Design & Development of Two Factor Hash Based Authentication Framework

[1]Sunaina Oberoi, [2]Harmandeep Singh

[1,2] Department of Computer Engineering, Punjabi University, Patiala, India

Abstract: **Current Authentication schemes suffer many weaknesses. Textual passwords are widely used; but this textual passwords easy to break and vulnerable to dictionary attacks or brute force attacks. Available Authentication schemes face many problems. Graphical passwords face lack of space. Smart cards or tokens can be lost or prone to theft. Many biometric authentication schemes have been proposed but users tend to resist using that because of their intrusiveness on their privacy. In this paper, we describe the method for implementing connectionless approach for stronger authentication. The proposed Grid-Pin scheme is two-factor authentication scheme which is totally based on knowledge based authentication scheme. It combines current existing textual password scheme and Grid based scheme in which user has to enter his/her PIN (Personal Identification Number) into PIGP(Personal Identification Grid Pattern) out of matrix 4*4 to login his/her account. This is a simple approach for a secure authentication which reduces the probability of breaking textual passwords to a large extent. The main purpose of this method is to provide the stronger authentication to organization's personal data. The secure method guarantees that Authenticating to services like ATM machine is done in very secure manner.**

Keywords: **Brute Force Attack, Dictionary Attack Authentication, PIN (Personal Identification Number), PIGP (Personal Identification Grid Pattern).**

I. INTRODUCTION

Authentication is the process of verifying the claimed identity of a user. There are three fundamental techniques used in authentication mechanism.

1) Something you know, which usually refers to passwords and PINs. The simplest implementations of passwords and personal identification numbers (PINs) yield the simplest of all authentication mechanisms.

2) Something you have, which usually refers to cards or tokens. Physical authentication devices, such as smart cards and password tokens, were developed to eliminate certain weakness associated with passwords. A major benefit of cards and tokens is that they can't be shared with the same freedom as sharing passwords.

3) Something you are, which refers to biometrics - the measurement of physical characteristics or personal traits. Common biometric verification techniques try to match measurements from one user's fingerprint, hand, eyes, face, or voice to measurements that were previously collected from him/her.

Each of these techniques has its own set of advantages and disadvantages [1]. Textual passwords are one of the most widely used authentication techniques. They are easy to implement. But as per a survey it was found out that 25% accounts out of 15,000 accounts having alphanumeric passwords were easily guessed by using a well formatted dictionary of 3X106 words [2]. This is mostly due to the user's carelessness in selecting a known password rather than a random one. Graphical passwords are hard to guess [3] [4] [5] but they are prone to shoulder-surfing attack. I.e. the attacker observes the legitimate user perform the graphical passwords and then imitate it. Tokens do not require the user to memorize the password [6] but they are vulnerable to loss or theft. Biometric passwords are unique for every individual. Unlike textual passwords they need not be memorized and they cannot be stolen [1]. But many users refrain from using biometric passwords due to intrusion on their privacy. Also special scanning devices are needed to authenticate the users which aren't available everywhere.

To overcome these drawbacks, Two-Factor Authentication scheme are introduced. It is an innovative authentication system which works as : At the time of login, along with the username and password, user have to enter his Personal Identification number called PIN into chose Grid pattern Called Personal Identification Grid Pattern for successful authentication. All the cells/grids are mouse controller i.e. to enter the digit into cell or grid user has to click on the same cell/grid. For Example, user want 6 number in (R1, C1) Cell/Grid then user click 6 times on (R1, C1) grid to enter 6 into that grid. On basis of number of clicks done by the user on grid cells, a Personal Identification Pin can be entered and from that values of grids are concatenated which acts as input for MD-5 Hash Algorithm. Then, this hashed grid value and hashed text password is encrypted with MD-5 hash Algorithm for obtaining Mash code.

Mash code=MD-5(Hashed text password+ Hashed grid value)

How PIGP is generated at Client Side?

We are using Grid Based approach. End user selects a set of "Likely to Be Chosen" grids/cells during Registration. In a chosen grids/cells, user can filled digits 1 to 9 by clicking on grids individually as discussed above (the number of times user clicked on cell/grid that is input of grid).So we can say there are 9^{16} possible combinations means 1853020188851841 possible combinations of only PIN which user enter into all grids. On the other hand, if user does not choose all cells or grids as his PIGP, he/she can choose different pattern of grids (horizontal/diagonals/vertical/any other) which is difficult to guess by the hackers. So this application is the combination of text password plus Pin password plus Pattern password which is totally knowledge based .No hardware needed for authentication.

How secure is our Generated value from Grid Approach?

We are using MD-5 Algorithm on the concatenated values/inputs of all cells or grids. As we know Hash algorithm is one way hash function, it is impossible to decrypt the hashed code. So this is the main feature of our proposed system. We also apply hash algorithm i.e. MD-5 on text password and then finally apply same algorithm on hashed text password plus hashed grid password and get Mash code which is sent to server for successful authentication. So we are using double hashing which is not easy to break by the hacker.

II. PASSWORD ATTACKS

Passwords play an important role in daily life in various computing applications like ATM machines, internet services, windows login, authentication in mobiles etc. The major aim for using passwords is to restrict unauthorized users to access the system. Passwords are necessary but, still they are not considered much safe to provide the security to the users because of many flaws in the conventional password systems. A large number of attacks on many systems are related to the passwords are as follows:

a) Brute force Attack: In this type of attack, all possible combinations of password apply to break the password [5]. The brute force attack is generally applied to crack the encrypted password where passwords are saved in the form of encrypted text. Early Linux systems use MD5 hashing schemes for storing the passwords. There is a password file in the operating system which contains the user's passwords with user names. If the Passwords file is stolen by the attacker then the password can be stolen. The original password is not in the file but it is encrypted in the form of MD5 Hash. The encrypted password seems to be safe but in fact it is also vulnerable to brute force attack. For this, the attacker first converts all combinations of passwords into their MD5 Hashes. In order to break the password the attacker first extracts the MD5 hash of suspected password from the password file placed in the system. The hash is then matched with all MD5 hashes one by one. When the hashes are matched, the corresponding password is selected [6].

Brute force attacks are very time consuming as searching a hash from all possibilities is a time taking process. For example a user enters a password of 8 characters and all characters are lower case letters then to break the password using the brute force attack it requires (26) combinations which is equal to 208827064576. If a single computer takes 1000 passwords to check in one second then total time will be 208827064576 / 1000 = 208827064.576 seconds which is equal to 58007.52 hours. This shows that brute force attack is effective for smaller passwords.

b) Dictionary Attack: This type of Attack is relatively faster than brute force attack [7]. Unlike checking all possibilities using brute force attack, the dictionary attack tries to match the password with most occurring words or words of daily life usage. Many users generally write passwords related to the names of birds, familiar places, famous actors names [8] etc. These passwords can be judged by the dictionary attack. The attacker makes the dictionary of most commonly used words that might have been be used as a password. The attacker then applies all these words to break the password. Although the dictionary attack is faster than brute force attack, it has some limitations too i.e. brute force attack contains limited words and sometimes it is unable to crack the password because it remains a possibility that password to be cracked may not be present in the dictionary itself.

c) Shoulder Surfing Attack: Shoulder Surfing is an alternative name of “spying” in which the attacker spies the user’s movements to get his/her password. In this type of attack, the attacker observes the user; how he enters the password i.e. what keys of keyboard the user has pressed.

Fig. 1: Shoulder Surfing

d) Video Recording Attack: In such type of attack the attackers with the help of camera equipped mobile phone or miniature camera, analyzes the recorded video of users which enters password. In it user’s password entry operations are recorded once or twice [5].

e) Phishing Attacks: It is a web based attack [3, 9] in which the attacker redirects the user to the fake website to get passwords/ Pin Codes of the user. To explain Phishing, suppose a user wants to open website say “www.yahoo.com”. The attacker redirects the user to another website e.g. “www.yah0o.com” whose interface is similar to that of the original website to disguise the user. The user then enters the login information which is retrieved by the attacker. The attacker then redirects the user to the original website and logins the user with the original website. Different phishing control filters are used nowadays but still they are not much reliable.

f) Key Loggers: The attacks through key loggers are similar to the login spoofing attacks discussed above [5,7, 10]. They are also called the Key Sniffers. The key loggers are the software programs which monitors the user activities by recording each and every key pressed by the user. The attacker installs the key logger software into the user system, either by installing that software himself or by tricking out the user to click to install that file into his (user) system. The key logger makes the log file of the keys pressed by the user and then sends that log file to the attacker’s e-mail address. The attacker then gets the password and can access to the target system.

III. AUTHENTICATION METHODS BASED ON PASSWORDS

a) Conventional Password Scheme: The Conventional Password Scheme is an old and most widely used password scheme. In this scheme the user enters or logs in into the system through his username and password. The system first authenticates the user from the user database and on the basis of authentication of the user and then grants the access to the system is granted.

The advantage of conventional password scheme is that it provides the security of data by allowing only authenticated users to access the system. However, such scheme is vulnerable to attacks like Shoulder Surfing, Key loggers, Phishing Attacks and Login Spoofing etc.

b) Keystroke Dynamics: The key stroke dynamics [11,12,13,14,15,16,17] (also called the typing dynamics) records the key press and key timings. It does not deal with "what" the user has entered the password; it deals with "how" the user has entered the password. The Key Stroke Dynamics stores the following time patterns of the user along with the conventional password:

- Time between the key pressed and release
- Time between the two keys pressed.
- The name of the key pressed
- Biometric password entering rhythm of individual users.

Advantages of key stroke dynamics include that no need of extra hardware, only good programming skills are required to implement such authentication system. It resists to password attacks like shoulder surfing, phishing, key loggers etc. Also the attacker cannot get into the system even if he/she gets the password. Disadvantages of Key Stroke Dynamics include that password rejection rate is high due to different levels of typing speed of users and User feels it as an extra overhead. It can be effective in different mental conditions of the user (i.e. happiness, sadness, hypertension etc.).

c) Click Patterns: Click Patterns is a type of mouse based password entering scheme described by [18 19]. In this type of password scheme, the user is provided with a click pad on the screen. The click pad can contain different color grids or it can be the combination of different symbols. The user can mislead the attacker by using the click pattern as a password. Along with the patterns, the click pattern scheme also tracks the user clicking rhythm.

Advantages of Click Patterns include that it does not require extra hardware and it is resistant to password attacks like shoulder surfing, phishing, key loggers etc. Also the attacker cannot get into the system even if he/she gets the password. The disadvantages include that the Password rejection rate is high due to different mental levels of users i.e. the system often cannot recognize the user. It gets affected by different mental conditions of user (i.e. happiness, sadness, hypertension etc.)

d) Graphical Passwords: Graphical passwords have many variations described by different authors [1, 2, 20, and 21]. In this scheme, the user first enters the user name to login. After that some graphical objects are displayed, which are necessary to be selected by the user. These selected objects are then drawn by the user using mouse, touch screen, stylus or touch pad etc. The system performs preprocessing on the user drawn objects and converts the sketches into hierarchical form. At last hierarchical matching is performed for user authentication. Advantages included reduced shoulder surfing and it is a more secure authentication. Disadvantages include that the system verifies the user only if proper sketch is drawn by the user and touch sensitive screens are required for sketching. Also it depends upon the ability of the user to draw sketches and its authentication processing time is much longer than other schemes.

e) Biometrics: Biometrics is also used as authentication procedure in which the recognition is based upon image processing. In this case to verify an image, it is first preprocessed to extract features from it and then the image based on these extracted features is matched with the database.

Advantages of such schemes include that it involves real and unique signatures and it cannot be stolen. The disadvantages includes that, it is costly and difficult to implement. It is still not mature and can be bypassed.

f) Authentication Panel: In these password schemes instead of pressing exact button for password, user is prompted to select the location of the password words from given panel [5, 22, and 23].

It provides resistance against brute force, dictionary, shouldering and video recording attacks. It does not required extra hardware and it is fast.

g) Reformation Based Authentication: In such scheme the password is shifted to new form before storing and whenever the password has to be read then it must be required to apply reform mapping to verify the user given password [24,25]. As it provide a layer above the original stored password. The reformation that is applied at the time of authentication of a user is dynamic in nature. Hence the hacker is unaware of the real password string even if the stored password is hacked. The main advantage of this scheme is as it resist strongly against dictionary attacks, shoulder surfing, video recording and brute force attacks.

h) Moving Balls Based Security Scheme: In this novel scheme the user click the mouse, then a user have number of balls moving in different columns and it all seen on screen, now the user just has to remember the number of columns and the respective balls [26].

i) Expression Based Security Scheme: This novel scheme provides two level securities as password on password. The user has to remember both the password and generated key by the system [26].

j) Virtual Password: This Novel password scheme offers secure user's password in on-line environments [27,28]. It can provide protection against different online attacks as phishing and password file compromise attacks.

Proposed Technique

This application having two parts:

1) Client Authentication Application

2) Grid Authentication Application

The Grid Authentication application is Web Application. This GrID-Pin application interacts with webserver through Grid Authentication Application which is going to deploy Glassfish server version 4. Other application is Client Authentication application through which end user are able to authenticate to protected resources which interacts with web application i.e. Grid authentication application. The technology used for Client Authentication Application is Swing Java application which is using Swing Servlet. This Protocol having two phases: Registration Phase and Login Phase. In Registration Phase, end user registers if he/she does not have account on that web application. End User registers his/her username in form of email-id (Gmail id or Yahoo id) & text password and chose Personal Identification Grid Pattern (PIGP) and enter desired pin in chosen PIGP by clicking on cells/grids individually. The number of clicked on individual cell is taken as its pin. In case if end user has already accounted on that web application the alert notification comes on screen. This username verification is done by function verify user. User can chose also one grid for its pin. There is not necessity to select number of grids for authentication. The key benefits of this grid approach is that it is less vulnerable to brute force attacks, Dictionary attack, Eavesdropping attack because this application is combination of grid pattern called PIGP and Pin password so there is no. of combinations possible of PIGP and in case if hacker is able to find out PIGP he is unable to predict what entry of pin that PIGP contain. So it advisable to user to select large PIGP pattern to confuse hacker. In this application, we use 4*4 matrix, we can 6*6/8*8 or any other to provide more security. At the backend user text password and grid value password is hashed with MD-5 hash algorithm and that hashed value is stored into server database for further operations.

In Login phase, end user enters his/her username, text password and pin into PIGP. At this time, at the backend, hash algorithm MD-5 is applied on both text password and grid value password and this both hashed value is combined and again MD-5 algorithm is applied on combined value and this value is sent to server. Web server generates hash value of combined hashed text and hashed grid value and result is compared with value coming for authentication if both values are same login will successful otherwise login failed.

In the meanwhile if user forgot his/her password text or grid, he/she has facility to reset his password either text or grid password. End user click on forgot password option and enter his/her username. Client authentication application verify username (exist or not) by verify user function. If user has already account on application, the verify code is sent to his/her mail id and from there user copy verify code and paste into verify code option, if verification code is correct then user can reset his/her password otherwise not. The more security has been given by applying double hash algorithm on text password and grid value password.

Features:

The application aimed towards the realization of a strong two factor authentication using Grid Pin to

- Provides with a cost effective and user friendly authentication.
- No hardware needed
- More Security
- No need to carry tokens like Smart card, ATM card.

- Not vulnerable to Brute Force Attack, Guessing Attack, Replay Attack.
- As one way hash function is used, inevitability is not possible means hash value to password value.
- Easy to use.
- No need of Server's calculations not like one time password technique.
- Less computation work on Client's system.
- Combination of password + pin
- No hardware needed to distribute.
- Ideal for protecting web based application.
- Avoids the use of a simple username and password system which is not secure anymore

IV. ALGORITHM

MD5 (Message-Digest algorithm 5) is a well-known cryptographic hash function with a 128-bit resulting hash value. MD5 is widely used in security-related applications, and is also frequently used to check the integrity of files. The MD5 value of file is considered to be a highly reliable fingerprint that can be used to verify the integrity of the file's contents. If as little as a single bit value in the file is modified, the MD5 value for the file will completely change. Forgery of a file in a way that causes MD5 to generate the same result as that for the original file is considered to be extremely difficult.

MD5 was developed by Rivest in 1991. It is basically MD4 with "safety-belts" and while it is slightly slower than MD4, it is more secure. The algorithm consists of four distinct rounds, which has a slightly different design from that of MD4. Message-digest size, as well as padding requirements, remains the same. Den Boer and Bosselaers have found pseudo-collisions for MD5. More recent work by Dobbertin has extended the techniques used so effectively in the analysis of MD4 to find collisions for the compression function of MD5. While stopping short of providing collisions for the hash function in its entirety this is clearly a significant step. For a comparison of these different techniques and their impact the reader is referred to.

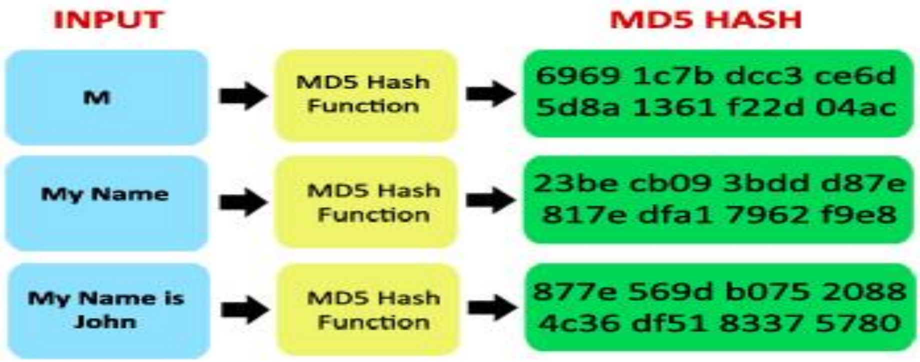
INPUT
MD5 HASH
M
MD5 Hash Function
6969 1c7b dcc3 ce6d 5d8a 1361 f22d 04ac
My Name
MD5 Hash Function
23be cb09 3bdd d87e 817e dfa1 7962 f9e8
My Name is John
MD5 Hash Function
877e 569d b075 2088 4c36 df51 8337 5780

Fig 2 Input to MD-5 Hash

Hashes compile a stream of data into a small digest (a summarized form: think "Reader's Digest"), and it's strictly a one way operation.

V. SYSTEM ANALYSIS

When the user wants to access the resources and do authentication, the existing system does not contain any additional password Security. She/he does not provide with additional technique rather than text password for authentication. This is not secure method for authentication because the passwords can be guessed or cracked. On the other hand one technique which is in trend is provide OTP (One Time Password) on mobile phones or cells but this application has also some disadvantages. First it is expensive and having more burden on server to generate One Time Passwords and send it to user‘s mobile phones. In the same way, if there is some network problem between server and user, there may be some delay in sending and receiving one time password on phones. In the case if user does not have mobile phone (it may be stolen or switched off) user cannot access applications and failing in authentication. The Advantage of this proposed application is that there is no hardware needed for authentication and no burden on server of generating passwords. This approach is totally based on knowledge memorability and we know very well hardware can be stolen but knowledge cannot. So this two factor Authentication scheme is totally based on what you know scheme only need end user‘s password as one factor and grid Pin as second factor for authentication. By this way, the applications themselves can obtain higher security guarantee than those use static password technology only. Using static passwords for authentication, as it is commonly done, has quite a few security drawbacks: passwords can be guessed, forgotten, written down and stolen, eavesdropped or deliberately being told to other people. A better, more secure way of authentication is the so called "two-factor" or "strong authentication" based on static password as well as Grid pin. Grid Pin provides a flexible method that allow user to enter his pin password in grids according to its pattern. It allows end users to secure data from hackers by using grid pin without requirement of hardware tokens. It works by presenting the end user with 4*4 matrixes of cells or grids. In the Registration phase, user selects a Personal Identification Grid Pattern (PIGP) and enters their pin into that by clicking on grid individually. Thereafter, when end user wishes to authenticate, the user have to enter static password and pin in Personal Identification Grid. No hardware to lose and far superior to static password. This Protocol is ideal for protecting web based application like bank applications websites. It can be used in enterprises for security of organization secret data. In this scheme user not need to remember difficult passwords for security purpose they can use easy password because this protocol has other security factor grid pin factor. The main objective of this protocol is to free the user for carrying multiple smarts cards with him or free user to remember multiple difficult passwords to secure its data from hackers. All the records of user are stored in database at backend in hash code. To provide more security hash algorithm (one way hash algorithm MD-5) is applied on static password as well on grid password. More security are provided by combining of hash value of static password and hash value of grid password and hash algorithm is applied on that combined value. In case user forget his/her password either static password or grid password, there is a facility to recover the passwords. When user is unable to enter his/her password, he/she simply click on forgot password option display on application and enter his/her username, he/she is provided with code from his/her email id and with that code user can reset his password either static or grid password. To avoid the usage of additional devices, the Grid Pin is used to provide strong authentication.

VI. RESULTS

The experimental design has been developed using SWING JAVA as front end and Glassfish as a server and the results have been observed and analyzed. We are successful in building secure totally knowledge based application which is flexible and unique authentication method which is totally based on knowledge (memory). There is no need to carry any smartcards, mobile phones and any other tokens for authentication. It is also less expensive and easy to use. On the other side the application is less vulnerable to brute force attacks, Dictionary attacks, eavesdropping attack, Shoulder Surfing attack. Basically this proposed technology is the combination of Password plus Pattern plus PIN (Personal Identification Number). Our first step was analysis where we studied the traditional authentication systems and how passwords are compromised in such systems and what can be done to negate the comprising factors. This was followed with the study of the limitations of the one factor authentication systems. Once the above were completed, the focus was shifted to the implementation of the two factor authentication method. The algorithm selected is MD-5 Algorithm. This was followed by an application development and testing our implementation of the two factor authentication system with such an application. In testing phase we analyzed registered user is able to login into his/her account by use of static password plus grid password and at the backend securely hash code of passwords and grid value has been generated. During the testing of the implementation, it is found that the system is working fine and that our implementation of the two way authentication system is working and has better security compared to the conventional one way authentication system. The authentication method which has been used is in order to authenticate, the user is asked to input his/her text password and PIN into preregistered pattern on a grid (that the user knows) and a grid value is generated by concatenating all the values of cells/grids and this generated grid value is put into MD-5 algorithm as a input and 32 bit hash code is generated into the database. To provide more security, Mash code is generated by applying hash algorithm on hashed password plus hashed grid value and this hashed mash code is sent to server. At the server side, server do same calculations by taking text password and grid value from his database. If mash code which received is same as mash code generated by server the user will authenticate otherwise login failed

VII. CONCLUSION

Today, single factor authentication, e.g. passwords, is no longer considered secure in the internet and banking world easy-to-guess passwords, such as names and age, are easily discovered by automated password-collecting programs. Two factor authentications recently have been introduced to meet the demand of organizations for providing stronger authentication options to its users. In most cases, a hardware token is given to each user for each account. The increasing number of carried tokens and the cost the manufacturing and maintaining them is becoming a burden on both the client and organization. Since many people use pattern based approach as his/her passwords for mobile phones. So it is easy to remember grid pattern as compared to long text or carrying multiple smart cards. This will help reduce the manufacturing costs and the number of devices carried by the client.

This paper focuses on the implementation of two-factor authentication methods using Grid Based approach. Though this proposed system has some limitations like vulnerable to Man in the Middle attack, phishing attack but it can be cured by applying safe network between client and server or we can use 3 way handshake techniques to protect from Man in the Middle Attacks or Phishing Attacks. So in the conclusion we can say organizations can adopt this method for his personal data security.

REFERENCES

[1] Anand Sharma and Vibha Ojha 2010,”Password based authentication”, Philosophical Survey, IEEE.

[2] C. Martin-Diaz, J. Galbally, J. Fierrez, "A Comparative Evaluation of Finger-Drawn Graphical Password Verification Methods", ICFHR, 2010, Frontiers in Handwriting Recognition, International Conference on, Frontiers in Handwriting Recognition, International Conference on 2010, pp. 375-380, doi:10.1109/ ICFHR .2010.65.

[3] Ilkka Uusitalo and Josep M. Catot, 2009. “Phishing and countermeasures in Spanish online Banking”,3rd International conference on emerging security information, System and Technologies.

[4] Ali, M. Eljetlawi and Norafia Ithnin, 2008. Graphical password: Comprehensive study of the use ability features of the recognition base graphical password methods. 3rd International conference on convergence and Hybrid Information Technology.

[5] Fujita, K. and Y. Hirakawa, 2008. A study of password authentication method against observing attacks. 6th International Symposium on Intelligent Systems and Informatics, SISY 2008.

[6] Muhammad Sharif and Aman Ullah Khan, 2007. Benchmarking of PVM and LAM/MPI Using OSCAR, Rocks and Knoppix Clustering Tools in ICCISSE 2007, XXI. International Conference on Computer, Information and Systems Science and Engineering May 25-27, 2007 Vienna, Austria.

[7] Arvind Narayanan and Vitaly Shmatikov, 0000. Fast dictionary attacks on passwords using time-space tradeoff, Conference on Computer and Communications Security, Proceedings of the 12th ACM Conference on Computer and Communications Security, pp.: 364-372.

[8] Kessler, Gary C., 2002. Passwords - Strengths and Weaknesses. Jan 1996.

[9] Fahad Ikram, Muhammad Sharif and Mudassar Raza, 2008.Protecting Users against Phishing Attacks in 7th CIIT Workshop on Research in Computing June 23, 2008 CIIT, Lahore - Pakistan.

[10] Baig, M.M. and W. Mahmood, 2007. A Robust Technique of Anti Key-Logging using Key-Logging Mechanism, Digital Ecosystems and Technologies Conference, 2007. DEST '07. Inaugural IEEE-IES, Feb 2007, (s): 314-318.

[11] Haider, S., A. Abbas and A.K. Zaidi, 2000. A Multi Technique Approach for User Identification through Keystroke Dynamics, 2000 IEEE International Conference on Systems, Man and Cybernetics, 2(s): 1336-1341.

[12] Nick Bartlow and Bojan Cukic, 2006. Evaluating the Reliability of Credential Hardening through Keystroke Dynamics,17International Symposium on Software Reliability Engineering, 2006. ISSRE apos06 Nov.(s): 117-126.

[13] Jarmo Ilonen1, 2003. Keystroke Dynamics, Advanced Topics in Information Processing 1 - Lectures, Wed Dec 10, 2003.

[14] Enzhe Yu Sungzoon Cho, 2003. GA-SVM wrapper approach for feature subset selection in keystroke dynamics identity verification, Proceedings of the International Joint Conference on Neural Networks, 2003. 3(s): 2253-2257 Vol. 3 ISSN: 1098-7576.

[15] Tai-Hoon Cho, 2006. Pattern Classification Methods for Keystroke Analysis, SICE-ICASE, 2006. International Joint Conference Oct. 2006, (s): 3812-3815.

[16] Attila Mészáros, Zoltán Bankó and László Czúni, 2007. Strengthening Passwords by Keystroke Dynamics, IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 6-8 September 2007, Dortmund, Germany.

[17] Dalia Abdul Hadi Abdul Ameer and Ahmed Abdulhakim Al-Absi, 2010. Anywhere On-Keyboard Password Technique. IEEE Student conference on Research and development 2010 Putrajaya Malaysia.

[18] Muhammad Sharif, Tariq Faiz and Mudassar Raza, 2008. Time Signatures - An Implementation of Keystroke and Click Patterns for Practical and Secure Authentication, The third International Conference on Digital Information Management (IEEE ICDIM 2008), 13-16 November, 2008, University of east London, London UK.

[19] Abdurazzag Ali Abura and Manal I. Al Fallah, 2008. Password generator based on mouse clicks signal and screen cursor position. IEEE Proceedings of the International Conference on Computer and Communication Engineering.

[20] Qurat-Ul-Ain Arshad, Muhammad Sharif, Mudassar Raza and Aman Ullah Khan, 2007. Secured and Handy Graphical Password System, National Conference of Information and Communication Technologies (NCICT-2007), June 09, 2007, at Main Campus University of Science and Technology, Bannu, NWFP, Pakistan.

[21] Mohd Ali Bin Mohd Isa and Mohd Nor Hajar Hasrol, 2008. User perception towards the use of colour as Authentication method: focus on FTMSK lecturer. Proceeding of the International Conference on Computer and Communication Engineering Malaysia.

[22] Manabo Hirano and Tomohiro Umeda, 2009. T-PIM: Trusted password Input method against data stealing Malware IEEE 6 International Conference on IT.

[23] Hirotaka Tazawa and Takashi Katoh, 2010. A user authentication scheme using Multiple Passphrases and its arrangements. ISITA Taiwan.

[24] Safdar, S., M.F. Hassan, M.A. Qureshi, R. Akbar and R. Aamir, 2010. Authentication model based on reformation mapping method " International Conference on Information and Emerging Technologies (ICIET).

[25] Shakir, M. and Abdul Ayaz Khan, 2010. S3TFPAS: Scalable shoulder surfing resistant Textual-Formula base Password Authentication system. IEEE.

[26] Shahid, M. and M.A. Qadeer, 2009. Novel scheme for securing passwords". IEEE 3rd International Conference on Digital Ecosystems and Technologies, DEST '09.

[27] Mohammadi, S. and S.Z. Hosseini, 0000. Virtual password using Runge-kutta method for internet banking. IEEE 2 International Conference on Communication Software and Networks.

[28] Qiang Wang and Zhiguang Qin, 2010. Stronger User authentication for web browser. 3rd International conference on advance computer theory and engineering (ICACTE) China.