ABSTRAKSI

Teknologi yang sudah berkembang saat ini memunculkan berbagai alternatif media penyimpanan berkas elektronik atau *file*. *File Hosting* merupakan alternatif sebagai media penyimpanan berkas elektronik karena dapat digunakan dimana saja secara *online*. Untuk menjamin keamanan dan keutuhan dari suatu data dalam *File Hosting* tersebut, dibutuhkan suatu proses penyandian seperti memberikan *password* pada *file* dan enkripsi dilakukan ketika *file* di *upload*. Sementara itu, proses dekripsi dilakukan ketika pengguna men-*download file*. Dengan cara penyandian tadi, data asli yang di *upload* kedalam *server* tidak akan terbaca oleh pihak yang tidak berkepentingan, melainkan hanya oleh penerima yang memiliki kunci dekripsi. Selain data *file*, *password* milik pengguna pun patut diamankan. *Password* pengguna disimpan dalam bentuk *hash* didalam *database*, agar pihak yang tidak berkepentingan seperti *admin* dan *hacker* tidak dapat membaca *password* sesungguhnya. Selain itu perlu dilakukan perubahan nama *file* untuk mencegah nama *file* yang mengandung *script* php mempengaruhi proses sistem. Dilakukan juga pembatasan jenis *file* yang boleh di *upload*, untuk mencegah jenis *file* berbahaya seperti virus memasuki komputer *server*. Sehingga dengan sistem keamanan yang diterapkan tersebut dapat meningkatkan keamanan informasi untuk pengguna dalam menyimpan data pribadi seperti *file* dan *password* yang bersifat rahasia dari pihak yang tidak berkepentingan.

Kata kunci : *AES*, enkripsi, dekripsi, *File Hosting*, *Hash Password*.

ABSTRACT

The technology has been developed at this time led to a variety of alternative electronic storage media file or files. File Hosting is an alternative for the storage of electronic files because it can be used anywhere online. To ensure the security and integrity of the data in the File Hosting, it takes a process of encoding such as password protect files and encryption are performed when a file is uploaded. Meanwhile, the decryption process performed when users download files. By way of encoding earlier, the original data is uploaded into the server will not be read by unauthorized parties, but only to recipients who have the decryption key. In addition to the data file, the user's password properly is secured. The user password is stored in hashed form in the database, so that unauthorized parties such as the admin and the hacker can not read the actual password. In addition it is necessary to change the file name to prevent the name of the file containing the php script affect the system. Do also restrictions on file types may be uploaded, to prevent these types of malicious files such as viruses enter a computer server. So that the security system implemented, could improve information security for the user to store personal data such as files and confidential passwords from unauthorized parties.

Keyword : AES, encryption, decryption, File Hosting, Hashing.