

ABSTRACT

Graphical passwords is one form of security system in the web application. User interaction with a device and to access their personal information. Such access should be protected from things that are cyber crime. One cyber crime in the graphical password is brute force attack.

Focused on the above issues, this final project implementing Graphical Password security with the use of methods of pattern and image CAPTCHA as a security during the process of direct downloads are useful for preventing auto downloader is usually done by a bot. The system will provide a path CAPTCHA is generated randomly as a password that will be used by the user on the input pattern. Each path can be done possibly by using a permutation approach as the brute force attack.

In this final project, has produced a system that is able to minimize the prevention of auto download. Path used in the implementation of this time is from four to eight nodes with a total of nine node node. The path of the generated value of the average execution time using accurate normal of 1.0964 ms with Brute Force Attack for 11 minutes 23 seconds and by using high accurate execution time of 1.3456 ms with Brute Force Attack for 13 minutes 58 seconds.

Keywords: Graphical Password, Brute-force attack, Bot, CAPTCHA, Normal Execution Accurate, High Accurate Execution