# SESSION BASED DATA SHARING WITH SESSION BASED PASSWORD

Jaffar Jasmine Begum[1] | R Sujitha[2]
[1](UG Student, Christ the King Engineering College, jasmine120597@gmail.com)
[2](Assistant Professor, Christ the King Engineering College, srisuji14@gmail.com)

***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 make system more powerful from security point of view.*

***Keywords— Security; Password Authentication; Anonymity; Smart Card***

## 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.

## 2. RELATED WORKS

### *2.1 Text Passwords*

Text passwords are the ubiquitous method of authentication in most modern computing environments. Unix systems initially implemented a simple text password system whereby account passwords were stored verbatim in a file. Although the file was protected from casual reading and writing, a privileged and knowledgeable user could gain access to the file, thereby instantly compromising all users' passwords. Wilkes proposed securing each new password with encryption before storing them during account creation. At login, such a system would encrypt the entered password, compare the result to the stored encrypted password for that user, and grant

access if they matched. Although encryption added a layer of security, if the encryption key were compromised or broken, all passwords would also be compromised. 13 To remedy this vulnerability, Evans and Kantrowitz proposed passing the entered password through a one-way hashing function, instead of using encryption. Such a hash function must have the following basic properties:

1. It must be computationally infeasible to reverse.
2. For two identical inputs, their outputs must also be identical.
3. It must be computationally infeasible to find two distinct inputs that result in the same output. An attacker who compromises a file of hashed passwords will be unable to obtain the plaintext passwords without performing a password guessing attack, whereby the attacker chooses and hashes a candidate password, and compares the result to each of the hashes contained in the

password file. Any hashes that match imply that the candidate password is the actual password for the corresponding account.

2.2 Graphical Passwords

Graphical password systems represent passwords in some form of visual format (as opposed to the lexical format of text passwords). Over the past decade, usable authentication researchers have taken great interest in graphical passwords, since humans have a better memory for visual stimuli than text Biddle et al. have recently published the most complete survey of graphical password research to date. They found that the usability and security of graphical passwords are generally inversely proportional, and advise that the next generation of graphical passwords (and usable security research in general) should aim to find solutions that increase usability and security simultaneously. They classify graphical passwords into three types. Recall-based systems require users to draw a password, either on a blank canvas or grid. An example of a recallbased system is Draw-A- Secret where the user draws on top of a grid, and the password is represented as the sequential movements from one grid square to another. Further studies have shown that users choose predictable patterns

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.

Systems sometimes provide on-screen advice on how to create more secure passwords (e.g., select something memorable that would be difficult for others to guess), give feedback about password choice (e.g., with a password strength meter), or force users to create passwords that comply with specific system- defined rules (e.g., the password must include both letters and numbers). Despite these strategies, users often select weak passwords that are predictable and are easy for attackers to guess. This occurs partially because users misunderstand the advice or requirements, underestimate the risks, and because limitations of human memory mean that they must employ coping mechanisms in order to reduce the burden of remembering so many passwords. These coping mechanisms may include reusing passwords across several accounts, using predictable alphanumeric combinations, or storing passwords in an easily accessible, insecure location. Although they have appealing characteristics, only limited success has been achieved through encouraging the use of passphrases (passwords are longer phrases) or mnemonic passwords (passwords are abbreviated from a longer word or phrase, for example by using the first letters of the words in a phrase, or including common character substitutions. At least in their basic form, both suffer from predictability problems because users choose common character substitutions or well known phrases. Such approaches also do not mitigate the problem of remembering which password corresponds to which account when users have multiple accounts. Furthermore, phishing and other social engineering attacks on

passwords have increased dramatically over the past few years since text passwords are easy for users to unintentionally reveal to attackers, complicating matters further.

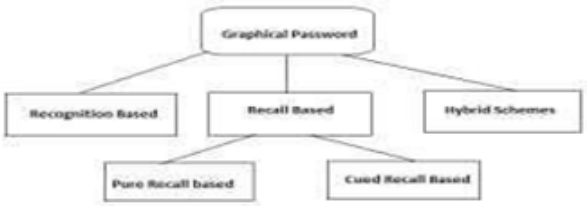
2.3 TF-AKE Scheme

we propose a new TF-AKE scheme to overcome the weaknesses of the previous schemes. Our ideas can be summarized as follows: (a) encrypt user ID for user anonymity as in Sun et al.'s scheme, and adopt a similar mechanism to Li et al.'s scheme for ensuring user untraceability, meanwhile introduce an additional mecha-nism for de-synchronization; (b) encrypt all data stored in smart card SC under either the server S's long-term secret number or user's password, and ensure that an adversary is unable to get the server's long-term secret number or user password through lost-smart-card attack; (c) introduce nonces in the messages flows for preventing the leakage of any information which facilitates an adversary to launch offline dictionary attack; and (d) use conventional method to defend against online dictionary attacks, namely, when a preset maximum number of consecutive failed attempts is reached, further run of the Login and Authentication process between SC and S will be prohibited.

2.4 Graphical password methods

Some existing graphical password methods are as follows. Graphical based password techniques have been proposed to solve limitations of conventional text based password techniques, because pictures are easier to remember than texts. Graphical password techniques show that techniques can be categorized into four groups as follows.

A. Recognition-Based Technique: In this category, users select images, icons or symbols from a collection of images. At the time of authentication, the users need to recognize their images, symbols, icons which are selected at the time of registration among a set of images.




B. Recall-Based Technique: This category is very easy and convenient, but it seems that users can hardly remember their passwords. Still it is more secure than the recognition based technique.

C. Cued Recall-Based Technique: In this category, users are provided with reminders or hints. Reminders help the users to reproduce their passwords or help users to reproduce the password more accurately. This is similar to recall based schemes but it is recall with cueing.

D. Hybrid Schemes: In this category, the authentication will be typically the combination of two or more schemes. These schemes are used to overcome drawbacks of single scheme, such as spyware, shoulder surfing.

2.5 Color keyboard implementation

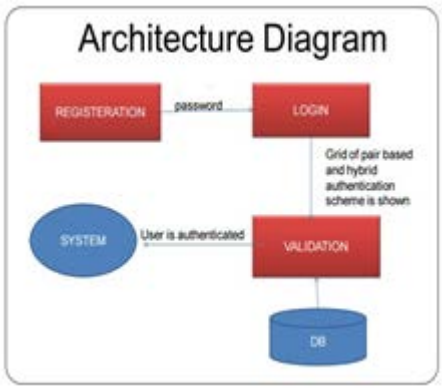
The principle behind the keyboard design is simple – but that doesn't mean its simple to use (unfortunately). Note that in some browsers it may be necessary to click on the keyboard with your mouse before doing any typing.

Typing is performed using four buttons; in this demonstration, the directional arrows on your computer keyboard are used. A fifth button, called the mode button is used to switch between keyboards (this provides access to a wider range of characters). In this demo, the space bar is used for this purpose.

Each arrow is associated with a colour. To enter a letter that appears on the keyboard, you are required to press the arrow buttons in the colour sequence indicated on the key. The sequence of colors is read left-to-right/top-to-bottom. If a letter appears 'ghosted' it means that that letter sequence is incompatible with the buttons you have pressed so-far (you can cancel an incomplete sequence of button presses - see below). If all the letters are ghosted, it means that the keyboard has lost focus, click on the keyboard with your mouse to restore control.

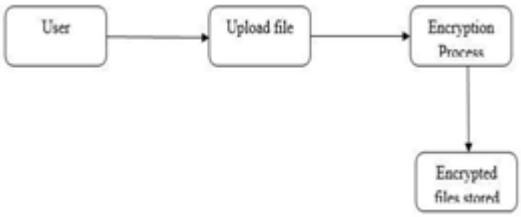
## 3. SESSION GRID ALGORITHM

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.


## 4. 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 systems.

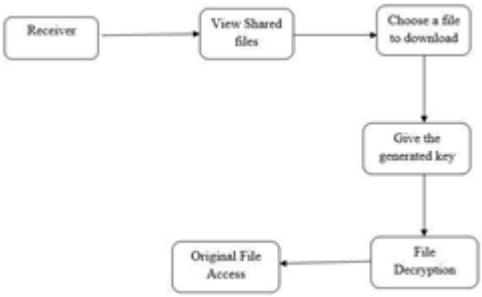



## 5.SESSION BASED DATA SHARING

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.

## 6. 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.




## 7.CONCLUSION

There are many techniques which are proposed for preventing shoulder surfing attack,with all proposed techniques thesession based password scheme using shuffling keyboard with Pair Based method is more effective and secure toshoulder surfing attack, as this technique is providing a particular session password for every session or transaction Also, it is easy to use and handle, hence in near future , this technique has scope to use in many fields for the security purpose. In this paper, we proposed an Anonymous Two-FactorAKE scheme which preserves security against various attacksincluding de- synchronization attack, lost-smart-cardattack and password guessing attack, and supports severaldesirable properties including perfect forward secrecy,anonymity or untraceability, adaptively password change,no centralized password storage, and no long-term publickey. Furthermore, our protocol maintain high efficiency interms of storage requirement, communication cost as well as computational complexity. Our protocol requires onlya few number of message flows and all the transmittedmessages are short in size. Additional, the proposed schemeis provably secure in our extended security model of AKE.Therefore, the proposed scheme is suitable for deploymentin various low-power networks, in particular, the pervasiveand mobile computing networks.

## REFERENCES

[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.