STORAGE – Jurnal Ilmiah Teknik dan Ilmu Komputer, Vol. 1 No. 1, Februari, 2022, 32-37
e-ISSN: 2828-5344 | DOI : 10.55123

# PEMANFAATAN ALGORITMA AES UNTUK KEAMANANN DATA KARYAWAN PT. TELKOM INDONESIA PEMATANGSIANTAR

**M. Fahri H Damanik[1*], Indra Gunawan[2], Zulaini Masruro Nasution[3], S Sumarno[4], Ika Okta Kirana[5]**
[1]Program Studi Teknik Informatika, STIKOM Tunas Bangsa, Pematangsiantar, Indonesia
*fahridamanik99@gmail.com

**INFO ARTIKEL**

**Riwayat Artikel :**
Diterima : 28 Februari 2022
Disetujui : 28 Februari 2022

**Kata Kunci :**
Keamanan data, AES, Enkripsi, Dekripsi

**ABSTRAK**

PT. TELKOM Indonesia (Persero) tbk merupakan Badan Usaha Milik Negara (BUMN) yang bergerak dibidang jasa layanan teknologi, informasi dan komunikasi (TIK). Pemegang saham mayoritas Telkom adalah Pemerintah Republik Indonesia sebesar 52.09%, sedangkan 47.91% sisanya dikuasai oleh Publik. Perusahaan tersebut menggunakan teknologi komputer yang diterapkan dalam pelayanannya, Penggunaan komputer dalam penyimpanan data karyawan maupun data-data penting yang bersifat rahasia lainnya. Untuk menghindari terjadinya pencurian dan manipulasi data maka perlu diterapkannya sebuah sistem keamanan. Salah satu metode yang dapat digunakan dalam pengamanan data atau informasi adalah algoritma Advanced Encryption Standard (AES). Penerapan algoritma kriptografi AES dalam pengamanan data menunjukkan bahwa algoritma ini dapat menghasilkan enkripsi yang tidak dapat dibaca atau dimengerti manusia dan menghasilkan dekripsi yang sama persis dengan data awal yang di inputkan. Perbedaan kunci yang digunakan serta ukuran suatu file ikut mempengaruhi waktu yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi.

***ARTICLE INFO***

***Article History :***
*Received : February 28, 2022*
*Accepted : February 28, 2022*

***Keywords****:*
*Data security, AES, Encryption, Decrypt*

***ABSTRACT***

*PT. TELKOM Indonesia (Persero) tbk is a State-Owned Enterprise (BUMN) which is engaged in technology, information and communication (ICT) services. Telkom's majority shareholder is the Government of the Republic of Indonesia with 52.09%, while the remaining 47.91% is controlled by the public. The company uses computer technology that is applied in its services, the use of computers in storing employee data and other important confidential data. To avoid theft and manipulation of data, it is necessary to implement a security system. One method that can be used in securing data or information is the Advanced Encryption Standard (AES) algorithm. The application of the AES cryptographic algorithm in securing data shows that this algorithm can produce encryption that cannot be read or understood by humans and produces an exact decryption of the initial data entered. The difference in the key used and the size of a file also affect the time it takes to perform the encryption and decryption process.*

## 1. PENDAHULUAN

File merupakan hasil pekerjaan yang berharga, terkadang pekerjaan itu tidak dapat diulangi. Boleh dikatakan data yang tersimpan dan dikirim dari komputer biasanya jauh lebih penting dari pada komputer itu sendiri (Ningsih and Saniati 2018). File mungkin berharga dan tidak dapat diganti, sehingga dibutuhkan

pengamanan. Pengamanan merupakan suatu hal yang sangat penting untuk melindungi sesuatu yang bersifat rahasia (Laoli, Sinaga, and Sinaga 2020; Manurung 2019; Perwira, Prasetyo, and Haryanto 2020). Pengamanan dilakukan agar apa yang dianggap rahasia bisa terjaga kerahasiaan nya dari hal yang tidak di inginkan (Aziz 2020; Malvi and Painem 2020; Simbolon et al. 2020).

Keamanan informasi merupakan suatu perlindungan informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau penghancuran yang tidak sah untuk memberikan kerahasiaan, integritas, dan ketersediaan informasi (Achmad and Agustina 2019). Keamanan informasi merupakan satu hal yang sangat penting yang harus dilakukan. Pada era sekarang ini sangat rawan pencurian dan penyalahgunaan data dari orang-orang yang tidak bertanggung jawab (Prasetyo et al. 2021). Akan tetapi, kasus keamanan ini kurang menerima perhatian menurut para pemilik dan pengelola sistem informasi, serta banyaknya perusahaan yang menghubungkan sistem informasinya dengan jaringan internet. Hal ini membuka akses secara global (maksud akses ini menjadi target dan pula menjadi penyerang).

Untuk menghindari terjadinya pencurian dan peretasan data maka perlu diterapkan sebuah system keamanan gunamenjaga data dari potensi pencurian. Kriptografi adalah suatu bagian penting yang melekat dengan system keamanan. Advanced Encyption System (AES) merupakan salah satu algoritma dalam kriptografi yang dapat digunakkan untuk mengamankan data (Fauzi et al. 2017). Penelitian sebelumnya membahas tentang Penerapan Algoritma AES: Rijndael dalam Mengenkripsi Data Rahasia (Alyanto 2016). Pada penelitian ini membahas tentang penerapan algoritma kriptografi Rijndael dalam pengamanan data. Dimulai dengan menganalisis cara kerja algoritma Rijndael dan kemudian merancang aplikasi yang dapat mengenkripsi dan mendekripsi input pengguna plaintext. Hasil evaluasi menunjukkan bahwa algoritma Rijndael dapat menghasilkan enkripsi yang tidak dapat dipahami oleh orang biasa, dan menghasilkan dekripsi yang tepat dari input plaintext awal oleh pengguna. Disini penulis menerapkan metode keamanan data yaitu AES (Advanced Encryption Standard) yang merupakan standar enkripsi kunci simetris yang diadopsi oleh pemerintah Amerika Serikat. Algoritma AES merupakan sistem pengkodean blok non-feistel karena AES menggunakan komponen yang selalu memiliki invers dengan panjang blok 128. Algoritma AES menggunakan proses berulang yang disebut putaran. jumlah putaran yang digunakan oleh AES tergantung pada panjang kunci yang digunakan. Setiap putaran membutuhkan kunci putaran dan masukan dari putaran berikutnya (Rumani 2015).

Dari permasalahan yang tertera diatas membuat penulis untuk melakukan penelitian terkait pengamanan dan perahasiaan file dengan menggunakan algoritma AES (Advanced Encryption Standard). Algoritma AES merupakan algoritma kriptografi yang dapat digunkan untuk mengamakan data. Algoritma AES adalah teknik penyembunyian data rahasia ke dalam sebuah wadah (media) sehingga data yang disembunyikan sulit untuk dikenali oleh indera manusia. Dengan adanya penelitian ini dapat dijadikan masukan bagi pegawai untuk membantu mencegah tindakan pencurian file dan dapat menjaga reputasi perusahaan untuk menjaga privasi dari pegawai.

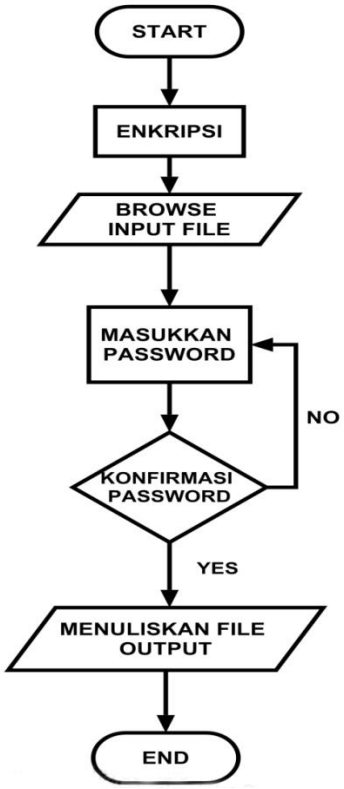
## 2. METODE

### 2.1. Pengumpulan Data

1. Metode Penelitian (Observasi)
   Dengan metode observasi penulis mendapatkan data dengan cara mendatangi langsung objek yang dijadikan tempat riset.
2. Metode Wawancara (Interview)
   Interview yang berupa tanya jawab penulis lakukan kepada beberapa staff yang terkait langsung dengan instansi.
3. Metode Study Pustaka (Library Search)
   Metode ini dilakukan guna mendapatkan gambaran secara teoritis yang berkaitan dengan penulisan laporan penelitian sebagai acuan. Penulis mengumpulkan data yang bersumber dari materi yang didapat semasa kuliah, seperti modul pemrograman PHP, berbagai buku panduan dalam mengerjakan laporan penelitian, contoh laporan-laporan terdahulu yang dibuat oleh para

mahasiswa yang sudah melakukan penelitian.

### 2.2. Tahapan Enkripsi File

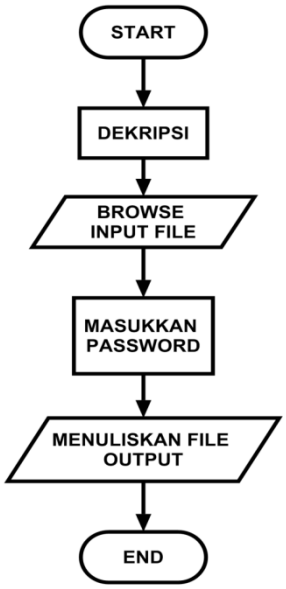



Gambar 1. Tahapan Enkripsi File

Tahapan enkripsi *file* dengan aplikasi kriptografi ini adalah sebagai berikut :

1. Lakukan enkripsi *file.*
2. Pilih *file y*ang akan dienkripsi. Dalam program ini ada beberapa tipe *file* yang dapat diinputkan, seperti : *.doc, .xls, .ppt, .pdf, .jpg dan .png*.
3. Masukkan *password* dan konfirmasi *password*. *Password* yang dimasukkan sesuai dengan keinginan *user*.
4. Program akan melakukan proses enkripsi *file* dan kemudian menuliskan *file* output. *File* hasil enkripsi akan tersimpan secara langsung di direktori yang sama dan menggantikan *file* asli.

### 2.3. Tahapan Dekripsi File



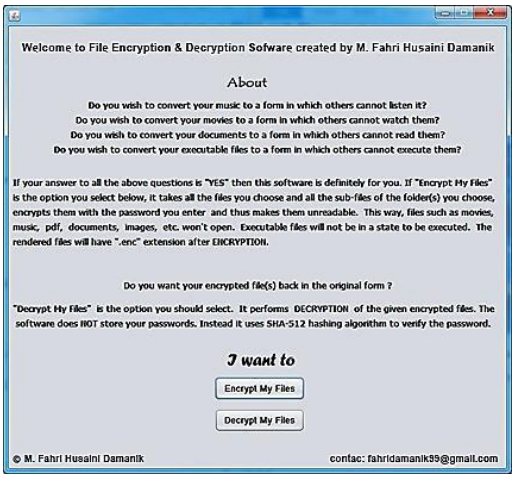

Gambar 2. Tahapan Dekripsi File

Tahapan dekripsi *file* dengan aplikasi kriptografi ini adalah sebagai berikut:

1. Lakukan dekripsi *file.*
2. Pilih *file* yang akan didekripsi (dengan ekstensi *.enc*).
3. Masukkan *password* yang digunakan saat proses enkripsi.
4. Program akan melakukan proses dekripsi *file* dan kemudian menuliskan *file* output. *File* hasil dekripsi akan tersimpan secara langsung di direktori yang sama dan kembali menjadi *file* asli

## 3. HASIL DAN PEMBAHASAN

Pada hasil ini ada 2 peran penting pada aplikasi ini, yaitu untuk melakukan enkripsi dan dekripsi *file*, yang mana dapat kita akses melalui menu utama, seperti gambar 3 berikut.

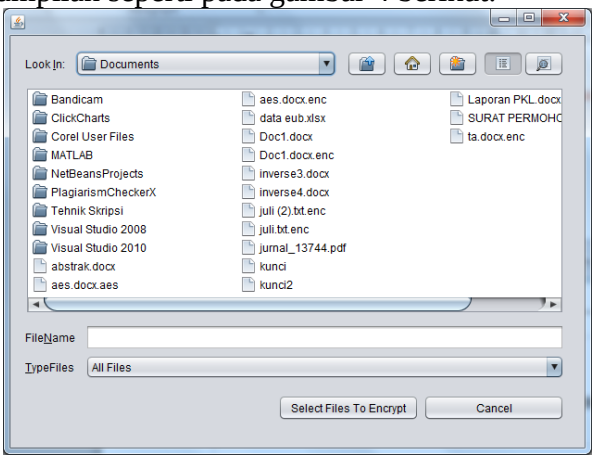



Gambar 3.Tampilan Menu Utama

Pada gambar 3 dapat dilihat bahwa menu utama terdapat 2 pilihan, yaitu *Encrypt My Files* dan *Decrypt My Files*.

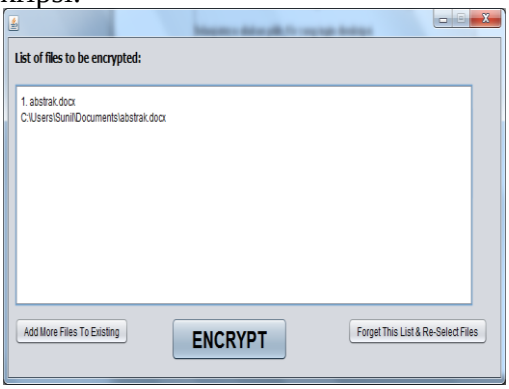
### 3.1. Tahapan Proses Enkripsi

Tahapan proses enkripsi file menggunakan aplikasi kriptografi ini adalah sebagai berikut : Pada menu utama terdapat pilihan 'Encrypt Files' dan saat menu ini klik maka muncul tampilan seperti pada gambar 4 berikut.




Gambar 4.Tampilan *Select File To Encrypt*

Selanjutnya silahkan pilih *file* yang ingin dienkripsi.




Gambar 5. Tampilan Daftar *File* Yang Akan Di enkripsi

Setelah tombol '*ENCRYPT'* diklik maka akan muncul *form* untuk meng-*input*-kan *password*.


Gambar 6. Tampilan *Insert Password To Encrypt*

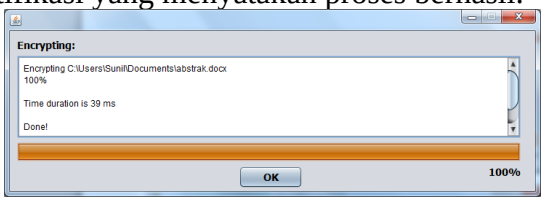
Adapun panjang *password* yang di-*input* harus sesuai atau tidak melebihi panjang *password* yang ditentukan. Untuk *AES* dengan panjang 128 *bit* berarti 16 *byte* (16 karakter). Apabila melanggar aturan tersebut maka program akan muncul pesan peringatan "*The password must be 16 characters in length*"


Gambar 7. Tampilan Pesan *Warning 1*

Selanjutnya akan diminta meng-*input* ulang *password* yang sama untuk proses verifikasi jika, *password* yang di-*input*-kan berbeda maka akan muncul pesan *warning* "*The passwords don't match!*"


Gambar 8. Tampilan Pesan *Warning 2*

Setelah kedua *password* cocok maka proses enkripsi akan dilakukan dan akan muncul notifikasi yang menyatakan proses berhasil.

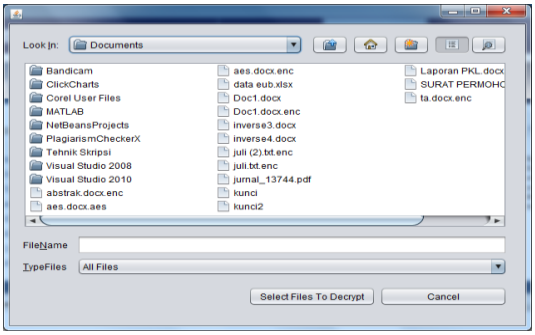



Gambar 9. Tampilan Proses Enkripsi Berhasil

### 3.2. Tahapan Proses Dekripsi

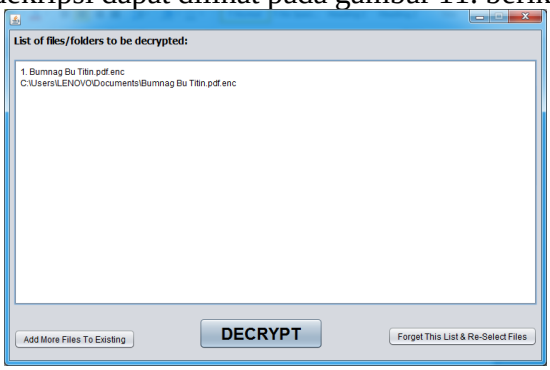
Tahapan dekripsi *file* menggunakan aplikasi kriptografi ini adalah sebagai berikut:

Pada menu utama terdapat pilihan '*Decrypt Files*' dan saat menu ini diklik maka akan muncul tampilan seperti pada gambar 10. berikut.



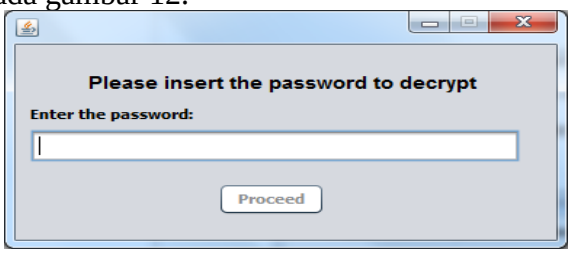

Gambar 10. Tampilan *Select File To Decrypt*

Selanjutnya silakan pilih *file* yang ingin didekripsi dapat dilihat pada gambar 11. berikut.



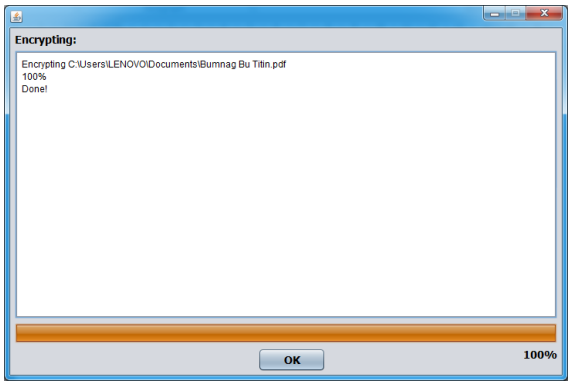

Gambar 11. Tampilan Daftar *File* Yang Akan Dideskripsi

Setelah tombol '*DECRYPT'* diklik maka akan muncul *form* untuk meng-*input*-kan *password*. *Password* yang diinputkan harus sesuai dengan *password* yang di-*input*-kan saat proses enkripsi. Apabila *password* yang di-*input*-kan berbeda maka tombol '*Proceed*' tidak dapat diklik. Maka akan muncul tampilan seperti pada gambar 12.



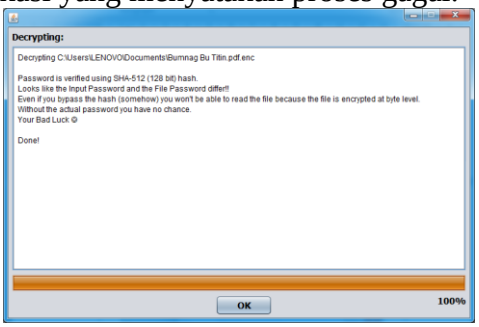

Gambar 12. Tampilan Insert Password To Decrypt

Setelah *password* cocok maka proses dekripsi akan dilakukan dan akan muncul notifikasi yang menyatakan proses berhasil. Dapat dilihat pada gambar 13.




Gambar 13. Tampilan Proses Dekripsi Berhasil

Jika *password* tidak cocok maka proses dekripsi tidak akan dilakukan dan muncul notifikasi yang menyatakan proses gagal.




Gambar 14. Tampilan Proses Dekripsi Gagal

Proses dekripsi adalah proses mengubah *ciphertext* menjadi *plaintext* yang bertujuan untuk mengubah data atau isi pesan yang terenkripsi agar dapat dibaca dan dipahami maknanya. Untuk melihat apakah *file* yang akan didekripsi dapat dibaca dan dipahami maknanya maka perlu dilakukan analisis isi *file*

## 4. PENUTUP

### 4.1. Kesimpulan

Setelah selesai melakukan analisis, implementasi serta perangcangan menggunakan algoritma *Advance Encryption Standard (AES)* dapat ditarik kesimpulan sebagai berikut : Dengan adanya system keamanan data karyawan pada PT. TELKOM Indonesia Pematangsiantar dapat terbantu dalam mengamankan data-data yang bersifat rahasia. Setelah dilakukan analisis maka dapat di lihat bahwa algoritma *AES* dapat mengamankan *file* dengan berbagai ekstensi, seperti : *doc, xls, ppt, pdf* dan juga *png*. Hasil dari data yang di enkripsi merupakan kumpulan kombinasi karakter yang tidak dapat dimengerti oleh manusia. Dengan menggunakan kunci yang sama maka hasil Enkripsi dan Dekripsi maka hasilnya akan selalu sama.

### 4.2. Saran

Adapun beberapa saran yang dapat diberikan penulis untuk meningkatkan system keamanan data karyawan ini adalah sebagai berikut : Penelitian ini dapat dikembangkan dengan menggunakan algoritma lain seperti *Blowfish, Twofish, RC6* dan lain-lain. Dapat menambah fitur untuk mengenkripsi *file* dengan ekstensi beragam. Dapat dikembangkan dengan bahasa program lain seperti *Visual Basic, C++, PHP,* dan sebagainya.

## 5. DAFTAR PUSTAKA

Achmad, Faizal, and Esti Rahmawati Agustina. 2019. "Perancangan Spesifikasi Keamanan Kontrol Akses Pada Aplikasi Layanan Informasi Di Lingkungan Instansi Pemerintah." *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)* 6(2): 195–200.

Alyanto, Dedi. 2016. "PENGENKRIPSIAN DATA RAHASIA."

Aziz, A. 2020. "Aplikasi Keamanan Data Multimedia Message Service (MMS) Pada Microsoft Office File Memanfaatkan Algoritma Rivest-Shamir Adleman (RSA) Dan Blowfish Berbasis Android." *Jurnal Ilmu-ilmu Informatika dan Manajemen STMIK* 14(2): 144–53. http://digilib.uinsgd.ac.id/2782/.

Fauzi, Achmad, Novriyenni, Yani Maulita, and Akim M.H. Pardede. 2017. "ANALISIS HYBRID CRYPTOSYSTEM ALGORITMA ALGORITMA RSA DAN TRIPLE DES." 1(2): 36–44.

Laoli, Desimeri, Bosker Sinaga, and Anita Sindar R M Sinaga. 2020. "Penerapan Algoritma Hill Cipher Dan Least Significant Bit (LSB) Untuk Pengamanan Pesan Pada Citra Digital." *JISKA (Jurnal Informatika Sunan Kalijaga)* 4(3): 138–47.

Malvi, Afif, and Painem Painem. 2020. "Pengamanan File Gambar Pada Media Video Dengan Kriptografi Algoritma RSA Dan Steganografi Algoritma End of File (EOF)." *Informatik : Jurnal Ilmu Komputer* 16(2): 67–74.

Manurung, Modesty Sri Pebriyani. 2019. "Penerapan Algoritma Advanced Encryption Standard Dalam Mengamankan File Pada Citra Dengan Metode Least Significant Bit." *Jurnal Teknik Informatika Unika St. Thomas (JTIUST)* 4(1): 62–69.

Ningsih, Sri, and Saniati Saniati. 2018. "Eksperimen Pengenalan Ucapan Aksara Lampung Dengan CMU Sphinx 4." *Jurnal Teknoinfo* 12(1): 33.

Perwira, Rifki Indra, Dessyanto Boedi Prasetyo, and Fandi Ahmad Juni Haryanto. 2020. "Steganografi Dengan AES Pada Media Suara Berbasis Internet." *Telematika* 17(1): 18–25.

Prasetyo, Kevin Yoga et al. 2021. "Pengaruh E-Commerce Terhadap Tindak Kejahatan Siber Di Era Milenium Untuk Generasi Milenial Kevin." *Journal of Education and Technology* 1(2): 81–86.

Rumani, R. 2015. "Desain Dan Implementasi Aplikasi Sms (Short Message Service) Pada Android Menggunakan Algoritma AES." *e-Proceeding of Engineering* 2(2): 3318–26.

Simbolon, Imelda Asih Rohani et al. 2020. "Penerapan Algoritma AES 128-Bit Dalam Pengamanan Data Kependudukan Pada Dinas Dukcapil Kota Pematangsiantar." *Journal of Computer System and Informatics (JoSYC)* 1(2): 54–60.