**JURNAL**

**Yudi Suharyadi**

**Magister Manajemen**

**Konsentrasi Sistem Informasi**

**ABSTRAK**

Kebutuhan menjaga keamanan informasi dari ancaman dan serangan siber pada sistem informasi yang ada terhadap keutuhan, keamanan dan ketersediaan informasi merupakan menjadi syarat mutlak yang harus dipenuhi pada organisasi. Begitu banyaknya ancaman dan serangan siber membutuhkan sumber daya siber yang terintegrasi sehingga memudahkan dalam memonitoring keberlangsungan pertukaran data dalam suatu jaringan komputer. Untuk memudahkan dalam memonitoring pertukaran data tersebut, maka dibutuhkannya suatu sistem informasi siber yang dapat memberikan solusi dan bahan pengambilan keputusan bagi pimpinan terhadap adanya ancaman dan serangan siber tersebut.

Metodologi penelitian yang dilakukan untuk membangun aplikasi ini adalah metode penelitian deskriptif, melalui tahap pengumpulan data dan pengembangan perangkat lunak dengan mengunakan metode *waterfall*. Model analisis perangkat lunak yang digunakan adalah pemodelan analisis terstruktur dan alat yang digunakan adalah *Unified Modeling Language* (UML). Penulis kemudian merancang sebuah program berbasis web dengan menggunaklan PHP dan Mysql sebagai database.

Pimpinan dapat dengan mudah membuat keputusan secara objektif karena sistem menyediakan data yang dapat digunakan Pimpinan dalam menentukan tindakan yang harus diambil akibat adanya ancaman dan serangan siber, dalam prosesnya disesuaikan dengan aturan yang sudah ada. Dalam sistem ini, kriteria yang digunakan masih terbatas dalam lingkup yang kecil, sistem ini juga masih dapat dikembangkan menjadi lingkup yang lebih besar.

Kata Kunci: Sistem Informasi, Siber, Keputusan.

**I. Latar Belakang**

Dunia maya atau dunia siber (*cyber space*) merupakan hal yang menjadi banyak dibicarakan baik oleh kalangan akademisi maupun di kalangan masyarakat umum, istilah dunia maya itu sendiri menurut Gibson, Neuromancer 1993 dalam sebuah jurnal yang dituliskan oleh Nobuo Kamioka di tahun 1998 berjudul *Cyberpunk Revisited : William Gibson's Neuromancer and the "Multimedia Revolution*" adalah “Sebuah halusinasi yang dialami oleh jutaan orang setiap harinya berupa representasi grafis yang sangat kompleks dan data di dalam sistem pikiran manusia diabstraksikan melalui *bank* data setiap komputer”. Menurut Prof. Richardus Eko Indrajit pada Pengantar Konsep Keamanan Informasi di Dunia Siber, artikel 1, *Cyber*-6 : Memahami Isu Keamanan Data dan Informasi di Ranah Maya (EKOJI999:Nomor 005, 2012) bahwa jenis ancaman siber itu terdiri dari tiga kategori, pertama teknologi informasi dan komunikasi sebagai alat, kedua komputer atau teknologi informasi sebagai sasaran dan ketiga merusak, merubah dan mengambil data dan informasi yang tersimpan pada perangkat teknologi informasi. *Espionage*, *warfare*, *crime*, *terorisme* dan *malware* merupakan termasuk kedalam kategori pertama, penyebaran virus, transaksi fiktif dan mengambil alih fungsi sistem termasuk kedalam kategori kedua sedangkan merubah, mengambil dan merusak sistem merupakan termasuk ke dalam kategori ketiga. Dari hasil pertemuan para praktisi keamanan internet yang bersepakat untuk mengembangkan standar interoperabilitas penanganan kasus-kasus kejahatan dunia maya yang diadakan di Konvensi Budapest sepakat bahwa jenis serangan siber itu sendiri berupa alat atau senjata yang digunakan untuk menyerang seperti komputer dan internet, *gadget* dan *email*. Pada dasarnya ancaman siber itu merupakan cara seseorang melakukan kejahatan siber dengan menggunakan peralatan pendukung siber.

Di bidang militer khususnya TNI, dalam pelaksanaan sistem informasi pada penggunaan *cyber space* memberikan keuntungan yang luas di bidang komando dan kendali terhadap perang informasi karena jangkauannya mencakup seluruh wilayah dunia tanpa harus memperhatikan hambatan geografis maupun astronomis. Namun disisi lain *cyber space* juga dapat menjadi ancaman siber (*cyber threat*) yang kemudian dieksplorasi dan dikuasai oleh pihak-pihak tertentu baik itu *state actor* maupun *non-state actor* untuk melakukan hal-hal yang bersifat kriminal (*cyber crime*) dan menyerang fasilitas negara, perusahaan maupun organisasi (*cyber attack*) yang dapat mengakibatkan kerusakan maupun bahaya yang meluas terutama pada organisasi yang memiliki ketergantungan pada penggunaan *cyber space*. Berkaitan dengan ancaman dan serangan siber tersebut serta penjelasan Panglima TNI pada saat memberikan materi kuliah umum di Universitas Pertahanan dengan tema Kebijakan TNI dalam menjaga kedaulatan dan keutuhan NKRI di Kawasan IPSC Sentul Bogor, Jawa Barat, Selasa (13/3). Bahwa kemajuan teknologi saat ini membawa nilai positif bagi kehidupan manusia, namun juga memiliki beberapa paradoks yang perlu dicermati, di antaranya adalah *cyber threat*, *bio threat* dan *inequality threat*, dimana masing-masing ancaman tersebut memiliki alasan tersendiri untuk terus diwaspadai, disamping penggunaan internet saat ini sudah menjadi gaya hidup manusia yang tidak memandang usia, oleh sebab itu ancaman siber menjadi perhatian utama, mengingat lebih dari separuh penduduk dunia telah terhubung dengan dunia siber dan tiga perempat waktunya dihabiskan di dunia maya. Jika dahulu penguasaan wilayah sebagai yang utama, maka dalam nuansa kekinian penguasaan itu lebih bersifat *virtual* yaitu penguasaan dan pengelolaan terhadap dunia maya yang tersimpan di *Big Data*. Melalui perkembangan teknologi dengan memanfaatkan *profiling* data dan data analisis, saat ini dimungkinkan untuk merekrut teroris tunggal (*lone wolf*), kondisi ini memicu timbulnya potensi konflik horizontal maupun vertikal di masyarakat. Kekuatiran masa depan yang utama bukan terletak pada krisis kelangkaan pangan dan energi melainkan lebih pada ketidakmampuan kita untuk beradaptasi terhadap transformasi, salah satunya adalah kemajuan teknologi digital yang sangat cepat.

Selain itu dalam pelaksanaan penanganan ancaman dan serangan siber di Mabes TNI, untuk unit yang bertugas dalam mencegah dan mengatasi ancaman siber dan untuk menanggulangi dampak dari serangan siber tersebut masih belum optimal, hal ini disebabkan belum adanya regulasi dan tata kelola yang secara jelas mendefinisikan unit siber tersebut sebagai unit untuk menjaga infrastruktur informasi ktiris di Mabes TNI. Saat ini dalam menghadapi ancaman dan serangan siber baru sebatas sektoral yaitu masing-masing unit kerja bertanggung jawab atas keberlangsungan sistem informasinya sehingga akan timbul celah keamananan karena tidak adanya petunjuk secara jelas bagaimana konsep pembangunan sistem informasi sesuai dengan budaya di TNI. Dalam penyimpanan data (*database*) masih belum terintegrasi dengan baik, masih adanya sistem informasi dengan *database* belum bersifat universal dan menyeluruh yang dapat memetakan diseluruh bidang di Mabes TNI, hal ini dapat menjadi kelemahan dalam menjaga ketersediaan, keutuhan dan kerahasiaan informasi. Untuk mengatasi kelemahan-kelemahan tersebut yang dapat menyerang, melumpuhkan, dan merusak sistem jaringan operasional khususnya di sektor militer tersebut, maka Mabes TNI secara terus berupaya untuk mengembangkan kemampuan keamanan sibernya, karena perkembangan siber sangat cepat seiring dengan transformasi dan perkembangan teknologi komunikasi dan informasi.

Kebijakan-kebijakan di ranah siber yang bersifat di level strategis memunculkan pemikiran-pemikiran strategis berupa doktrin-doktrin yang kemudian direspon pada level operasional berupa tindakan-tindakan yang bersifat taktik, teknik dan operasional guna mengontrol perkembangan siber di ranah militer. Kolaborasi dan integrasi kedua level tersebut merupakan modal utama dalam menghadapi permasalahan siber yang semakin kompleks. Kebijakan-kebijakan keamanan siber yang telah dibuat, harus mampu melindungi operasional sistem jaringan dan penggunaan siber dengan mengintensifkan integrasi antar lembaga baik pemerintah maupun swasta. Dinamika yang ada di bidang siber, pada level operasional strategis Mabes TNI harus terus merencanakan, mengintegrasikan, dan sinkronisasi sistem informasi dalam pengambikan keputusan untuk mendukung kebijakan pimpinan di Mabes TNI, serta menetapkan dan mengembangkan doktrin, kebijakan dan menghubungkan taktik, teknik dan prosedur untuk menghadapi ancaman-ancaman siber di masa depan.

Berdasarkan latar belakang tersebut dan permasalahan yang dihadapi, maka dibutuhkannya suatu sistem informasi yang dapat mengolah data dan menyajikan informasi kepada pimpinan, dengan adanya perancangan sistem informasi siber sebagai bahan pengambilan keputusan pimpinan dalam menghadapi ancaman dan serangan siber, diharapkan permasalahan tersebut dapat teratasi sesuai dengan lingkupnya.

**II. Kajian Pustaka**

Leonardo Hasahatan Siregar (2007) manajemen sistem informasi adalah : “Sistem yang terstruktur dan dipakai dalam pengelolaan data berbasis komputer. Pada proses pengelolaannya dalam sebuah sistem informasi manajemen terdapat berbagai fungsi yang diperlukan seperti pencarian, pemutakhiran, presentasi data, dan fungsi penyimpanan data”.

Danu Wira Pangestu (2007) sistem informasi manajeman adalah : “Kumpulan dari interaksi sistem-sistem informasi yang bertanggung jawab mengumpulkan dan mengolah data untuk menyediakan informasi yang berguna untuk semua tingkatan manajemen di dalam kegiatan perencanaan dan pengendalian”.

Mangkunegara (2013) bahwa “Sumber daya manusia merupakan suatu perencanaan, pengorganisasian, pengkoordinasian, pelaksanaan dan pengawasan terhadap pengadaan, pengembangan, pemberian balas jasa, pengintegrasian, pemeliharaaan dan pemisahan tenaga kerja dalam rangka mencapai tujuan organisasi”.

Perancangan sistem menurut Diana dan Setiawati (2011:48) mendefinisikan bahwa : “Perancangan sistem merupakan sekumpulan prosedur yang dilakukan untuk mengubah spesifikasi logis menjadi desain yang dapat diimplementasikan ke sistem komputer organisasi”.

McLeod (2004) dikutip oleh Yakub dalam buku Pengantar Sistem Informasi (2012:1) mendefiniskan sistem adalah : “sekelompok elemen-elemen yang terintegrasi dengan tujuan yang sama untuk mencapai tujuan. Sistem juga merupakan suatu jaringan kerja dari prosedur-prosedur yang saling berhubungan, terkumpul bersama-sama untuk melakukan suatu kegiatan atau untuk tujuan tertentu”.

Tata Sutabri (2012:22) pada buku Analisis Sistem Informasi adalah : “Informasi adalah data yang telah diklasifikasikan atau diolah atau diinterpretasikan untuk digunakan dalam proses pengambilan keputusan”.

Sutarman (2012:14), Informasi adalah : “Sekumpulan fakta (data) yang diorganisasikan dengan cara tertentu sehingga mereka mempunyai arti bagi si penerima”.

Tata Sutabri (2012:36) dalam bukunya yang berjudul Konsep Sistem Informasi, bahwa : “Jenis informasi itu terbagi menjadi 2 (dua) macam yaitu pertama informasi individual yaitu informasi yang ditujukan kepada individual perseorangan dengan fungsinya sebagai bahan untuk membantu dalam membuat kebijakan. Kedua adalah infornasi komunitas yaitu informasi yang ditujukan kepada orang banyak dan atau kumpulan orang-orang di luar dari organisasi tertentu di masyarakat”.

Konsep Sistem Informasi karangan Tata Sutabri (2012:31) mengatakan bahwa :

“Fungsi utama dari informasi adalah menambah pengetahuan. Informasi tersebut berasal dari hasil data yang sudah terkumpul kemudian diolah dengan sistem aplikasi untuk diperoleh informasi-informasi yang diinginkan oleh pimpinan (user)”.

Menurut Wahyudi (2012:3), data adalah “Suatu file ataupun field yang berupa

Sutarman (2012:15), database adalah : “Sekumpulan file yang saling berhubungan dan terorganisasi atau kumpulan record-record yang menyimpan data dan hubungan diantaranya”.

Ladjamudin (2013:129), database adalah “Sekumpulan data store (bisa dalam jumlah yang sangat besar) yang tersimpan dalam magnetic disk, oftical disk, magnetic drum atau media penyimpanan sekunder lainya”.

Nugroho (2010:6), UML (Unified Modeling Language) adalah : “‘bahasa’ pemodelan untuk sistem atau perangkat lunak yang berparadigma ‘berorientasi objek’. Pemodelan (modeling) sesungguhnya digunakan untuk penyederhanaan permasalahan-permasalahan yang kompleks sedemikian rupa sehingga lebih mudah dipelajari dan dipahami”.

Herlawati (2011:10) adalah : “Bahwa beberapa literature menyebutkan bahwa UML menyediakan sembilan jenis diagram, yang lain menyebutkan delapan karena ada beberapa diagram yang digabung, misanya diagram komunikasi, diagram urutan dan diagram pewaktuan digabung menjadi diagram interaksi”.

Onno, Purbo dan Aang dalam bukunya tentang Mengenal e-commerce menuliskan bahwa “internet dengan berbagai aplikasinya seperti Web, VoIP, E-mail pada dasarnya merupakan media yang digunakan untuk mengefesiensikan proses komunikasi”.

**III. Metode Penelitian**

a. Observasi. Observasi juga dilakukan oleh penulis guna mengetahui mekanisme hubungan kerja dan struktur organisasi dari unit kerja tersebut, sumber daya manusia dan teknologi serta memperoleh dan mengumpulkan data yang dibutuhkan berdasarkan pengamatan baik secara tertulis, visual maupun bacaan serta didukung oleh ingatan peneliti dalam pemahamannya.

b. Wawancara. Wawancara dilakukan dengan mengajukan pertanyaan dan informasi yang dibutuhkan dalam perancangan sistem serta proses penanganan siber di Mabes TNI tersebut. Pada tehnik komunikasi wawancara dengan user dalam hal ini terbagi dalam beberapa level diantaranya level Pimpinan adalah Komandan Satuan Siber. Untuk level Pelayanan adalah Asisten Operasi dan Kepala Tata Usaha Urusan Dalam, sedangkan di level Pelaksana adalah Komandan Satuan Pelaksana dan staf Satuan Pelaksana. Wawancara ini untuk memahami terhadap apa yang menjadi keinginannya baik dari sisi kesisteman aplikasi komputer.

c. Studi Dokumentasi. Pada kegiatan pengumpulan data berupa dokumentasi tersebut berguna bagi penulis di dalam mencari keterangan untuk mendukung penelitian berupa catatan, tulisan dan gambar tentang permasalahan yang ada sehingga dapat dipelajari dan diterapkan pada proses metode.

d. Studi Literatur. Studi literatur merupakan data dari penelitian terdahulu, pembelajaran dari berbagai macam literatur, website dan dokumen seperti artikel atau tulisan ilmiah tentang ancaman siber, undang-undang, jurnal dan teori-teori yang mendukung penelitian, tools yang akan digunakan dan data penunjang lainnya yang berkaitan dengan sistem informasi berbasis web.

**IV. Analisis dan Hasil Perancangan**

a. Analisis Permasalahan

Pada analisis permasalahan ini merupakan bagian dalam mengalisis masalah-masalah yang timbul pada sistem yang sedang berjalan, ada beberapa permasalahan yang dapat digolongkan dalam merancang suatu sistem informasi siber kali ini, diantaranya:

1. Sistem yang ada belum mempunyai keamanan untuk penanganan ancaman secara kesisteman, sehingga menyebabkan penanganannya dilakukan setelah terjadi serangan.

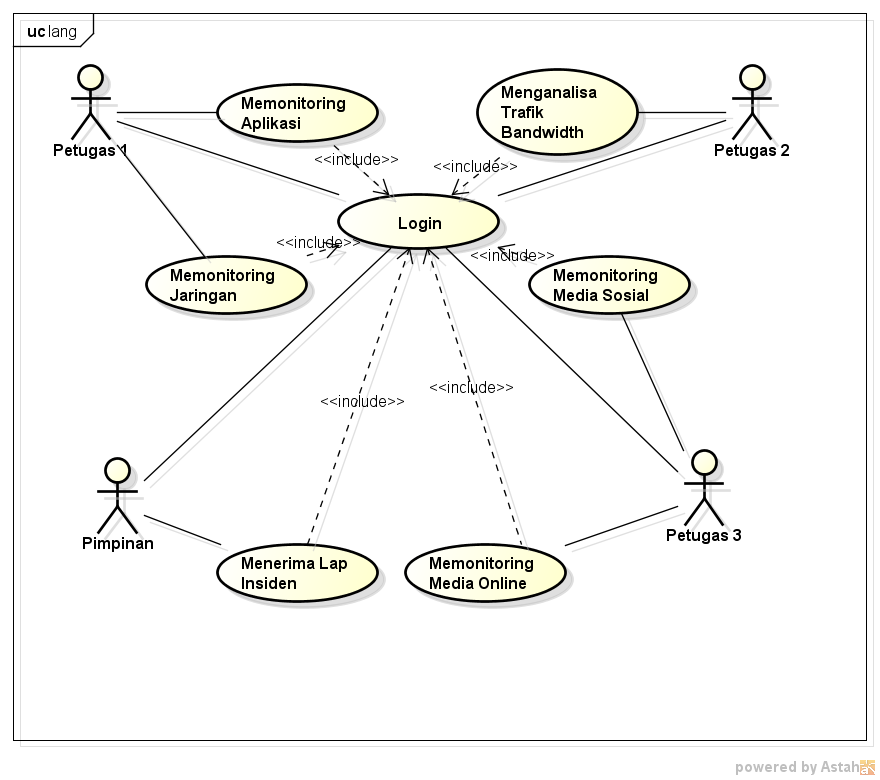
2. Tidak adanya sistem basis data yang dapat meyimpan data-data dari hasil kegiatan sehingga sulit untuk diolah menjadi informasi yang dibutuhkan, data yang tersimpan saat ini berupa file-file *Microsoft Office*.

3. Proses laporan tidak berjalan secara *realtime,* sehingga laporan tersebut belum dapat digunakan untuk bahan analisis dalam menunjang keputusan Pimpinan.

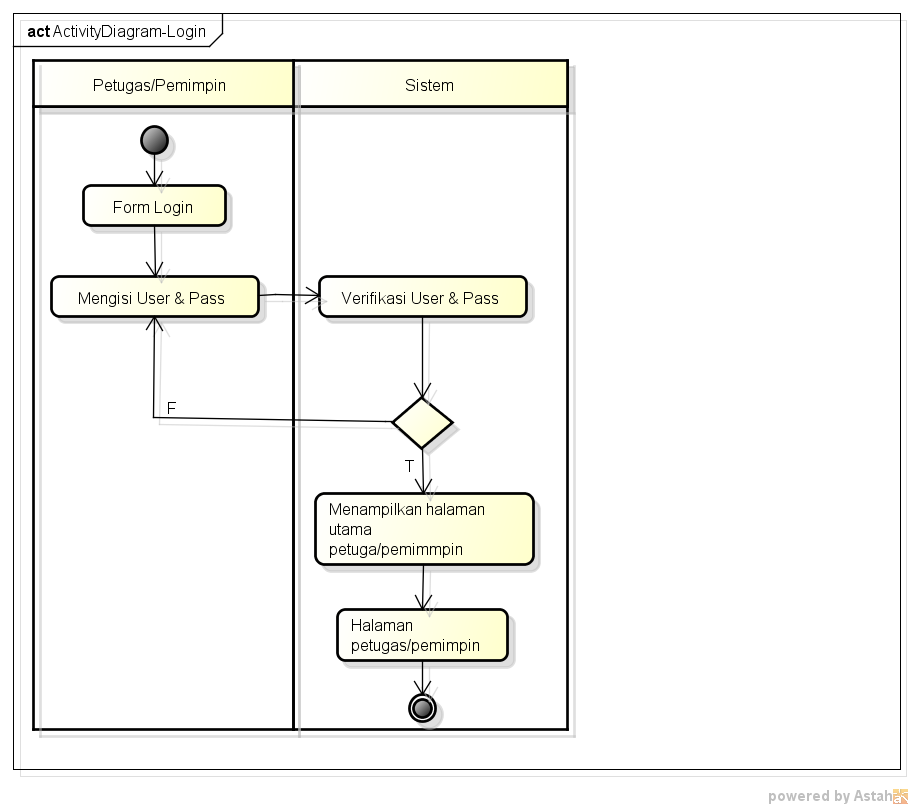
4. Sistem yang ada di entitas eksternal belum terintegrasi, sehingga menyebabkan pengamanan sistem optimal.

5. Hasil penanganan tersebut berupa *hardcopy,* sehingga akan sulit dalam olah data selanjutnya.

b. Perancangan

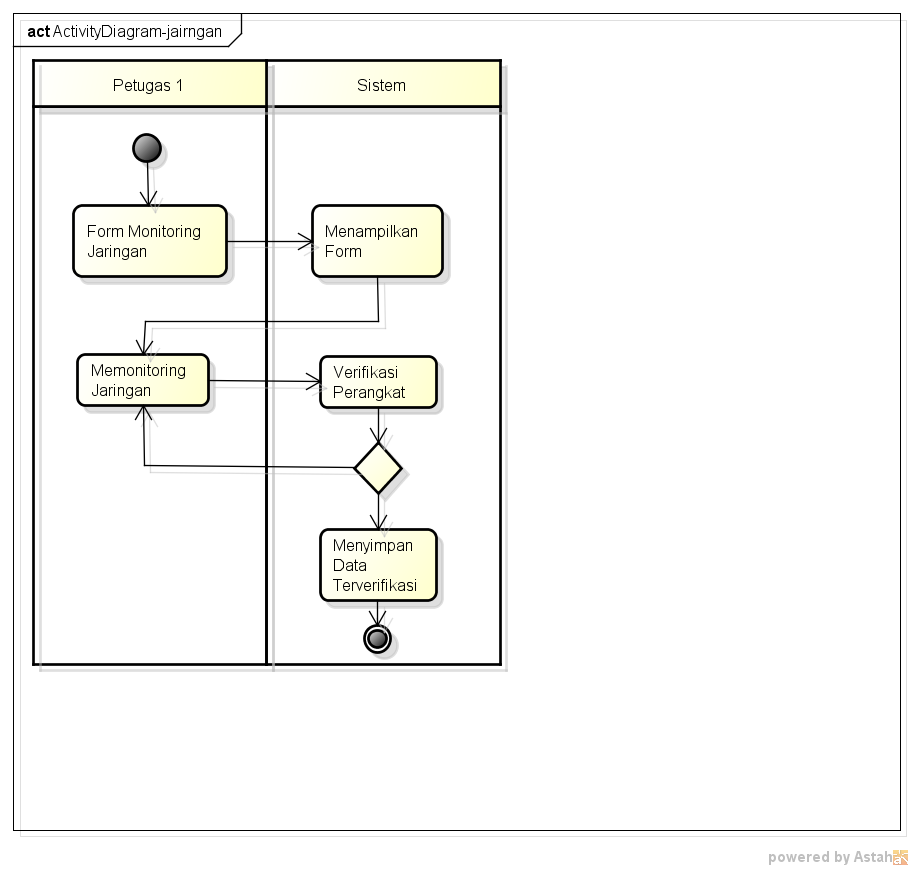
 Penjelasan dari gambar tersebut, terdapat use case yang terdiri dari 4 (empat) aktor yaitu Petugas 1 yang memonitoring terhadap aktivitas yang ada di jaringan dan koneksi, Petugas 2 yang memonitoring terhadap aktivitas baik di media sosial maupun media online, petugas 3 yang menganalisa trafik bandwidth dan Komandan yaitu menerima laporan dari hasil monitoring. 7 (tujuh) entitas yaitu memonitoring jaringan, aplikasi, login, media online, media sosial, menganalisa trafik bandwidth, media sosial dan online dan terakhir adalah menerima laporan insiden. Adapun activity diagram dapat disajikan sebagai berikut :

1. *Activity Diagram* Login

****

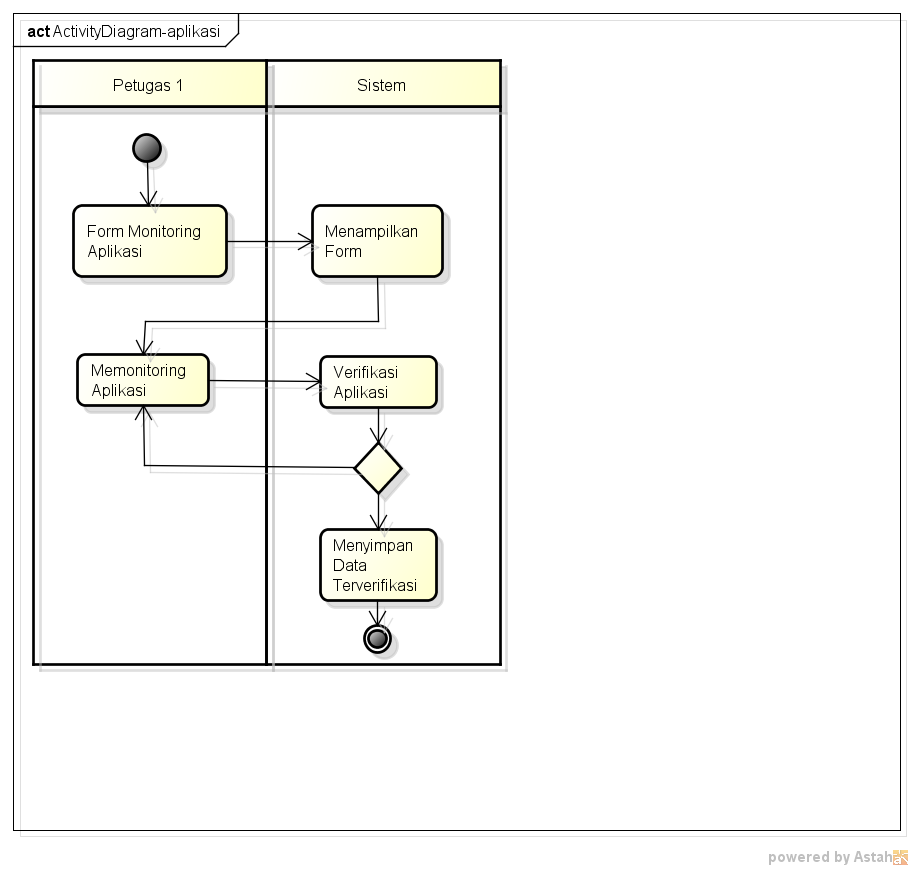
Penjelasan dari gambar tersebut menggambarkan tentang proses jalannya seorang petugas/pemimpin dalam melakukan login dengan terlebih dahulu petugas/pemimpin mengakses form login untuk memasukan *username* dan *password*, ketika username dan password tersebut terverifikasi maka akan menampilkan form menu sesuai dengan autoritas dari masing-masing user, apabila gagal maka kembali ke form login.

2. *Activity Diagram* Petugas 1 Monitoring



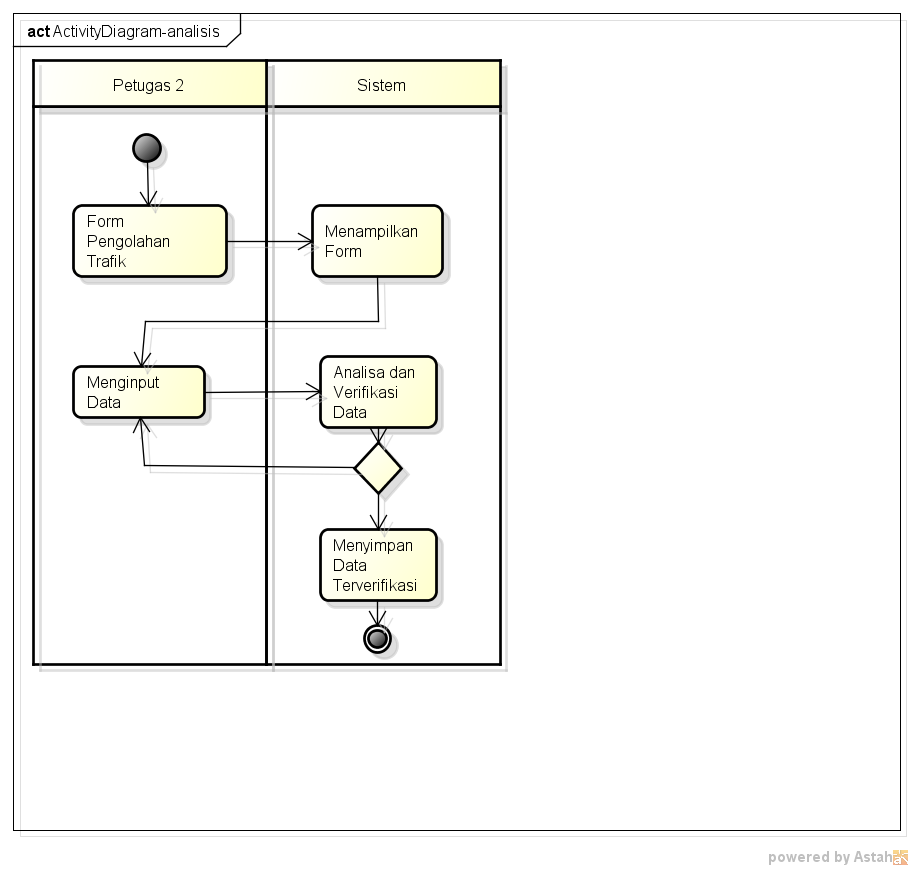
Gambar tersebut merupakan gambaran tentang petugas 1 monitoring yang telah berhasil melakukan login dan menampilkan form monitoring jaringan dan melakukan monitoring terhadap jaringan yang menjadi tugasnya, kemudian dilakukan verifikasi perangkat baik yang sudah teridentifikasi maupun belum dan disimpan ke dalam database.

3. *Activity Diagram* Petugas 1 Aplikasi



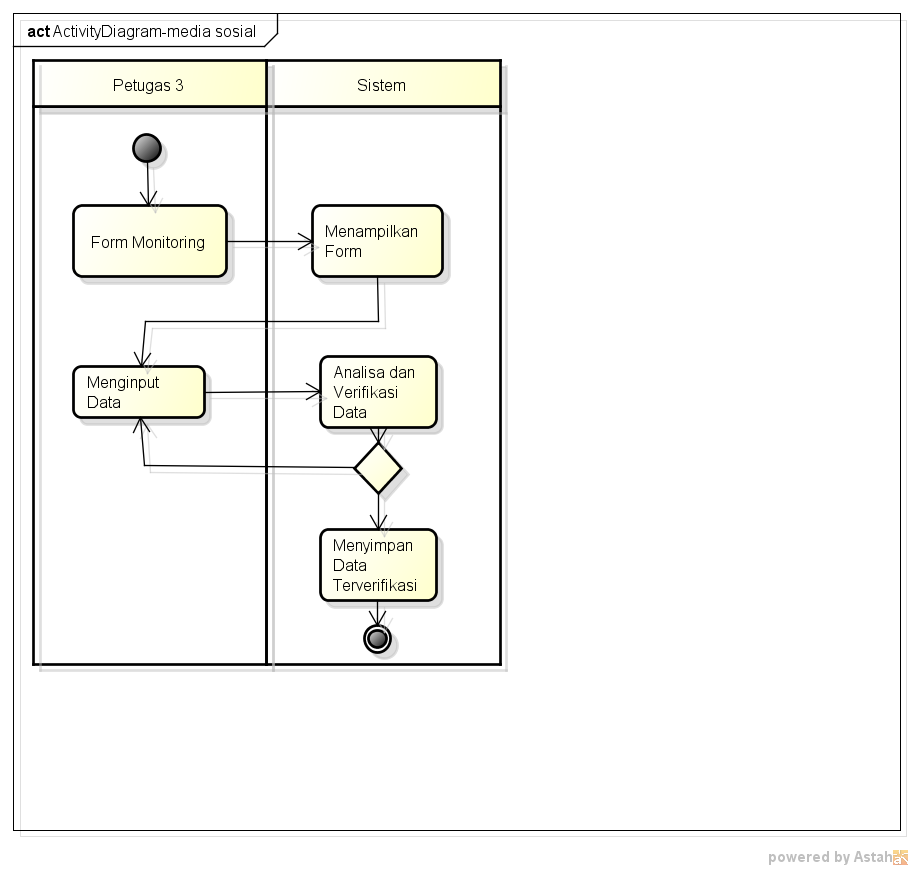
Pada gambar tersebut dijelaskan tentang petugas 1 aplikasi yang berhasil melakukan login sehingga dapat menampilkan form monitoring aplikasi dan melakukan monitoring terhadap aplikasi yang menjadi tugasnya, kemudian dilakukan verifikasi aplikasi baik yang sudah teridentifikasi maupun belum dan disimpan ke dalam database.

4. *Activity Diagram* Petugas 2 Menganalisa Trafik *Bandwidth*



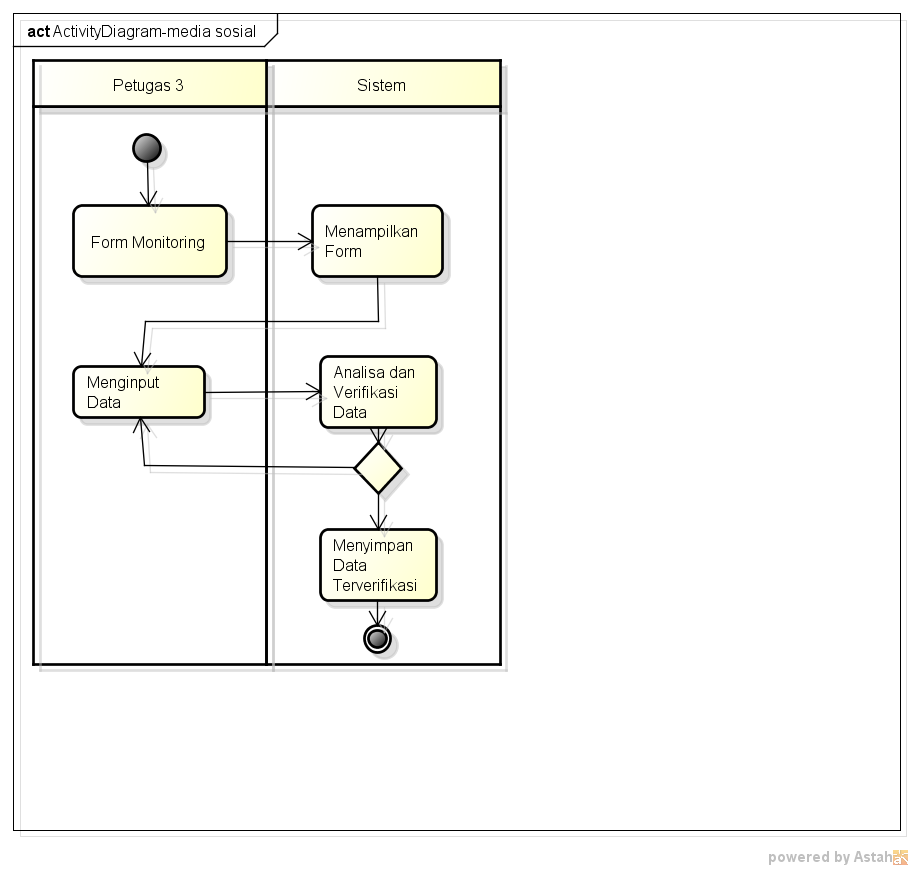
Dalam gambar tersebut dijelaskan tentang petugas 2 sebagai analisis trafik *bandwidth*, aplikasi, media sosial dan media onlie yang berhasil melakukan login sehingga dapat menampilkan form analisis trafik *bandwidth*, aplikasi, media sosial dan media onlie dan melakukan monitoring terhadap trafik *bandwidth*, aplikasi, media sosial dan media onlie yang menjadi tugasnya, kemudian dilakukan verifikasi baik yang sudah teridentifikasi maupun belum dan disimpan ke dalam database.

5. *Activity Diagram* Petugas 3 Media Sosial



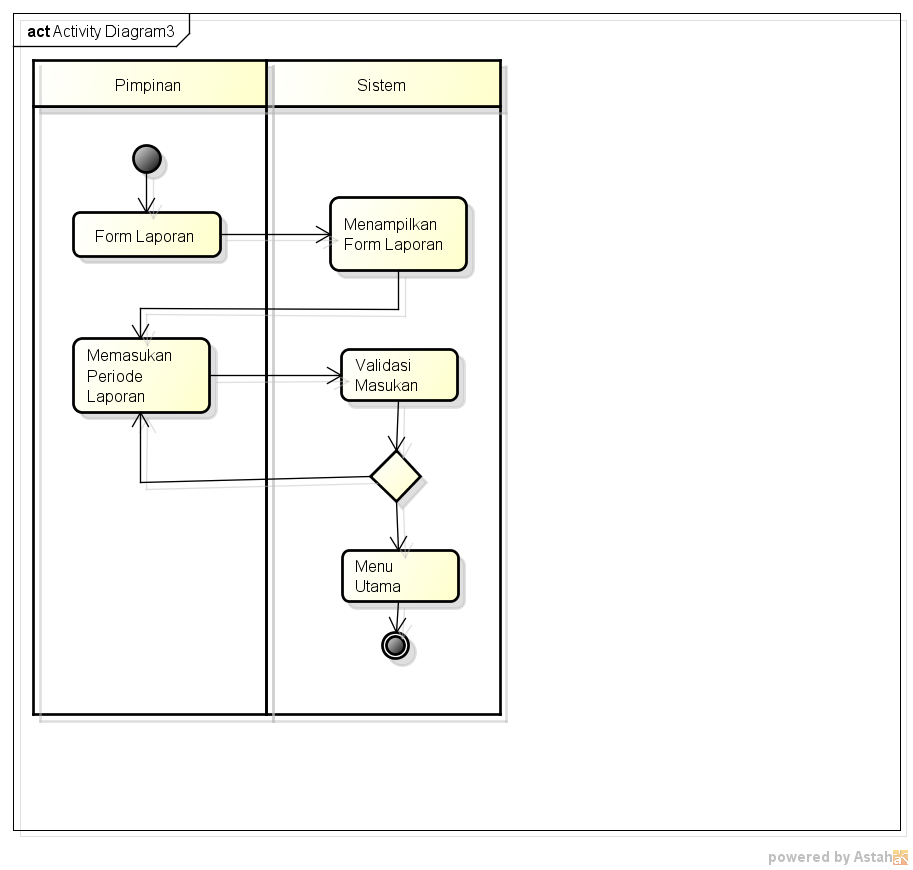
Menjelaskan prihal petugas 3 yang berhasil melakukan login dan mendapatkan serta menampilkan form monitoring media sosial, kemudian melakukan pengolahan dari hasil monitoring media sosial yang dilanjutkan dengan analisis dan verifikasi data, setelah dilakukan verifikasi maka data tersebut disimpan dalam database.

6. *Activity Diagram* Petugas 3 Media Online



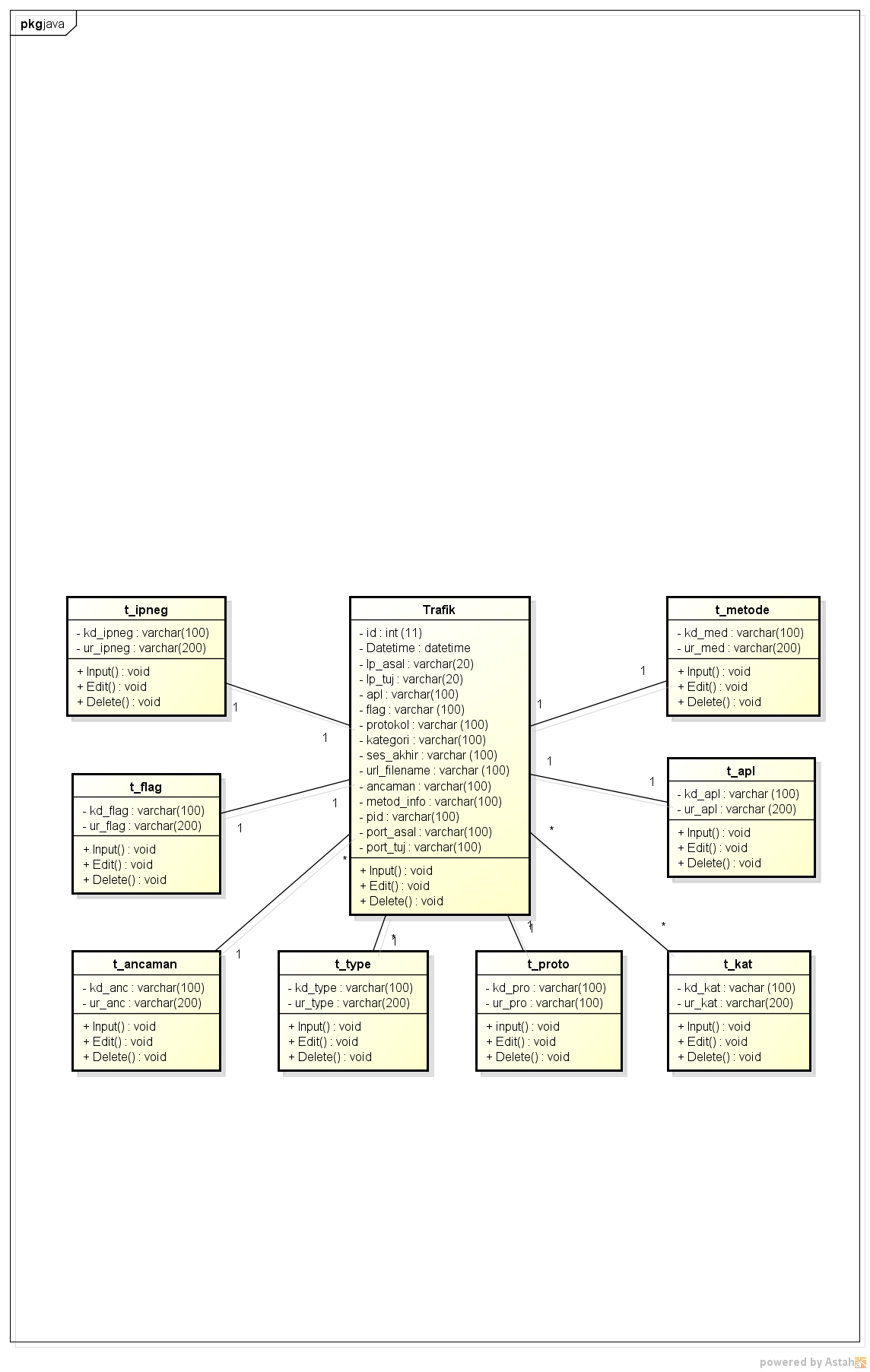
Dari gambar tersebut merupakan prihal petugas 3 yang berhasil melakukan login dan mendapatkan serta menampilkan form monitoring media sosial, kemudian melakukan pengolahan dari hasil monitoring media sosial yang dilanjutkan dengan analisis dan verifikasi data, setelah dilakukan verifikasi maka data tersebut disimpan dalam database.

7. *Activity Diagram* Pimpinan



Penjelasan dari gambar tersebut merupakan prihal aktivitas dari aktor pemimpin yang berhasil melakukan login dan mendapatkan hak akses terhadap sistem, kemudian dapat melihat halaman laporan dari hasil kegiatan petugas 1, petugas 2 dan petugas 3 yang merupakan hasil monitoring trafik bandwidth, media online dan media sosial yang sudah dianalisis dan diverifikasi data. Untuk mendapatkan laporan aktor pemimpin memasukan periode laporan yang kemudian oleh sistem akan diverifikasi.

Adapun rancangan database dapat disajikan sebagai berikut :



Adapun penjelasan dari spesifikasi *database* pada sistem informasi siber ini, adalah sebagai berikut:

1. Tabel Trafik

Nama Tabel : trafik

Media : hardisk

*Primary Key* : id

*Type File* : Master

Struktur :

**Tabel Tabel Trafik**

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Nama Field** | **Jenis** | **Keterangan** |
| 1. | id | Int(11) | Identitas |
| 2. | Datetime | Datetime | Waktu |
| 3. | IP\_asal | Varchar(20) | IP negara asal |
| 4. | IP\_Tuj | Varchar (20) | IP negara tujuan |
| 5. | Apl | Varchar (100) | Aplikasi |
| 6. | Flag | Varchar (100) | Flag/tanda |
| 7. | Protokol | Varchar (100) | Protokol pemakaian |
| 8. | Kategori | Varchar (100) | Kategori |
| 9. | Ses\_akhir | Varchar (100) | Sesi akhir |
| 10. | url\_filename | Varchar (100) | Nama file sebagai anomali |
| 11. | Ancaman | Varchar (100) | Insiden ancaman |
| 12. | Metod\_info | Varchar (100) | Informasi metode serangan |
| 13. | Pid | Varchar (100) | Proportional Integral Derivative controller |
| 14. | Port\_asal | Varchar (100) | Port asal aplikasi |
| 15. | Port\_tujuan | Varchar (100) | Port tujuan aplikasi |

2. Tabel IP Negara

Nama Tabel : t\_ipneg

Media : hardisk

*Primary Key* : kd\_ipneg

*Type File* : Master

Struktur :

**Tabel Tabel T\_Ipneg**

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Nama Field** | **Jenis** | **Keterangan** |
| 1. | Kd\_ipneg | Varchar(100) | Ip negara |
| 2. | Ur\_ipneg | Varchar(200) | Uraian IP negara |

3. Tabel IP Flag

Nama Tabel : t\_flag

Media : hardisk

*Primary Key* : kd\_flag

*Type File* : Master

Struktur :

**Tabel Tabel T\_Flag**

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Nama Field** | **Jenis** | **Keterangan** |
| 1. | Kd\_flag | Varchar(100) | Kode flag |
| 2. | Ur\_flag | Varchar(200) | Uraian flag |

4. Tabel Acaman

Nama Tabel : t\_ancaman

Media : hardisk

*Primary Key* : kd\_anc

*Type File* : Master

Struktur :

**Tabel Tabel T\_Ancaman**

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Nama Field** | **Jenis** | **Keterangan** |
| 1. | Kd\_anc | Varchar(100) | Kode ancaman |
| 2. | Ur\_anc | Varchar(200) | Uraian ancaman |

5. Tabel Type

Nama Tabel : t\_type

Media : hardisk

*Primary Key* : kd\_type

*Type File* : Master

Struktur :

**Tabel Tabel T\_Type**

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Nama Field** | **Jenis** | **Keterangan** |
| 1. | Kd\_type | Varchar(100) | Kode type |
| 2. | Ur\_type | Varchar(200) | Uraian type |

6. Tabel Proto

Nama Tabel : t\_proto

Media : hardisk

*Primary Key* : kd\_pro

*Type File* : Master

Struktur :

**Tabel Tabel T\_Proto**

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Nama Field** | **Jenis** | **Keterangan** |
| 1. | Kd\_pro | Varchar(100) | Kode protokol |
| 2. | Ur\_pro | Varchar(200) | Uraian protokol |

7. Tabel Kategori

Nama Tabel : t\_kat

Media : hardisk

*Primary Key* : kd\_kat

*Type File* : Master

Struktur :

**Tabel Tabel T\_Kat**

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Nama Field** | **Jenis** | **Keterangan** |
| 1. | Kd\_kat | Varchar(100) | Kode kategori |
| 2. | Ur\_kat | Varchar(200) | Uraian kategori |

8. Tabel Aplikasi

Nama Tabel : t\_apl

Media : hardisk

*Primary Key* : kd\_apl

*Type File* : Master

Struktur :

**Tabel Tabel T\_Apl**

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Nama Field** | **Jenis** | **Keterangan** |
| 1. | Kd\_apl | Varchar(100) | Kode aplikasi |
| 2. | Ur\_apl | Varchar(200) | Uraian aplikasi |

9. Tabel Metode

Nama Tabel : t\_metode

Media : hardisk

*Primary Key* : kd\_med

*Type File* : Master

Struktur :

**Tabel Tabel T\_Metode**

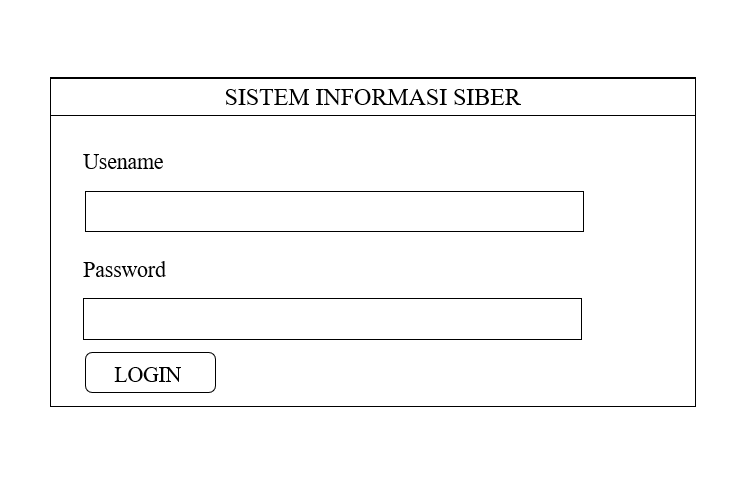
|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Nama Field** | **Jenis** | **Keterangan** |
| 1. | Kd\_med | Varchar(100) | Kode metode |
| 2. | Ur\_med | Varchar(200) | Uraian metode |

c. Rancangan Tampilan

Pada konsep rancangan tampilan sistem informasi siber yang dihasilkan adalah sebagai berikut:

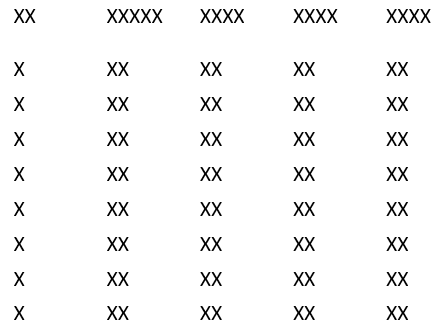
1. Tampilan Awal

Untuk tampilan awal pada sistem informasi siber ini berupa halaman login dengan ketentuan pengguna/*user* harus memasukan *username* dan *password* jika hendak menggunakan sistem ini, adapun tampilannya terdapat pada gambar dibawah ini.

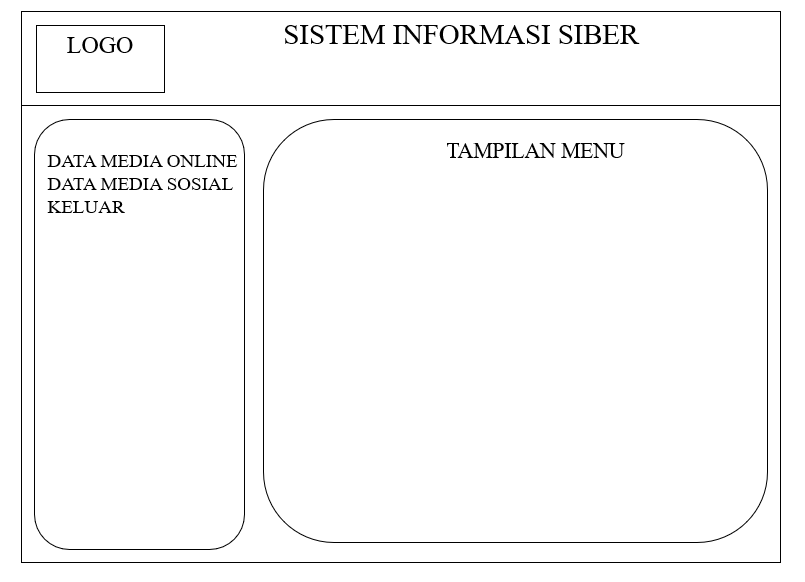
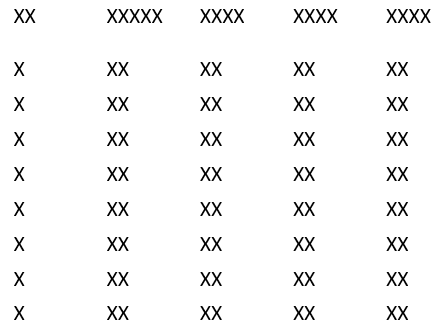


2. Tampilan Level Operator

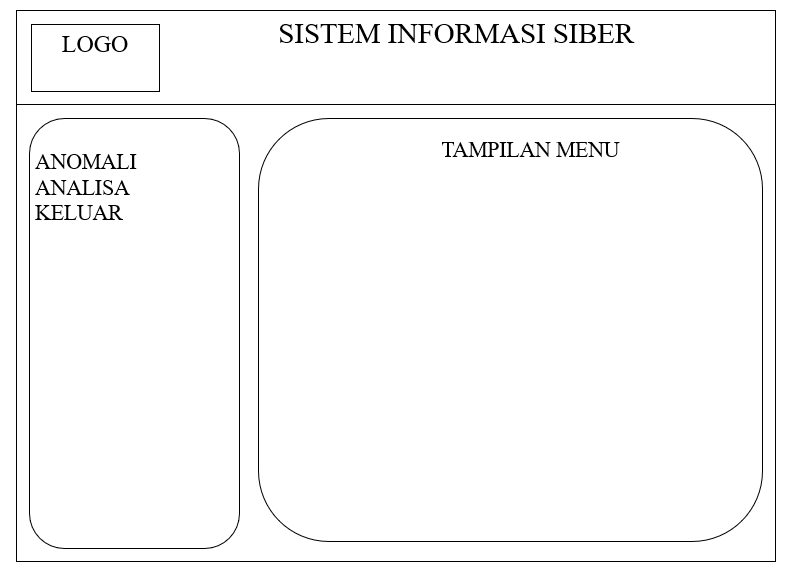
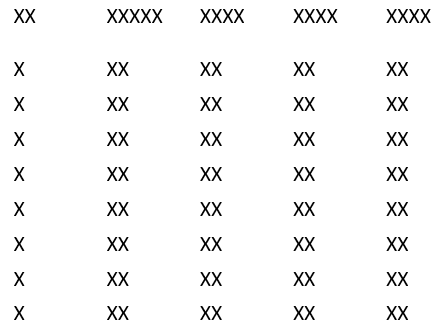
a. Operator Jaringan, untuk tampilan petugas jaringan mempunyai otoritas akses yaitu data jaringan dan data aplikasi.



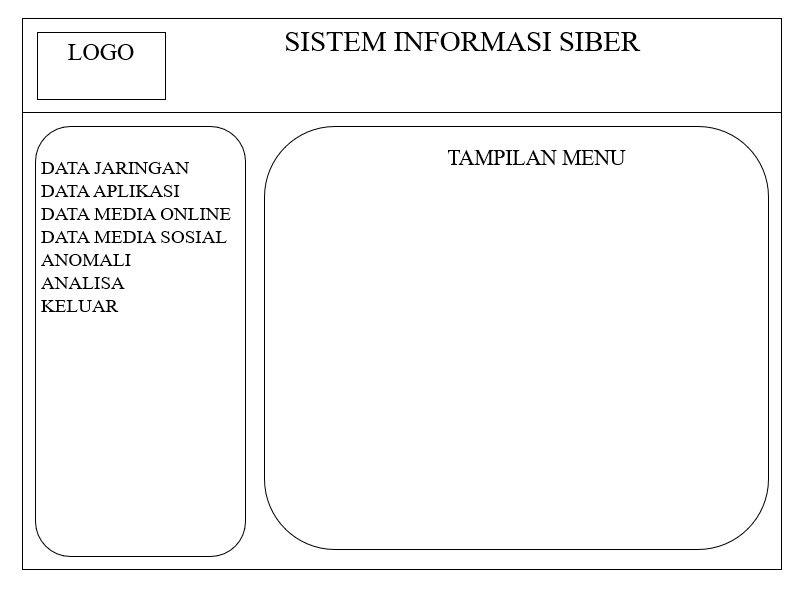
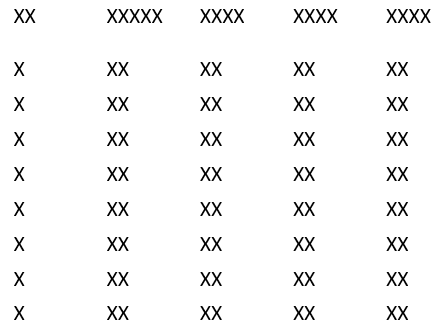
b. Operator Media, untuk tampilan petugas jaringan mempunyai otoritas akses yaitu data media online dan data media sosial.



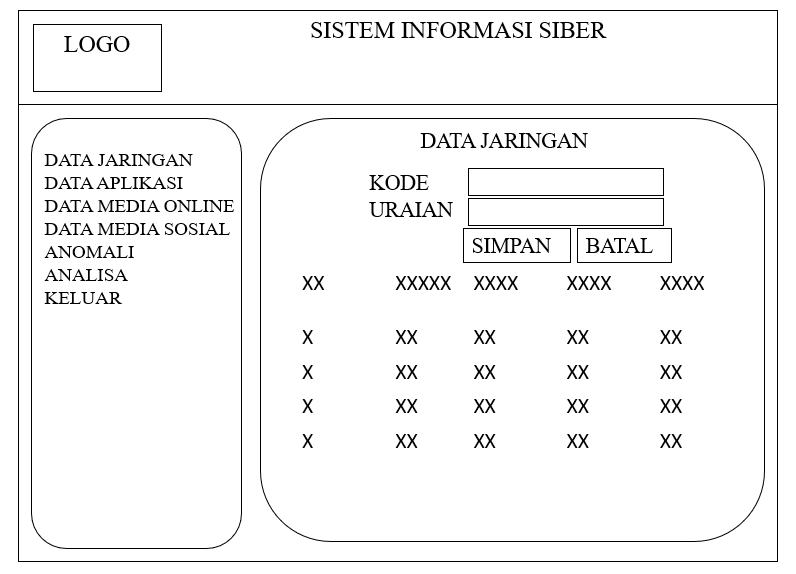
c. Operatos Analis, untuk tampilan petugas analis mempunyai otoritas akses yaitu anomali dan analisa.



d. Pimpinan, untuk tampilan pimpinan mempunyai otoritas akses yaitu data jaringan, data aplikasi, data medsos, data medline, anomali dan analisa.



3. Tampilan Update Data, pada tampilan update data yaitu data jaringan, data aplikasi, data medsos, data medline, anomali dan analisa.



**V. Kesimpulan**

Berdasarkan hasil dan analisis dari bab sebelumnya maka penulis dapat menyimpulkan tentang pelaksanaan hasil proses perancangan sistem informasi siber sebagai bahan pengambilan keputusan pimpinan dalam menghadapi ancaman dan serangan siber di Mabes TNI Jakarta, sebagai berikut:

1. Perkembangan penggunaan teknologi menuntut penggunanya untuk dapat menjaga keutuhan, kerahasiaan dan ketersediaan informasi di lingkungan kerjanya.

2. Informasi yang dihasilkan oleh sistem informasi siber, memberikan masukan kepada Pimpinan dalam menentukan kebijakan untuk menangani ancaman dan serangan siber.

3. Pengimplementasian sistem informaasi siber ini secara terintegrasi dengan sistem lain secara otomasisasi akan memberikan manfaat terutama dalam memperbanyak basis data terhadap adanya anomali ancaman dan serangan siber.

4. Sistem informasi siber ini merupakan sistem yang dapat dikembangkan sesuai dengan perkembangan teknologi, hal ini pembuatan sistem informasi siber ini menggunakan open programming sehingga bermanfaat bagi pihak lain untuk dikembangkan lebih sempurna lagi.

5. Dengan makin banyaknya basis data yang terhimpun untuk diolah oleh tim analis, maka dapat membantu Pimpinan terutama Dansatsiber dalam mewujudkan penanganan ancaman dan serangan di lingkungan Mabes TNI.

**DAFTAR PUSTAKA**

**Buku :**

Onno, Purbo dan Aang, 2001, **Mengenal e-commerce**, PT.Elex media, Komputindo. Jakarta.

Nurs. 2003, **Pengambilan Keputusan**, Jakarta: Gunung Agung.

Tata Sutabri, 2005, **Sistem Informasi Manajemen**, Andi Offseat, Yogyakarta.

Sholiq, 2006, **Pemodelan Sistem Informasi Berorientasi Objek Dengan UML**, Graha Ilmu, Yogyakarta.

Pressmanm R.S, 2012, **Rekayasa Perangkat Lunak Pendekatan Praktisi**, Andi, Offseat, Yogyakarta.

Azhar Susanto, 2017, **Sistem Informasi Manajemen Konsep dan Pengembangan Secara Terpadu**, Lingga Jaya, Bandung.

Herdiansyah, Heri. 2010, **Metodologi Penelitian Kualitatif: untuk ilmu-ilmu sosial,** Jakarta: Salemba Humanika.

Sugiyono, 2011, **Metode Penelitian Pendidikan: Pendekatan Kuantitatif, Kualitatif, dan R&D**, Bandung: Alfabeta.

Huberman, dan Miles, 2014, **Analisis Data Kualitatif**, Jakarta: Universitas Indonesia.

Creswell W, John, 2013, **Research Design Pendekatan Kualitatif, Kuantitatif, dan Mixed**, Yogyakarta : Pustaka Pelajar.

Ghony, M.D. dan Almanshur. F, 2012, **Metodologi Penelitian Kualitatif.** Yogyakarta: Ar-ruzz Media.

**Jurnal :**

Yanthi, Rusmanida, Evy, 2018, **Analisis Kontribusi Komponen Teknologi (*Technoware, Humanware, Infoware, Orgaware*) Pada Perusahaan Jasa Transportasi Kereta Api Barang Dengan Pendekatan Model Teknometrik,**Tesis, IPB, Hal. 3

Ginanjar Wiro Sasmito, 2017, **Penerapan Metode *Waterfall* Pada Desain Sistem Informasi Geografis Industri Kabupaten Tegal**, Jurnal Informatika, Vol. 2, No. 1, Hal. 8.

Achmad Ismail, 2015, **Pembangunan Sistem Informasi *Cyber* Koseling di Telkom University**, Sistem Informasi, Vol. 1, No. 1.

Ahmad Sabri, Juli 2013, **Kebijakan Dan Pengambilan Keputusan Dalam Lembaga Pendidikan Islam,** Al-Ta’lim, Jilid 1, No. 5, Hal. 373-379.

Riska, Harihanto, Agustin Nurmanina, 2013, **Studi Tentang Penggunaan Internet Oleh Pelajar (Studi Pada Penggunaan Internet Oleh Pelajar SMP N 1 Samarinda),** e-Jurnal Sosiatri-Sosiologi, Vol. 1, No. 4, Hal. 37-49.

Liputasasi, Anastasia, 2013, **Peran Sistem Informasi Manajemen (SIM) Dalam Pengambilan Keputusan**, Jurnal STIE, Vol. 5, No. 1, Hal. 26-37.

Permadi Setiawan, Sulistiowati, Julianto Lemantara, September 2015, **Rancang Bangun Aplikasi Pengolahan Data Evaluasi Proses Belajar Mengajar Berbasis Web Pada STIKES Yayasan Rs. Dr. Soetomo Surabaya**,JSIKA, Vol. 4, No. 2.

Literary Freeware, June 1992, ***The Magazine Of Fantasy And Science Fiction***, http://lib.ru/STERLINGB/f\_sf\_01.txt\_with-big-pictures.html.

Kelly, Kevin (1994), ***Out of control:******The new biology of machines, social systems and the economic world***. Boston: Addison-Wesley. ISBN 0-201-48340-8. OCLC 221860672 32208523 40868076 56082721 57396750.

Couffignal, Louis, ***Essai d’une définition générale de la cybernétique****, The First International Congress on Cybernetics*, Namur, Belgium, June 26–29, 1956, Gauthier-Villars, Paris, 1958, pp. 46-54.

**Forum Diskusi :**

*CYBCON discusstion group* 20 September 2007 18:15

**Dokumen :**

Peraturan Presiden Nomor 97 Tahun 2015 tentang Kebijakan Umum Pertahanan Negara Tahun 2015-2019.

Peraturan Presiden Nomor 133 Tahun 2017 tentang Perubahan Atas Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN).

Peraturan Panglima TNI Nomor 17 Tahun 2017 tanggal 18 Maret 2017 tentang Organisasi dan Tugas Satuan Siber TNI.

**Referensi :**

https://idsirtii.or.id/doc/IDSIRTII-Artikel-6\_aspek\_menjaga\_dan\_melindungi\_dunia\_maya.pdf, diakses Jumat, 20/07/2018, 15:45 WIB.

http://jurnalmanajemen.com/fungsi-manajemen-menurut-henry-fayol/, diakses Selasa, 7 Agustus 2018, 11:00 WIB.

http://fadhlaniouz.blogspot.com/2013/11/perencanaan-sumber-daya-manusia.html, diakses Jumat, 10 Agustus 2018, 21:20 WIB.

http://bl4cyberr.blogspot.com/2011/09/pengertian-cyber.html, diakses Sabtu, 11 Agustus 2018, 04:25 WIB.

https://symfoniacy.wordpress.com/2012/11/17/ruang-lingkup-cyber/, diakses Selasa, 14 Agustus 2018, 13:30 WIB.

http://wartawarga.gunadarma.ac.id/2010/01/kemampuan-sistem-informasi-manajemen/, diakses Senin, 20 Agustus 2018, 21:23 WIB.

https://inet.detik.com/security/d-3005339/sekilas-tentang-cyber-crime-cyber-security-dan-cyber-war, diakses, Selasa 21 Agustus 2018, 14:40 WIB.

http://suryaarma.blogspot.com/2016/04/mengenal-cyber-crime-cyber-law-cyber.html, diakses Selasa, 21 Agustus 2018, 14:55 WIB.

https://afidburhanuddin.wordpress.com/2013/05/21/pengumpulan-data-dan-instrumen-penelitian/, diakses Rabu, 12/09/2018, 21:40 WIB.

http://uchiuwik.blogspot.com/2014/11/metode-metode-pengembangan-sistem.html, diakses Sabtu, 9/9/2018, 10:00 WIB.

https://www.matadunia.id/2016/02/metodologi-pengembangan-perangkat-lunak.html, diakses, sabtu 8/9/2018, 09:30 WIB.

https://www.noficahyono.com/2015/07/perancangan-sistem-informasi\_13.html, diakses Sabtu, 8/9/2018, 09:00 WIB.

https://www.course-net.com/empat-jenis-ancaman-cyber-terkini/, diakses Minggu, 15 Jul 2018, 22:46 WIB.

https://www.dictio.id/t/apakah-yang-dimaksud-dengan-teori-tradisi-sibernetika-tradisi-cybernetic/9038, diakses Jumat, 7 Desember 2018, 21:00 WIB.