BAB 1
PENDAHULUAN

Pada bab ini akan menjelaskan tentang latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan kerangka penelitian. Dari uraian yang dijabarkan, diharapkan dapat menguraikan permasalahan dan dapat menyelesaikan permasalahan yang ada.

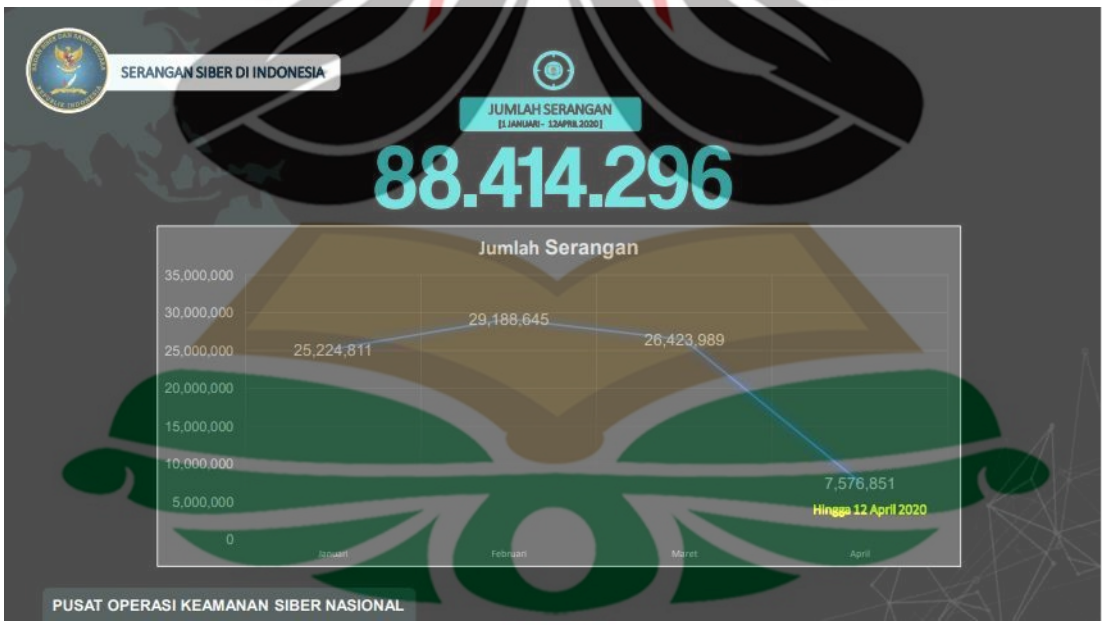
1.1 Latar belakang

Perkembangan teknologi informasi dan komunikasi pada era digitalisasi saat ini telah berkembang sangat cepat dan sangat berpengaruh dalam kehidupan manusia. Dalam penggunaan komputerisasi, maka diperlukan keamanan aset informasi, mulai dari aset pribadi hingga aset organisasi. Semua aset informasi yang diberi keamanan, maka secara langsung maupun tidak langsung akan dihadapi dengan kejahatan komputer. Para pelaku kejahatan komputer yang tidak bertanggung jawab akan mengincar semua informasi yang sebuah instansi miliki. Karena semua informasi yang di miliki sangat rentan terhadap risiko (Simarmata, et al., 2020). Informasi merupakan hal yang sangat penting bagi sebuah organisasi, oleh karena itu diperlukan persiapan untuk mengamankan informasi. Persiapan yang dilakukan dapat mengurangi kerugian yang akan menimpa suatu organisasi jika data atau informasi organisasi tersebut disalahgunakan oleh pihak yang tidak bertanggung jawab.

Persiapan agar memperkecil kerugian dapat dilakukan dengan mengamankan data dan informasi. Hal ini dikarenakan keamanan dan kerahasiaan menjadi aspek yang sangat penting bagi pengguna teknologi informasi (Anwar, 2017). Aset pribadi maupun aset organisasi sangat penting dan rentan terhadap pihak-pihak yang tidak berkepentingan untuk mendapatkan apa yang mereka inginkan. Dari semua aset yang mereka

dapatkan, mereka dapat menyalahgunakan data tersebut. Dan untuk menjaga aset pribadi maupun organisasi dari para pelaku kejahatan teknologi informasi dapat diminimalisir dengan melakukan pengamanan data dan informasi yang penting. Dalam dunia internet, banyak kejahatan yang memicu untuk menyalahgunakan informasi yang didapatkan untuk kepentingan diri sendiri maupun kepentingan kelompok.

Kejahatan yang terjadi melalui internet sudah banyak terjadi. Dimana kejahatan ini akan memanfaatkan celah yang kecil sekalipun untuk melakukan kejahatan. Para pelaku kejahatan ini akan melakukan apa saja agar yang mereka inginkan tercapai. Pada rekap serangan siber yang ada di BSSN (Badan Siber dan Sandi Negara) telah diungkapkan jika pada tahun 2020 telah terjadi banyak serangan siber yang dimulai dari tanggal 1 Januari hingga 12 April. Dimana insiden siber merupakan suatu kejadian dimana hal ini akan menyebabkan system akan mengalami gangguan. Gangguan pada sistem ini dapat berupa pencurian data, informasi pribadi, serangan virus, *web defacement*, hak kekayaan intelektual perusahaan, dan gangguang pada akses di layanan elektronik (Negara, 2020). Berikut ini merupakan jumlah serangan dari awal Januari hingga bulan April.



Gambar 1. 1 Jumlah Serangan (Negara, 2020)

www.itk.ac.id

Pada **Gambar 1.1** terdapat grafik jumlah serangan di Indonesia tahun 2020. Dimana terjadi peningkatan pada bulan Februari sebanyak 29.188.645 serangan. Urutan kedua pada bulan Maret dengan total serangan sebanyak 26.423.989. Dan pada bulan Januari serangan mencapai angka 25.224.811 serangan. Dan mengalami penurunan drastis pada bulan April, sehingga serangan siber menjadi sebanyak 7.576.851 serangan. Dari banyaknya serangan siber yang terjadi di tahun 2020, maka hal ini perlu disikapi oleh organisasi agar dapat memperbaiki kebijakan terkait keamanan informasi untuk menghindari serangan siber. Dengan memiliki persiapan yang baik, maka dapat memperkecil kerugian akibat informasi yang dicuri atau meminimalisir gangguan pada layanan (Negara, 2020).

Dari penjelasan terkait data kejahatan internet dapat diketahui bahwa setiap tahun kejahatan internet pasti akan selalu terjadi. Dan ini merugikan bagi semua orang, khususnya bagi sebuah organisasi. Karena hal ini akan berdampak bagi pelayanan yang mereka berikan, bisnis yang mereka jalankan, dan lain sebagainya. Dari berbagai kerugian yang akan dialami organisasi, maka informasi yang ada perlu dijaga kerahasiaan dan keamanannya, ada berbagai cara untuk mengamankan data, seperti dengan menyembunyikan atau menyisipkan ke media lainnya. (Ika Yusnita Sari, 2020). Teknik untuk mengamankan data tergantung dari kebutuhan dari setiap organisasi yang membutuhkan.

Pada salah satu organisasi, yaitu Dinas Komunikasi dan Informatika Penajam Paser Utara. Permasalahan utama yang ada di dinas tersebut adalah terkait dengan keamanan data yang kurang maksimal. Hal ini didukung oleh 2 faktor, yaitu komputer yang masih digunakan bersama dan penerapan kriptografi yang masih kurang maksimal. Dilihat dari faktor pertama, pada dinas tersebut dalam penggunaan komputer yang masih digunakan secara bersama. Karena penggunaan yang bersamaan, data yang ada di satu komputer akan sangat rawan untuk disalahgunakan. Bisa saja data tersebut dapat disalahgunakan oleh pihak yang tidak memiliki kepentingan. Jika data telah disalahgunakan, maka akan berpengaruh pada dinas tersebut terkait dengan kinerja dan data yang disalahgunakan. Faktor kedua terkait dengan

www.itk.ac.id

teknik kriptografi yang telah diterapkan di dinas tersebut. Aplikasi yang diterapkan di dinas tersebut menggunakan teknik kriptografi dengan nama Stoner. Setelah diterapkannya Stoner ternyata keamanan datanya masih kurang maksimal. Hal ini dikarenakan dari hasil pengamanan data yang telah dienkripsi dapat menimbulkan rasa curiga pihak lain untuk menganalisis atau bahkan mengungkapkan pesan yang telah dienkripsi. Jika pesan yang telah dienkripsi diungkap oleh pihak yang tidak memiliki kepentingan akan menyebabkan masalah pada dinas terkait. Dari kedua faktor yang menjadi pendukung untuk masalah utama di dinas ini, maka permasalahan ini menjadi hal yang harus diprioritaskan oleh pihak dinas untuk saat ini dan kedepannya. Selain dari faktor tersebut, dinas ini juga pernah mengalami kehilangan data. Data yang hilang merupakan data yang ada di dvisi keamanan, hal ini dikarenakan komputer yang digunakan bersamaan. Dilihat dari data yang telah disampaikan oleh pihak BSSN, kejahatan siber merupakan kejahatan yang akan selalu mengawasi setiap organisasi. Kejahatan ini pula dapat menyebabkan kerugian yang besar bagi organisasi.

Kejahatan di era saat ini pastinya lebih merujuk pada kejahatan melalui internet. Dimana para penjahat akan memanfaatkan celah sekecil apapun untuk mencapatkan data atau informasi yang diinginkan. Dan dan informasi merupakan aset yang sangat penting bagi organisasi, seperti Dinas Komunikasi dan Informatika Penajam Paser Utara. Pada dinas ini terdapat banyak sekali data. Setiap data yang ada akan diklasifikasikan menjadi beberapa klasifikasi. Ada data yang bersifat umum dan ada data yang bersifat rahasia. Data rahasia merupakan data yang harus dijaga kerahasiaan dan keamanannya. Dalam dinas ini, terdapat banyak data yang bersifat data rahasia, salah satunya adalah data terkait infrastruktur jaringan yang ada di dinas ini. Data infrastruktur jaringan yang ada di dinas ini harus dijaga agar tidak bocor dan kebocoran ini mengakibatkan kerugian bagi dinas. Data infrastruktur jaringan dianggap sebagai data rahasia karena data ini dapat meningkatkan produktivitas dan efisiensi dinas tersebut. Jika kerahasiaan data ini tidak ada, maka akan berdampak secara signifikan terhadap *revenue*

dinas dan pada pelayanan yang diberikan kepada masyarakat. Selain itu jika data tidak dijaga kerahasiaan dan keamanannya maka akan mengakibatkan sumber daya sistem akan dimodifikasi, interupsi, dan diganggu oleh pihak yang tidak berkepentingan. Oleh karena itu, diperlukan suatu teknik untuk mengamankan data selain menggunakan teknik kriptografi.

Dalam sebuah penelitian yang telah dilakukan, dengan mengkombinasikan algoritma kriptografi dan steganografi akan membuat data lebih aman karena memiliki keamanan yang lebih kuat. Salah satu cara untuk mengamankan data informasi yang penting adalah dengan menyisipkan data ini ke dalam media lain, hal ini juga disebut sebagai steganografi (Zahrul Basim, 2020). Dimana steganografi merupakan salah satu ilmu yang yang menerapkan algoritma dalam proses kinerjanya untuk menyisipkan data yang penting ke dalam sebuah media. Media yang digunakan bisa teks, gambar, suara, video, dan lainnya. Media yang digunakan untuk melapisi data informasi disesuaikan dengan kebutuhan organisasi. Namun, media yang sering digunakan adalah media gambar. Dimana media ini akan lebih efektif berdasarkan dari penelitian yang telah dilakukan sebelumnya. Media ini juga memiliki kapasitas yang medium untuk ukuran steganografi daripada teksa dan lain sebagainya (Widianto, 2018).

Steganografi memiliki kelebihan dimana *output* dari data yang disembunyikan tidak akan menimbulkan kecurigaan pihak luar. Hal ini dikarenakan steganografi menggunakan wadah penampung sebagai *cover* untuk menyembunyikan pesan yang perlu diamankan. Steganografi memiliki kaitan erat dengan *steganalysis*. Dimana *steganalysis* merupakan anti-steganografi sehingga dapat mengetahui apakah suatu *cover* telah disisipi pesan atau tidak disisipi pesan. Sebelum menerapkan sebuah teknik mengamankan data pada sebuah organisasi, maka diperlukannya analisis untuk menganalisis apakah teknik yang akan digunakan telah sesuai dengan kebutuhan atau tidak. Hal ini dikarenakan jika sebuah aplikasi yang digunakan tidak sesuai dengan algoritma dan kebutuhan, maka akan memiliki kesalahan yang fatal karena bisa saja penjahat akan lebih mudah

www.itk.ac.id

untuk melakukan kejahatan. Oleh karena itu, diperlukan analisis terkait dengan aplikasi dari steganografi agar dapat mengetahui algoritma yang diterapkan di aplikasi tersebut benar adanya (Rohmanu, 2017).

Pada teknik steganografi untuk melakukan analisis tekniknya disebut dengan *steganalysis. Steganalysis* digunakan untuk mengetahui algoritma yang ada di suatu aplikasi dari steganografi benar adanya atau tidak sesuai. Untuk melakukan *steganalysis* digunakan alat bantu yang dapat menentukan algoritma dan perhitungannya (Songtao Wu, 2017). Dimana terdapat banyak alat bantu yang dapat digunakan untuk membantu mengetahui perhitungan algoritma yang ada. Aplikasi untuk melakukan *steganalysis* menurut salah satu sumber terdapat beberapa aplikasi terkait *steganalysis*, yaitu Anubis, BDV DataHider, BMPSecrets, Camouflage, Cloak, CryptaPix, StegoShare, StegoStick, Stegosuite, Stegotif, StegSpy V2.I, Hex Editor Neo, dan lain sebagainya (Mukesh Dalal, 2020). Dari berbagai macam aplikasi yang ada, terdapat kekurangan dan kelebihan dari masing-masing aplikasi. Semua aplikasi ini digunakan berdasarkan keadaan suatu organisasi yang ingin menerapkan aplikasi ini untuk menjaga keamaan data yang ada.

Seperti pada penelitian yang dilakukan oleh Yudo Bismo Utomo dan Danang Erwanto pada tahun 2019 dengan judul Analisa Teknik Steganografi dan *Steganalysis* Pada File Multimedia Menggunakan Net Tools dan Hex Editor Neo. Permasalahan yang diangkat dalam jurnal ini terkait dengan keamanan data yang masih sangat kurang, dilihat dari semakin canggih perkembangan teknologi. Dan jurnal ini juga mengatakan bahwa jika dalam mengirim ppesan dan pihak yang tidak bertanggung jawab melihat celah kecil untuk disusupi, maka pihak yang tidak bertanggung jawab ini akan menyusupi celah tersebut dan mengambil data yang diinginkan. Oleh karena itu, dilakukan penelitian untuk menerapkan teknik yang dapat mengatassi permasalahan ini. Teknik yang digunakan adalah teknik steganografi dengan menggunakan Net Tools dan akan menganalisis dengan menggunakan Hex Editor Neo. Proses analisis ini dinamakan *steganalysis.* Setelah dilakukan penelitian, didapatkan hasil bahwa Net Tools memenuhi dua parameter dari steganografi, yaitu *fidelity*

dan *recovery*. Dan Hex Editor Neo dapat mendeteksi gambar yang telah disisipi pesan dan yang belum disisipi pesan (Yudo Bismo Utomo, 2019). Berdasarkan pada acuan penelitian ini, maka steganografi dan *steganalysis* dapat memaksimalkan keamanan dan kerahasiaan dari data dan informasi.

Dengan menerapkan teknik steganografi pada Dinas Komunikasi dan Informatika Penajam Paser Utara dapat menambah keamanan data rahasia yang dimiliki oleh dinas. Tetapi jika ingin menerapkan suatu teknik untuk mengamankan data, diperlukannya analisis terhadap apa yang akan diterapkan. Untuk teknik steganografi, diperlukan analisis *steganalysis* yang berguna untuk mengukur keakuratan dari teknik steganografi yang akan diterapkan. Analisis yang akan dilakukan akan sesuai dengan parameter dari steganografi, yaitu *imperceptibility*, *robustness*, *fidelity*, dan *recovery*. Pada parameter *imperceptibility*, perlu dilakukan penyebaran kuisioner yang berguna untuk mengetahui seberapa baik aplikasi steganografi menerapkan parameter ini. Dalam kuisioner akan berisi media digital yang telah disisipi pesan rahasia dan media digital yang belum disisipi pesan rahasia. Jika pada parameter *robustness* akan dilakukan operasi manipulasi para *stego image*, seperti *resize* dan *rotate*. Parameter ini berguna untuk mengetahui ketahanan *stego image* jika telah dimanipulasi. Kemudian untuk parameter *fidelity* akan menggunakan dua pengujian, yaitu dengan menyisipkan pesan rahasia ke dalam *cover image* yang berbeda-beda dan melakukan perhitungan MSE *(Mean Square Error)* dan PSNR *(Peak Signal to Noise Ratio)*. Dan untuk parameter yang terakhir adalah parameter *recovery*, parameter ini dilakukan dengan cara mengungkap kembali pesan yang telah disembunyikan. Keempat parameter ini dilakukan dengan subjektif dan objektif, sehingga menghasilkan hasil yang lebih akurat. Aplikasi steganografi yang akan dianalisis adalah OpenStego. Sedangkan untuk *steganalysis* menggunakan bantuan aplikasi Hex Editor Neo. Dengan permasalahan yang telah dijabarkan, maka penulis melakukan penelitian dengan judul "Analisis Teknik Steganografi pada Data di Dinas Komunikasi dan Informatika Penajam Paser Utara Menggunakan OpenStego dan Hex Editor Neo". Penelitian ini diharapkan dapat memberikan sebuah solusi untuk

www.itk.ac.id

mengamankan data rahasia dengan menggunakan teknik steganografi dan solusi ini dapat diimplementasikan di Dinas Komunikasi dan Informatika Penajam Paser Utara.

www.itk.ac.id

1.2 Perumusan Masalah

Berdasarkan dari latar belakang yang telah dijabarkan, terdapat permasalahan pada Dinas Komunikasi dan Informatika Penajam Paser Utara terkait dengan keamanan data dan informasi yang masih rentan dari berbagai serangan. Hal ini dapat mengakibatkan data dan informasi akan mengalami kejahatan internet, seperti pencurian data dan penyalahgunaan data. Oleh karena itu, berikut ini merupakan pertanyaan penelitian yang sesuai dengan rumusan permasalahan ini.

1. Bagaimana cara mengamankan data infrastruktur jaringan menggunakan teknik steganografi pada Dinas Komunikasi dan Informatika Penajam Paser Utara?
2. Bagaimana cara mengimplementasikan steganografi sebagai solusi dalam membantu mengamankan data infrastruktur jaringan pada Dinas Komunikasi dan Informatika Penajam Paser Utara dengan menggunakan OpenStego?
3. Bagaimana cara menganalisis steganografi dengan teknik analisis *steganalysis* sesuai dengan parameter *imperceptibility, robustness, fidelity,* dan *recovery* pada Dinas Komunikasi dan Informatika dengan bantuan Hex Editor Neo dan MATLAB?
4. Rekomendasi apakah yang dapat dirumuskan berdasarkan hasil dari steganografi dan *steganalysis* pada data di Dinas Komunikasi dan Informatika Penajam Paser Utara?

1.3 Batasan Masalah

Berdasarkan dari perumusan masalah yang telah dijabarkan, maka batasan masalah pada penelitian ini adalah sebagai berikut.

www.itk.ac.id

1. Parameter yang digunakan untuk melakukan *steganalysis* adalah parameter *imperceptibility*, *robustness*, *fidelity*, dan *recovery*.
2. Data yang digunakan untuk diamankan dengan teknik steganografi adalah data infrastruktur jaringan yang dimiliki oleh Dinas Komunikasi dan Informatika Penajam Paser Utara.
3. Aplikasi yang akan dianalisis menggunakan teknik *steganalysis* adalah OpenStego.
4. Aplikasi yang digunakan untuk melakukan teknik *steganalysis* adalah Hex Editor Neo. Namun MATLAB juga digunakan dalam penelitian ini sebagai aplikasi tambahan untuk melakukan *steganalysis* pada parameter *fidelity*.
5. *Media Digital* yang digunakan sebagai *cover image* dalam steganografi adalah citra digital.

1.4 Tujuan Penelitian

Berdasarkan dari perumusan masalah yang telah ditentukan, maka tujuan dari penelitian ini adalah sebagai berikut.

1. Penggunaan teknik steganografi pada Dinas Komunikasi dan Informatika Penajam Paser Utara dengan menggunakan aplikasi OpenStego dalam rangka mengamankan data infrastruktur jaringan.
2. Memperoleh hasil analisis *steganalysis* sesuai dengan hasil analisis Hex Editor Neo dan pada parameter *imperceptibility*, *robustness*, *fidelity*, dan *recovery* di Dinas Komunikasi dan Informatika Penajam Paser Utara dengan menggunakan MATLAB pada hasil *steganalysis* berdasarkan parameter *fidelity*.

1.5 Manfaat Penelitian

Dengan melakukan penelitian ini, maka manfaat yang diharapkan adalah sebagai berikut.

1. Hasil analisis dapat dijadikan sebagai bahan pertimbangan untuk diimplementasikan di lingkungan Dinas Komunikasi dan Informatika

www.itk.ac.id

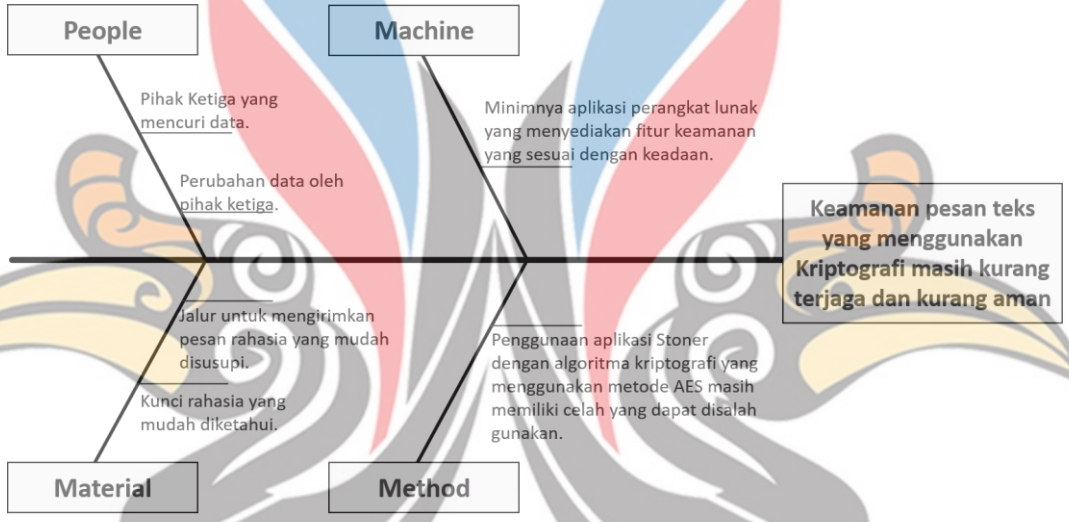
Penajam Paser Utara terkait dengan teknik pengamanan data dan informasi.

www.itk.ac.id

2. Hasil penelitian tugas akhir ini dapat menjadi salah satu referensi terkait dengan penelitian berikutnya yang berhubungan dengan keamanan data dan informasi secara umum serta steganografi dan *steganalysis* secara khusus.

1.6 Kerangka Pemikiran Penelitian

Berikut ini merupakan kerangka pemikiran penelitian yang digunakan.



Gambar 1. 2 Kerangka Pemikiran Penelitian

Dari **Gambar 1.2** yang merupakan kerangka pemikiran dari penelitian yang dilakukan, permasalahan utama dari penelitian ini adalah keamanan data informasi pada dinas ini sangat rentan sehingga dapat merugikan pihak dinas. Permasalahan ini didasarkan oleh empat kategori, yaitu *people*, *machine*, *material*, dan *method*. Pada kategori pertama, dimana pihak ketiga kemungkinan besar memiliki celah untuk mencuri data dan akan disalahgunakan. Hal ini dikarenakan komputer yang berada di dinas ini digunakan secara bersama-sama dan memiliki celah yang sangat besar jika data rahasia dicuri dan disalahgunakan. Selain itu, jalur pengiriman pesan yang masih rentan. Dengan adanya berbagai celah, maka

www.itk.ac.id

hal ini dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk menyalahgunakan data dan informasi.

Kategori kedua, dimana pada kategori ini aplikasi yang dapat mengamankan data rahasia tidak semuanya dapat digunakan. Hal ini karena dari beberapa aplikasi yang ada, terdapat aplikasi yang tidak sesuai dengan kebutuhan dan tidak sesuai dengan algoritma yang diterapkan di aplikasi tersebut. Pada kategori ketiga, dimana jalur yang digunakan untuk mengirimkan data rahasia sangat mudah disusupi dan juga kunci rahasia sangat mudah diketahui. Hal ini berdasarkan dari hasil observasi dan wawancara yang telah dilakukan. Dan pada kategori yang terakhir, dimana dinas ini telah mengimplementasikan salah satu teknik untuk mengamankan data rahasia, yaitu dengan mengimplementasikan teknik kriptografi. Pada teknik yang telah diimplementasikan, dinas ini telah melakukan kerja sama dengan pihak Badan Siber dan Sandi Negara (BSSN) untuk mengamankan data rahasia. Pada saat melakukan kerja sama, BSSN memberikan satu aplikasi yang dapat digunakan oleh dinas ini digunakan. Aplikasi yang diberikan memiliki nama Stoner. Dimana aplikasi ini menggunakan algoritma AES untuk mengamankan datanya. Namun, setelah beberapa saat menggunakan aplikasi ini, pihak dari dinas merasakan bahwa keamanan data masih memiliki celah karena hasil dari enkripsi dan deskripsi akan terlihat jelas oleh pihak yang tidak berkepentingan dan kemungkinan besar akan disalahgunakan.

www.itk.ac.id