International Journal of Computer Science Engineering & Technology
IJCSET
Approved by
National Science Library (NSL)
National Institute of Science Communication and Information Resources (NISCAIR)
Council of Scientific and Industrial Research (CSIR)– New Delhi India .
ISSN :2455-9091

SECURE DATA SHARING USING SESSION PASSWORD IN CLOUD

[1] Bijubalakrishnan M.E., (Ph.D)., [2] K. Christian Joel, [3] G. Neena, [4] M. Palani Kumar, [5] J. Soniya,
[1] Associate Professor (SG), [2, 3, 4, 5] B.E.,
[1, 2, 3, 4, 5] Nehru Institute of Technology, Coimbatore.

ABSTRACT: When we consider the online service or desktop application there is major issue of security breaching. Old password schemes has some drawbacks like hacking of password, shoulder-surfing attack as far as password is concern, online password guessing attack, relay attack. Hence there must be system that provides good solution for such password cracking attacks. There are many solutions for it and various password schemes available that achieves this. The main drawback of these schemes is users have to deal with complicated and tedious steps as far as registration and login of user is concern as its logic contains some intense AI processes. In our proposed scheme introduced a session password is a password uniquely generated for every session. The scheme allows the system to automatically generate a session password each time the user logs in. The session password is generated randomly based on the randomly generated grid. The grid is used as a medium for password generation. Now the system stores this password and uses it to generate a unique session password while user logs in the next time. This session based authentication system uses the user password and compares alphabets contained alongside a 6*6 grid with letters a-z and numbers 0-9. The user needs to know the original password and the generation scheme to enter the exact password. Further graphical passwords are coming to the existence but the graphical passwords have their own disadvantages like they require more time to Authenticate and the usability issues. Thus we proposed a session password scheme in which the passwords are used only once for each and when session is terminated the password is no longer in use. It provides all benefits of session and makes system more powerful from security point of view.

Keywords: [Cloud Computing, session based authentication system, grid based password generation.]

1. INTRODUCTION

With the rapid development of low-power and highly efficient networks, mobile users can pay bills, buy goods online, and carry out electronic transactions by subscribing to various remote services. Though mobile computing devices are highly portable, they are usually unprotected and easy to be stolen or get lost. Unless precautions are taken, an unauthorized person may gain access to the information stored on them. For instance, illegal access may be acquired by intruders if the data is "sniffed out of the air" in wireless communications or some malware is installed. The lack of Authentication and privacy may cause even

more severe results like crippled devices, personal data loss, disclosure of non-public data, or charge of abused usage against the device owner. Mobile computing devices are of great security concern not only because of the data stored on them, but also for that they may provide access to other services that store or display non-public data. For almost all these transactions, mutual authentication and user privacy are required in the key exchange before remote servers start providing services to users. The most common method used for authentication is textual password. The vulnerabilities of this method like eves dropping, dictionary attack, social engineering and shoulder surfing are well known. Random and lengthy passwords can make the system secure. But the main problem is the difficulty of remembering those passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can be easily guessed or cracked. The alternative techniques are graphical passwords and biometrics. But these two techniques have their own disadvantages. Biometrics, such as finger prints, iris scan or facial recognition have been introduced but not yet widely adopted. The major drawback of this approach is that such systems can be expensive and the identification process can be slow. There are many graphical password schemes that are proposed in the last decade. But most of them suffer from shoulder surfing which is becoming quite a big problem. There are graphical passwords schemes that have been proposed which are resistant to shoulder-surfing but they have their own drawbacks like usability issues or taking more time for user to login or having tolerance levels. Personal Digital Assistants are being used by the people to store their personal and confidential information like passwords and PIN numbers. Authentication should be provided for the usage of these devices.

This proposes to enable and support a diversity of multiple authentication schemes in practice. This endeavour is advanced through the following contributions to the field of usable security and authentication: A user-centred authentication feature framework for identifying and comparing the features supported by knowledge-based authentication schemes. This framework can used by authentication scheme researchers when designing or comparing authentication schemes, as well as administrators and users, who can use the framework to identify desirable features in schemes available for selection.

2. RELATED WORKS

Despite the large number of options for authentication, text passwords remain the most common choice for several reasons. Text passwords are easy and inexpensive to implement, and are familiar to most users. Passwords allow users to authenticate themselves without violating their privacy, as biometrics could, since users can select passwords that do not contain personal information. And finally, passwords are portable since users simply have to recall them, as opposed to tokens which must be carried. However, text passwords also have a number of the inadequacies from both security and usability viewpoints, such as being difficult to remember and being predictable if user-choice is allowed. Passwords are only secure if they are difficult for attackers to guess, yet are only usable if users can remember them.

Authentication Session Password Scheme Using Texts And Color [1] Most of the graphical schemes are vulnerable to shoulder surfing. To consider this problem, text can be combined with colors to generate session passwords for security purpose. Session passwords can be used only once and every time a new password is generated. To generate session passwords using text and colors which are protect data from dictionary attack, shouldering etc. Session Passwords Using Grids And Colors For Web Applications And PDA [2] Random and lengthy passwords can make the system

secure. But the main problem is the difficulty of remembering those passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. This approach is that such systems can be expensive and the identification process can be slow. D´Ej`A Vu: A User Study Using Images For Authentication [3]
Our findings indicate that D´ej`a Vu has potential applications, especially where text input is hard (e.g., PDAs or ATMs), or in situations where passwords are infrequently used (e.g., web site passwords). One approach to improve user authentication systems is to replace the precise recall of a password or PIN with the recognition of a previously seen image, a skill at which humans are remarkably proficient. Secure Authentication Using Dynamic Virtual Keyboard Layout [4] we have designed a virtual keyboard that is generated dynamically each time the user access the web site. Also after each click event of the user the arrangement of the keys of the virtual keyboard are shuffled. The position of the keys is hidden so that a user standing behind may not be able to see the pressed key. Our proposed approach makes the usage of virtual keyboard even more secure for users and makes it tougher for malware programs to capture authentication details. Spy-Resistant Keyboard: More Secure Password Entry On Public Touch Screen Displays [5] This can be difficult on touch screens that are placed in locations that make blocking it inconvenient or that are larger than the user can physically block with their body. Users may also adopt other strategies, such as quickly adding and deleting characters that are not in the intended password in order to confuse observers.
The Design and Analysis of Graphical Passwords [6] An approach to user authentication that generalizes the notion of a textual password and that, in many cases, improves the security of user authentication over that provided by textual passwords. We design and analyze graphical passwords, which can be input by the user to any device with a graphical input interface. User Authentication Using Graphical Password Scheme: A More Secure Approach Using Mobile Interface [7] User will click on different points on same image or different image. Click based Graphical password scheme provides protection offers protection against online dictionary attacks and relay on passwords, which have been for long time a major security threat for various online services.

3. PROPOSED SYSTEM

In this project, session based authentication scheme is proposed. This scheme authenticates the user by session passwords by using pair based scheme. Session passwords are passwords that are used for only one transaction. Once the session is terminated, the session password is not useful. For every login process, users have to enter different passwords. The session passwords provide better security against shoulder surfing attack as password changes according to each transaction. the main objective is to avoid shoulder surfing attack using pair based scheme which will generate session password for the particular session or transaction where there will be virtual keyboard which will shuffle at every another transaction accordingly. At the time of registration user have to submit password. Particularly the length of the password is 8 and it can be named as secret key. The secret key consists of even or odd number of characters. Then next stage is the login phase, when the user enters his username as an interface, the 6 x 6 grid display of row and column size screened before user. The grid display consists of alphabets and numbers. These are sequentially placed on the grid at every cell and this interface changes every time according to every transaction.

- We proposed a system called Session password ,in this it provides a new password for each session.
- Need not to transfer password form server each time for authentication purpose

that's why Session password scheme provides more security than the other existed systems.

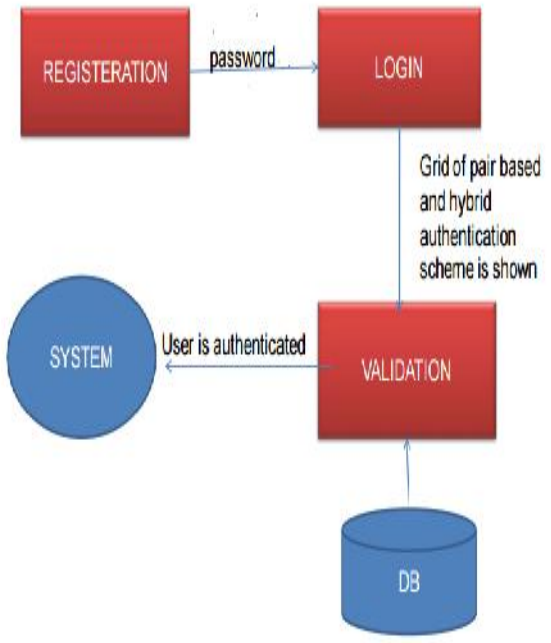


Figure - 1 Architecture Diagram

3.1 Session Grid algorithm

The session password is generated randomly based on the randomly generated grid. The grid is used as a medium for password generation. While registration the user must normally enter his username and password while registering into the system. Now the system stores this password and uses it to generate a unique session password while user logs in the next time. This session based authentication system uses the user password and compares alphabets contained alongside a 6*6 grid with letters a-z and numbers 0-9. The user needs to know the original password and the generation scheme to enter the exact password.

3.2 File upload and Encryption

Each file which is to be uploaded is encrypted with encryption key. Once file is encrypted, next step is to upload it to the storage system along with data decryption key. Owner specifies the set of attributes for access structure, it then encrypts the file. Finally, owner uploads encrypted file and encryption key and set of attributes to the storage system.

3.3 Session based data sharing

The users can view the files which are uploaded by them, then the users can share the files to the receiver by giving the time limit to accessing the data. Based on the time limit, the session key is generated for that file access. The key is only valid for that user given time, after the time limit the receiver have no access for that file.

3.4 File Decryption and Download

User requests the file by providing details and in response system replies with encrypted file. Before that the system will check the role and signature of the users whether the receiver have the same role as the sender mentioned. It will avoid the unauthorized users or hackers. The receiver receives the encrypted file, and he has correct role and signature, if it's correct, the original file gets decrypted for the receiver. This allows them to access information without authorization and thus poses a risk to information privacy.

4. METHODOLOGY

Grid Matrix (Hash Function)

The main function of salt is to protect against dictionary attacks and rainbow table attacks. A salt is randomly generated string for each password. The generated salt and User's password are concatenated and processed with the Cryptographic hash function and result is stored with salt in a Database. Hashing allows for late authentication. while defending against compromise of the plaintext.

Steps for generating Hash password:

1. Get password.
2. Generate random function.
3. Append original password.
4. Generate Hash password using appropriate hash function.
5. Finally store Hash in the Database.

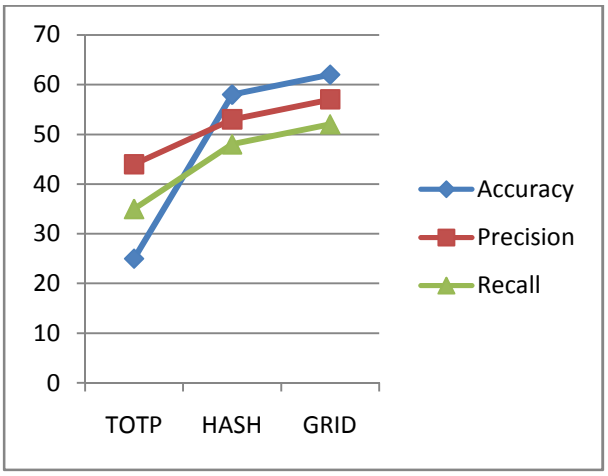
According to above steps Hash Password is generated. First original password is taken from the user and using Random function Salt is gets generated. After this

generated Salt is appended to the original user's password. Then this Salt appended password is passes to Hash function. This Hash function is used to generate Salt Hash Password. Finally this generated Salt Hash Password and Salt is stored in database. In this iteration count is used which is refers to the number of time that the hash function with which we are digesting is applied to its own this means that, once we generate a salt and concatenated with the password then apply the hash function, get the result and again pass that result as a input to the same hash function .This process is repeated again and again a number of times. The minimum number of iteration is 1000 for more security.

5. EXPERIMENTAL RESULT

There are six main security features that are used on existing graphical password schemes. The possible attack method is not classified as the security feature, it is only for the guidance and supporting reason of why the security features is needed. The possible attack method is divided into six types of attacks which are brute force, dictionary, guessing, spyware, shoulder-surfing and social engineering. These are the current active attack methods in graphical authentication environment. It can be concluded that all of the existing schemes are vulnerable to brute force, guessing and shoulder-surfing attack. As we can see, the Draw-A-Secret (DAS) scheme is the only scheme that is capable of defending against brute force attack. This is because DAS provides the largest password space compared to other schemes. The Pict-OLock scheme has a strong resistance to guessing. This scheme used the image variation where a same imageis displayed in different colors. Overall, the existing schemes have strong security mechanisms to counter dictionary, spyware and social engineering attacks.

In order to protect against brute force and guessing, the scheme needs to provide a large password space. The larger the password space, the harder for brute force and guessing to succeed. To increase the security of graphical authentication, seven schemes used randomly assigned image and decoy images features. The purpose of using these features is mainly to defend against shoulder surfing attacks. As we can see, almost all of the schemes using these features are less susceptible to shoulder-surfing attacks. A total of four schemes used the hash visualization function. In order to strengthen the security of the selected password, some of these schemes combined hash and salt functions. Among all of these recognition and recall based security features, we will select the large password space, hash function and decoy images features to protect against the possible attack methods in graphical authentication environment.



The repeat verifications, randomly assign images and image variation will not be used in the development of our scheme. As we can see, by repeating the process of verification it will make the authentication process slower which will affect scheme usability. We conducted the user study of the proposed techniques with 10 participants for each technique. As the techniques are new, first the participants were briefed about the techniques. They were given demonstrations for better understanding purpose. Then each user was requested to login. After that, the usability study was conducted with the students in two sessions. The sessions were conducted in time frame of one week.

CONCLUSION

In this paper, we proposed Session based GRID Matrix scheme which preserves security against various attacks including de-synchronization attack, lost-smart-card attack and password guessing attack, and supports several desirable properties including perfect forward secrecy, anonymity or untraceability, adaptively password change, no centralized password storage, and no long-term public key. Furthermore, our protocol maintain high efficiency in terms of storage requirement, communication cost as well as computational complexity. Our protocol requires only a few number of message flows and all the transmitted messages are short in size. Additional, the proposed scheme is provably secure in our extended security model. Therefore, the proposed scheme is suitable for deployment in various low-power networks, in particular, the pervasive and mobile computing networks.

REFERENCE

[1] A. Valenzano, L. Durante, and M. Cheminod, "Review of security issues in industrial networks," IEEE Trans. Ind. Inf., vol.9, no. 1, pp. 277-293, 2013.

[2] V. C. Gungor, and G. P. Hancke, "Industrial wireless sensor networks: challenges, design principles and technical approaches," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4258-4265, Oct. 2009.

[3] D. Liu, M. C. Lee, and D. Wu, "A Node-to-Node Location Verification Method," IEEE Trans. Ind. Electron., vol. 57, no. 5, pp. 1526 - 1537, May 2010.

[4] C. Chang and C. Lee, "A secure single sign-on mechanism for distributed computer networks," IEEE Trans. Ind. Electron., vol. 59, no. 1, pp. 629-637, Jan. 2012.

[5] G. Wang, J. Yu, and Q. Xie, "Security analysis of a single sign-On Mechanism for Distributed Computer Networks," IEEE Trans. Ind. Inf., vol. 9, no. 1, pp. 294-302, 2013.

[6] L. Barolli and F. Xhafa, "JXTA-OVERLAY: A P2P platform for distributed, collaborative and ubiquitous computing," IEEE Trans. Ind. Electron., vol. 58, no. 6, pp. 2163-2172, Oct. 2010.

[7] Y. Huang, W. Lin, and H. Li, "Efficient Implementation of RFID Mutual Authentication Protocol," IEEE Trans. Ind. Electron., vol. 59, no. 12, pp. 4784 - 4791, 2012.

[8] B.Wang and M. Ma, "A server independent authentication scheme for RFID systems," IEEE Trans. Ind. Inf., vol. 8, no. 3, pp. 689-696, Aug. 2012.

[9] B. Fabian, T. Ermakova, and C. Muller, "SHARDIS: A privacyenhanced discovery service for RFID-based product information," IEEE Trans. Ind. Inf., vol. 8, no. 3, pp. 707-718, Aug. 2012.

[10] M. Hwang, and L. Li, "A new remote user authentication scheme using smart cards," IEEE Trans. Consum. Electron., 2000, 46(1): 28-30.