Multiple Features Based Multilevel Authentication Method

Kushal Nigam[1], Amit Ranjan[2]
[1] Dept of CSE
[2] Assistant Professor, Dept of CSE
[1, 2] Shri Ram Institute of Science & Technology, Jabalpur, Madhya Pradesh, India.

Abstract*- With the increasing role of numerous Internet services, more and more private data must be protected. One of the mechanisms which is used to ensure data security is user authentication. A reliable authentication mechanism is a foundation of security of a remote service but, on the other hand, it is also a source of user frustration because of fear of losing access in case of three failures. A remedy to this problem could be contextual secure authentication. Such a protocol should provide multi-level authentication mechanism which increases user satisfaction without decreasing a protection level. In this thesis we propose a risk analysis procedure of a new authentication management model using contextual data and image data oriented on user experience. We describe an approach to risk assessment of the mechanism, which supports a process of choosing the proper multi-step authentication procedure. On this basis, it is possible to provide a security solution which keeps balance between user satisfaction (related to QoE) and the obtained Level of Security (related to QoP).*

Keywords- Authentication, Risk assessment, Authentication systems management, Contextual security, Quality of Experience, Quality of Protection.

I. INTRODUCTION

User authentication is the first step in system security when accessing resources on a network. Passwords are the most popular way to authenticate a user on a network. The Text-based passwords have been a used for a very long time. But the vulnerabilities of alphanumeric Text-based passwords are well known. The main usability problem is on the memorability aspect. User defined password are easy to guess if an attacker uses social engineering skills on a victim, and the system defined password are difficult to remember as the user can not relate itself to the password and are very complex. They are also vulnerable to dictionary attacks, shoulder surfing attacks, key-logging attacks, etc. The alternative techniques for text-based password are biometrics, token-based and graphical passwords. Token-based passwords such as a magnetic card are susceptible to loss of token and also require additional hardware. Whereas Biometrics password, such as palm prints, voice scans iris scan, etc. Are not used on a large scale due to high cost and needs to be changed with time due to change in human body caused by aging and other natural factors.

Over the past years, computing paradigms have greatly evolved with the rapid development of computer network and information technologies. Transparent computing [1] is one of the emerging technologies, which allows users to enjoy user-controlled services by extending the stored program concept in the von Neumann architecture into the networking environments spatio-temporally. Transparent computing loads a variety of heterogeneous OSs and applications dynamically on different device. This feature enables users to focus on the available application services without caring about which physical device will be used and what OS should be run on it.

The new mechanism comes with many advantages in information security aspect [2]. The centralized management at servers can bring convenience to the protection of user’s data, and reduce the risks of information leakage and data theft. However, this uniqueness has brought new challenges in service reliability and security, since the OSs, applications and data are centralized in servers, and they are shared by all users in transparent computing system. We envision such a scenario: An enterprise introduces the transparent computing as its office system, due to the desired features of transparent computing. Some information, (e.g., files, tables, data, etc.) will be produced during the day-to-day work of the employees in this enterprise. The produced data has different security levels and access permissions. For example, the open files can be shared with everyone, but some sensitive tables may be revealed to specific users, and other private personal information can not be disclosed to anyone.

Thus, according to their sensitivity, users classify the information into three categories: public information, sensitive information, private information. While users in transparent computing are supposed to reserve no storage space on their clients, all execution results and data must be stored to the Transparent Servers (TSs). Without users’ consent, the data stored in servers may be abused or misused by unauthorized accesses or server managers. Therefore, a secure protection scheme is imperative to protect the private information of each user before storing data into TSs, and the scheme is supposed to protect user information with multilevel security, and provide precise access control to them as well. Some existing multiple-receiver encryption schemes use Attribute-Based Encryption (ABE) [3] to achieve multilevel confidentiality and fine-grained access control, but these methods consume large computation cost due to the bilinear map operations during encryption and decryption. Moreover, effective user revocation is an intractable issue in these schemes, since the data should be re-encrypted when privilege is revoked. How to protect multilevel data security and achieve authorized resource sharing in an efficient and flexible way in such an environment has become a problem. In this thesis, we propose a Multilevel Access Security Scheme (MASS) to protect user data with different security levels. The proposed scheme introduces an Authentication Server (AS), which acts as "Authentication Authority", to perform multilevel access control and identity authentication, dealing with user data access, storage, transmission, and processing in transparent computing environment. The scheme is essentially based on the following attractive characteristics and capabilities of transparent computing.

1) We are among the first to consider the problem of multilevel authentication of user in transparent computing environment. We design a multilevel access control scheme, which enables a privilege user to access the specified files under the verification of different level access control polynomials.
2) Our scheme has an overall consideration of multilevel security, effective access control, and user authentication for integrated technologies to provide a security structure in transparent computing.
3) Beyond the traditional model, it can be applied to cross-platform, and thus it is more suitable for transparent computing applications.
As we all know, nearly all the websites have their own login protection mechanism. For example, the websites will lock the accounts with too many login errors. On the other hand, the password policies of website may force the user to set the password no less than eight characters at least, and so on. Users need to manage dozens or even hundreds of passwords [4], so they will reuse their passwords in several websites and use weak passwords with low entropy inevitably.

Graphical password compromises of graphical images instead of text or words. Studies have shown humans perform far better when remembering graphical pictures than words. But they are prone to shoulder surfing attack which is common in public area and is becoming quite a big problem; also problem of threshold level reduces the usability of graphical password.

1.2 Authentication Requirements:

Various attacks like brute force and dictionary attacks can be resisted by text password based authentication if users' select strong password to provide sufficient breakup [5]. However, the limitation of password-based user authentication is that it is difficult to remember the text strings. Due to this, most of the users always end up setting up easy passwords that is, weak passwords in spite of knowing that their accounts can be easily hacked. Using the same password throughout various accounts is another major problem [6]. Difficulty of password authentication is present in several application regions, which has made it easy for criminals to gain access to user's confidential data that includes financial and personal details. This information can be used to commit fraudulent crimes. A legal user login can be impersonated by the adversary to get access to the system. It requires knowledge and diligence to remember these passwords.

Given enough time and resources, an attacker can breach password based security systems. There has been a quest in the computer industry to search for a better alternative, however many present systems use basic authentication schemes that are text based. To change the limitations of passwords based on text, researchers turned their attention towards graphical objects. Another alternative for password generation and authentication is Graphical Authentication. A device with input which is graphical is used which is the main difference between them. Entering the password is done by clicking a couple of images or pixels of an image. Human faces, icons or custom images are a few graphical presentations that are used to create a password in most of the schemes. Graphical passwords provide better usability compared to traditional text passwords. Even though graphical passwords are a great idea, they are not widely used and are also prone to several attacks. Employing multi factor authentication is another method of enhancing the security. The method of authentication where in two or more independent factors are used as part of the credentials is called Multi factor authentication [7]. This is usually done by aggregating the traditional text based authentication with a new factor. Some of the examples of such factors can include handheld devices, smartcards, one-time password tokens or USB tokens. Incorporating two or more factors strengthens the process of authentication. Two-factor authentication has been with us for a while now. An extra layer of security is added by the two-factor authentication in addition to the password. Multi-factor authentication processes have become common place for logins and transactions within systems with high-security requirements. To authenticate the users, our scheme uses two-factor authentication.

1.2.1 Two Factor Authentication [8]

Two Factor Authentication (2FA) is a process where in the identity of the client is verified by using two ways of identification: First is a token such as a card, and second is something that has be remembered, like a code or even a text-string. The two-factor authentication combines:

- What the client has (cell phone, smart card, ID card, software token).
- What the client has (cell phone, smart card, ID card, software token).
- What that the client remembers (personal identification number, pass phrase, password or file).
- What the client is (finger print or retina pattern, voice parameters, or another biometric identifiers) through which the correct person is identified.

Two factor authentications make the login systems strong by using two methods or factors to check user's identity. It is one of the most reliable methods to resist remote attacks such as credential exploitation and attempts use your account. Without physical tokens, the adversary can't pretend to be the user and gain unauthorized access to corporate networks, financial information or user's personal details. By integrating two-factor authentications with the applications, the attacker is unable to access the user's account without possessing the physical token needed to complete the second factor. An example for two-factor authentication is a bank card: The card is the first factor which is a physical token, something the user has and the personal identification number (PIN) along with it acts as a second factor. One of the most widely used services; Gmail employs two-factor authentications. It requires two things for authentication: user's password (something which we know) and Smartphone (something which we have). Google will send a one-time verification code via SMS to the user's phone which provides a second layer of security apart from password [8]. Several usable authentication schemes are PassText, PassDoodle, PassMaps, PassMark and Passphrase.

Roman.et.al in 2007 proposed **PassText** for user authentication. At the PassText creation stage during registration, users are presented with a large body of text to which they are asked to make modifications. Possible modifications include addition or deletion of characters from the text. A system where unique finger traces or doodle is used to quickly identify users in an integrated computing environment is called a PassDoodle [9]. A doodle basically means an ordered set of points, each of which is employed with an extra timestamp that captures the time of creation from the first point (in milliseconds). The unique movement and also shape of the user's PassDoodle is taught to the system so that it can distinguish the other user's PassDoodle during the initial training period. After the end of this period, authentication of the user happens by tracing the user's doodle on a touch screen or any other similar technology. Limitations are present in this scheme. Various attacks like guessing, spyware, key-logger and shoulder surfing reduce the security of the PassDoodle [10].

Map-based graphical password method of authentication is a **PassMap**. This is similar to passwords. National Tsing Hua University researchers proposed this concept. A set of points on a world map is chosen by the customer. This becomes a major criterion for authentication. PassMaps are more memorable and user-friendly. Google Maps are displayed on the user's screens. They can magnify and select any two dots. This is the PassMap password. PassMap cannot be used if the user's device does not have internet access. This is the limitation of this concept. The zoom level has no constraints and users are permitted to choose dots at lower levels.

1.2.2 Multi-Factor Authentication:

Multifactor authentication is one of the de facto standards for systems requiring strong security. In most cases, multifactor authentication is complex and not user-friendly because it requires additional steps as far as end users are concerned. With two-factor authentication, in addition to entering a username and a password (first factor), users need to enter an additional code (second factor) manually that they receive by short message service or look up in a previously printed list of passwords, or that is generated by a hardware or software token. So, although introducing additional authentication factors greatly increases the level of security, it could also become frustrating for end users.

Generally, the authentication evolution is shown in Fig. 1.2.

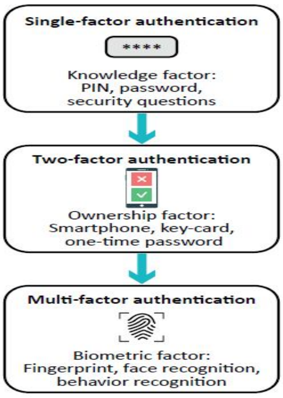


Fig 1.2: Multifactor Authentication.

For multifactor authentication to be conducted properly, one or multiple of these standards are coupled to heighten security standards. Li et al. [11] first introduced the concept of using biometrics as a factor in a three-factor authentication system in order to help the grim situation of network security. In this paper, they proposed using passwords, smart cards, and biometrics as a viable solution towards three-factor authentication. It was through this proposal and the analysis of the progression of modern technology and the in-depth look into the drawbacks of fewer security measures which prompted the use of facial recognition as part of the app to be developed for this project. The discussion of the speed/flow of biometrics, as opposed to other authentication factors, was very influential to the progression of this research. The presented scheme could resist many kinds of attacks and protect the host's multimedia and web resources, which in response, made it very attractive as a potential starting off point.

In Native Autonomous Process Authentication, Olmsted analyzed the promise of multifactor authentication when it came to users while also analyzing the issues that arise when applications try to give credentials to autonomous software processes. Autonomous software processes when allowed credential privileges leave gaps for malicious incursions and attacks [12]. The importance of this paper was paramount as it proposed that in order to have a more secure system, autonomous background processes should not be allowed credentials which in hindsight they should not possess in the first place, as issues can arise.

MFA is supposed to be utilized in cases where safety requirements are higher than usual. For example, consider the daily use case of the ATM cash withdrawal. Here, the user has to provide a physical token (a card) representing an ownership factor, and accomplish it with a PIN code representing knowledge factor to be able to access his account and withdraw money. This system could be easily made more complex by adding the second channel like, for example, one-time password to be entered after the card and password are present [13]. Giving more interesting scenario, it could be done with, for example, facial recognition method. Recent survey found that 30 percent of enterprises plan to implement an MFA solution in 2017, with 51 percent claiming they already utilize MFA, and 38 percent saying they use it in "some areas" of operation.

1.3 Bio-metric Authentication:

Traditional authentication systems use one or both of the following methods for identification: Knowledge based (Ex: remembering a password) or Token based (Ex: carrying an ID card). But these two methods have their own drawbacks which have led to the birth of biometrics method of authentication which is based on something about a person (Ex: face feature). This method makes use of unique features of a human being which vary from a person to person. Biometric is a measurable unique physiological (biological) and behavioral characteristic of a human being. An accurate and most reliable identification or authentication system can be implemented using various biometric characteristics (traits) of a person such as fingerprint, facial features, speech, iris, palm print, signature, DNA, body odour and vein pattern etc. These techniques are preferred over traditional approaches for various reasons:

Unlike in classical methods, Physical presence of a person is mandatory in biometric authentication system in order to claim his identity. The major advantages are:

- Avoids memorizing a password.
- No need of any token to be carried.
- Automated authentication.
- Increased security and reduced ID fraud.

II. REVIEW OF LITERATURE

First time, Leslie Lamport introduced remote user authentication scheme based on one way function to encode password in insecure communication. Later, Hwang et al. proposed authentication scheme in which password table or verifier table is not stored at server so that issue will not arise of stolen password table or verifier table in 1990. In 1998, Jan and Chen introduced scheme for authentication in which password table or verifier table is not stored at server side and password of user is culled by user so that users have reliability in password selection. In 2000, Hwang et al. proposed authentication scheme using smart card based on ElGamal public key cryptosystem and it can withstand against replay attack. In 2003, Lin et al. proposed newly remote user authentication scheme in multiserver architecture and scheme can resist against reply attack and modification attack. In 2004, Juang introduced authentication scheme with more merits like mutual authentication, forward secrecy, session key security and scheme can withstand against replay attack.

In 2008, Lee et al. proposed newly authentication scheme for mobile equipment by utilizing modular, hash, XOR functions and it can withstand against stolen verifier attack, server spoofing attack, parallel session attack [14]. In 2011, Chang and Cheng introduced that Lee and Lee's scheme is vulnerably susceptible to forgery attack and then proposed scheme with overcome impotency of Lee and Lee's scheme which can withstand against server spoofing attack, parallel session attack, forgery attack, replay attack, smart card lost attack and forward secrecy attack [15]. In 2012, Li, Weng and Fan identified that Chang and Cheng's scheme cannot withstand against smart card lost attack, leak of verifier attack and session key disclosure attack and Li, Weng and Fan proposed new scheme with overcome impuissance of Chang and Cheng's scheme and new proposed scheme is secure against password guessing attack, leak of verifier attack, impersonation attack and session key disclosure attack and withal achieves session key agreement, mutual authentication [16]. Recently in 2014, Adela introduced that Li, Weng and Fan's scheme can't withstand against impersonation attack session key disclosure attack and then Adela proposed new scheme to surmount impuissance of Li, Weng and Fan's scheme [17]. The purpose of this study is to review different attacks on remote user authentication schemes. We came to know that there are various attacks in those schemes so that service will be interrupted during accessing system. We identified different attacks like Replay attack, Modification attack, Stolen Verifier attack, Server Spoofing attack, Parallel Session attack, attack, Forgery attack, Smart Card Lost attack, Leak of Verifier attack, Forward Secrecy attack, Impersonation attack, Session Key Disclosure attack and Password Guessing attack in most of authentication schemes. We discussed three schemes in details and theses schemes are Chang-Cheng's scheme, Li-Weng-Fan's scheme and Adela's scheme.

1. Exploiting Predictability in Click-based Graphical Passwords [18]:

The authors were surveyed the security of click-based graphical password schemes by exploring hotspots or PassPoints and probing strategies to predict passwords and exploiting the strategies in guessing attacks. They were used human-computation method to reap PassPoints or click points from the users and to foretell the hotspots. A human-computed data set indexes the click-points which is the initiation of predicting the password. The data set is processed to determine a set of points that creates a human seeded attack. They were engendered click-order pattern attacks which are improvement of independent model-based attacks. Click-based Graphical Password scheme yields 7-10% of correct passwords within 3 guesses. The graphical password schemes are exposed to offline and online attacks, even on systems that implement conservative lock-out policies.

2. Graphical passwords: Learning from the first twelve years [19]:

The authors were surveyed graphical password schemes such as PassFaces and GrIDsure used to authorize e-transactions via handheld devices. PIN-level graphical password schemes better than password-level schemes were used to unlock Android smart phones. They were classified the graphical password schemes into three main categories: recall based graphical password scheme (drawmetric scheme), recognition based graphical password scheme and cued-recall based graphical password scheme. At the same time, they were segregates two types of attacks such as guessing attacks and capture attacks. With the drawmetric systems, the users remind and reproduce a secret design (i.e.) Draw-a- Secret (DAS). Recognition based systems (cognometric systems or searchmetric systems) asks the user to remember images during password generation. With the cued-recall systems, the target specific locations marked within the image must be memorized by the user, thus reducing memory load on users. These systems protect the users from shoulder-surfing attacks and provide usability and security advantages.

3. Against Spyware using CAPTCHA in graphical password scheme [20]:

The authors were proposed a new method called CAPTCHA to prevent spyware attacks. This authentication scheme combines the graphical passwords and text-based CAPTCHAs. This scheme is used in many practical security applications like online polls, e-mail services and search engines. CAPTCHA is a standard method for identifying undesirable or malicious Internet bot programs. The sign-in time is shorter with this authentication scheme. This scheme prevents the users from spyware attack. The password setup by using this authentication scheme can increase cost and time of human intervention attack.

4. FaceDCAPTCHA: Face Detection based color image CAPTCHA [21]:

The authors were proposed a FaceDCAPTCHA algorithm to provide better human guessing power and lower machine attack rates and to effectively eliminate automated attacks. In this authentication scheme, the users must correctly identify visually-deformed human faces fixed in a complex background. The genuine face images and fake images are mixed on an image display that is shown to the users. The users have to manifest the centre point of the genuine face images. If the approximate centre of the genuine face images is correctly marked then the test is solved by the user. After this CAPTCHA test, the user can enter into the login page.

III. PROPOSED SYSTEM

3.1 Proposed System

Proposed system authenticates user at multiple levels. It generates passwords at multiple levels and then concatenates them into one single password. In multi-level authentication, password is entered in stages. Password for next level will be concatenation of the passwords entered for previous levels and the one required for the next level.

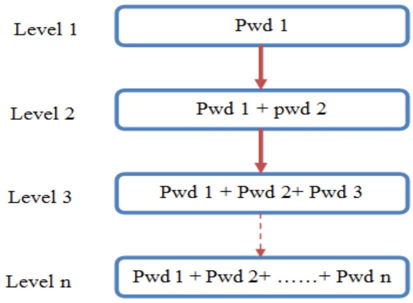


Fig 3.1: Structure of multilevel authentication system

Figure 3.1 indicates structural implementation of multi-level password authentication. At Level-1, password ‘Pwd 1’ is required. On level 2, passwords Pwd 1 and Pwd 2 are concatenated. In the same way, this system can be applied to n levels. After nth level a strong password will be generated.

Figure 3.2 represents proposed methods used at different level for multi-level password authentication. At Level-1, text characteristics of user name like font and color will be used for generating password. At Level-2, one image among many will be selected by user which will be treated as password. At Level-3, predefined pattern grid will be displayed among which user has to select one pattern grid and at last level user has to draw a five point pattern for authentication.

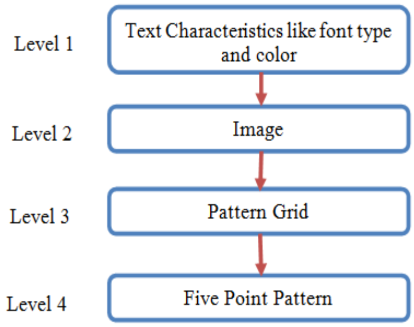


Fig 3.2: Factors used in proposed multilevel authentication system.

Proposed system removes drawback of traditional methods of authentication like one time password, biometric authentication, face recognition etc. They are costly means. One time password need some channel to send OTP like SMS. Biometric and face recognition requires extra device, they are also time expensive. Proposed system is secure, easy, efficient and cost effective also.

Proposed system contains two phases:

- Registration and
- Authentication.

3.2 Registration Phase

Every user should register in the system for using it. In this phase, user registers in the system with choosing his/ her preference of generating password, which will be utilized at the time of login. Steps for this process are as follows:

Step-1: Enter user name and email id.
Step-2: Select font type and color for user name.
Step-3: Select an image from predefined set of images.
Step-4: Select a pattern grid from predefined set of grids.
Step-5: Draw five point patterns on grid.
Step-6: Generate password and its hash.
Step-7: Store hashed password and other details in database.

3.3 Authentication Phase

When user login in the system, system will ask for user name and checks that user exist or not. After that, user should select font & colour of user name, same image, pattern grid and pattern as selected at the time of registration. They are matched with stored data. If matched than user is genuine otherwise not. Steps for this process are given below:

Step-1: Enter user name.
Step-2: Check user exist or not. If exist then go for next step otherwise try again.

Step-3: Select Font and colour for user name (which should be same that are saved at the time of registration for genuine user)
Step-4: Select an image and a pattern grid from predefined set (which should be same that are saved at the time of registration for genuine user)
Step-5: Draw five point patterns on grid.
Step-5: Generate password and its hash.
Step-6: Check this hash pattern with stored pattern.
Step-7: If matched than user is genuine and open the system for further working otherwise try again.

IV. IMPLEMENTATION AND EVALUATION

4.1 Module Description

Proposed system will have following main modules:

- Registration module
- Password creation module
- Hash conversion module
- Pattern matching module

Interfacing of these modules will be shown in figure below. Where, blue arrow represents flow for authentication process and maroon arrow shows flow for registration.

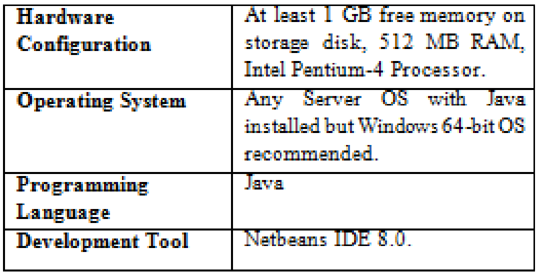
In registration module user enters user name, email id. Then user should select font and colour, an image and a pattern grid from predefined set of images and then draw pattern with five points, convert it into hash and store it. These entire selections user should remember because same should be entered at the time of authentication. They are easy to remember also.

Hash conversion module convert generated password that consist of selection of font, colour, image, pattern grid and five point pattern into hash value using a secure Java Password-Based Key Derivation Function 2 **(**PBKDF2) hashing implementation written by Hornby (2013). This PBKDF2 key derivation function is supposedly more difficult to crack, by requiring more computation on the part of the attacker to compute the hash, depending on the number of iterations used, increasing the time required for each hash computation. It could produce derived keys up to 160 bits long.

4.2 Technical Specifications

Following are minimum specifications for development of the system:

Table 4.2: Technical Specifications.



Hardware Configuration	At least 1 GB free memory on storage disk, 512 MB RAM, Intel Pentium-4 Processor.
Operating System	Any Server OS with Java installed but Windows 64-bit OS recommended.
Programming Language	Java
Development Tool	Netbeans IDE 8.0.

4.3 Predefined Pattern Grid

Proposed system uses following predefined pattern grid:

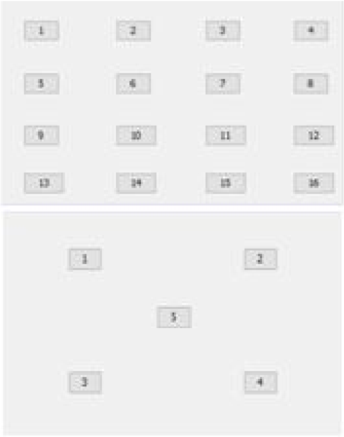


Fig 4.3: Predefined pattern grid

4.4 User Record Structure

User records will be stored in a text file with following fields:

- User Name
- Font and colour ID
- Image ID
- Pattern Grid ID
- Hashed Pattern

4.5 Results & Evaluation

Each single level authentication scheme has limitations and drawbacks if scheme is used alone. Textual password authentication model is easy to break and vulnerable to dictionary and brute force attacks. Third party authentication is not recommended due to cost factor. Graphical passwords are based on the idea that users can recall and recognize pictures better than words. Nevertheless, some graphical password mechanism is time and memory consuming. Bio-metric authentications scheme such as, fingerprints, hand geometry, face recognition, and voice recognition has been used for cloud services authentication. One of the key challenge and disadvantage of applying biometrics is its intrusiveness upon a client's personal characteristic. Furthermore, biometric scheme require a special scanning device to validate users characteristic, which is not appropriate for internet users. Single level password based authentication are not secure enough and are suspected to various attack such as **dictionary attack, brute force attacked and shoulder surfing attacks** etc. Proposed solution prevents system from all these type of attacks.

If all authentication is done by typing passwords into the same device (your desktop client) - then, yes, **key stroke loggers** are still going to be an issue. Keep in mind that when you separate authentication systems, you open up options to go to multifactor authentication, as well - if not now, then in the future - where you could use tokens, separate key pads, etc. - which could limit a simple key logger's ability to get the high privilege access.

Social Engineering (including phishing) - Usually multilevel authentication comes with multiple rounds of training. In the case of an admin account and a regular employee account, the employees usually get a long boring training session on the importance of security, which may or may not be effective. Quite often admins with high risk accounts are given a secondary round of training that is more pointed, and more along the lines of "mess this up in a big, careless way, and you'll be fired". By giving and separating the password, it's often easier, administratively, to enforce this.

Separate security processes - with two levels of passwords, there's an option to let the low level password store compromise on the side of availability while the high risk password store tends towards privacy. For example:

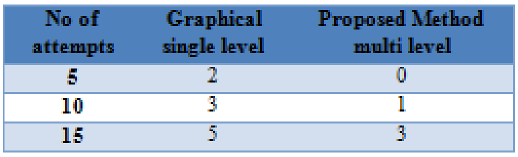
- The low level may provide federation services, remote access, services that support non-company devices, etc. The high level store may require physical access to the building, encryption capabilities that aren't available on all devices, and higher-grade password quality.
- Separate storage - both live and in backup and in logging. A high end system may require encrypted tape backup, securely stored audit logs for a certain period of time - being able to totally separate the infrastructure can be very helpful here. High end storage is expensive, so less to store is a big win.
- Access monitoring - live monitoring of access attempts - a system far in the front of an infrastructure may invoke so many brute force attempts a day that you don't worry much about it until it becomes a DDOS. A system nested deeply inside the infrastructure may be of serious concern every time the intrusion detection raises a flag. Access monitoring may be staffed differently, monitored differently and reacted to differently.

Following are points that kept in mind for threat prevention:

- Password is made from text font, text colour, image, pattern grid and five point patterns, which improves security.
- Password will be stored securely in hashed form using Java PBKDF2 hashing implementation, which is difficult to crack.
- By increasing number of fonts, colours, images and pattern grid system will increase randomness for creating password combinations.

We have also tested our proposed method for shoulder surfing attacks manually. Data and comparison chart is shown below:

Table 5.1: Comparison according to shoulder surfing attacks.



No of attempts	Graphical single level	Proposed Method multi level
5	2	0
10	3	1
15	5	3

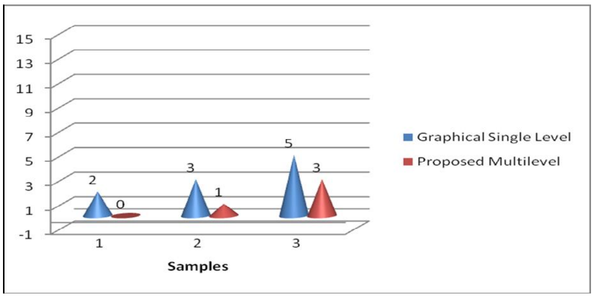


Fig 5.8: Comparison for shoulder surfing attacks.

V.CONCLUSION

This thesis studied about graphical password among authentication methods that can replace text based authentication method, and describes PassPositions which is a new concept of graphical password system implementation technique. PassPoints generate the authentication code by taking advantage of the relative positions of the selection points, making it easy for people who cannot select the correct absolute position.

In this thesis, we proposed a Multi-layer graphical password scheme. Unlike the existing methods, our method employs a Pattern and Recognition-Based Image Layer, and Recall Image Layer. These layers rely on the user's natural cognitive abilities. As user gets different independent challenge for the first and second authentication layers, this scheme is robust to dictionary, rely and brute-force attacks. The cracking probability is lower for a larger number of possible showed images on layer 1, and for patterns with larger amount of sub-patterns.

Hence we can conclude that our proposed system is highly usable and completely robust against key logging attack and shoulder surfing attack. Also our system is resistant to dictionary attack up to some extent. Thus our user credentials are kept safe and not gained by the attacker.

REFERENCE

[1] Y. Zhang and Y. Zhou, "Transparent Computing: Spatio-temporal Extension on Von Neumann Architecture for Cloud Services," Tsinghua Science and Technology, vol. 18, no. 1, 2013, pp. 10–21.

[2] G. Wang, Q. Liu, Y. Xiang, and J. Chen, "Security from the Transparent Computing Aspect," Pro. 2014 IEEE Conf. Computing, Networking and Communications (ICNC), 2014, pp. 216–220.

[3] Khaled W. Mahmoud. Elastic Password: A New Mechanism for Strengthening Passwords using Time Delays between Keystrokes. 2017 8th International Conference on Information and Communication Systems (ICICS), pp.316-321, 2017.

[4] D. Wang, H. Cheng, Q. Gu and P. Wang, Understanding passwords of Chinese users: Characteristics, security and implications. CACR Report, Presented at China Crypt, 2015.

[5] Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin. oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks. IEEE Transactions on Information Forensics and Security, Vol.7, No.2, April 2012.

[6] Misbahuddin, M., Aijaz Ahmed, M., and Shastri, M. H. (2006). A simple and efficient solution to remote user authentication using smart cards. Proceedings of IEEE Conference on Innovations in Information Technology, pp. 1–5.

[7] Aloul, F., Zahidi, S., and El-Hajj, W. (2009). Two-factor authentication using mobile phones. Retrieved from http://www.silicon.com/financialservices/0,3800010322,3915 3981, 00. htm.

[8] Archana B.S., Ashika Chandrashekar, Anusha Govind Bangi," Survey on Usable and Secure Two-Factor Authentication", 978-1-5090-3704-9/17/$31.00 © 2017 IEEE.

[9] PassDoodle; a Lightweight Authentication Method Christopher Varenhorst under the direction of Max Van Kleek and Larry Rudolph Massachusetts Institute of Technology.2016.

[10] Ms Vina S Borkar, Mrs.Priti C.Golhar. Review on Click Based Graphical Password Authentication: International Engineering Journal For Research & Development-ISSN: 2349-0721.@2017.

[11] Z. Xiong Li, "Rhobust three-factor remote usesr authentication scheme with key agreement for multimedia systems," *Security and Communication Networks*, 2016.

[12] R. D. Xinyi Huang, "A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems," *IEEE*, vol. 22, no. 8, pp. 1390-1397, 2010.

[13] F. Aloul, S. Zahidi, and W. El-Hajj, "Two factor authentication using mobile phones," in *Proc. of International Conference on Computer Systems and Applications*, pp. 641–644, ACS/IEEE, 2009.

[14] Lee, Jun Ho, and Dong Hoon Lee. "Efficient and secure remote authenticated key agreement scheme for multi-server using mobile equipment." Consumer Electronics, 2008. ICCE 2008. Digest of Technical Papers. International Conference on. IEEE, 2008.

[15] Chang, Chin-Chen, and Ting-Fang Cheng. "A robust and efficient smart card based remote login mechanism for multi-server architecture." International Journal of Innovative Computing, Information and Control 7.8 (2011): 4589-4602.

[16] Li, Chun-Ta, Chi-Yao Weng, and Chun-I. Fan. "Two-factor user authentication in multi-server networks." International Journal of Security and Its Applications6.2 (2012): 261-267.

[17] Georgescu, Adela. "Vulnerabilities in a Two-Factor User Authentication in Multi-server Networks Protocol." International Joint Conference SOCO'14-CISIS'14-ICEUTE'14. Springer International Publishing, 2014.

[18] P. C. van Oorschot and J. Thorpe, "Exploiting predictability in click-based graphical passwords," J. Comput. Security, vol. 19, no. 4, pp. 669-702, 2011.

[19] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Comput. Surveys. Vol. 44, no.4, 2012.

[20] L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, "Against spyware using CAPTCHA in graphical password scheme," in Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl., Jun. 2010, pp. 1-9.

[21] M.Motoyama, K.Levchenko, "FaceDCAPTCHA: Face Detection based color image CAPTCHA," 2010.