|| Volume 3 || Issue 10 || October 2018 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

Authentication Scheme for Session Password Using Pair Based Algorithm

Khan Sana Zarrin[1],Prof. Vijay S. Karwande
PG Student, Computer Science Department, College Engineering & Technology Aurangabad (MS)[1]
Assistant Professor, Computer Science Everest College Engineering & Technology Aurangabad (MS)[2]

Abstract— **At the start of any application the authentication process is run before the permission checks occurs and before any code is allowed to proceed. Different system may require different types of credentials to ascertain a user's identity. The credential is in the form of password which is secret and known only to the user and the system. Textual password are the most common method used for authentication .But hacker are trying to know the password through different techniques for access the information .the password may stole through shoulder surfing, Eves dropping, dictionary attacks, social engineering . And other alternative technique of textual password is graphical password but it has its own disadvantages. In this paper, To overcome these problem we are introducing a new authentication technique for creating a session password for a particular session using pair based algorithm. we are implementing pair based algorithm in android developing the android application for generating session password for particular session. Which provide high security for accessing the application.**

Keywords: *Authentication, Textual, Graphical password, session password,*

I INTRODUCTION

Textual passwords are commonly used in day to day life of people. Generally user wish to choose easy memorable password it means that the passwords tend to follow patterns if lengthy password is create it is difficult to remember and this password can be cracked by guessing attack . Another alternative technique of textual password is graphical password but this technique has its own disadvantages it can be expensive for user and attacker may hack these password by shoulder surfing, eves dropping, dictionary attacks. In this paper we are introducing a new technique for authentication this is called authentication scheme for session password using pair based algorithm. This authentication scheme is highly secure.

II LITERATURE SURVEY

2.1 Existing system:

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. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. 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.

2.2 Disadvantages of Existing System:

1. Very difficult to remembering the passwords.
2. The major drawback of this approach is that such systems can be expensive a identification process can be slow.

2.3 Biometric:

Biometrics is the measurement and statistical analysis of people's unique physical and behavioral characteristics. The technology is mainly used for identification and access control, or for identifying individuals who are under surveillance. The basic premise of biometric authentication is that every person can be accurately identified by his or her intrinsic physical or behavioral traits. While high-quality cameras and other sensors help enable the use of biometrics, they can also enable attackers. Because people do not shield their faces, ears, hands, voice or gait, attacks are possible simply by capturing biometric data from people without their consent or knowledge.

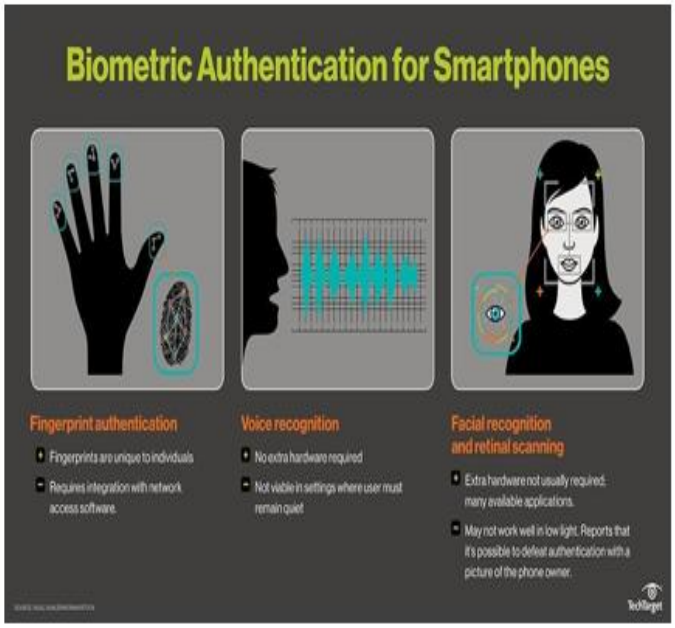

Figure 1 Biometric

2.4 A Graphical Password:

A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA).A graphical password is easier than a text-based password for most people to remember. Suppose an 8-character password is necessary to gain entry into a particular computer network.

Figure 2 Graphical password

2.5 Digital signature:

A digital signature (not to be confused with a digital certificate) is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. The digital equivalent of a handwritten signature or stamped seal, but offering far more inherent security, a digital signature is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide the added assurances of evidence to origin, identity and status of an electronic document, transaction or message, as well as acknowledging informed consent by the signer.

Figure 3 Digital signature

2.6 Voice Recognition:

Voice recognition refers to the recognition of human speech by computers and then performing a voice initiated program or function. The challenge that is handled so easily by the human brain, of interpreting speech amidst all accents, pitch, tone, articulation, nasality, vocalizations and pronunciation is a challenge when a computer tries to do it. Voice recognition systems enable consumers to interact with technology simply by speaking to it, enabling hands-free requests, reminders and other simple tasks.

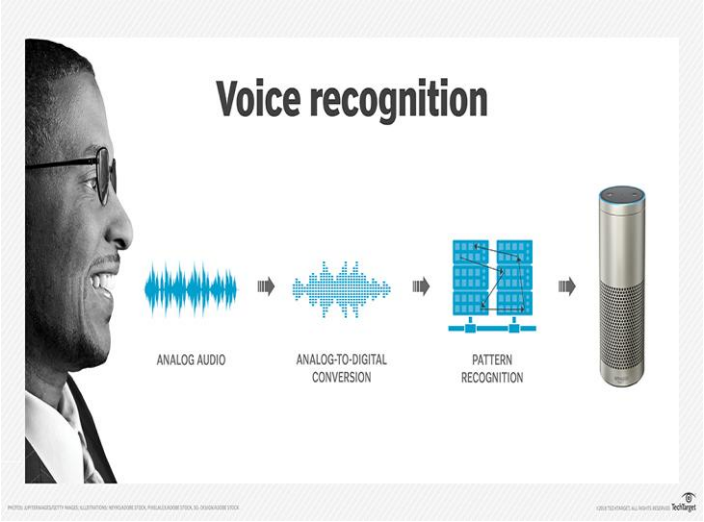

Figure 4 Voice recognition

III PROPOSED SYSTEM

In this paper we are introducing the new technique of authentication for user to provide high security. We are implementing a pair based algorithm in android for developing android application to produce authentication scheme for creating session password for a particular session. This technique is secured for accessing the any application. It may protect user from attackers by shoulder surfing, eves dropping, and guessing attacks because session password are valid for a particular session after termination of session it is invalid and useless.

The proposed system consisting of following steps

1) Registration of the user
2) Login process
3) Enter newly generated session password
4) Verification process

Following is the flow diagram of proposed system

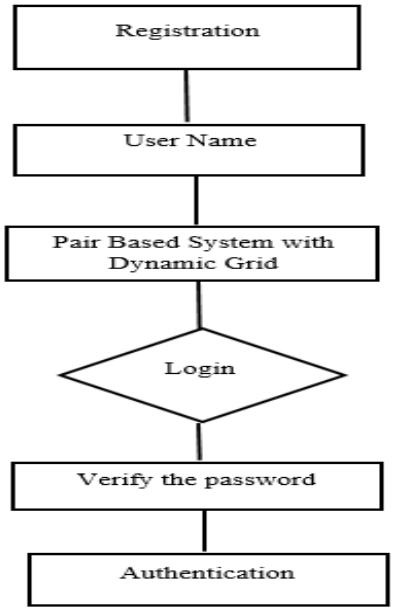

Figure 5 Flow diagram of Pair Based Dynamic Grid

3.1 Pair based authentication technique:

In an android application during registration user have to enter user name and password this password is used for generating the session password .this password should be of minimum 8 character and should be of even number always . At the time of login process after enter user name an interface grid is present for creating session password. This 6 x 6 grid contains alphabets and numbers randomly placed. Every time at the time of login process this interface grid is changed. User has to consider his password in terms of pairs.

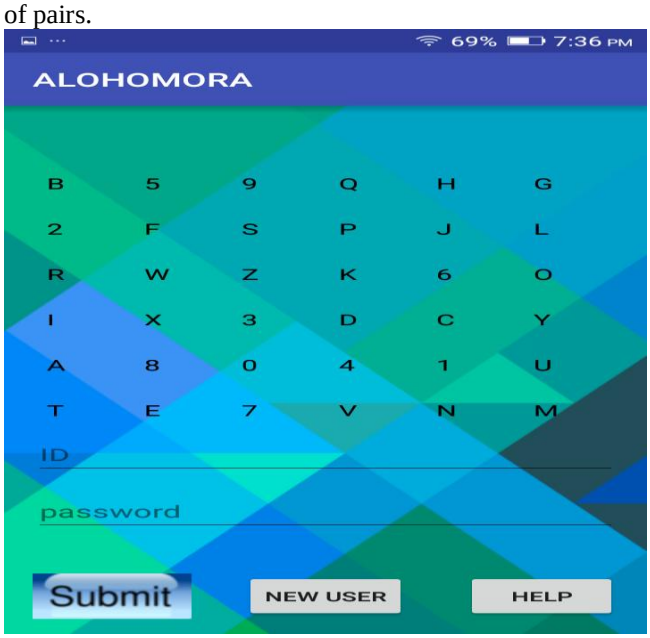

Figure 6 Pair Based Dynamic Grid Authentication Scheme

In this pairs first letter is used for selecting the row and the second letter is used for selecting the column from interface grid. The intersection letter is used for the session password. This is repeated for all pairs. With this process whole session password is created if it is correct then it can used for this particular session.

IV CONCLUSION

With this authentication scheme for session password using pair based algorithm we provide a more security to the user for accessing any application from hackers any type of attack .And user is satisfied with the security of the system. And this technique is easy to understand and affordable technique.

REFERENCES

[1] M. Weir, S. Aggarwal, B. de Medeiros, and B. Glodek, “Password cracking using probabilistic context-free grammars,” in Proc. IEEE Symposium on Security and Privacy, 2009.

[2] Fujita, K. and Y. Hirakawa, “A study of password authentication method against observing wrapper approach for feature subset selection in Attacks”, 6th International Symposium on Intelligent keystroke dynamics identity verification, Systems and Informatics, SISY 2008. [

[3] D. Florencio and C. Herley, “A large-scale study of web password habits,” in Proc. WWW’07, 2007.

[4]Eljetlawi, A.M.; Fac. of Eng., Univ. of Tajoura, Tripoli, Libya," Graphical password: Existing recognition base graphical password usability", IEEE, March 2010

[5]Almulhem, A.; Comput. Eng. Dept., King Fahd Univ. of Pet. & Miner., Dhahran, Saudi Arabia,"A graphical password authentication system", IEEE, FEB 2011

[6]XiaoyuanSuo,; Ying Zhu; Owen, G.S, "Graphical passwords: a survey", IEEE, DEC 2005.

[7] Ahmed, A.A.E. and I. Traore, “Anomaly Intrusion Detection Based on Biometrics, IEEE Proceedings, IAW '05.

[8]Varun Kacholia and Shashank Pandit,”Biometric Authentication Using Random Distribution”, Canadian IT Security Symposium (CITSS), 2003

[9]VAISHNAVI PANCHAL*, CHANDAN P. PATIL,“Authentication Schemes for Session Password”, IJSER 2013

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