Dr. Megha Gupta **2020-till now**

Proceedings of the Third International Conference on Intelligent Sustainable Systems [ICISS 2020]
DVD Part Number: CFP20M19-DVD; ISBN: 978-1-7281-7088-6

A contemporary Pictorial Password technique based on Character Set and Direction

Megha Gupta, Vivek Kumar Sharma, Aakanksha Chopra
Department of Computer Science, MSCW, University of Delhi, Delhi, India
Department of Engineering and Technology, Jagannath University, Jaipur, India
Department of Information Technology, JIMS, Rohini, New Delhi, India

***Abstract*- Passwords have always been a medium of authentication which is widely used and implemented for accessing control over devices or an account. With COVID- 19 pandemic, the entire world is sitting home, doing WFH, bank transactions, and data transfers through online modes only. Situations like these where offline mode has taken a back seat, the online attacks, and security breaches have drastically increased. People can't move and have to serve from their homes but feel protected as they deal and transact through passwords only. But, what if these passwords are not full proof, have leakages, and are easily guessable; such kind of situations is risky and breaks user's trust. To avoid such repetitive circumstances user has to be more cautious while keeping passwords. In this paper, a secure and easy password generating technique has been proposed based on an attractive Graphical User Interface. This technique is efficient in terms of privacy, security, and memorability.**

Keywords*- *Password, authentication, graphical authentication, hybrid technique.

1. INTRODUCTION

With changing times as the data has evolved and became important and crucial the methodology of protecting the data has become very difficult as normal textual passwords are no longer considered reliable for data accessing. Passwords are secrets that are hidden from everyone to restrict access to a computer system. Passwords can be defined as a collection of the string of characters, numbers, and special symbols; kept to verify the identity of the user during the authentication phase.

In current times, where every document is confidential and is password protected; keeping a strong password is a big challenge. Passwords are kept by users as per user's downloading a file requires a password, downloading an application requires authentication; using the same application is also password or pattern protected. With cash in hand to plastic money, things and economy have evolved to an extent where buying products and commodities also require PIN numbers or password.

It is also certainly proven that users tend to keep predictable passwords. The human tendency is to keep well memorable passwords with fewer efforts taken towards keeping a more secure password; they use multiple codes with the same trend or pattern, so users tend to keep repetitive, easily memorable passkeys which, therefore, result in easily 'guessable' passwords. Multiple predictable tools like- dictionaries or probabilistic models are used by intruders for guessing passwords. Basically, multiple attempts are done by intruders for a particular attack. At this stage, it has become crucial to rethink how to make our computer systems or devices which are using passwords as entry-mode to become more and more secure. It is, therefore, very important to figure out their capacity to all guessing attacks.

One important component for gaining authentication is a password. For analyzing the need of the hour it is essential to understand various authentication techniques of password and how they are different from each other. Authentication is a process of giving access to a legitimate user after entering the correct password. Authentication verifies whether a user is legitimate or not or a robot. Broadly authentication techniques can be divided into three categories- Token- based, Biometric, Knowledge- based [4] as discussed below:

Springer Link

A Survey on Spectrum Sharing Techniques in Cognitive Radio-Based Smart Grids

International Conference on Wireless Intelligent and Distributed Environment for Communication

WIDECOM 2020: 3rd International Conference on Wireless, Intelligent and Distributed Environment for Communication pp 113-122 | Cite as

- Megha Gupta (1) (2)
- Vinesh Kumar (2) (3)

1. Department of Computer Science, Mata Sundri Devi College for Women, , Delhi, India
2. University of Delhi, , Delhi, India
3. Department of Computer Science, Acharya Narender Dev College, , Delhi, India

Conference paper
First Online: 24 June 2020

Part of the Lecture Notes on Data Engineering and Communications Technologies book series (LNDECT, volume 51)

Abstract

The traditional electrical grid or power grid is presently undergoing a range of serious efforts to become a smart grid. In the present scenario, the energy or power is distributed from the power plants to the consumers via long-range transmission and distribution networks in the traditional grid networks. In these networks, information monitoring and management are limited to the distribution networks that distribute the electric power within a specified area to the consumer. The main reasons to introduce the concept of smart grid include reliability, rising demands, renewable energy resources, and utilization to name a few. The collaboration of cognitive radio technology with smart grid system fulfills the complex communication necessities of the smart grid. With the help of cognitive radio-based communications in smart grid, the problem of underutilization/shortage of spectrum via flexible usage of licensed frequency bands for future application of smart grid can be overcome. The cognitive radio-based smart grid system can also reduce the consumption of power and interoperability among heterogeneous communication networks. This paper presents a survey of spectrum sharing techniques in cognitive radio-based smart grid along with the advantages and disadvantages of the techniques.