ABSTRAK

Graphical password merupakan salah satu bentuk sistem keamanan didalam *web application*. *User* melakukan interaksi dengan sebuah *device* dan melakukan akses yang bersifat pribadi. Akses tersebut harus terhindar dari hal–hal yang bersifat *cyber crime*. Salah satu *cyber crime* di dalam *graphical password* yaitu *brute force attack.*

Bertitik tolak pada permasalahan diatas, tugas akhir ini melakukan implementasi keamanan *Graphical Password* dengan metode penggunaan *pattern* dan *image* CAPTCHA sebagai keamanan pada saat proses *direct download* yang berguna untuk mencegah *auto downloader* yang biasa dilakukan oleh *bot.* Sistem akan memberikan sebuah *path* CAPTCHA yang di *generate* secara random sebagai sandi yang akan digunakan oleh *user* pada *pattern input.* Setiap *path* bisa dilakukan kemungkinan dengan menggunakan pendekatan permutasi sebagai proses *brute force attack.*

Dalam tugas akhir ini, telah dihasilkan sistem yang mampu meminimalisir pencegahan *auto download*. *Path* yang digunakan pada implementasi kali ini yaitu dari empat sampai delapan node dengan keseluruhan *node* yang berjumlah sembilan node. Dari *path* tersebut dihasilkan nilai waktu eksekusi rata–rata menggunakan *normal accurate* sebesar 1.0964 ms dengan *Brute Force Attack* selama 11 menit 23 detik dan dengan waktu eksekusi menggunakan *high accurate* sebesar 1.3456 ms dengan *Brute Force Attack* selama 13 menit 58 detik.

.**Kata Kunci :** *Graphical Password, Brute force attack, Bot,* CAPTCHA, *Normal Accurate Execution, High Accurate Execution*