heavy burden on wireless communication, especially in ad hoc network and sensor network. In this paper, we propose a rendezvous based trust propagation scheme. Trust requester and trust provider send out trust-request and computed-trust tickets respectively, which will meet in some common rendezvous node with certain probability. Computed-trust will then be propagated to the requester. We carry out detailed performance evaluations of our scheme. The results show that our method achieves up to 66% overhead reduction in trust propagation compared to flood based methods.

McCune [2009] Current mechanisms for authenticating communication between devices that share no prior context are inconvenient for ordinary users, without the assistance of a trusted authority. We present and analyse Seeing-Is-Believing (SiB), a system that utilises 2D barcodes and camera-phones to implement a visual channel for authentication and demonstrative identification of devices. We apply this visual channel to several problems in computer security, including authenticated key exchange between devices that share no prior context, establishment of the identity of a TCG-compliant computing platform, and secure device configuration in the context of a smart home.

V. THEORITICAL ASPECTS OF THE WORK

A. System Security

Authentication is a function where a user presents some credentials to the system. If the system recognizes this set of credentials or the credentials match a given set on the system, then the user is said to be authorized otherwise the user is not authorized. Authentication is needed to let the system perform some tasks for the user. The user needs to be authorized to request services from the system. Before a user can be authenticated to the system, he has to be registered with the system for the first time. This step is called registration. So, for a new user, he has to get registered with a system and then authenticated before he can request services. In a basic authentication process, a user presents some credentials like user ID and some more information to prove that the user is the true owner of the user ID. This process is simple and easy to implement. An example of this type of authentication process is the use of user ID and password. A complicated process involves a user ID, password and a key value generated with time and which changes constantly at fixed intervals. A user is authenticated only if all three values are right. This is better and more secure than the basic authentication process as the user has to be there physically to use the changing key.

B. Graphical Password

This is a simple system where a user presents a user ID and a password to the system. If the user ID and password match with the one stored on the system, then the user is authenticated. A user may have many accounts on many computers. He has to remember many passwords. Research on human cognitive ability has generated a lot of knowledge on what an individual can remember. For example, domain names are used instead of IP addresses and telephone numbers are broken in to chunks for an individual to remember easily. It is also proved that individuals can remember images more easily than the text. The general tendency is that an individual may not remember text passwords easily and he may write it down. This can lead to stealing password to gain unauthorized access to a system.

Since passwords cannot be very long, they are easy to break using brute force attacks like attempting different passwords (online attack) or by offline attack on the password hash file. There are many other ways to break passwords like packet sniffing, by accidental discovery. Network traffic is easy to capture and analyze using the tools available in the web. Network protocol

analyzers, such as Ethereal Packet Sniffer and tcp dump can be used to accumulate both incoming and outgoing network data including text based passwords.

Graphical password systems are a type of knowledge-based authentication that attempts to leverage the human memory for visual information. A comprehensive review of graphical passwords is available elsewhere. Of interest herein are cued-recall click-based graphical passwords (also known as loci metric). In such systems, users identify and target previously selected locations within one or more images. The images act as memory cues to aid recall. Example systems include Pass Points and Cued Click-Points (CCP).

C. PCCP

A precursor to PCCP, Cued Click-Points (CCP) was designed to reduce patterns and to reduce the usefulness of hotspots for attackers. Rather than five click-points on one image, CCP uses one click-point on five different images shown in sequence. The next image displayed is based on the location of the previously entered click-point, creating a path through an image set. Users select their images only to the extent that their click-point determines the next image. Creating a new password with different click-points are results in a different image sequence.

VI. EXPERIMENTATIONAND RESULTS

A. Algorithm Techniques

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

B. Bitmap Representation

In computing, a bitmap is a mapping from some domain (for example, a range of integers) to bits, that is, values which are zero or one. It is also called a bit array or bitmap index. In computer graphics, when the domain is a rectangle (indexed by two coordinates) a bitmap gives a way to store a binary image, that is, an image in which each pixel is either black or white (or any two colors).The more general term pixmap refers to a map of pixels, where each one may store more than two colors, thus using more than one bit per pixel. Often bitmap is used for this as well. In some contexts, the term bitmap implies one bit per pixel, while pixmap is used for images with multiple bits per pixel. A bitmap is a type of memory organization or image file format used to store digital images. The term bitmap comes from the computer programming terminology, meaning just a mapofbits, a spatially mapped arrayofbits. Now, along with pixmap, it commonly refers to the similar concept of a spatially mapped array of pixels. Raster images in general may be referred to as bitmaps or pixmaps, whether synthetic or photographic, in files or memory.

C) Pixel Storage

In typical uncompressed bitmaps, image pixels are generally stored with a color depth of 1, 4, 8, 16, 24, 32, 48, or 64 bits per pixel. Pixels of 8 bits and fewer can represent either grayscale or indexed color. An alpha channel (for transparency) may be stored in a separate bitmap, where it is similar to a grayscale bitmap, or in a fourth channel that, for example, converts 24-bit images to 32 bits per pixel. The bits representing the bitmap pixels may be packed or unpacked (spaced out to byte or word boundaries), depending on the format or device requirements. Depending on the color depth, a pixel in the picture will occupy at least n/8 bytes, where n is the bit depth. For an uncompressed, packed within rows, bitmap, such as is stored in Microsoft DIB or BMP file format, or in uncompressed TIFF format, a lower bound on storage size for a n-bit-per-pixel (2^n colors) bitmap, in bytes, can be calculated as: Size = width • height • n/8, where height and width are given in pixels. In the formula above, header size and color palette size, if any, are not included. Due to effects of row padding to align each row start to a storage unit boundary such as a word, additional bytes may be needed.

VII. RESULT

Image-based-authentication (I.B.A.) is a good alternative to traditional password system. Images are easier to recall than alphanumeric password. Image based password authentication system by using touch screen sensor based graphical LCD interfacing

provides an image based security system which can be installed in various sectors like industrial, educational institute, banking and medical also. This system provides a better security system for all users. Images are more easy to recall in comparison to string of character. To develop a hard to guess and crack password system keeping it very easy & interactive for the user. Graphical passwords provide a promising alternative to traditional alphanumeric passwords. They are attractive since people usually remember pictures better than words. In this extended abstract, has propose a simple graphical password authentication system. Slider based authentication provides the set of counter points which has used to set the pin number for ATM application. Using this three authentication process provides efficient security level.

VIII. CONCLUSION

A. Contribution

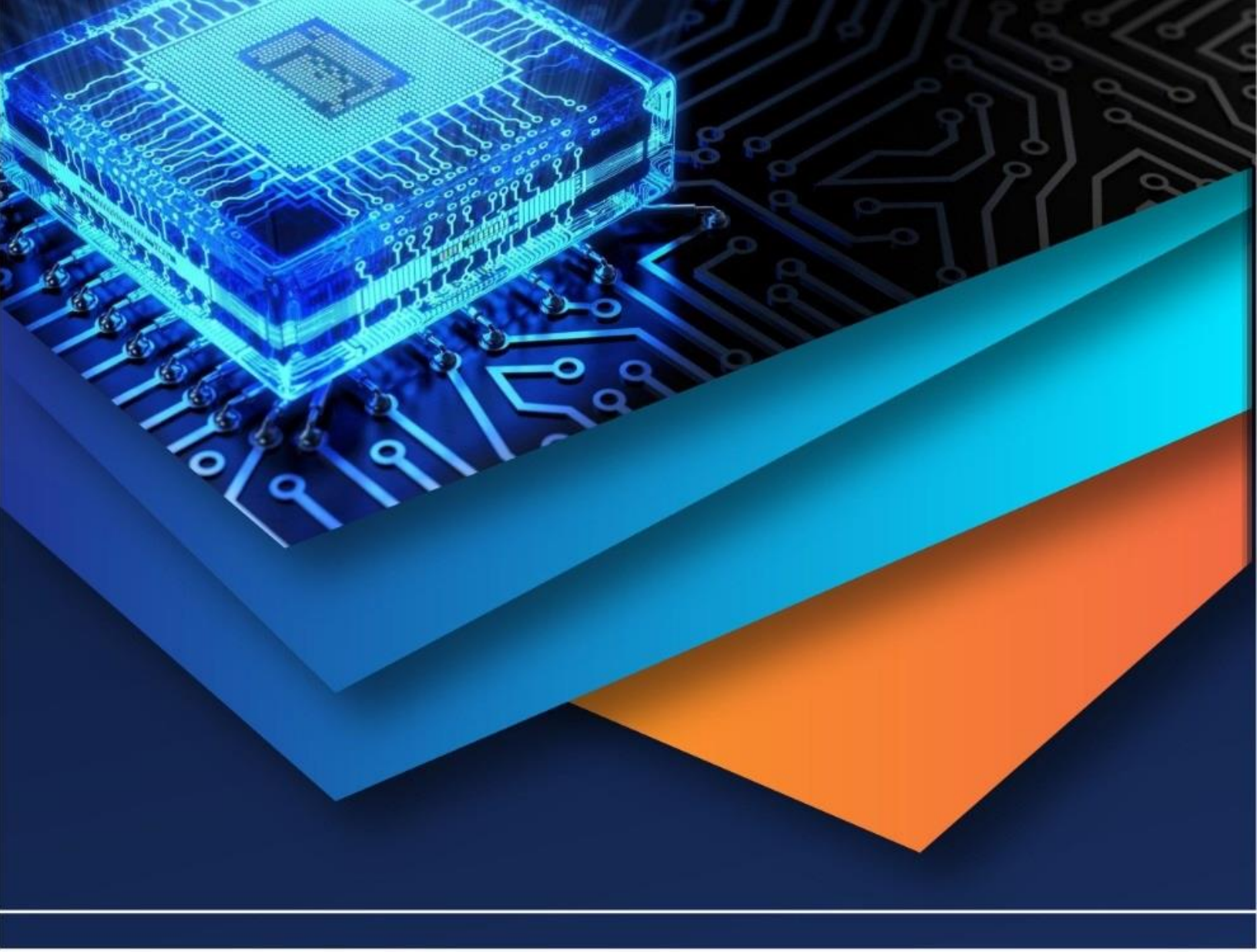
The proposed proficient multilevel scheme is implemented and it shows promise as a usable and memorable authentication mechanism. By taking advantage of users' ability to recognize images and the memory trigger associated with seeing a new image, it has advantages over Pass Points in terms of usability. Being cued as each images shown and having to remember only one click-point per image appears easier than having to remember an ordered series of clicks on one image. This System offers a more secure alternative to Pass Points. CCP increases the workload for attackers by forcing them to first acquire image sets for each user, and then conduct hotspot analysis on each of these images. Security is achieved because only legal user is known that what kind of colour image block selected and in what sequence Image- based authentication techniques, although currently in their infancy, might have a wider applicability in future common security goal in password-based authentication systems is to maximize the effective password. We perceive it more user-friendly technique that helps to increase the password quality tremendously compared to a text-based approach. In this paper we have proposed simple secure authentication technique issues of how better to protect the available information.

B. Future Orientation

Nothing will be useful until it is update & enhanced timely just like IT field. In such a way that this software can have more future enhancement such as. In this thesis mode is restricted to DD, which can be used in future by connecting it to the bank server such that e-payments are enabled. Authentication on administrator side can be moved over to biometrics for more secure access and captcha system is also possible to implement Database used has limited storage, Which can be switched to SQL etc Virtual auction can be enabled through web cams Virtual reality for the products can be achieved with the development of technology It can be enhanced according to the client user friendliness Can be enhanced with blogs in future for tie up with different organization.

REFERENCES

[1] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin, The Design And Analysis Of Graphical Passwords, Proceedings of the 8th USENIX Security Symposium Washington, D.C., USA, August 23–26, 1999.
[2] D. Davis, F. Monrose, and M. Reiter. On user choice in graphical password schemes. In 13th USENIX Security Symposium, August 2004
[3] S. Chiasson, R. Biddle, and P. van Oorschot. A second look at the usability of click-based graphical passwords. In the proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS), July 2007.
[4] Susan Wiedenbeck, Jim Watersa, Jean-Camille Birget, Alex Brodskiy, NasirMemon, PassPoints: Design and longitudinal evaluation of a graphical password system, Int. J. Human-Computer Studies 63 (2005) 102–127
[5] Sonia Chiasson1,2, P.C. van Oorschot1, and Robert Biddle , Graphical Password Authentication Using Cued Click Points, April 10, 2007.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY