SECURE FILE SHARING USING ADVANCED ENCRYPTION STANDARD (AES) 256

MAGANG & STUDI INDEPENDEN BERTSERTIFIKAT
***CLOUD STORAGE DATA* HUAWEI**
DI PT. HUAWEI TECH. INVESTMENT

AJI PANGESTU
18101074

PROGRAM STUDI SARJANA TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO
INSTITUT TEKNOLOGI TELKOM PURWOKERTO
2021

Lembar Pengesahan

SECURE FILE TRANSFER USING ADVANCED ENCRYPTION STANDARD (AES) 256

MAGANG & STUDI INDEPENDEN BERSERTIFIKAT

CLOUD STORAGE

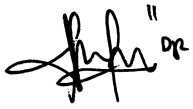
DI PT.HUAWEI TECH. INVESTMENT

Disusun oleh :

Aji Pangestu

18101074

Telah disetujui oleh :

Pembimbing : 1. Afifah Dwi Ramadhani, S.ST., M.Tr.T ()

NIK/NIP/NIDN : 20960016

2. Raditya Artha Rochmanto, S.T., M.T ()

NIK/NIP/NIDN : 030920194

Mengetahui,

Ketua Program Studi S1 Teknik Telekomunikasi

IT Telkom Purwokerto

Prasetyo Yuliantoro, S.T., M.T.

NIDN. 0620079201

KATA PENGANTAR

Dengan memanjatkan Puji Syukur ke hadirat Tuhan Yang Maha Esa, kami dapat menyelesaikan Laporan Akhir Magang & Studi Independent Bersertifikat (MSIB) dengan judul *"Secure File transfer using Advanced Encryption Standard* (AES) 256*"*.

Penyusunan laporan akhir ini digunakan sebagai persyaratan pertanggung jawaban atas keikutsertaan dalam program Studi Independen Bersertifikat yang dilaksanakan di PT. Huawei Tech Investment pada tanggal 01 September 2021 sampai dengan 31 Januari 2022.

Selesainya kegiatan Magang dan Studi Independent Bersertifikat (MSIB) ini tidak lepas dari bantuan banyak pihak, sehingga penulis sangat terbantu dalam berbagai hal. Oleh karena itu penulis menyampaikan rasa terimakasih kepada :

1. Afifah Dwi Ramadhani, S.ST., M.Tr.T. Selaku Dosen Pembimbing sekaligus Mentor. Yang telah membimbing, mengarahkan, memberi motivasi serta inspirasi.
2. Prasetyo Yuliantoro, S.T., M.T. selaku Ketua Program Studi S1 Teknik Telekomunikasi.
3. Dr. Arfianto Fahmi, S.T., M.T., IPM sekalu Rektor Institut Teknologi Telkom Purwokerto.
4. Teman-teman satu kelas MSIB *Cloud Storage* yang telah bekerja sama, memberikan *support* serta motivasi dan semangat.
5. Ayah, Ibu, dan Adik yang mensupport dari segi mental dan material.

Penulis menyadari bahwa penulisan laporan ini masih jauh dari kesempurnaan baik materi maupun cara penulisannya. Oleh sebab itu penulis mengharapkan kritik dan saran yang membangun dari pembaca, sehingga penilis dapat menjadi lebih baik lagi dalam penulisan laporan selanjutnya. Semoga laporan ini bermanfaat bagi pembaca serta bermanfaat untuk bidang Pendidikan.

Purwokerto, Februari 2022

Aji pangestu

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

1. HCIA : Huawei *Certified* ICD *Associate*
2. AES : *Advanced Encryption Standard*
3. SIB : Studi Independen Bersertifikat
4. HKI : Hak Kekayaan Intelektual

ABSTRAK

Pemrograman soket memiliki banyak keuntungan untuk mengirimkan data. Pemrograman soket banyak digunakan untuk membuat sistem komunikasi untuk menghubungkan satu *host* ke *host* lain. Selain untuk mentransmisikan data berupa teks, *socket programming* juga dapat digunakan untuk mentransmisikan gambar, video, rar, music, dokumen, serta pdf. Dalam sebuah sistem komunikasi, integritas data merupakan hal yang krusial sehingga diperlukan sistem keamanan untuk menjamin kerahasiaan data yang dikirimkan. Terutama untuk membangun sistem komunikasi yang dianggap rahasia. Ini juga berlaku untuk mengirim berbagai file melalui jaringan. Solusinya adalah dengan menggunakan kriptografi yang dapat menyandikan informasi dengan menggunakan kunci sehingga data yang dikirimkan tidak dapat dibaca oleh pihak yang tidak berwenang. Enkripsi AES diperkirakan merupakan algoritma yang paling aman dibandingkan dengan algoritma lainnya. Pada penelitian ini akan dibuat sebuah sistem *Secure File Transfer Using Advanced Encryption Standard(AES) 256.* Hasil penelitian menunjukkan bahwa Algoritma Enkripsi *Advanced Encryption Standard (AES) 256* dapat mengamankan file tipe .docx, .pdf, .txt, .rar, .jpg, .mp3, dan mp4 dengan waktu dekripsi lebih lama dibanging waktu enkripsi.

Kata Kunci : *Socket Programming,* Kriptografi, AES

ABSTRACT

Socket programming has many advantages for transmitting data. Socket programming is widely used to create communication systems to connect one host to another. In addition to transmitting data in the form of text, socket programming can also be used to transmit images, videos, rar, music, documents, and pdf. In a communication system, data integrity is crucial, so a security system is needed to ensure the confidentiality of the data sent. Especially to build a communication system that is considered secret. This also applies to sending various files over the network. The solution is to use cryptography which can encode information using a key so that the data sent cannot be read by unauthorized parties. AES encryption is estimated to be the most secure algorithm compared to other algorithms. In this research, a Secure File Transfer Using Advanced Encryption (AES) 256 system will be created. The results show that the Advanced Encryption Standard (AES) 256 encryption algorithm can secure files of .docx, .pdf, .txt, .rar, .jpg, .mp3, and mp4 types with a longer decryption time than encryption time.

Keywords : Socket Programming, Cryptography, AES

BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Pada perkembangan teknologi saat ini kemanan suatu data merupakan hal harus diperhatikan dalam menjaga kerahasiaan informasi. Khususnya informasi yang hanya boleh diketahui oleh pihak tertentu. Pada umumnya, data atau informasi yang ditransmisikan tanpa dilakukan proses pengamanan. Hal ini beresiko terhadap adanya upaya penyadapan sehingga informasi tersebut bisa diketahui oleh pihak lain yang tidak berhak.

Salah satu upaya pengamanan data adalah dengan menggunakan metode kriptografi. Kriptografi merupakan sebuah ilmu yang mempelajari Teknik enkripsi dari data asli (*plaintext)* yang tersusun acak melakukan proses enkripsi pada data tersebut. Enkripsi merupakan suatu cara dalam proses perubahan pesan dari pesan jelas (*plaintext)* menjadi pesan yang disandikan (*ciphertext*). Sedangkan Dekripsi merupakan proses sebaliknya dari Enkripsi.

Algoritma digunakan untuk menjaga keamanan data. Baik data berupa dokumen, audio, gambar, dan video. Jenis algoritma yang bisa digunakan untuk mengamankan data salah satunya adalah *Advanced Encryption Standard* (AES). Dalam keamanan *socket programming* dilindungi dengan pemilihan port yang bisa saja diketahui oleh pihak lain.

Implementasi algoritma AES pada semua jenis berkas diharapkan dapat meningkatkan keamanan data yang ditransferkan agar terhindar dari penyadapan serta informasi tidak dapat diketahui oleh pihak lain.

Saat ini algoritma AES merupakan salah satu algoritma enkripsi yang cukup aman serta memiliki performa yang bagus untuk melindungi data atau informasi yang bersifat rahasia. Untuk mengtahui performa dari algoritma AES dapat dilihat dari waktu yang diperlukan untuk melakukan enkripsi dan dekripsi. Berdasarkan permasalahan tersebut penulis mengambil topik "***Secure File Transfer Using Advanced Encryption Standard (AES) 256".***

1.2 RUMUSAN MASALAH

Berdasarkan latar belakang yang diuraikan diatas, dapat disimpulkan rumusan masalah, yaitu:

1. Bagaimana sistem keamanan dengan menggunakan *socket programming* dan algoritma AES 256 ini bekerja?
2. Berapa waktu yang diperlukan algoritma aes dalam melakukan enkripsi dan dekripsi *file*?
3. Bagaimana hasil dari performa sistem keamanan dengan menggunakan *socket* programming dan algoritma AES 256 ini bekerja?

1.3 TUJUAN KEGIATAN

Adapun tujuan dari *project* ini adalah untuk membuat sistem keamanan yang dikombinasikan dengan *socket programming* dan algoritma AES 256 pada *file* sharing menggunakan python.

1.4 MANFAAT KEGIATAN

Dari penelitian yang dikerjakan, terdapat beberapa manfaat yaitu :

1. Memberikan gambaran mengenai sistem keamanan *file sharing* dengan menggunakan enkripsi AES 256 pada *socket programming* menggunakan *phyton.*
2. Dengan adanya penelitian ini diharapkan dapat meminimalisir tindakan kriminal penyalahgunaan keamanan pada *file* sharing.
3. Memberikan pengetahuan mengenai pentingnya keamanan *data* pada *file sharing.*

BAB II
PROSEDUR KERJA

2.1 DESKRIPSI PENUGASAN KERJA

Selama mengikuti program Studi Independen bersertifikat (SIB) *Cloud Storage* di PT. Huawei Tech. Investment yang dilakukan selama 5 bulan mulai dari tanggal 01 September 2021 sampai dengan 31 Januari 2022, penulis mendapatkan ilmu tentang *Cloud Storage* yang terbagi menjadi beberapa 6 bab, yaitu *Storage Technology Trends, Storage Basic Technologies, Storage Common Advanced Technologies, Storage Business Continuity Solutions, Storage System O&M Management,* dan *Scenario-based Pratcice.* Pembelajaran pada SIB ini dilakukan secara *online learning,*

Pada pembelajaran ini penulis dapat memahami konsep dari teknologi dari *Cloud Storage,* mengasah *softskill* dan *hardskill,* serta mempraktekkan hasil pembelajaran melalui kegiatan proyek yang dilakukan secara kelompok maupun individu. Selama pembelajaran SIB *Cloud Storage* ini penulis menggunakan akun untuk dapat mengakses web yang telah disediakan oleh mitra SIB yaitu Huawei, yang mana pada web tersebut berisi materi-materi pembelajaran untuk sertifikasi tingkat global mengenai *Cloud Storage*. Pembelajaran berjalan kurang lebih berjumlah 560 jam, dimana kegitan yang dilakukan berupa *live session* dengan mentor, dan *self study* melalui web *e-learning* yang disediakan oleh Huawei.

Pada akhir *session* pembelajaran terdapat beberapa *exam* yang harus dikerjakan oleh penulis, selain itu pihak mitra juga memberikan kesempatan kepada penulis untuk mengikuti sertifikasi tentang Huawei *Cloud Storage*. Sebagai penutup pada kegiatan SIB ini, penulis diberikan sebuah proyek kelompok oleh mentor yang berhubungan dengan *Secure File Transfer*. Pada proyek ini penulis dan kelompok dibimbing langsung oleh mentor, *output* yang diharapkan dari proyek ini adalah berupa HKI, *papper*, dan hasil dari proyek kelompok yang diberikan oleh mentor.

2.2 TEORI DASAR PENDUKUNG

2.2.1 KRIPTOGRAFI

Kriptografi berasal dari dua kata Yunani, yaitu *Cryto* yang berarti rahasia dan *Grapho* yang berarti menulis. Secara umum kriptografi dapat diartikan sebagai ilmu dan seni penyandian yang bertujuan untuk menjaga keamanan dan kerahasiaan suatu data.

Kriptografi mendukung kebutuhan dari dua aspek kemanan informasi, yaitu *secrecy* (Perlindungan terhadap kerahasiaan data informasi) dan *authenticity* (perlindungan terhadap kerahasiaan pemalduan dan pengubahan informasi yang tidak diinginkan). Kriptografi tidak hanya memberikan kemanan informasi saja, namun lebih kea rah Teknik-tekniknya.

Algortima-algoritma kriptografi dapat dibedakan menjadi dua macam yaitu simetrik dan asimetrik. Algoritma simetrik (model enkripsi konvensional) merupakan algoritma yang menggunakan satu kunci untuk proses enkripsi dan dekripsi data. Sedangkan algoritma asimetrik (model enkripsi kunci public) menggunakan kunci yang berbeda dalam proses enkripsi dan dekripsi pesan [1].

2.2.2 ALGORITMA AES

Algoritma AES merupakan algoritma chipper yang aman untuk melindungi data atau informasi yang bersifat rahasia. AES dipublikasikan oleh NIST (*National Institute of Standard and Technology*) pada tahun 2001 yang digunakan untuk menggantikan algoritma DES yang sudah dianggap kuno dan mudah dibobol.

Input dan *output* dari algoritma AES terdiri dari urutan data sebesar 128 bit. Urutan data dalam satu kelompok 128 bit tersebut disebut juga sebgai blok data atau *plaintext* yang nantinya akan dienkripsi menjadi *chipertext*. Panjang kunci dari AES terdiri dari panjang kunci 128 bit, 192 bit, dan 256 bit. Perbedaan panjang kunci ini yang nantinya mempengaruhi jumlah putaran pada algoritma AES ini. *Input* dan *output* dari algoritma AES terdiri dari urutan data sebesar 128 bit.

Urutan data dalam satu kelompok 128 bit tersebut disebut juga sebagai blok data atau *plaintext* yang nantinya akan dienkripsi menjadi *chipertext*. Panjang kunci dari AES terdiri

dari panjang kunci 128 bit, 192 bit, dan 256 bit. Perbedaan panjang kunci ini yang nantinya mempengaruhi jumlah putaran pada algoritma AES ini. Jumlah putaran yang digunakan algoritma ini ada tiga macam seperti pada tabel di bawah.

Tabel 2. 1 Jumlah Putaran Pada Algoritma AES

Tipe	Panjang Kunci	Panjang Blok Input	Jumlah Putaran
AES-128	128 bit	128 bit	10
AES-192	192 bit	128 bit	12
AES-256	256 bit	128 bit	14

2.2.3 *SOCKET PROGRAMMING*

Socket adalah sebuah *Class* yang disediakan oleh beberapa bahasa pemrograman. Dengan *socket*, sebuah aplikasi di suatu komputer dapat Tentu saja aplikasi di komputer yang dihubungi menerima koneksi juga menggunakan *socket*. Dengan kata lain *socket* adalah suatu Class yang digunakan oleh aplikasi untuk saling berhubungan.

Hampir semua sistem operasi menyediakan *application programming interface* (API) yang memungkinkan sebuah aplikasi komputer mengkontrol dan menggunakan socket jaringan komputer. API *socket* internet biasanya berdasarkan pada standar *berkeley sockets*.

Sebuah alamat *socket* terdiri atas kombinasi sebuah alamat ip dan sebuah nomor *port*, mirip seperti sebuah koneksi telpon yang memiliki nomor telpon dan nomor ekstensinya. Berdasarkan alamat ini, *socket* internet mengirim paket data yang masuk ke sebuah proses atau thread aplikasi tujuan.

Socket programming adalah pemrograman yang menggunakan *socket*. *Socket* ini semacam terowongan/*tunnel* yang bisa dipakai untuk komunikasi/pertukaran arah secara bolak-balik. Dengan *socket programming*, komunikasi dapat terjalin antara bahasa pemrograman yang berbeda, antara tingkatan user yang berbeda, bahkan antar komputer yang berbeda atau gabungan ketiganya [2].

2.2.4 VIRTUALBOX

Gambar 2. 1 Logo VirtualBox

Oracle VM VirtualBox merupakan perangkat lunak virtualisasi, yang dapat digunakan untuk mengeksekusi *system* operasi tambahan disistem operasi utama. VirtualBox berfungsi untuk melakukan virtualisasi sistem operasi. Penggunaan VirtualBox ditargetkan untuk Server, Desktop, dan penggunaan *Embeded*. Berdasarkan jenis VMM yang ada, VirtualBox merupakan jenis *hypervisor type2* [3].

2.2.5 PYTHON

Gambar 2. 2 Logo *Python*

Bahasa pemrograman *python* merupakan Bahasa pemrograman tinggi yang dapat melakukan eksekusi sejumlah intruksi multi guna secara langsung (*interpretative*) dengan metode orientasi objek (*Object*

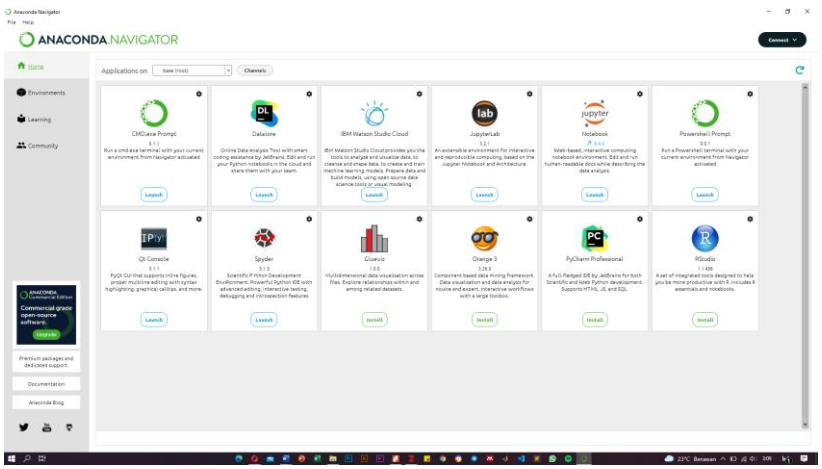
Oriented Programming) serta menggunakan semantic dinamis untuk memberikan tingkat keterbacaan *syntax.*

Python dapat digunakan secara bebas, bahkan untuk kepentingan komersial sekalipun. Banyak perusahaan yang mengembangkan Bahasa pemrograman *python* secara komersial untuk memberikan layanan. Misalnya *Anaconda Navigator*, adalah salah satu aplikasi untuk pemrograman *python* yang dilengkapi dengan *tool-tool* pengembangan aplikasi [4].

2.2.6 ANACONDA

Gambar 2. 3 *Logo Anaconda*

Anaconda merupakan sebuah *platform* untuk memberdayakan *asset,* kolaborasi, dan meluncurkan projek-projek sains. *Anaconda Navigator* merupakan sebuah *Graphical User Interface* (GUI) yang dapat digunakan untuk menjalankan aplikasi dan mengelola *packages* untuk menggunakan *library* dalam kode program yang dibutuhkan untuk *data learning.* Dalam *Anaconda Navigator* terdapat beberapa aplikasi salah satunya adalah *Spyder* [5].



Gambar 2. 4 *Anaconda Navigator*

2.2.7 *SPYDER*

Gambar 2. 5 Logo Spyder

Spyder (*Scientific Python Development Environment*) adalah *software open source* yang berfungsi sebagai IDE Python dengan berfokus kepada pengembang, peneliti, dan analis data. Spyder mempunyai fitur unik berupa *editing* kode tingkat lanjut, analisis, *debugging*, dan pembuatan profil IDE (*profiling functionality*). Fitur *profiling functionality* mengizinkan pengguna untuk mengatur tampilan *software* Spyder seperti tema, *font*, dan *scaling*. Sehingga menulis kode menjadi lebih nyaman. Spyder juga dilengkapi dengan alat-alat komprehensif untuk eksplorasi data, eksekusi interaktif, inspeksi mendalam, dan kemampuan visualisasi yang bagus [6].

2.2.8 UBUNTU

Gambar 2. 6 Logo Ubuntu

Ubuntu merupakan salah satu distribusi Linux yang berbasis Debian. Ubuntu didistribusikan sebagai perangkat lunak bebas dengan sumber terbuka yang dirilis pada tanggal 20 Oktober 2004.

Proyek Ubuntu ini dikembangkan oleh Canonical Ltd dan beberapa komunitas pengembang lainnya. Canonical Ltd merupakan sebuah perusahaan yang dimiliki oleh pengusaha Afrika Selatan dengan nama

Mark Shuttleworth. Perusahaan tersebut menyediakan pembaruan keamanan dan dukungan untuk setiap rilis Ubuntu, dimulai dari tanggal rilis hingga mencapai tanggal akhir masa pakai (EOL) yang ditentukan.

Sejak perilisannya, Ubuntu dapat dikatakan sebagai sistem operasi pilihan bagi banyak pengguna distribusi Linux yang masih pemula karena kemudahan dalam menginstall dan mengoperasikannya. Terlebih dengan antarmuka *default* Ubuntu terbaru dari edisi Desktop adalah GNOME, di mana pengguna disediakan tampilan yang handal, stabil, bersih dan juga dekorasi yang minimalis [7].

BAB III
METODE KERJA

3.1 WAKTU DAN TEMPAT

Untuk waktu dan tempat pelaksanaan program Studi Independent Bersertifikat (SIB) yaitu :

Tempat : PT. Huawei Tech. Invesment

Waktu : 1 September 2021 – 31 Januari 2022

3.2 ALAT DAN BAHAN

Alat dan bahan yang digunakan selama mengikuti program Studi Independent Bersertifikat (SIB) di PT. Huawei Tech Investment yaitu :

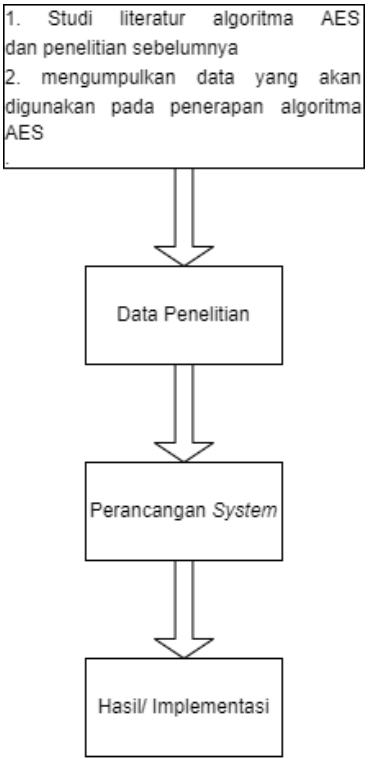
1. Virtual Box
2. Anaconda Navigator 2.1.1
3. Spyder 5.1.5
4. Linux Ubuntu

3.3 METODE PENELITIAN DAN PROSES KERJA

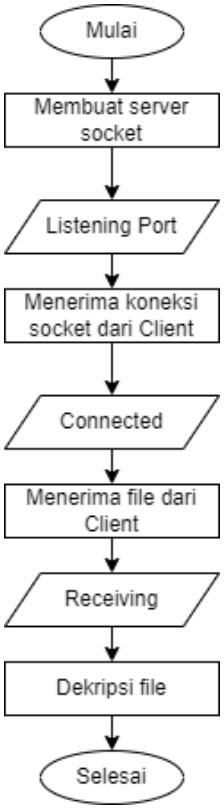
A. Metode Penelitian

Metode yang diterapkan dalam penelitian ini meliputi metode pengumpulan *data* dan metode pengembangan *system*. Metode Pengumpulan *Data* yang digunakan dalam Penelitian yaitu metode yang digunakan untuk mempelajari dan mengumpulkan *literature* yang berkaitan dengan penerapan algoritma AES untuk proses enkripsi dekripsi. Dan mempelajari penelitian sebelumnya terkait dengan enkripsi dekripsi. Metode ini bersumber dari jurnal-jurnal ilmiah, makalah, artikel, serta ilmiah lainnya. Tahapan-tahapan penelitian yang peneliti lakukan adalah:

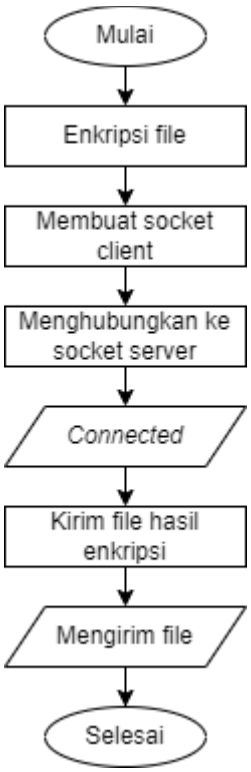
1) Studi literature yang mempelajari Algoritma AES dan penelitian sebelumnya.
2) Mengumpulkan *data* yang akan digunakan pada penerapan Algoritma AES dalam proses enkripsi dekripsi.
3) *Data* penelitian.
4) Implementasi.



Gambar 3. 1 Desain Penelitian



Gambar 3. 2 Diagram Alir Proses Pada *Server*



Gambar 3. 3 Diagram Alir Proses Pada *Client*

B. Proses Kerja

Selama mengikuti program Studi Independen *Cloud Storage* di PT. Huawei Tech. Investment yang dilakukan secara online learning. Dimana pada periode SIB selama 5 bulan mulai dari tanggal 01 September 2021 sampai dengan 31 Januari 2022 mahasiswa mendapat ilmu dari unit *Cloud Storage.* Selama mengikuti kegiatan terdapat beberapa tahapan proses kerja yang dilakukan mahasiswa sebagai mantee, berikut merupakan tahapan proses kerja yang dilakukan mahasiswa di program Studi Independen Huawei dengan topik *Cloud Storage.*

1. Materi kursus HCIA storage MOOC Huawei talent dari iLearningX

   Pada tahap pemahaman materi ini, mahasisawa sebagai *mentee* melakukan *self learning* guna mempelajari lebih lanjut materi yang ada di *course* Huawei dan berlatih mengerjakan quiz untuk menguji kepahaman *mentee* terhadap materi yang sudah diajarkan. Terdapat 6 modul materi yang harus *mentee* pelajari diantaranya adalah *Storage*

Technology Trends, Storage Basic Technologies, Storage Common Advanced Technologies, Storage Business Continuity Solutions, Storage System O&M Management, Scenario-based Pratcice.

2. Mengikuti Sesi Pematerian dengan Mentor

   Pada kegiatan ini, *mentee* mengikuti pematerian dengan mentor untuk mempelajari materi lain yang menunjang program Studi Independen ini. Beberapa materi yang diajarkan yaitu mengenai yaitu IoT dan *Big Data, Internet Programming, Network Security, dan Scientific Writin*g. Pematerian ini dilakukan secara *online* melalui *Google Meet* dengan jadwalnya mulai dari Hari Senin sampai dengan Jum'at. *Progress report* terjadwal dilakukan setiap minggu guna memantau perkembangan *project* agar dapat selesai sesuai jadwal dan memberikan masukan pada proyek yang sedang dikerjakan

3. Pengerjaan *Mock Exam* dan Mengikuti Sertifikasi Huawei

   Pada tahap ini, *mentee* diberikan tugas untuk mengerjakan *Mock Exam* setelah menyelesaikan modul dalam *course*. Pengerjaan *Mock Exam* ini bertujuan sebagai sarana latihan bagi *mentee* sebelum mnegikuti sertifikasi. *Mock Exam* bisa dikerjakan sebanyak 3 kali dalam sehari dengan durasi pengerjaannya selama 90 menit. Soal *Mock Exam* terbagi menjadi 3 tipe yaitu soal *True False, Single Answer* dan *Multiple Answer* untuk lulus *Mock Exam*, *mentee* harus mendapatkan skor minimal 600.

4. Pengerjaan *Project* Kelompok

   Terdapat 4 topik *project* yang ditawarkan mentor kepada *mentee*. *project* ini dilakukan secara kelompok dengan masing-masing anggota kelompoknya berjumlah 3-4 orang dan setiap topik proyek akan dibimbing oleh satu mentor. Pada proyek ini topik yang dikerjakan untuk *Secure File Transer Using Advanced Encryption System (AES) 256*. Proyek kelompok berupa sistem keamanan untuk mengantisipasi akan rentannya terjadi kebocoran data pada *system file transfer*. Teknik keamanan yang kami gunakan menggunakan enkripsi AES 256 karena teknik ini merupakan sistem yang saat ini

dipercaya secara luas di berbagai industri yang membutuhkan tingkat keamanan yang sangat tinggi. Putaran enkripsi yang dimiliki AES membuat AES tidak bisa ditembus. Sebuah superkomputer membutuhkan waktu yang lama bahkan bertahun-tahun lebih lama dari perkiraan usia alam semesta untuk dapat memecahkan kode AES[8].

Tabel 3. 1 Jadwal Kegiatan Studi Independen

No	Kegiatan		MINGGU															
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
A	Pembelajaran Terjadwal																	
	A1	Pembelajaran Utama: Cloud Storage Technology																
	A2	Pembelajaran pendukung: Internet of Things dan Big Data																
	A3	Pembelajaran pendukung: Internet Programming																
	A4	Pembelajaran pendukung: Network Security																
	A5	Pembelajaran pendukung: Scientific Writing																
	A6	Pembelajaran pendukung: Kelas Persiapan Sertifikasi																
	A7	Pembelajaran pendukung: Progres Report Tugas Akhir																
B	Pembelajaran Mandiri																	
C	Pembelajaran Tamu																	
	C1	Pembelajaran Tamu 1: Workshop Storage dan sertifikasi																
	C2	Pembelajaran Tamu 2: Sharing Session: Skil yang dibutuhkan untuk bekerja di Bidang Telekomunikasi																
D	Pengerjaan Project																	

Mengacu pada Rencana Pembelajaran Semester (RPS) yang telah di tetapkan, tabel 3.1 merupakan Jadwal kerja kegiatan mahasiswa selama mengikuti Studi Indepen PT. Huawei Tech. Investment. Kelas *live session* bersama mentor dilaksanakan setiap hari Senin – Jumat. Total pertemuan dilakukan sebanyak 16 sesi. Kegiatan SIB Huawei *Cloud* ini dilakukan dimulai tertanggal 01 September 2021 – 31 Januari 2022. *Project review* dilakukan setiap minggu terakhir yaitu hari jum'at untuk diadakan memantau perkembangan *project* agar dapat selesai sesuai jadwal dan memberikan masukan pada projek yang sedang dikerjakan.

BAB IV
HASIL DAN PEMBAHASAN

Pada hasil dan pembahasan ini, penulis telah menyelesaikan *project* dengan topik *Cloud Storage* yang berjudul "*Secure File Sharing using Advanced Encryption Standard (AES)* 256*"* berhasil diselesaikan sesuai jadwal pengumpulan yang telah ditentukan. Pada projek ini berfokus pada mengetahui system keamanan *data* pada *file* sharing. Dari *project* ini penulis dapat mengetahui Algoritma *Advanced Encription System* (AES) terbukti mampu melakukan enkripsi *file* menjadi lebih *secure*. Kemudian berdasarkan hasil pengujian yang kami lakukan, diketahui bahwa *system* ini bekerja dengan baik dalam melakukan enkripsi, mengirim *file*, dan dekripsi sehingga sangat membantu dalam mengamankan *file* informasi dari pihak yang tidak bertanggung jawab.

Project ini berfokus pada keamanan *data* pada *file* sharing dimana tujuannya yaitu untuk mengetahui waktu yang diperlukan algoritma AES dalam melakukan enkripsi dan dekripsi *file*, serta untuk mengamankan *data*/informasi agar tidak bocor ke orang yang tidak bertanggung jawab. Proyek dibangun pada sebuah *system file* sharing yang dikombinasikan dengan algoritma *Advanced Encryption System* (AES) 256 dan *socket* programming.

Pada *project* ini implementasinya yaitu, *client* akan melakukan enkripsi terlebih dahulu menggunakan AES 256 pada *file* yang akan dikirimkan, kemudian setelah *file* diterima oleh *server* kemudian akan di dekripsi guna mengembalikan ke bentuk semula. Beberapa tipe *file* dengan berbagai macam ukuran seperti tampak pada *table.*

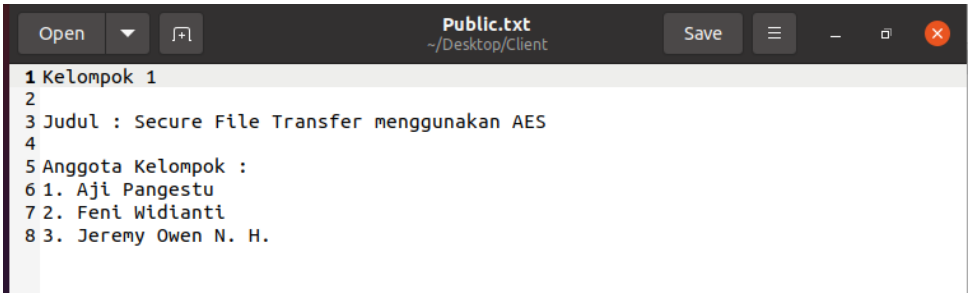
Tabel 4. 1 *File-file* Uji *System*

No	Nama *File*	Tipe *File*	Ukuran (*byte*)
1.	LaporanMBKM	*Microsoft Office Word Document* (.docx)	280.714
2.	BukuPanduan	PDF *Document* (.pdf)	7.460.661
3.	*Public*	*Text Document* (.txt)	137

4.	Kelompok1	WinRAR *archieve* (.rar)	13.388
5.	PresidenRI	JPG *File* (.jpg)	5.113
6.	VivaLaVida	MP3 *File* (.mp3)	9.685.485
7.	VivaLaVida	MP4 *File* (.mp4)	50.642.336

Untuk mengetahui hasil dari *system* yang telah dibuat, maka perlu dilakukan percobaan untuk mengetahui hasil dari setiap proses yang ada, yaitu proses enkripsi, pengiriman, dan dekripsi.

Setelah dilakukan percobaan terhadap sebuah *file* teks dengan format txt untuk enkripsi maka didapatkan hasil sebagai berikut. Contoh percobaan dilakukan menggunakan *file Public.txt* dengan ukuran 137 *byte*.



Gambar 4. 1 *File* Teks Asli Sebelum Dienkripsi

Jika gambar 4.1 merupakan *file* asli atau pesan sebelum dilakukan enkripsi. Setelah dilakukan enkripsi *file* asli tersebut akan Nampak seperti berikut.

Gambar 4. 2 *File* Teks Setelah Dienkripsi

File diatas merupakan tampilan *file* teks setelah dienkripsi. Tampak seperti teks dengan huruf-huruf acak. Setelah dilakukan enkripsi *file* teks memiliki ukuran yang lebih besar yaitu 176 *byte*.

Gambar 4. 3 *File* Teks Setelah Didekripsi

File diatas merupakan *file* teks setelah dilakukan dekripsi pada *server*. Teks tampak seperti teks awal sebelum dilakukan enkripsi, dan ukuran *file* tersebut mengalami penurunan menjadi berukuran 137 *byte* sama seperti *file* aslinya.

Dari beberapa tipe *file* diatas maka dilakukan proses pengujian system yaitu dilakukan enkripsi, kirim *file*, dan dekripsi menggunakan algoritma AES 256 yang dikombinasikan dengan *socket programming* dan hasil yang diperoleh dapat dilihat pada tabel berikut ini :

Tabel 4. 2 Hasil Pengujian Implementasi *System*

No	Tipe *File*	Enkripsi		Dekripsi	
		Ukuran (byte)	Waktu (second)	Ukuran (byte)	Waktu (second)
1.	Txt	176	0.0005	137	0.0006
2.	Rar	13.424	0.0004	13.388	0.0009
3.	Docx	280.752	0.0013	280.714	0.0018
4.	Jpg	5.152	0.0004	5.113	0.0004
5.	Mp3	9.685.520	0.0313	9.685.485	0.0317
6.	Mp4	50.642.368	0.1671	50.642.336	0.1831
7.	Pdf	7.460.704	0.0293	7.460.661	0.0391

Dari percobaan *system* terhadap beberapa *file* yang berekstensi berbeda, didapatkan hasil seperti tabel diatas. Pada tabel diatas terdapat *file* yang berbeda-beda ekstensi. Dari tabel diatas menyatakan bahwa setiap *file* yang telah dienkripsi akan mengalami penambahan ukuran, tetapi setelah dilakukan deskripsi ukuran akan kembali ke ukuran *file* asli. Berdasarkan table 4.2 dapat dilihat bahwa waktu yang diperlukan untuk melakukan dekripsi file memiliki waktu yang lebih lama dibanding saat melakukan enkripsi. Hal ini disebabkan karena adanya perbedaan ukuran pada file yang diproses. File yang didekripsi memiliki ukuran lebih besar

dibandingkan dengan ukuran file yang dienkripsi karena adanya penambahan header yang berisi informasi ekstensi file.

BAB V
KESIMPULAN DAN SARAN

A. KESIMPULAN

Berdasarkan pemaparan dari Bab I, II, dan III maka peneliti dapat menyimpulkan beberapa hal sebagai berikut:

1. *Algoritma Advanced Encryption System* (AES) 256 terbukti mampu melakukan enkripsi *file* menjadi lebih *secure*.
2. Berdasarkan tabel hasil pengujian dapat dilihat bahwa enkripsi AES dapat menambah ukuran *file*, tetapi setelah *file* didekripsi ukuran akan Kembali seperti semula.
3. Berdasarkan hasil pengujian, *system* ini bekerja dengan baik dalam melakukan enkripsi, mengirim *file*, dan dekripsi sehingga sangat membantu dalam mengamankan *file* informasi dari pihak yang tidak bertanggung jawab.

B. SARAN

Saran penulis setelah melakukan penelitian ini adalah sebagai berikut. Saran ini disampaikan guna mengembangkan sistem sehingga di dapat sistem yang lebih baik lagi.

1. *Object* penelitian dapat lebih diperluas agar lebih bermanfaat untuk pengguna.
2. Algoritma yang digunakan untuk proses enkripsi-dekripsi dapat diterapkan dengan algoritma lain.
3. Penulis menyarankan menambahkan sistem otentikasi supaya pihak penerima dan pengirim dapat mengetahui identitas masing-masing serta sumber *data* yang sedang digunakan.

DAFTAR PUSTAKA

[1] G. W. Bhaudhayana and I. M. Widiartha, "Implementasi algoritma kriptografi aes 256 dan metode steganografi lsb pada gambar bitmap," *Jurnal ilmu komputer Universitas Udayana*, vol. 8, no. 2, pp. 15–25, 2015.

[2] "Pembuatan Sockets," *School of Computer Science*. https://socs.binus.ac.id/2020/11/16/pembuatan-sockets/ (accessed Feb. 05, 2022).

[3] M. K. ANam, D. Sudyana, A. N. Ulfah, and N. Lizarti, "Optimalisasi penggunaan virtualbox sebagai virtual computer laboratory untuk kegiatan praktikum," *J-PEMAS-Jurnal Pengabdian Masyarakat*, vol. 1, no. 2, pp. 39–44, 2020.

[4] F. M. Alwy, "MASKER DETEKTOR SEBAGAI HAK AKSES PINTU MASUK GEDUNG B POLITEKNIK HARAPAN BERSAMA MENGGUNAKAN WEB CAMERA BERBASIS RASPBERRY PI," PhD Thesis, Politeknik Harapan Bersama Tegal, 2021.

[5] "s-1621013-chapter2.pdf." Accessed: Feb. 07, 2022. [Online]. Available: http://repository.uib.ac.id/2396/5/s-1621013-chapter2.pdf

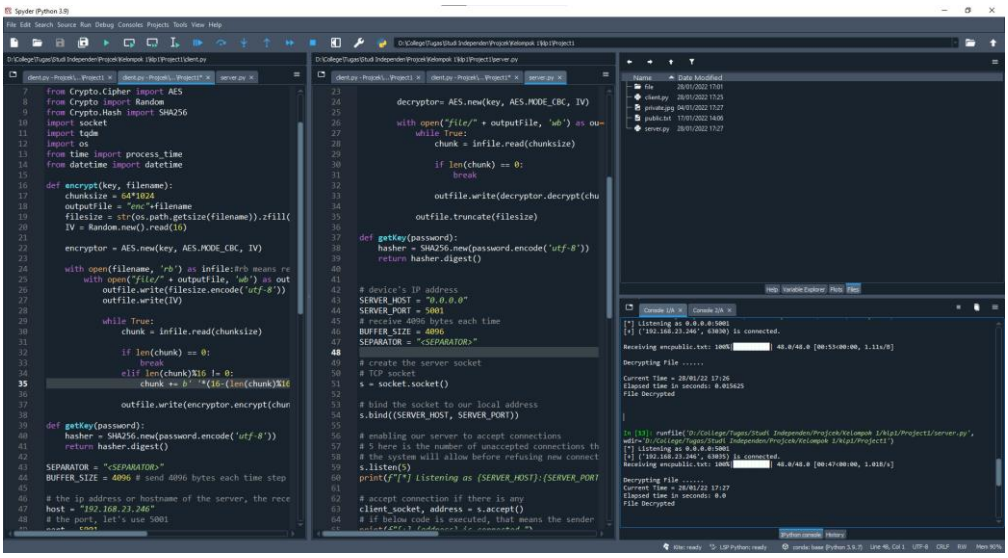
[6] "Cara Install Spyder Python IDE di Windows," *Advernesia*, Sep. 22, 2021. https://www.advernesia.com/blog/python/cara-install-spyder-python-ide-di-windows/ (accessed Feb. 07, 2022).

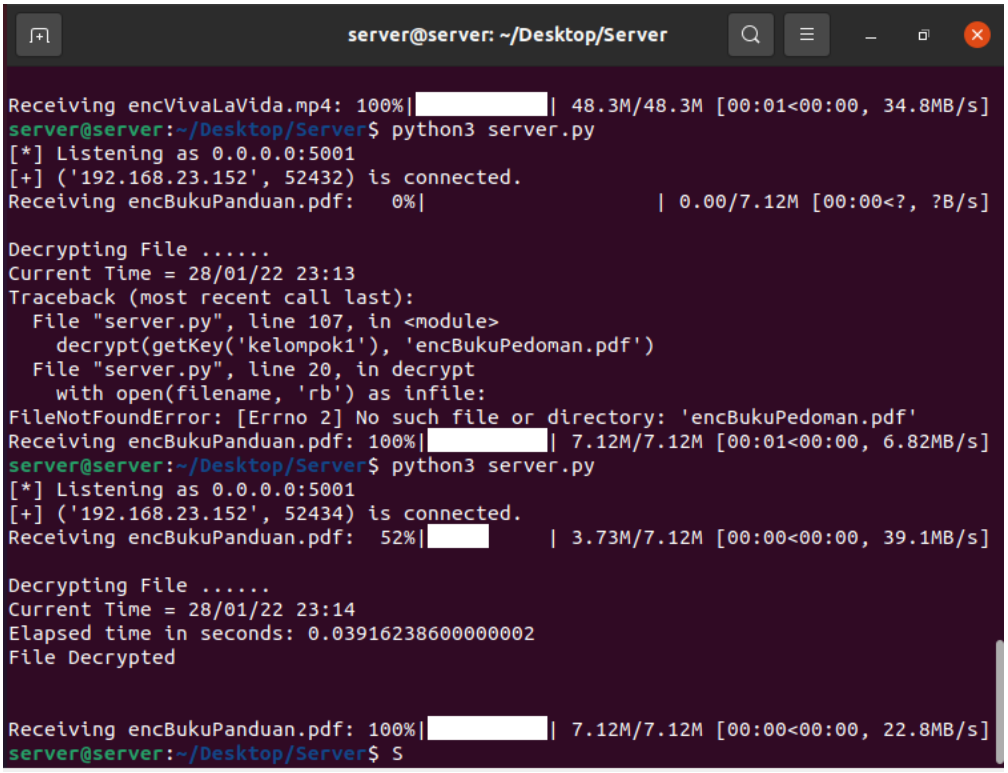
[7] "Pengertian Ubuntu Adalah | Sejarah, Jenis, Kelebihan & Kekurangan," *Dianisa.com*, Mar. 26, 2021. https://dianisa.com/pengertian-ubuntu/ (accessed Feb. 07, 2022).

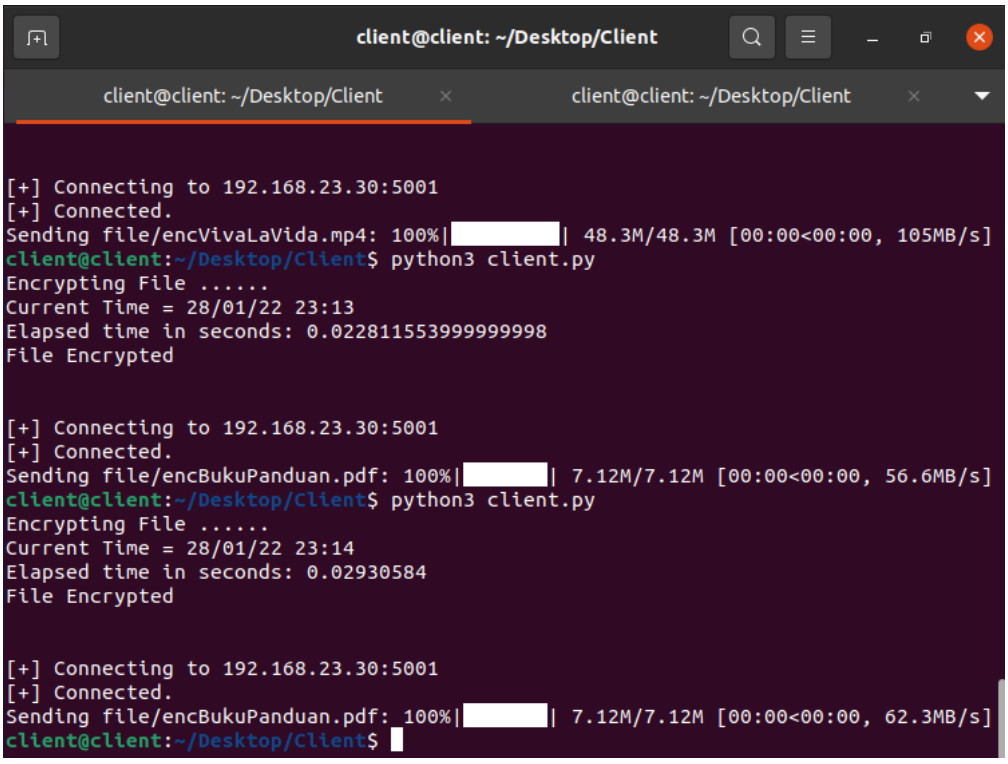
[8] M. Ahlgren, "Apa itu Enkripsi AES-256 dan Bagaimana Cara Kerjanya?," 2022. https://www.websiterating.com/id/cloud-storage/what-is-aes-256-encryption/ (accessed Jan. 28, 2022).

LAMPIRAN


REKAM
MUHAMMAD ...
RICHI RIYAN
Muhammad P...
IMAM YULIANO
ENGGAR YU...
THOBIB KHOI...
REZA FAJRITA...
ANGGA BAGUS
ANGGIH WIS...
ANETA SYAH ...
THIRAFI DZAKI ...
DEVA OURELIA
VENDIANTO B...
MUH. FAHMI
RAHMAT PUT...
LANANG PRAY...
EKA AYU
ALIF HASANUD...
THOFAN MALIY...
MELLIANA TIFF...
FERDY RAKA...
TIO SASMITA
ADITYA NURC...
FENI WIDIANTI
RAFFIKA HAN...
IKHLASUL AM...
DIGKY REVAN
KHARISMA RI...
NAREZA OCHA
NUR AZIZAH
ANANDYA SAL...
THIRAFI DZAK...
Fida Sabriani
LEFI NUR AN...
17 lainnya
Anda
20.01 | Bincang-bincang MBKM




server@server: ~/Desktop/Server
Receiving encVivaLaVida.mp4: 100%| | 48.3M/48.3M [00:01<00:00, 34.8MB/s]
server@server:~/Desktop/Server$ python3 server.py
[*] Listening as 0.0.0.0:5001
[+] ('192.168.23.152', 52432) is connected.
Receiving encBukuPanduan.pdf: 0%| | 0.00/7.12M [00:00<?, ?B/s]
Decrypting File ......
Current Time = 28/01/22 23:13
Traceback (most recent call last):
File "server.py", line 107, in <module>
decrypt(getKey('kelompok1'), 'encBukuPedoman.pdf')
File "server.py", line 20, in decrypt
with open(filename, 'rb') as infile:
FileNotFoundError: [Errno 2] No such file or directory: 'encBukuPedoman.pdf'
Receiving encBukuPanduan.pdf: 100%| | 7.12M/7.12M [00:01<00:00, 6.82MB/s]
server@server:~/Desktop/Server$ python3 server.py
[*] Listening as 0.0.0.0:5001
[+] ('192.168.23.152', 52434) is connected.
Receiving encBukuPanduan.pdf: 52%| | 3.73M/7.12M [00:00<00:00, 39.1MB/s]
Decrypting File ......
Current Time = 28/01/22 23:14
Elapsed time in seconds: 0.03916238600000002
File Decrypted
Receiving encBukuPanduan.pdf: 100%| | 7.12M/7.12M [00:00<00:00, 22.8MB/s]
server@server:~/Desktop/Server$ S


client@client: ~/Desktop/Client
client@client: ~/Desktop/Client
client@client: ~/Desktop/Client
[+] Connecting to 192.168.23.30:5001
[+] Connected.
Sending file/encVivaLaVida.mp4: 100%| | 48.3M/48.3M [00:00<00:00, 105MB/s]
client@client:~/Desktop/Client$ python3 client.py
Encrypting File ......
Current Time = 28/01/22 23:13
Elapsed time in seconds: 0.022811553999999998
File Encrypted
[+] Connecting to 192.168.23.30:5001
[+] Connected.
Sending file/encBukuPanduan.pdf: 100%| | 7.12M/7.12M [00:00<00:00, 56.6MB/s]
client@client:~/Desktop/Client$ python3 client.py
Encrypting File ......
Current Time = 28/01/22 23:14
Elapsed time in seconds: 0.02930584
File Encrypted
[+] Connecting to 192.168.23.30:5001
[+] Connected.
Sending file/encBukuPanduan.pdf: 100%| | 7.12M/7.12M [00:00<00:00, 62.3MB/s]
client@client:~/Desktop/Client$