OPTIMALISASI KEAMANAN DATA DAN INFORMASI PADA PERANGKAT LUNAK DAN IMPLEMENTASINYA

Richard David Tedja

Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pelita Harapan

Jl. M.H. Thamrin Boulevard 1100, Kelapa Dua, Karawaci, Tangerang, Banten 15811, Indonesia

Email: rdtedja@gmail.com

ABSTRAK

Paper ini membahas mengenai langkah-langkah untuk mengoptimalisasi keamanan data pada perangkat lunak yang sesuai dengan standar keamanan data yang berlaku di seluruh dunia, dan disertai dengan contoh implementasi pada organisasi-organisasi yang mengandalkan manajemen sistem informasi dalam operasionalnya. Teknologi yang saling menghubungkan komputer didunia memungkinkan untuk dapat saling bertukar informasi dan data, bahkan saling berkomunikasi berupa gambar dan video. Semakin berharga sebuah informasi maka diperlukan sebuah standar kemanan pada perangkat lunak untuk menjaga informasi tersebut. Sistem perangkat lunak yang aman akan memberikan tingkat kepercayaan yang tinggi dari *user*, dan *user* akan merasa nyaman dan aman ketika berhubungan dengan sistem yang sudah kita bangun. Begitu pentingnya aspek keamanan dalam teknologi informasi sehingga beberapa perusahaan pengembang perangkat lunak lantas menjadikan keamanan sebagai prioritas bisnisnya. Perangkat lunak yang "aman" menjadi nilai jual tersendiri bagi perusahaan pengembang dan menjadi pertimbangan utama bagi perusahaan pengguna yang mengutamakan stabilitas sistem dan kerahasiaan datanya. Banyak orang mulai berpikir untuk memproteksi komputer dan tidak membiarkan akses data tanpa izin. Sistem keamanan merupakan salah satu bagian penting dalam setiap proses pengembangan suatu bisnis dan investasi, karena dengan sistem keamanan yang baik resiko atas kehilangan sejumlah nilai yang diinvestasikan dalam data dan informasi menjadi lebih kecil.

Kata kunci: optimalisasi, keamanan, data, informasi, perangkat lunak, implementasi

ABSTRACT

This paper will discuss about steps to optimalize the security in software systems in accordance to world data security standards, with examples of implementations in organizations that rely heavily on information systems management in its daily operations. The technology that connects each and every computer in the world makes it possible for us to exchange data and information, and even communicate through photos and videos. As the value of information increases, the need to set up a standard for software security to protect the information rises. A secure software will result in a high level of trust by the software user, and they will feel safe and comfortable when interacting with the system that we have built. Software security in information technology is very crucial that a lot of software developers set software security as a priority in their business. A safe software has its own market value for software developers and it has become a huge consideration for software users to prioritize system stability and data confidentiality. A lot of people are thinking to protect their computer and prevent unauthorized data access. Software security system is one of the most important part of business and investation development, since a good security system will minimize the risk of losing the value stored in data and informations.

Keywords: optimalization, security, data, information, software, implementation

I. PENDAHULUAN

Dalam membahas optimaslisasi keamanan data dan informasi serta implementasinya, diperlukan latar belakang, rumusan masalah, serta tujuan penelitian yang akan mendukung dan meninjau apa tujuan awal dari pembuatan makalah ini dan apakah tujuan tersebut dapat tercapai.

1.1 Latar Belakang

Data adalah catatan atas kumpulan fakta. Data merupakan bentuk jamak dari datum, berasal dari bahasa Latin yang berarti "sesuatu yang diberikan". Dalam penggunaan sehari-hari data berarti suatu pernyataan yang diterima secara apa adanya. Pernyataan ini adalah hasil pengukuran atau pengamatan suatu variabel yang bentuknya dapat berupa angka, kata-kata, atau citra. Dalam keilmuan (ilmiah), fakta dikumpulkan untuk menjadi data. Data kemudian diolah sehingga dapat diutarakan secara jelas dan tepat sehingga dapat dimengerti oleh orang lain yang tidak langsung mengalaminya sendiri [1]. Sedangkan informasi, menurut *Kadir* dan *McFadden*, merupakan data yang telah diproses. Pemrosesan data tersebut dilakukan sedemikian rupa sehingga data yang telah diproses tersebut dapat meningkatkan pengetahuan orang yang menerima dan menggunakannya [2]. Data dan informasi merupakan asset yang sangat penting dan berharga bagi suatu organisasi. Tentunya data dan informasi tersebut harus diamankan agar tidak terjadi *data loss*, *data theft* maupun *data corruption*. Namun sayangnya, banyak organisasi yang belum mengetahui ataupun mengimplementasikan pengamanan data secara optimal. Dengan mengetahui langkah-langkah yang tepat, diharapkan orang-orang dapat lebih memahami dan memaksimalkan pengimplementasian pengamanan data dan informasi sehingga data keamanan data pengguna dapat lebih terjamin.

1.2 Rumusan Masalah

Melalui pembahasan latar belakang, sebagai solusinya maka akan dibuat analisis mengenai langkah-langkah yang dapat ditempuh untuk mengoptimalkan keamanan data dan informasi beserta implementasinya dalam suatu organisasi, sehingga para *stakeholder* dapat mengambil keputusan lebih tepat berkaitan dengan keamanan data dan informasi. Oleh sebab itu, rumusan masalah pada penelitian ini adalah:

1) Bagaimana model proses yang dapat diimplementasikan untuk mengoptimalkan langkah pengamanan data yang telah ditempuh oleh suatu organisasi?

1.3 Pembatasan Masalah

Dalam penelitian ini, ruang lingkup yang akan dibuat berfokus pada hal-hal sebagai berikut:

1) Penelitian ini ditujukan bagi pembaca umum, khususnya yang tergabung didalam sebuah organisasi.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah didefinisikan, maka tujuan dari penelitian ini adalah:

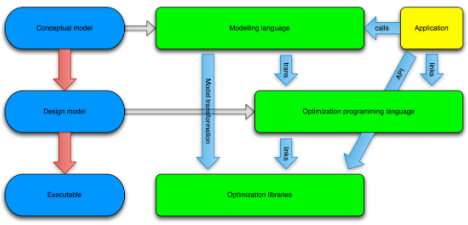
1) Mengkaji serta menganalisis model proses yang dapat diimplementasikan untuk mengoptimalkan langkah pengamanan data yang telah ditempuh oleh suatu organsiasi sehingga dapat mengambil keputusan yang lebih baik di masa mendatang

II. TINJAUAN PUSTAKA

Pada bab ini, penulis akan membahas teori pada topik optimalisasi keamanan data pada perangkat lunak dan implementasinya.

2.1 Optimalisasi Teknologi

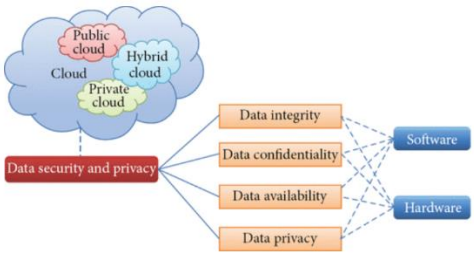
Memasuki era modernisasi dimana teknologi berkembang dengan sangat pesat yang ditandai dengan semakin cepatnya informasi menyebar melalui perangkat telekomunikasi, maka diperlukan langkah-langkah optimisasi agar informasi yang berasal dari sumber dapat sampai kepada penerima melalui tahapan yang efisien dan menekan kebutuhan sumber daya [3]. Menurut *de la Banda*, *Stuckey*, *van Hentenryck* dan *Wallace* (2014), optimalisasi teknologi adalah sebuah proses yang fleksibel dan terus menerus berubah dengan pesat mengikuti pola perkembangan zaman, dua tantangan dalam prosesnya, yaitu 1) ***Modelling and Solving***, yaitu sebuah langkah yang bertujuan untuk merumuskan masalah yang sedang dihadapi teknologi saat ini dan merancang sebuah *prototype* yang diharapkan dapat menjadi solusi dari masalah tersebut. Solusi yang akan diimplementasikan adalah solusi yang memenuhi syarat sebagai solusi terefisien dan dapat dipadukan dengan teknologi yang tersedia; 2) ***Optimization Tools***, dimana untuk merancang solusi yang mumpuni dibutuhkan setidaknya tiga alat yaitu, sebuah bahasa perancangan universal yang mudah dipahami dan fleksibel, sebuah bahasa pemrograman untuk menerapkan optimisasi dan integrase berdasarkan solusi yang telah dirancang, dan sebuah *Optimization Library* yang merupakan inti dari proses optimisasi yang dijalankan [4].



Gambar 2.1: Komponen Optimalisasi Teknologi [4]

2.2 Keamanan Data

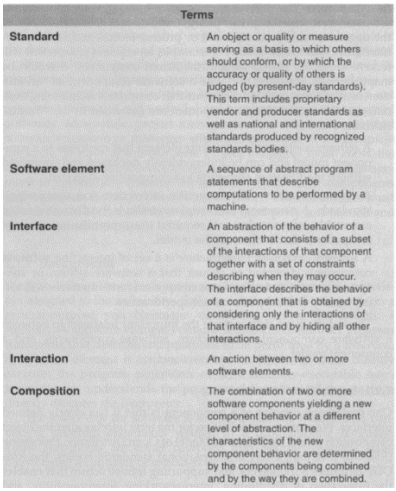
Keamanan data adalah salah satu masalah penting dalam dunia teknologi informasi, terutama pada era *cloud computing*, dimana keseluruhan data tersimpan secara terpisah dari komputer lokal. Keamanan sendiri merupakan kombinasi dari berbagai faktor, yaitu *confidentiality*, *prevention of unauthorized disclosure of information*, *integrity*, *prevention of the unauthorized amendment or deletion of information*, *availability*, dan *prevention of unauthorized withholding of information* [5]. Menurut *Rao* dan *Selvamani* (2015), ada sembilan tantangan yang harus dihadapi untuk mengamankan data, yaitu 1) ***Security,*** dimana keamanan data tersebut harus tetap terjamin dari segala serangan seperti *Cross-site Scripting* dan *Access Control Mechanisms*. 2) ***Locality***, pengguna data wajib mengetahui secara tepat lokasi dimana data mereka tersimpan. 3) ***Integrity***, keamanan data wajib dipertahankan sehingga hanya pemilik data yang dapat mengakses, merubah atau menghapus data miliknya, hal ini untuk mengantisipasi terjadinya *data lost* atau *data theft*. 4) ***Access***, penyedia jasa wajib menjamin bahwa data seseorang hanya dapat diakses oleh pemilik data yang bersangkutan dengan cara melakukan *encryption* atau *key management* sehingga hanya pengguna yang memiliki *hashkey* yang sesuai dengan sistem yang akan diperbolehkan untuk mengakses data. 5) ***Confidentiality***, data yang tersimpan dalam sistem wajib terjaga kerahasiaannya. 6) ***Breaches***, keamanan data harus dipertahankan dari segala ancaman dan serangan pencurian data, dan sistem keamanan data harus dioptimalisasi sebaik mungkin untuk menghindari *breaches* atau pengaksesan data secara tidak sah. 7) ***Segregation***, untuk menghindari resiko kehilangan data secara keseluruhan pada saat terjadi serangan, dapat diterapkan langkah *segregation* atau pemisahan data menjadi beberapa bagian yang masing-masing bagian disimpan secara terpisah pada sistem yang berbeda-beda. 8) ***Storage***, data yang tersimpan pada sistem yang berbeda (*cloud storage*) tentu memiliki resiko pencurian data yang lebih besar jika dibandingkan dengan data yang tersimpan secara fisik. 9) ***Data Center Operation***, pada saat terjadi bencana, penyedia jasa wajib penjamin keutuhan data yang tersimpan [6].



Gambar 2.2: Komponen Keamanan dan Privasi Data [5]

2.3 Perangkat Lunak

Perangkat lunak adalah sebuah perangkat multiguna yang dibuat untuk melakukan eksekusi program berbasis *von Neumann architecture*. Elemen perangkat lunak berisi langkah-langkah (*sequence*) pengoperasian program tersebut secara abstrak serta hasil program yang diharapkan. Perangkat lunak bersifat *machine-executable*, dimana program dapat langsung mengerti pernyataan-pernyataan yang terdapat pada elemen perangkat lunak dan dapat langsung mengeksekusinya dan menghasilkan keluaran program yang diharapkan [7]. Menurut *Kusuma Dewi* dan *Azhari SN*, terdapat beberapa kesalahan dalam perancangan perangkat lunak yang dapat mengancam keamanan, seperti 1) **Kesalahan persyaratan spesifikasi** (*Requirement specification*) dimana terdapa kesalahan atau kekurangan persayaratan pada saat perancangan perangkat lunak. 2) **Kesalahan Desain**, yaitu kesalahan pada *logical decision*, yang merupakan representasi dari keputusan desain sehingga menyebabkan kesalahan pada tahap pembuatan desain. 3) **Kesalahan *Source Code***, kesalahan yang di sebabkan karena desain akan bedampak pada saat coding sehingga dapat menyebabkan kesalahan pada saat tahap implementasi [8].

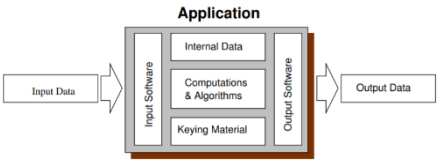


Terms	
Standard	An object or quality or measure serving as a basis to which others should conform, or by which the accuracy or quality of others is judged (by present-day standards). This term includes proprietary vendor and producer standards as well as national and international standards produced by recognized standards bodies.
Software element	A sequence of abstract program statements that describe computations to be performed by a machine.
Interface	An abstraction of the behavior of a component that consists of a subset of the interactions of that component together with a set of constraints describing when they may occur. The interface describes the behavior of a component that is obtained by considering only the interactions of that interface and by hiding all other interactions.
Interaction	An action between two or more software elements.
Composition	The combination of two or more software components yielding a new component behavior at a different level of abstraction. The characteristics of the new component behavior are determined by the components being combined and by the way they are combined.

Gambar 2.3: Komponen Perangkat Lunak [7]

2.4 Keamanan Perangkat Lunak

Keamanan perangkat lunak adalah sebuah cabang ilmu yang mempelajari proteksi perangkat lunak berikut elemen data yang terkandung di dalamnya, terhadap ancaman-ancaman eksternal seperti pengaksesan dan pemodifikasian data tanpa izin, eksploitasi data, dan sebagainya. Keamanan perangkat lunak sangat bergantung pada langkah-langkah yang diambil untuk memproteksi elemen data yang terkandung dalam perangkat lunak tersebut. Menurut *Main* dan *van Oorschot* (2003), proteksi keamanan perangkat lunak bergantung pada kumpulan prinsip, teknik dan pendekatan yang ditujukan untuk meningkatkan keamanan perangkat lunak, memberikan perlindungan terhadap serangan yang berbasis *buffer flow* hingga *reverse engineering and tampering*. Tingkat keamanan perangkat lunak bergantung pada konsep dan pendekatan yang diterapkan teknisi terhadap kemungkinan serangan terhadap perangkat lunak tersebut, dan pengetahuan yang mumpuni akan tipe-tipe serangan terhadap keamanan data sangat krusial untuk menjamin keamanan perangkat lunak [9].



Gambar 2.4: Aplikasi Keamanan Perangkat Lunak [9]

2.5 Implementasi Keamanan Data dan Perangkat Lunak

Seperti yang telah dibahas pada subbab-subbab sebelumnya, keamanan data dan perangkat lunak merupakan isu penting yang memiliki resiko tinggi, sehingga dibutuhkan langkah-langkah yang cerdas untuk menyikapinya. Menurut *Bublitz* (2013), terdapat tujuh langkah untuk mengimplementasikan optimalisasi keamanan data dan perangkat lunak, yaitu 1) ***Quick Evaluation and Planning***, melakukan evaluasi mengenai keadaan terkini keamanan data dan perangkat lunak pada suatu organisasi, mengerti titik kelemahan sistem keamanan, kemudian membuat suatu perencanaan untuk peningkatan proteksi pada perangkat lunak, baik untuk jangka pendek maupun jangka panjang. 2) ***Specify the risk and threats to the software***, menganalisa dan mengidentifikasi ancaman-ancaman yang mungkin dihadapi oleh perangkat lunak untuk memudahkan perancangan peningkatan keamanan data dan perangkat lunak. 3) ***Review the code***, memeriksa kembali kode pemrograman yang digunakan oleh perangkat lunak saat ini, kemudian menganalisa dan mengidentifikasi dengan metode *filtering, querying and sorting*, celah-celah keamanan yang memungkinkan terjadinya serangan seperti kebocoran data atau pencurian data. 4) ***Test and verify***, melakukan ujicoba terhadap celah-celah keamanan yang telah ditemukan, untuk mendapatkan solusi perbaikan yang tepat. Metode yang digunakan pada umumnya adalah *trial and error penetration testing*, yaitu menguji suatu celah keamanan secara terus menerus menggunakan berbagai *input* yang dimungkinkan. 5) ***Build a security gate***, yang merupakan sebuah metode pencegahan yang senantiasa berjalan seiring perangkat lunak dirilis ke pasaran, pada umumnya metode yang diterapkan adalah pemindaian keamanan secara terus menerus untuk menemukan celah keamanan baru dan memperbaikinya sebelum dapat dieksploitasi oleh peretas. 6) ***Measure***, melakukan pengukuran dan pencatatan perubahan tingkat kerentanan data setiap optimalisasi dilakukan. Optimalisasi keamanan data dan perangkat lunak berhasil jika jumlah serangan dan pembobolan data menurun setelah dilakukan optimalisasi. 7) ***Educate***, mengedukasi pengguna awam mengenai pentingnya keamanan data dan perangkat lunak, sehingga mereka lebih sadar mengenai bahaya peretasan data dan dapat mengimplementasikan secara otodidak langkah-langkah optimalisasi yang telah disebutkan diatas [10].

Gambar 2.5: Komponen Implementasi Keamanan Data dan Perangkat Lunak [10]

2.7 Tabel Penelitian Relevan

Tabel dibawah ini membahas mengenai duabelas paper terpublikasi yang membahas dan membantu memperkuat studi kepustakaan ini.

No	Nama Pengarang (Tahun)	Rumusan Masalah	Metode Penelitian	Hasil
1.	Harika, P dan Venkata Ramana (2018) [11]	Bagaimana proses pertukaran data yang aman berdasarkan skema *Key Generations Center* (KGC) ?	Pendekatan deskriptif kualitatif	Protokol KGC merupakan skema *Key Agreement* yang merupakan salah satu skema protokol pertukaran data untuk komputasi awan teraman. Berikut langkah-langkah operasi protokol KGC: 1) *Initialization of KGC* 2) *User Registration* 3) *Group Key Generation and Distribution*
2.	Jumardi, Rio (2018) [12]	Apa kebijakan yang harus diambil berkaitan dengan keamanan sistem informasi sebagai bentuk perlindungan informasi suatu organisasi?	Pendekatan deskriptif kualitatif	Perlindungan yang diberikan tidak hanya terhadap informasi sebuah organisasi akan tetapi perlindungan juga akan diberikan terhadap kerahasiaan pribadi personel organisasi tersebut. Oleh karena itu perlu diambil kebijakan pemeliharaan sistem, penanganan resiko, pengaturan hak akses dan sumber daya manusia, keamanan dan pengendalian asset informasi dan kebijakan keamanan server.

3.	Islami, Maulia Jayantina (2017) [13]	Apa saja yang menjadi tantangan dalam implementasi strategi keamanan siber nasional?	Studi literatur	Tantangan dan hambatan implementasi strategi nasional keamanan siber dari sisi sumber daya manusia, prosedur dan kebijakan pencegahan dan keamanan yang masih memerlukan koordinasi dengan seluruh pemangku kebijakan bagi dari sektor swasta, pemerintah, masyarakat, dan institusi luar negeri yang merupakan pengembang dari aplikasi-aplikasi yang seringkali dipergunakan sebagai media kejahatan siber, dan teknologi yang harus dikembangkan seiring dengan meningkatnya jenis serangan siber.
4.	Kusumawati, Diah, Bagus Winarko, Riva'atul Adaniah Wahab dan Wirianto Pradono (2017) [14]	Apa saja aspek keamanan yang perlu diregulasi agar menjamin perkembangan *Internet of Things* (IOT) ?	Pendekatan kualitatif	Aspek yang perlu diregulasi adalah perlindungan data pribadi, keamanan data, manajemen akses data, tata kelola data, interoperabilitas, keamanan transmisi data, enkripsi data, keamanan jaringan, keamanan konektivitas, dan keamanan pada aplikasi IoT.

5.	Sonia dan Kirti Bhatia (2017) [15]	Apa saja kebijakan utama dari penerapan model keamanan data *Security Inclusive Policy Driven Cloud Model* ?	Analisis permodelan	Dalam mengembangkan sistem keamanan data inklusif berbasis *Policy Driven*, perlu diperhatikan empat kebijakan utama berikut: 1) *User level policy* 2) *Data localization policy* 3) *Security policy* 4) *Service selection policy*
6.	Wahyu, Ari Purno (2017) [16]	Bagaimana langkah optimasi keamanan jaringan LAN menggunakan VLAN dan dukungan VOIP?	Eksperimen	Optimasi jaringan LAN menggunakan VLAN ternyata bisa dan mudah diimplemetasikan, jaringan akan lebih aman dan memiliki security yang tinggi karena menggunakan IP *virtual* yang bisa dengan mudah di-setting oleh admin. Sedangkan penggunaan VOIP sangat mendukung kerja dalam hal proses komunikasi keluar negeri yang biasanya menggunakan tarif SLJJ yang relatif mahal sekarang bisa menggunakan VOIP dengan kapasitas bandwith yang diperbesar bisa digunakan untuk komunikasi webbex. Pengembangan VOIP dapat menggunakan *device* dengan penambahan layer security antara lain menggunakan PBAX, *asterix* atau *firewall*.

7.	Hernikawati, Dewi (2016) [17]	Bagaimana hubungan antara *risk tolerance* dan *risk perception* terhadap keamanan informasi?	Pendekatan kuantitatif dengan metode *sampling*	Variabel Keamanan Informasi dipengaruhi oleh variabel *risk tolerance* dan risk perception. Koefisien korelasi untuk variabel *risk perception* adalah -0.253 dapat disimpulkan bahwa semakin rendah *risk perception* seseorang maka akan semakin tinggi kemanan informasi orang tersebut. Untuk nilai koefisien korelasi dari *variable risk tolerance* terhadap keamanan Informasi adalah -0.264. Hal ini menunjukkan bahwa terdapat hubungan negatif yang signifikan antara *risk tolerance* dengan keamanan informasi. Semakin rendah *risk tolerance* seseorang maka akan semakin tinggi keamanan informasi orang tersebut
8.	Hernikawati, Dewi (2016) [18]	Bagaimana penerapan teori perilaku sumber daya manusia dalam menghadapi ancaman keamanan data?	Studi literatur untuk menghasilkan model penelitian	Premis yang dapat diterapkan adalah, sebagai langkah awal seseorang akan menerima informasi yang akan mengarah pada evaluasi dan reaksi baik secara *verbal persuasion* maupun *observational learning*. Kemudian dapat dihasilkan dua metode penerapan teori perilaku sumber daya manusia terhadap ancaman keamanan data, yaitu persepsi ketidapkastian (*Threat Appraisal*) dan kepercayaan pada kemampuan (*Threat Coping*)

9.	Karima, Aisyatul dan Saputro, Ari (2016) [19]	Bagaimana algoritma *ElGamal* dapat melindungi dan menjaga keamanan data?	Penelitian dan eksperimen dengan menggunakan *model*	Algoritma kriptografi kunci publik *ElGamal* merupakan algoritma blok *chipper* yaitu algoritma yang melakukan proses enkripsi pada blok-blok plainteks yang kemudian menghasilkan blok-blok *chipertext*, yang nantinya blok-blok *chipertext* tersebut akan didekripsi kembali dan hasilnya kemudian digabungkan menjadi plainteks semula. Keamanan algoritma *ElGamal* terletak pada kesulitan perhitungan logaritma diskrit pada modulo prima yang besar, sehingga upaya untuk menyelesaikan masalah logaritma ini menjadi sulit untuk dipecahkan.
10.	Marco, Robert (2016) [20]	Apa saja langkah-langkah *risk assessment* yang perlu dilakukan untuk mengetahui tingkat keamanan data	Metode deskriptif dengan pendekatan penelitian kualitatif dan kuantitatif	Dalam tahapan risk assessment terdiri dari beberapa langkah, meliputi: 1. Melakukan identifikasi asset 2.Melakukan identifikasi kerawanan dan ancaman 3. Menentukan prioritas resiko 4. Mengembangkan *control* 5. *Monitoring*

11.	Prabowo, Ramadhan Triyanto dan Mochamad Teguh Kurniawan (2015) [21]	Bagaimana susunan infrastruktur pusat data yang tepat dan aman mengacu pada analisis keamanan jaringan Indonesia?	Analisis berkelanjutan	Berdasarkan hasil analisis, permodelan infrastruktur pusat data yang tepat dan aman sesuai tingkat resiko keamanan jaringan data di Indonesia disarankan dilakukan penambahan perangkat *intrusion detection and prevention system* yang terletak antara *firewall* dan klien sebagai *aggression system*, serta penempatan layanan pusat data yang terpusat pada satu titik dibelakang *agression system*, sehingga pusat data akan lebih terlindungi
12.	Srivastava, Arpit Kumar, Apoorv Agarwal dan Abhinav Mathur (2015) [22]	Apa saja resiko keamanan data yang dihadapi oleh perangkat *Internet of Things*?	Studi literatur	Resiko keamanan data yang dihadapi oleh perangkat *Internet of Things* mencakup 1) *Terminal security issue* 2) *Sensor network security* 3) *Information transmission security* 4) *Information processing security* 5) *Encryption security*

13.	Syarif, Akmal Rifqi dan Agung Nugroho (2015) [23]	Bagaimana penerapan standar keamanan informasi organisasi yang sesuai dengan ISO 27001?	Studi literatur	Untuk sebuah organisasi menerapkan standar keamanan informasi ISO 27001, organisasi tersebut perlu terlebih dahulu mendefinisikan rencana kebijakan keamanan informasi yang akan ditempuhnya. Kemudian, berdasarkan kebijakan tersebut, menganalisa resiko secara *risk assesment* yang akan timbul terhadap keamanan informasi. Setelah organisasi terbukti mampu melakukan mitigasi resiko dan ancaman yang timbul (*risk treatment*), organisasi dapat mendefinisikan standar kemampuan perlindungan keamanan informasi, untuk kemudian diukur menurut standar ISO 27001.
14.	Kinasih, Bondan Satrio dan Albari (2012) [24]	Apa saja fitur yang harus diimplementasikan untuk meningkatkan persepsi keamanan data pada masyarakat?	Pendekatan kuantitatif dengan metode *sampling*	Diperlukan evaluasi dalam fitur dan atribut keamanan, yang meliputi kemungkinan: 1) Situs tersebut menyediakan enkripsi, 2) Situs yang mengharuskan pengguna untuk mengatur akun dengan ID dan password 3) Konfirmasi di tampilkan layar setelah pengguna melakukan perubahan data 4) Pemakaian Secure Socket Layer, dalam transaksi *online*
15.	Kartika, I Made, Restyandito dan Sri Suwarno (2010) [25]	Bagaimana cara kerja *Software Encryption Algorithm* untuk menjaga kerahasiaan data?	Studi literatur	Enkripsi dan dekripsi dilakukan oleh komputer dengan mengambil *ciphertext* dan mengubahnya ke dalam bentuk *byte* untuk kemudian dimasukkan ke dalam algoritma *Secure Hash Algorithm* yang akan terbentuk tabel T, S dan R yang akan dilakukan operasi XOR satu sama lain.

16.	Albone, Aan (2009) [26]	Bagaimana langkah pembuatan rencana keamanan informasi berdasarkan analisis dan mitigasi resiko teknologi informasi?	Studi literatur	Analisis risiko menghasilkan tingkatan risiko, berdasarkan identifikasi kelemahan, ancaman dan kecenderungan, yang dihadapi oleh perusahaan, serta rekomendasi kontrol keamanan untuk menurunkan risiko. Rencana keamanan informasi disusun berdasarkan tujuan dan sasaran keamanan informasi perusahaan, yang didukung oleh hasil penilaian dan mitigasi risiko yang komprehensif. Sehingga dapat menjadi panduan dalam penerapan keamanan informasi, dengan langkah implementasi kontrol keamanan, untuk mencapai tujuan dan sasaran keamanan informasi tersebut harus diturunkan dengan mengimplementasikan beberapa kontrol keamanan yang direkomendasikan.
17.	Paryati (2008) [27]	Apa saja cara yang dapat dimplementasikan untuk mengamankan data pada suatu sistem?	Studi literatur	Ada banyak cara mengamankan data atau informasi pada sebauh sistem. Beberapa diantaranya adalah: 1) Pengendalian akses 2) Memantau serangan 3) Penggunaan enkripsi
18.	Supriyanto, Aji (2007) [28]	Apa yang menjadi pokok keamanan data dan informasi?	Studi literatur	Prinsip keamanan informasi akan digunakan sebagai acuan dalam mengembangkan sistem keamanan dalam sebuah organisasi oleh para user, rekayasa sistem, spesialis IT, manajer program dan petugas keamanan sistem informasi. Prinsip tersebut memiliki 6 kelompok yaitu sebagai landasan keamanan, pokok keamanan, mudah digunakan, nyaman dan menyenangkan, dapat mengurangi ancaman serangan, serta digunakan untuk merancang dan menjaga keamanan.

19.	Triantono, Henricus Bambang (2007) [29]	Bagaimana standar keamanan sistem manajemen data yang sesuai dengan BS 7799 / ISO 17799?	Studi literatur	Dalam menciptakan keamanan informasi berikut ini ada sepuluh langkah yang akan dilakukan bila perusahaan betul-betul ingin mewujudkan keamanan informasinya sesuai dengan standar BS 7799 / ISO 17799. 1) Mendefinisikan kebijakan keamanan data perusahaan, 2) Dapat dilakukan penunjukan penannggung jawab keamanan data, 3) Melakukan inventarisasi asset informasi, 4) Melakukan seleksi terhadap staf kunci, 5) Meliindungi asset informasi secara fisik, 6) Mempraktikkan pengelolaan jaringan yang efektif, 7) Menciptakan aturan pengendalian akses yang ketat, 8) Bangun keamanan di dalam semua sistem dan aplikasi, 9) Merencanakan pengembangan terhadap kelangsungan bisnis, 10) Pastikan kepatuhan terhadap peraturan perundang-undangan yang berlaku
20.	Murti, Hari (2006) [30]	Apa saja tujuan keamanan sistem komputer secara umum?	Studi literatur	Tujuan keamanan komputer secara umum adalah mengamankan sumber daya (*resources*) komputer seperti hardware, software, jaringan komunikasi, dan yang paling penting adalah dokumen (data/informasi). Data atau informasi dianggap aman jika memenuhi persyaratan berupa kerahasiaan (*confidentiality*), integrasi (*integration*), dan otentikasi (*authentication*). Persyaratan tersebut merupakan bagian dari aspek keamanan yang harus dipenuhi, yang merupakan bentuk pertimbangan yang menyatakan sebuah komputer dapat dinyatakan aman.

Berdasarkan tabel 2.7 mengenai perbandingan beberapa penelitian serupa yang memperkuat topik "Optimalisasi Keamanan Data dan Informasi Pada Perangkat Lunak dan Implementasinya", dapat disimpulkan bahwa keamanan data dan informasi merupakan suatu hal yang penting dalam dunia teknologi, dan dibutuhkan investasi yang cukup besar untuk menjaga agar data pengguna tetap aman dari ancaman dan serangan. Untuk menentukan implementasi keamanan data yang tepat untuk suatu organisasi, tentu harus dilakukan analisis resiko (*risk assessment*) dan pengembangan persepsi terlebih dahulu, untuk kemudian ditentukan berapa *variable risk acceptance* dan *risk tolerance*. Terdapat beberapa langkah yang sesuai dengan standar internasional yang dapat diimplementasikan untuk meningkatkan keamanan data dan informasi, seperti pengendalian akses dan enkripsi.

III. METODOLOGI PENELITIAN

Pada bab ini penulis akan membahas mengenai jenis penelitian, metode pengumpulan data dan analisis data dari topik optimalisasi keamanan data dan informasi pada perangkat lunak dan implementasinya.

3.1 Jenis Penelitian

Penelitian ini merupakan penelitian dengan menggunakan jenis penelitian studi literatur dengan memberikan referensi dari setidaknya duapuluh paper atau jurnal terpublikasi secara nasional untuk memperkuat penulisan makalah ini yang sesuai dengan topik "Optimalisasi Keamanan Data dan Informasi Pada Perangkat Lunak dan Implementasinya".

3.2 Metode Pengumpulan Data

Metode yang dipakai pada penlitian ini adalah studi literatur. Oleh karena itu, data dan sumber dari penulisan penelitian ini dihimpun dari jurnal dan buku yang membahas tentang topik serupa di masa lampau.

3.3 Metode Analisis Data

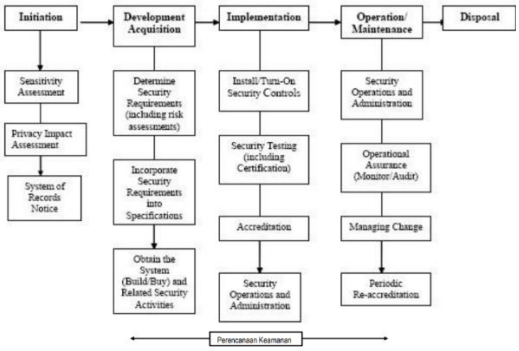
Data dan sumber yang telah diperoleh dan dituliskan di penelitian ini kemudian dianalisa dengan metode analisis deskriptif. Metode ini dilakukan dengan cara mendeskripsikan teori dan fakta yang didapat dari fakta yang berasal dari jurnal dan buku, untuk kemudian di pahami dan di analisa, sehingga dari teori yang telah diuraikan, penulis juga memberikan pemahaman dan penjelasan yang berkaitan dengan teori tersebut.

IV. ANALISIS DAN PEMBAHASAN

Berdasarkan landasan teori pada Bab II, dapat di analisis bahwa optimalisasi keamanan data sangat penting untuk dilakukan, agar data yang tesimpan terjaga kerahasiaannya dan terhindar dari akses dan modifikasi oleh pihak-pihak yang tidak bertanggungj jawab. Dalam prakteknya, optimalisasi keamanan data menemui dua tantangan, yaitu merumuskan *Modelling and Solving* dan menggunakan *Optimalization Tools* yang tepat. Keamanan data wajib memerhatikan sembilan aspek, yaitu, 1) *Security,* 2) *Locality*, 3) *Integrity*, 4) *Access*, 5) *Confidentiality*, 6) *Breaches*, 7) *Segregation*, 8) *Storage* dan 9) *Data Center Operation*. Tujuan optimalisasi keamanan data adalah untuk mengeliminasi kesalahan persyaratan spesifikasi, kesalahan desain dan kesalahan *source code* pada tahap pengembangan aplikasi keamanan data. Dalam implementasinya, optimalisasi keamanan data perlu mempertimbangkan tujuh aspek yaitu, 1) *Quick Evaluation and Planning*, 2) *Specify the risk and threats to the software*, 3) *Review the code*, 4) *Test and verify*, 5) *Build a security gate*, 6) *Measure,* dan 7) *Educate*.

4.1 Prinsip Keamanan Informasi

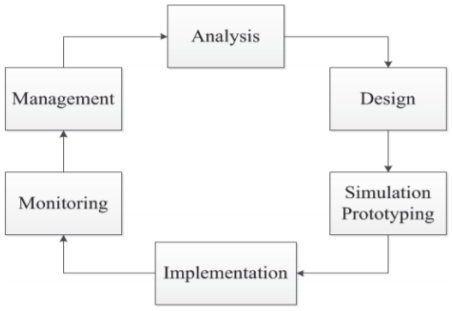
Tujuan keamanan komputer secara umum adalah mengamankan sumber daya (*resources*) komputer seperti hardware, software, jaringan komunikasi, dan yang paling penting adalah dokumen (data/informasi). Data atau informasi dianggap aman jika memenuhi persyaratan berupa kerahasiaan (*confidentiality*), integrasi (*integration*), dan otentikasi (*authentication*). Persyaratan tersebut merupakan bagian dari aspek keamanan yang harus dipenuhi, yang merupakan bentuk pertimbangan yang menyatakan sebuah komputer dapat dinyatakan aman. Dalam mengimplementasikan keamanan informasi, sebuah organisasi dapat menggunakan permodelan rumusan masalah berikut ini. Pertama, menentukan manfaat penggunaan sistem informasi bagi organisasi. Kedua, menentukan prosedur keterhubungan jaringan sistem informasi organisasi. Ketiga, menentukan keterhubungan komputer lokal dalam jaringan organisasi tersebut. Keempat, menentukan personalia yang memiliki akses fisik terhadap jaringan komputer organisasi. Kelima, menentukan personalia ahli yang bertanggungjawab terhadap implementasi keamanan informasi pada organisasi. rinsip keamanan informasi akan digunakan sebagai acuan dalam mengembangkan sistem keamanan dalam sebuah organisasi oleh para user, rekayasa sistem, spesialis IT, manajer program dan petugas keamanan sistem informasi. Keamanan informasi yang akan dikembangkan memiliki enam prinsip, yaitu 1) Sebagai landasan untuk menetapkan kebijakan ukuran keamanan sebagai dasar perancangan sistem informasi yang menggambarkan secara jelas batasan ancaman integral dari sistem informasi yang dimaksud. 2) Sebagai pokok keamanan yang mengasumsikan bahwa sistem eksternal tidaklah aman sehingga organisasi harus mengidentifikasikan potensi resiko keamanan yang mungkin terjadi agar dapat menerapkan penyesuaian ukuran sistem keamanan organisasi yang dapat mengurangi resiko hingga level yang tepat, sehingga kemanan informasi tetap terjamin. 3) Sistem keamanan informasi harus mudah digunakan dan menggukan bahasa yang umum, dengan menerapkan standar terbuka untuk protabilitas dan interoprabilitas dan dapat memberikan adopsi terhadap teknologi baru yang lebih maju. 4) Sistem keamanan informasi harus dapat digunakan dengan nyaman dan menyenangkan, dengan menggunakan mekanisme pembatasan untuk memisahkan sistem komputer dengan infrastruktur jaringan yang dirancang untuk membatasi kerusakan dan serangan yang diterapkan pada lapis keamanan sehingga tidak ada celah serangan. 5) Sistem keamanan informasi harus dapat mengurangi ancaman serangan namun mengusahakan agar sistem tetap sederhana dan hanya menerapkan mekanisme keamanan yang diperlukan. 6) Sistem keamanan informasi harus dapat mengimplementasikan keamanan sampai pada kombinasi distribusi secara fisik dan logis dengan cara mengotentikasi *user* dan menerapkan identitas yang unik untuk menjamin akuntabilitas.



Gambar 4.1 Siklus Hidup Keamanan Informasi [28]

4.2 Keamanan Jaringan Komputer

Keamanan jaringan komputer merupakan hal yang tidak terpisahkan dalam jaringan komputer. Keamanan jaringan komputer yang tidak dirancang dengan baik dapat menyebabkan kebocoran data, pelanggaran privasi, hingga kerugian finansial. Oleh karena itu, dibutuhkan rancangan keamanan jaringan komputer yang dapat memenuhi kebutuhan dari pengguna layanan jaringan komputer. permodelan infrastruktur pusat data yang tepat dan aman sesuai tingkat resiko keamanan jaringan data di Indonesia disarankan dilakukan penambahan perangkat *intrusion detection and prevention system* yang terletak antara *firewall* dan klien sebagai *aggression system*, serta penempatan layanan pusat data yang terpusat pada satu titik dibelakang *agression system*, sehingga pusat data akan lebih terlindungi. Dari segi server, dapat diimplementasikan tiga hal, 1) Simulasi serangan DoS/DDos. Hal ini ditujukan untuk mengantisipasi terjadinya UDP *flooding*. Simulasi dilakukan untuk mengetahui dampak dari serangan tersebut, dan dilakukan dengan cara mengirimkan paket UDP secara terus-menerus oleh beberapa *host*, lalu diukur jumlah lalu lintas paket UDP pada *server*. 2) Pengaktifan *Intrusion Detection/Prevention System* (IDPS). Perangkat ini bertujuan untuk mendeteksi serangan TCP SYN *flood* dan serangan UDP *flood* sehingga langkah-langkah mitigasi yang tepat dapat diimplementasikan. 3) Menggunakan VPN untuk Koneksi SSH. Koneksi SSH diperlukan untuk mengakses dan mengendalikan *server* dari jarak jauh. Koneksi ini harus aman karena koneksi ini memperbolehkan pengguna dari jarak jauh untuk dapat melakukan perubahan sistem pada server. Oleh sebab itu, diperlukan implementasi VPN untuk mengamankan koneksi SSH. Setelah koneksi VPN berhasil dilakukan, maka pengguna dapat melakukan koneksi SSH pada *server* menggunakan private IP *address* milik *server*. Dari segi terminal jaringan lokal (*Local Area Network*), optimasi jaringan LAN dapat menggunakan VLAN sehingga jaringan akan lebih aman dan memiliki *security* yang tinggi karena menggunakan IP *virtual* yang dapat dengan mudah diatur oleh admin. Sedangkan penggunaan VOIP sangat mendukung kerja dalam hal proses komunikasi keluar negeri yang biasanya menggunakan tarif SLJJ yang relatif mahal sekarang bisa menggunakan VOIP dengan kapasitas bandwith yang diperbesar bisa digunakan untuk komunikasi webbex. Pengembangan VOIP dapat menggunakan *device* dengan penambahan layer security antara lain menggunakan PBAX, *asterix* atau *firewall*.

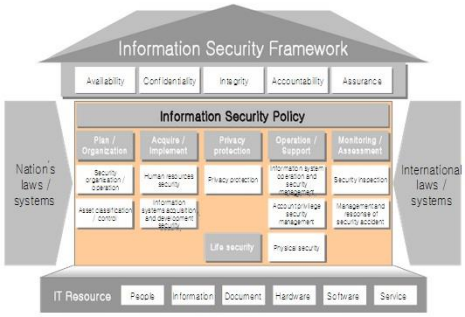


Gambar 4.2: *Network Development Life Cycle (NDLC)* [21]

4.3 Kebijakan Keamanan Sistem Informasi

Kebijakan keamanan sistem informasi dapat didefinisikan sebagai sebuah rencana tindakan untuk menangani masalah keamanan informasi, atau satu set peraturan untuk mempertahankan kondisi atau tingkat keamanan informasi tertentu. Setidaknya terdapat lima kebijakan yang dapat ditempuh oleh sebuah organisasi untuk menjamin keamanan sistem informasi. 1) Kebijakan Perawatan Sistem, diperlukan untuk memaksimalkan perawatan terhadap sistem yang berjalan sehingga sistem informasi yang diimplementasikan berjalan dengan baik. 2) Kebijakan Penanganan Resiko, mengidentifikasi dan menganalisis resiko-resiko yang mungkin terjadi pada saat implementasi sistem informasi pada sebuah organisasi. 3) Kebijakan Pengendalian

Akses, diperlukan untuk mengatur batasan-batasan dari pengguna sistem informasi suatu organisasi sebagai upaya pengurangan resiko dari penyalahgunaan fungsi atau wewenang akibat kesalahan manusia. Langkah yang dapat ditempuh sebagai berikut; identifikasi pengguna (*user identification*), pembuktian keaslian pengguna (*user verification*), dan otorisasi pengguna (*user authorization*). 4) Kebijakan Keamanan dan Pengendalian Aset Informasi, diperlukan untuk mengatur dan mengelola asset informasi perusahaan untuk memberikan perlindungan yang sesuai dengan tingkat resiko keamanan asset. Organisasi dapat mengimplementasikan sistem pemantau (*monitoring system*) yang dapat digunakan untuk mengetahui adanya penyusup yang masuk kedalam sistem (*intruder*) atau adanya serangan (*atta*ck) dari *hacker*. 5) Kebijakan Keamanan Server, diperlukan untuk memaksimalkan keamanan terhadap server data yang secara langsung juga akan menjaga kerahasiaan data terhadap kejahatan komputer yang akan merugikan organisasi. Salah satu mekanisme untuk meningkatkan keamanan sistem yaitu dengan menggunakan teknologi enkripsi data. Data-data yang dikirimkan diubah sedemikian rupa sehingga tidak mudah diketahui oleh orang lain yang tidak berhak.



Gambar 22. Kerangka kerja keamanan informasi

Gambar 4.3: Kerangka Kebijakan Keamanan Sistem Informasi [12]

4.4 Standar Keamanan Sistem Informasi

Untuk sebuah organisasi menerapkan standar keamanan informasi ISO 27001, organisasi tersebut perlu terlebih dahulu mendefinisikan rencana kebijakan keamanan informasi yang akan ditempuhnya. Kemudian, berdasarkan kebijakan tersebut, menganalisa resiko secara *risk assesment* yang akan timbul terhadap keamanan informasi. Setelah organisasi terbukti mampu melakukan mitigasi resiko dan ancaman yang timbul (*risk treatment*), organisasi dapat mendefinisikan standar kemampuan perlindungan keamanan informasi, untuk kemudian diukur menurut standar ISO 27001. Standar tersebut menetapkan sasaran kontrol-kontol keamanan informasi yang meliputi sebelas area pengamanan, yaitu 1) Kebijakan keamanan informasi; 2) Organisasi keamanan informasi; 3) Manajemen aset; 4) Sumber daya manusia menyangkut keamanan informasi; 5) Keamanan fisik dan lingkungan; 6) Komunikasi dan manajemen informasi; 7) *Access control*; 8) Penggandaaan/akuisisi, pengembangan dan pemeliharaan sistem informasi; 9) Pengelolaan insiden keamanan informasi; 10) Manajemen kelangsungan usaha , dan 11) Kepatuhan. Dalam menciptakan keamanan informasi, organisasi dapat mengimplementasikan sepuluh langkah yang yang dapat mewujudkan keamanan informasi. Pertama, mendefinisikan kebijakan keamanan informasi perusahaan. Pengelolaan keamanan informasi yang baik dimulai dengan penyusunan kebijakan keamanan secara tertulis yang menggariskan seluruh persyaratan keamanan untuk dapat memenuhi kepatuhan, standar dan tujuan yang akan dijalankan perusahaan. Kedua, dapat dilakukan penunjukan penanggung jawab keamanan, dimana penting untuk menunjuk seseorang di dalam perusahaan yang bertanggung jawab kepada tim manajamen untuk menegakkan dan mengamankan informasi di seluruh bagian organisasi. Ketiga, melakukan inventarisasi aset informasi. Perusahaan harus menyusun daftar aset informasi yang dimilikinya, termasuk peranti lunak, perlengkapan komputer, database, dan file-file, dan mendokumentasikan lokasinya, klasifikasi keamanannya dan pemilik internalnya. Keempat, melakukan seleksi terhadap staf kunci, untuk melindungi keamanan internal organisasi. Kelima, melindungi aset informasi secara fisik. Hal ini memberikan tingkat keamanan informasi yang lebih tinggi. Keenam, mempraktikkan pengelolaan jaringan yang efektif untuk mencegah kegagalan sistem, kehilangan data atau terjadinya kebocoran informasi yang sangat berharga dan rahasia. Ketujuh, menciptakan aturan pengendalian akses yang ketat.

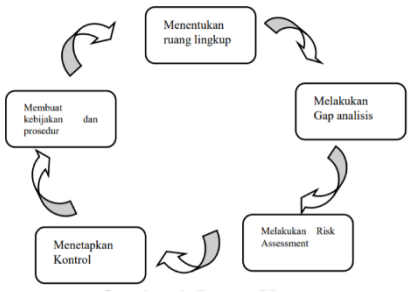
Perusahaan harus secara ketat mendefinisikan ijin akses yang diberikan kepada pekerjanya. Hal ini tidak saja dapat menghindari akses tak berwenang ke data rahasia, tetapi juga melindungi integritas sumber komputasi dan melindungi diri dari penggunaan peranti lunak dan yang tidak memiliki kewenangan. Kedelapan, bangun keamanan di dalam semua sistem dan aplikasi. Jika sebuah perangkat keras atau peranti lunak diinstal, pastikan kompatibilitasnya dengan sistem yang dimiliki untuk menghindari kegagalan sistem, dan mengkonfigurasikan tingkat keamanan yang sesuai sehingga tidak menimbulkan celah kelemahan. Kesembilan, merencanakan pengembangan terhadap kelangsungan bisnis atau sebuah contingency plan yang menggariskan langkah-langkah yang harus diambil perusahaan untuk meminimalkan gangguan jika terjadi bencana dan memulihkan aplikasi penting secepat mungkin agar dapat terus berbisnis. Kesepuluh, pastikan kepatuhan terhadap peraturan dan UU yang dapat diterapkan. Pendokumentasian dan pengendalian harus diterapkan tidak saja sesuai dengan undang-undang setempat, propinsi atau nasional yang mengatur tata usaha perusahaan. Agar pengguna sistem informasi merasa aman dan nyaman memercayakan data dan informasinya pada suatu organisasi, diperlukan evaluasi dalam fitur dan atribut keamanan, yang meliputi empat hal berikut, yaitu; 1) Situs menyediakan enkripsi; 2) Situs mengharuskan pengguna unutk mengatur akun dengan ID dan *password*; 3) Konfirmasi di tampilkan layar setelah pengguna melakukan perubahan data; 4) Pemakaian *Secure Socket Layer* dalam transaksi *online*.

Gambar 4.4: Standar Keamanan Sistem Infomasi [23]

4.5 Analisis Resiko Keamanan Informasi

Resiko keamanan informasi berdasarkan lubang keamanan (*security hole*) dapat diklasifikasikan menjadi empat bagian utama yaitu, 1) Keamanan yang bersifat fisik (*physical security*), mencakup akses manusia terhadap perangkat yang digunakan. 2) Keamanan yang berhubungan dengan personalia (*personal security*), mencakup resiko yang berhubungan dengan pihak atau karyawan yang mempunyai akses. 3) Keamanan dari data dan media serta teknik komunikasi (*communications security*), mencakup kelemahan dalam perangkat lunak (*software*) untuk pengelolaan data, serta aplikasi yang digunakan untuk mentransimiskan data. 4) Keamanan dalam operasional/manajemen teknologi informasi (*management security*), mencakup kebijakan dan prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan. Untuk menganalisis resiko keamanan dalam suatu organisasi, diperlukan lima langkah *risk assesment* yang harus ditempuh, yaitu 1) Melakukan identifikasi asset untuk memperoleh pemahaman *what is at risk* pada sebuah asset informasi. 2) Melakukan identifikasi kerawananan dan ancaman, dengan cara membuat model resiko untuk memberi gambaran secara komprehensif mengenai peristiwa dan kondisi yang mungkin terjadi, baik eksternal maupun internal organisasi. 3) Menentukan prioritas resiko, dilakukan proses membandingkan tingkat risiko dengan kriteria risiko pada basis yang sama. Hasil penilaian risiko adalah berupa daftar prioritas risiko untuk mengembangkan *control* dimana area yang dinilai berisiko tinggi ditindaklanjuti dan yang berisiko rendah dipantau. 4) Mengembangkan *control*, berdasarkan prioritas resiko yang telah ditentukan, dapat diambil langkah-langkah seperti menghindari resiko, mengurangi kemungkinan resiko, mengurangi konsekuensi resiko, mentransfer resiko, atau menahan resiko. 5) Monitoring, penilaian terhadap efektifitas pengendalian resiko. Dalam melakukan evaluasi pengendalian resiko keamanan informasi, organisasi dapat melakukan audit keamanan informasi. Audit keamanan informasi adalah suatu alat atau perangkat dalam menentukan, mendapatkan, dan mengelola setiap level keamanan dalam suatu organisasi. Audit keamanan informasi dimaksudkan untuk meningkatkan level keamanan informasi, mencegah rancangan keamanan informasi

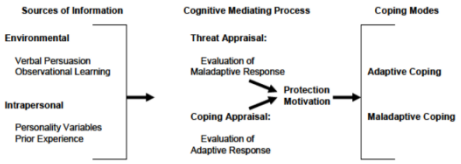
yang tidak layak, dan mengoptimalkan efisiensi benteng keamanan, dan proses keamanan informasi itu sendiri. Audit ini akan memastikan atau menjamin berjalannya proses operasional, reputasi dan aset suatu organisasi. Hasil dari audit keamanan informasi adalah tersusunnya dokumen laporan audit yang terkait pada keamanan teknologi informasi yang digunakan di lingkungan organisasi tersebut.



Gambar 4.5: Proses Perencanaan Analisis Resiko Keamanan Informasi [20]

4.6 Peran Sumber Daya Manusia dalam Menghadapi Ancaman Keamanan Data dan Informasi

Sebagai langkah awal, sumber daya manusia akan menerima informasi yang akan mengarah pada evaluasi dan reaksi baik secara *verbal persuasion* maupun *observational learning*. Kemudian dapat dihasilkan dua metode penerapan teori perilaku sumber daya manusia terhadap ancaman keamanan data, yaitu persepsi ketidapkastian (*Threat Appraisal*) dan kepercayaan pada kemampuan (*Threat Coping*). *Threat Appraisal* bisa dikatakan sebagai persepsi terhadap resiko dimana terdapat konsep ketidakpastian dan konsekuensi. *Threat Appraisal* mengarah pada ketidakpastian dan mengarah untuk mengetahui bagaimana pemikiran orang yang memiliki resiko terhadap suatu ancaman. Sedangkan *Threat Coping* terdiri dari *security self-efficacy, response efficacy, dan prevention cost. Security self-efficacy* adalah kepercayaan individu pada kemampuannya untuk mencegah atau mengurangi peristiwa keamanan mengancam. *Response efficacy* adalah keyakinan individu terhadap perilaku yang direkomendasikan untuk mencegah atau mengurangi keamanan. Setelah informasi di evaluasi dengan penerapan kedua teori diatas, sumber daya manusia bertanggungjawab atas delapan aspek keamanan informasi. 1) Mengelola secara keseluruhan berjalannya keamanan informasi organisasi. 2) Membuat laporan dan penjelasan kepada konsumen dan umum. 3) Merancang kebijakan keamanan, prosedur, program dan pelatiahan keamanan informasi. 4) Melakukan respon terhadap kejadian/insiden keamanan informasi dengan melakukan investigasi, mitigasi, dan penuntutan. 5) Melakukan respon terhadap laporan hasil audit mengenai keamanan informasi. 6) Melakukan audit, penilaian kesesuaian dan kebutuhan terhadap kontrol keamanan. 7) Mengkomunikasikan dan mensosialisasikan kebijakan, program dan pelatihan kepada seluruh karyawan terkait keamanan informasi. 8) mengimplementasikan dan melaksanakan seluruh kebijakan, prosedur dan program keamanan informasi, serta melaporkan jika ditemukan kerawanan/kelemahan keamanan.



Gambar 4.6: Penerapan Teori Perilaku Sumber Daya Manusia Terhadap Ancaman Keamanan Data [18]

4.7 Kebijakan Keamanan Siber Nasional

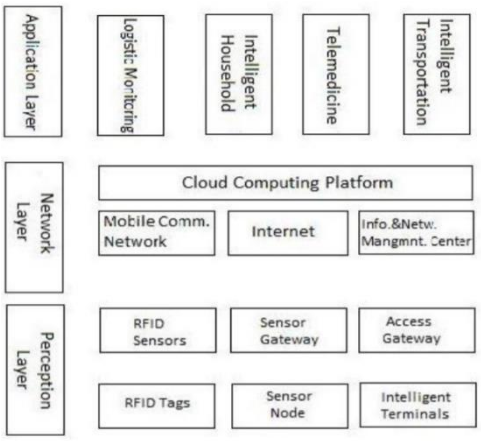
Keamanan Siber (*cybersecurity*) dapat disimpulkan sebagai sebuah rangkaian aktifitas dan pengukuran yang dimaksudkan untuk melindungi dari serangan, disrupsi, atau ancaman yang lainnya melalui elemen-elemen *cyberspace* (*hardware, software, computer network*). Jumlah serangan siber di Indonesia semakin meningkat, dari 28,430,843 pada tahun 2015 meningkat menjadi 135.672.984 pada tahun 2016. Dan 47% dari keseluruhan kasus yang terjadi merupakan serangan malware, 44% merupakan penipuan, sedangkan sisanya berbentuk kejahatan siber lainnya, seperti website defacement, dan aktivitas manipulasi data dan kebocoran data. Kebijakan keamanan siber nasional yang direkomendasikan terbagi menjadi lima aspek. Pertama, aspek *capacity building*. Diperlukan pelatihan profesional keamanan siber bagi Apratur Sipil Negara serta peningkatan sosialisasi keamanan informasi melalui edukasi publik untuk menumbuhkan pemahaman dan kesadaran publik mengenai

keamanan siber. Kedua, aspek *legal*. Pemerintah perlu mempercepat pengesahan Undang-undang Perlindungan Data untuk mendukung kepastian hukum perlindungan data pribadi. Ketiga, aspek *organizational structure*. Pemerintah diharapkan dapat membentuk *National Cyber Security Centre* sebagai wujud nyata penanganan kejahatan siber di Indonesia, serta sebagai lembaga rujukan formal keamanan siber nasional. Keempat, aspek *international cooperation*. Penguatan kerjasama pemerintah, masyarakat, dan *stakeholder* internasional (seperti pemilik aplikasi media sosial yang seringkali dimanfaatkan untuk media kejahatan), serta lembaga terkait di dunia international dalam pencegahan maupun penanganan kejahatan siber. Kelima, aspek teknikal dan prosedural. Pembaharuan perangkat teknologi informasi yang selaras dengan standar keamanan siber untuk mengantisipasi ragam ancaman siber yang menyertai perkembangan teknologi.

Gambar 4.7: *National Cybersecurity Index* [13]

4.8 *Internet of Things (IoT)*

Frasa *Internet of Things* (IoT) mengacu pada perangkat teknologi informasi yang terhubung satu sama lain secara nirkabel untuk mengumpulkan data melalui sensor dan aktuator yang teritegrasi. IoT merupakan sebuah sistem yang majemuk. Kemajemukannya bukan hanya karena keterlibatan berbagai entitas seperti data, mesin, RFID, sensor dan lain-lain, tetapi juga karena melibatkan berbagai peralatan dengan kemampuan komunikasi dan pengolahan data. Banyaknya entitas dan data yang terlibat, membuat IoT menghadapi resiko keamanan yang dapat mengancam dan membahayakan konsumen. Ancaman ini utamanya dilakukan dengan cara memungkinkan orang yang tidak berhak untuk mengkases data dan menyalahgunakan informasi personal, memfasilitasi serangan terhadap sistem yang lain, serta mengancam keselamatan personal penggunanya. Ancaman-ancaman yang dapat mempengaruhi entitas IoT sangat beragam, tergantung dari target serangan tersebut. Ancaman terhadap IoT dapat dikategorikan sebagai berikut: 1) *Denial of Service*, serangan yang menyebabkan pihak yang sah tidak dapat mengkses layanan. 2) Merusak secara fisik objek-objek dalam IoT. 3) *Eavesdropping*; serangan pasif yang dapat dilakukan pada berbagai kanal komunikasi dengan tujuan mengekstrak data dari aliran informasi. 4) *Node capture*; penyerang mengekstrak informasi dari node maupun dari infrastruktur lain yang memiliki kemampuan penyimpanan data. 5) *Controlling*; di mana penyerang berusaha mendapatkan kontrol terhadap entitas IoT dan mengganggu layanan maupun data dari entitas tersebut. Berbagai jenis ancaman di atas, dapat menyerang berbagai entitas dalam IoT, terutama RFID dan jaringan sensor.



Gambar 4.8: Struktur *Internet of Things* [22]

4.9 Kriptografi Awan

Seiring dengan pertumbuhan komputasi awan yang begitu pesat, pengguna dapat berbagi data dan informasi dengan mudah dan tanpa biaya. Namun demikian, kemudahan tersebut memunculkan resiko keamanan yang sangat besar. Salah satu metode pengamanan data yang paling tepat adalah algoritma KGC (*Key Generations Center*). KGC merupakan protokol dimana dua atau lebih anggota pengamanan data menyepakati suatu kunci untuk mengamakan data yang dimaksud. Tahap pertama, KGC memilih angka secara acak dua bilangan prima p dan q dengan syarat t p=(p-1)/2 dan q=(q-1)/2. Tahap kedua, semua anggota pengamanan data harus mendaftarkan diri pada KGC untuk mendapatkan suatu kunci akses data. Kemudian proses berlanjut pada saat satu kelompok pengamanan data yang terdiri dari pengirim dan penerima data,

untuk kemudian bertukar kunci akses. Jika kunci akses kedua pihak mendapatkan kecocokan, proses pertukaran data dapat dilanjutkan.

$$P_n(x) \equiv \sum_{i=0}^{n} f_i \prod_{k \neq i, k=0}^{n} \frac{x - x_k}{x_i - x_k}. \qquad (1)$$

Newton's Interpolation Formula

Newton's Interpolation Formula adopts divided differences to construct

$$f_{i_0 i_1 \ldots i_k} = \frac{f_{i_1 \ldots i_k} - f_{i_0 \ldots i_{k-1}}}{x_{i_k} - x_{i_0}}. \qquad (2)$$

$P_n(x)$

x_i	f_i	$k=1$	$k=2$	$\cdots$	$k=n$
x_0	f_0				
x_1	f_1	f_{01}			
x_2	f_2	f_{12}	f_{012}		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	
x_n	f_n	$f_{n-1,n}$	$f_{n-2,n-1,n}$	$\cdots$	$f_{012\ldots n}$

Table 1: Divided Difference Scheme

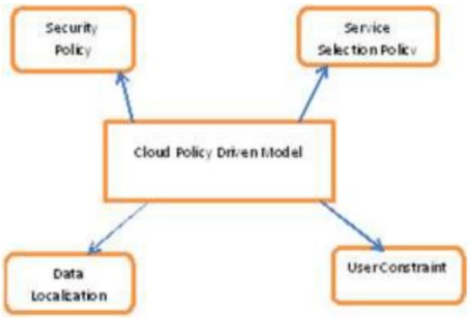
we can calculate divided differences. And with the descending diagonal of the divided difference scheme, the coefficients $f_{i0i1\ldots ik}$ can be calculated, the interpolation problem with the Newton's interpolation formula is solved by

$$P_n(x) \equiv f_0 + f_{01}(x - x_0) + \cdots + f_{01\ldots n}(x - x_0)(x - x_1)\ldots(x - x_{n-1}). \qquad (3)$$

Gambar 4.9: Algoritma Kriptografi Awan [11]

4.10 *Security Inclusive Policy Driven Cloud Model*

Security Inclusive Policy Driven Cloud Model merupakan sebuah permodelan arsitektur komputasi awan yang mengedepankan aspek keamanan data dan informasi pada pengembangan aristekturnya. Model tersebut dibagi menjadi empat tahapan *policy*. Pertama, *security policy*. Keamanan merupakan kebutuhan utama dan terpenting dalam pengembangan arsitektur komputasi awan. Tahap ini bertujuan untuk mengidentifikasi tingkat keamanan yang dibutuhkan dalam suatu infrastruktur. Berbagai aspek perlu diperhatikan untuk ditingkatkan, seperti keamanan data dan informasi, keamanan pengguna layanan, dan keamanan komunikasi data. Peningkatan aspek-aspek tersebut dapat diimplementasikan pada *middleware* antara *hardware* dan *server* komputasi awan. *Security Policy* dapat dikatakan berhasil jika komunikasi data yang aman (*secure communication*) dapat terlaksana. Tahap kedua, *service selection policy* adalah sebuah tahap dimana arsitektur perantara menyediakan pilihan layanan yang efektif dan sesuai dengan kebutuhan pengguna. Parameter yang perlu diperhatikan termasuk namun tidak terbatas pada ketersediaan layanan komputasi awan, skala pemanfaatan jaringan, dan *response time* arsitektur. Tahap ketiga, *data localization policy*, adalah tahapan dimana pengguna mendefinisikan ketersediaan informasi pada *cloud server* melalui proses integrasi data pada komputer pengguna dengan data yang terdapat pada *server*. Proses lokalisasi data perlu memerhatikan tiga faktor, yaitu transparansi (*transparency*), skalabilitas (*scalability)*, dan kekohohan (*robustness)*. Ketika pengguna melakukan permintaan akses data, pengguna mengirimkan batasan atribut data yang dikehendaki kepada *server* untuk dilakukan analisis atribut secara spesifik untuk kemudiaan dicocokkan dengan lokasi data yang dimaksud. Tahap keempat. *user policy*, merupakan tahap dimana pengguna melakukan permintaan akses data kepada *cloud server*. Permintaan tersebut kemudian diterima oleh *middle layer architecture* untuk kemudian diproses oleh *cloud server*. Tahap ini perlu memerhatikan beberapa faktor seperti pemrosesan berbasis *server*, pemenuhan batasan data yang dikehendaki, dan batasan keamanan yang harus dipenuhi. Berdasarkan empat tahapan diatas, permintaan akses data awan oleh *user* dapat terpenuhi melalui proses yang aman dan efisien.

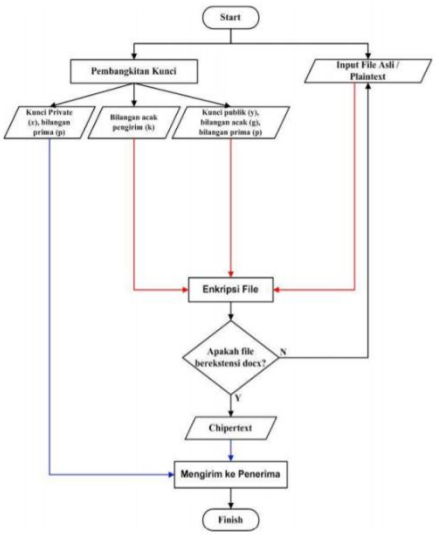


Gambar 4.10: *Security Inclusive Policy Driven Cloud Model* [15]

4.11 Kriptografi *Block Cipher*

Block Cipher adalah algoritma enkripsi yang akan membagi-bagi *plaintext* yang akan dikirimkan dengan ukuran tertentu (disebut blok) dengan panjang t, dan setiap blok dienkripsi dengan menggunakan kunci yang sama. Pada umumnya, *block cipher* memproses *plaintext* dengan blok yang relatif panjang lebih dari 64 bit, untuk mempersulit penggunaan pola-pola serangan yang ada

untuk membongkar kunci. Salah satu algoritma *block cipher* adalah algoritma ElGamal, yang melakukan proses enkripsi pada blok-blok plainteks yang kemudian menghasilkan blok-blok *chipertext*, yang nantinya blok-blok *chipertext* tersebut akan didekripsi kembali dan hasilnya kemudian digabungkan menjadi plainteks semula. Keamanan algoritma *ElGamal* terletak pada kesulitan perhitungan logaritma diskrit pada modulo prima yang besar, sehingga upaya untuk menyelesaikan masalah logaritma ini menjadi sulit untuk dipecahkan. Adapun proses enkripsi diawali dengan pembangkitan kunci secara acak yang menghasilkan beberapa bilangan diantaranya bilangan prima, bilangan acak pengirim, kunci *public* serta kunci *private*. Selanjutnya, proses enkripsi ElGamal dilaksanakan menggunakan bilangan acak dan kunci *public* disertai dengan bilangan prima yang sudah ditentukan sebelumnya. Setiap blok *plaintext* *m* dienkripsi dengan rumus $a = gk \bmod p$; $b = ykm \bmod p$, dengan *g* dan *y* sebagai kunci *public*, *p* sebagai kunci *private*, dan k sebagai bilangan acak. Pasangan *a* dan *b* adalah *ciphertext* untuk blok pesan *m.* Jadi, ukuran *ciphertext* dua kali ukuran *plaintext*-nya. Proses dekripsi menggunakan kunci *private* *g* dan *y* untuk mendekripsi nilai *a* dan *b* dari masing-masing blok *ciphertext* menjadi *plaintext*.

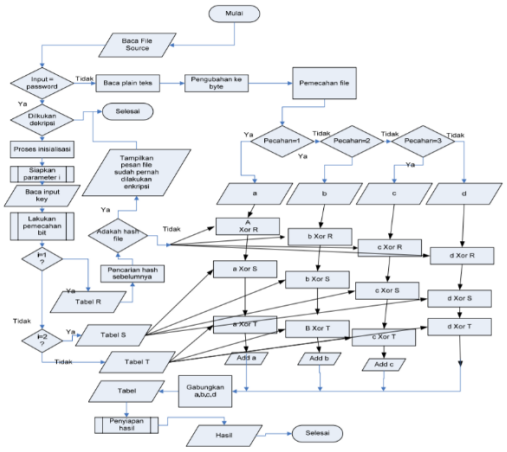


Gambar 4.11: Kriptografi *Block Cipher ElGamal* Dalam Enkripsi File Bertipe .docx [19]

4.12 Kriptografi *Stream Cipher*

Salah satu algoritma enkripsi yang sangat penting dan paling banyak digunakan adalah *stream chiper*. *Stream Cipher* adalah algoritma enkripsi yang mengenkripsi data persatuan data, seperti bit, byte, nible atau per 5 bit. Setiap mengenkripsi satu satuan data digunakan kunci yang merupakan hasil pembangkitan dari kunci sebelumnya Algoritma ini bekerja dengan cara mengenkrip informasi per karakter dalam bentu *digit binary* dari *plaintext*. Algoritma ini secara umum digunakan untuk mengenkrip *plaintext* yang berukuran kecil, dan bekerja jauh lebih cepat dibangdingkan dengan algoritma pendahulunya, yaitu *block chiper*. Suatu *stream chiper* akan menghasilkan apa yang disebut dengan suatu *keystream*, atau suatu barisan bit yang digunakan sebagai kunci untuk menghasilkan *pseudo-random sequence*. *Sequence* tersebut kemudian diinisialisasikan dengan menggunakan kunci rahasia yang kemudian dilakukan operasi XOR dengan *plaintext* untuk menghasilkan *ciphertext*. Menurut Penulis, algoritma *stream chiper* yang paling tepat digunakan untuk orgaanisasi yang sangat mementingkan aspek keamanan data adalah algoritma SEAL, atau (*Software Encryption Algorithm*). Diciptakan oleh Rogaway dan Coppersmith dan kemudian dipatenkan oleh IBM pada tahun 1993, SEAL digunakan secara luas pada beberapa aplikasi dan dinyatakan sangat aman, bahkan hingga kini tidak terdapat satu orang pun yang dapat memecahkan atau membongkarnya. Proses enskripsi SEAL diawali dengan komputer mengambil data dari file *ciphertext* dan *password*. *Ciphertext* dan *password* diubah ke dalam bentuk *byte*. *Password* yang berupa kumpulan *byte* merupakan input untuk kemudian diproses ke dalam algoritma SHA (*Secure Hash Algorithm*). Hasil dari SHA kemudian dimasukkan kembali ke dalam algoritma SHA yang telah dimodifikasi sehingga terbentuk tabel T, S dan R. Pada tahap pertama, *ciphertext byte* dilakukan operasi XOR dengan tabel S, sehingga diperoleh output a, b, c, d. Kemudian masing-masing *output* tersebut dilakukan proses XOR dengan tabel T dan R. Tahap berikutnya, seluruh *output* a, b, c, d dijumlahkan menjadi satu dan hasil penambahan tersebut disimpan ke dalam *output*. Proses dekripsi SEAL merupakan kebalikan dari proses enkripsinya. Komputer mengambil data dari file *ciphertext* dan

password. *Ciphertext* dan *password* diubah ke dalam bentuk *byte*. *Password* yang berupa kumpulan *byte* merupakan input untuk diproses ke dalam algoritma SHA (*Secure Hash Algorithm*). Hasil dari SHA kemudian dimasukkan kembali ke dalam algoritma SHA yang telah dimodifikasi sehingga terbentuk tabel T, S, R. Pada tahap pertama *ciphertext byte* dilakukan XOR dengan tabel S, sehingga diperoleh *output* a, b, c, d. Kemudian masing-masing *output* tersebut dilakukan XOR dengan tabel T dan R. Tahap berikutnya *output* a, b, c, d dijumlahkan menjadi satu dan hasil terserbut disimpan ke dalam *output*.



Gambar 4.12: Kriptografi *Stream Cipher* Dalam Algoritma SEAL [25]

.

Tabel 4.1

Dampak Variabel Terhadap Optimalisasi Keamanan Data dan Informasi Pada Perangkat Lunak dan Implementasinya

Variabel 1: Prinsip Keamanan Informasi
• Memenuhi persyaratan berupa kerahasiaan, integrasi, dan otentikasi • Memenuhi prinsip landasan pokok, keamanan pokok, kemudahan, kenyamanan, pengurangan ancaman, implementasi otentikasi
Variabel 2: Keamanan Jaringan Komputer
• Penambahan perangkat *intrusion detection and prevention system* • Jaringan LAN dapat menggunakan VLAN dan VOIP
Variabel 3: Kebijakan Keamanan Sistem Informasi
• Perawatan sistem • Penanganan resiko • Pengendalian akses • Keamanan dan pengendalian aset • Keamanan server
Variabel 4: Standar Keamanan Sistem Informasi
• Kebijakan keamanan informasi • Organisasi keamanan informasi • Manajemen aset • Sumber daya manusia • Komunikasi dan manajemen informasi • Kontrol akses • Pengadaan, pengembangan, dan pemeliharaan sistem informasi • Pengelolaan insiden keamanan informasi • Manajemen kelangsungan usaha • Kepatuhan terhadap hukum
Variabel 5: Resiko Keamanan Informasi
• Resiko fisik • Resiko personalia • Resiko komunikasi • Resiko operasional dan manajemen
Variabel 6: Sumber Daya Manusia
• *Threat appraisal* • *Threat coping*
Variabel 7: Kebijakan Keamanan Siber Nasional
• *Capacity building* • *Legal* • *Organizational structure* • *International cooperation*
Variabel 8: Ancaman Terhadap *Internet of Things* (IoT)
• *Denial of Service* • *Physical damage* • *Eavesdropping* • *Node capture* • *Controlling*
Variabel 9: Kriptografi Awan
• Penggunaan algoritma *Key Generations Center* (KGC) untuk meningkatkan keamanan data, sehingga informasi yang terkandung menjadi mustahil untuk dibongkar

Variabel 10: *Security Inclusive Policy Driven Cloud Model*
• *Security policy* • *Service selection policy* • *Data localization policy* • *User policy*
Variabel 11: Kriptografi *Block Cipher*
• Pemrosesan teks dengan blok yang relatif panjang (lebih dari 64 bit), efektif mempersulit penggunaan pola-pola serangan yang ada untuk membongkar kunci.
Variabel 12: Kriptografi *Stream Cipher*
• Pemrosesan teks dengan blok yang efisien sehingga proses enkripsi lebih cepat dan penggunaan *code* jauh lebih sedikit.

V. PENUTUP

5.1 Kesimpulan

Melalui penelitian yang telah dilakukan, maka dapat ditarik kesimpulan bahwa optimalisasi keamanan data dan informasi pada perangkat lunak harus memerhatikan prinsip keamanan informasi agar memenuhi persyaratan berupa kerahasiaan, integritas dan keotentikan data dengan memerhatikan berbagai resiko yang mungkin timbul, seperti resiko fisik, resiko personalia, resiko komunikasi dan resiko operasional manajemen. Untuk menghadapi berbagai resiko tersebut, diperlukan standarisasi keamanan data dan informasi dalam berbagai aspek seperti kebijakan dan organisasi keamanan informasi, sumber daya manusia, komunikasi dan manajemen informasi, kontrol akses dan mitigasi insiden, serta dalam praktisnya diperlukan pengawasan terhadap perawatan sisten keamanan informasi, serta pengendalian keamanan akses, aset dan server guna menghadapi serangan siber seperti *denial of service*, *physical damage*, *eavesdropping, node capture*, dan *unauthorized controlling*. Dengan bergesernya pola pengelolaan data menuju penyimpanan berbasis awan, perlu diimplementasikan pula langkah-langkah pengamanan inklusif *Security Inclusive Policy Driven Cloud Model*, yang berdasar pada kebijakan keamanan, layanan, data, dan pengguna, dan ditunjang dengan enkripsi data berbasis kriptografi *block cipher* dan *stream cipher*.

5.2 Saran

Keamanan data dan informasi sangat penting bagi keberlangsungan suatu organsisasi. Berdasarkan penelitian yang telah dilakukan, untuk mengoptimalkan keamanan data dan informasi maka disarankan untuk melakukan analisis resiko keamanan untuk mendapatkan permodelan yang tepat. Kemudian dapat diambil kebijakan keamanan sistem informasi yang sesuai dengan standar untuk memenuhi prinsip keamanan informasi untuk menghadapi ancaman keamanan siber yang mungkin terjadi. Untuk organisasi yang bergerak dalam bidang penyimpanan awan, dapat diterapkan permodelan *Security Inclusive Policy Driven Cloud Model* serta enkripsi data dan informasi menggunakan kriptografi.

5.3 Penelitian Lanjutan

Studi pustaka ini membuktikan bahwa optimalisasi keamanan data dan informasi pada perangkat lunak merupakan hal yang sangat penting bagi suatu organisasi. Namun, karena berbagai keterbatasan yang dihadapi dalam penelitian ini, diharapkan peneliti lainnya dapat mengembangkan aspek-aspek optimalisasi keamanan data dan informasi pada perangkat lunak lainnya yang tidak tercakup pada penelitian ini, dan tidak terbatas pada duapuluh paper terpublikasi serta duabelas variabel optimalisasi keamanan data dan informasi. Kedepannya, Penulis mengharapkan agar penelitian ini dapat dijadikan referensi bagi peneliti lain yang akan melakukan penelitian serupa dengan sudut pandang yang berbeda.

DAFTAR PUSTAKA

[1] Vardiansyah, Dani. "Filsafat Ilmu Komunikasi: Suatu Pengantar". 2008.

[2] Kadir, Abdul. "Pengenalan Sistem Informasi". 2003.

[3] Hardiyana, Andi. "Optimalisasi Pemanfaatan Teknologi Informasi dan Komunikasi Dalam Pembelajaran PAUD". AWLADY Jurnal Pendidikan Anak. 2016.

[4] de la Banda, Maria Garcia, Peter Stuckey, Pascal van Hentenryck dan Mark Wallace. "The Future of Optimalization Technology". University of Melbourne. 2014.

[5] Sun, Yunchuan, Junsheng Zhang, Yongping Xiong dan Guangyu Zhu. "Data Security and Privacy in Cloud Computing". International Journal of Distributed Sensor Network. 2014.

[6] R. Velumadhava, Rao dan K. Selvamani. "Data Security Challenges and Its Solutions in Cloud Computing". Procedia Computer Science. 2015.

[7] Councill, Bill dan George Heineman. "Definition of a Software Component and Its Elements". Universitetet i Oslo. 2001.

[8] Dewi, Ervin Kusuma dewi dan Azhari SN. "Analisis Sistem Keamanan Perangkat Lunak". Seminar Nasional Aplikasi Teknologi Informasi. 2012.

[9] Main, A. dan P. C. van Oorschot. "Software Protection and Application Security: Understanding the Battleground". University of Carleton. 2003.

[10] Bublitz, Jorge. "Seven Steps to Software Security". Business White Paper. 2013

[11] Harika, P dan Venkata Ramana. "A Secure Data Sharing Scheme for Groups in Cloud". International Journal of Engineering and Technical Research, Volume 8 Issue 6. 2018.

[12] Jumadi, Rio. "Kajian Kebijakan Keamanan Sistem Informasi Sebagai Bentuk Perlindungan Kerahasiaan Pribadi Karyawan Perusahaan XYZ". Journal Scientific and Applied Informatics. 2018.

[13] Islami, Maulia Jayantina. "Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index". Jurnal Masyarakat Telematika dan Informasi, Volume 8:137-144. 2017.

[14] Kusumawati, Diah, Bagus Winarko, Riva'atul Adaniah Wahab dan Wirianto Pradono. "Analisis Kebutuhan Regulasi Terkait dengan Internet of Things". Buletin Pos dan Telekomunikasi, Volume 15 Nomor 2:121-138. 2017.

[15] Sonia dan Kirti Bhatia. "*A Study on Various Security Aspects in Cloud Policy Oriented Architecture*". International Journal of Advanced Engineering Research and Science, Volume 4 Issue 3: 191-195. 2017.

[16] Wahyu, Ari Purno. "Optimasi Jaringan Local Area Network Menggunakan VLAN dan VOIP". Jurnal Informatika: Jurnal Pengembangan IT, Volume 2 Nomor 1: 54-57. 2017.

[17] Hernikawati, Dwi. "Hubungan Risk Tolerance Dan Risk Perception Terhadap Perilaku Keamanan Informasi". Jurnal Studi Komunikasi dan Media Volume 20:165-174. 2016.

[18] Hernikawati, Dwi. "Dampak Penggunaan Broadband Terhadap Perilaku Keamanan Informasi". Jurnal Studi Komunikasi dan Media. Volume 20 Nomor 1:77-87. 2016.

[19] Karima, Aisyatul dan Ari Saputro. "Pembangkitan Kunci pada Algoritma Asimetris ElGamal untuk Meningkatkan Keamanan Data bertipe .docx". Jurnal Ilmiah SISFOTENIKA Volume 6:170-181. 2016.

[20] Marco, Robert. "Indeks Penilaian Tingkat Kematangan (Maturity) IT Governance Pada Manajemen Keamanan Layanan Teknologi Informasi. Jurnal Ilmiah DASI Volume 17:76-82. 2016.

[21] Prabowo, Ramadhan Triyanto dan Mochamad Teguh Kurniawan. "Analisis dan Desain Keamanan Jaringan Komputer dengan Metode *Networdk Development Life Cycle*". Jurnal Rekayasa dan Sistem Industri, Volume 2 Nomor 1:1-7. 2015.

[22] Srivastava, Arpit Kumar, Apoorv Agarwal dan Abhinav Mathur. "*Internet of Things and its Enhanced Data Security*". International Journal of Engineering and Applied Sciences, Volume 2 Issue 2: 79-81. 2015.

[23] Syarif, Akmal Rifqi dan Agung Nugroho. "Analisis Tingkat Kematangan Sistem Manajemen Keamanan Informasi Direktorat Jenderal Perbendaharaan Diukur Dengan Menggunakan Indeks Keamanan Informasi". Jurnal PKN STAN. 2015.

[24] Kinasih, Bondan Satrio. "Pengaruh Persepsi Keamanan Dan Privasi Terhadap Kepuasan Dan Kepercayaan Konsumen Online" Jurnal Siasat Bisnis Volume 16:25-38. 2012.

[25] Kartika, I Made, Restyandito dan Sri Suwarno. "Implementasi Algoritma SEAL Pada Keamanan Data". Jurnal Informatika Volume 6:25-34. 2010.

[26] AlBone, Aan. "Pembuatan Rencana Keamanan Informasi Berdasarkan Analisis Dan Mitigasi Risiko Teknologi Informasi" Jurnal Informatika Volume 10:44-52. 2009.

[27] Paryati. "Keamanan Sistem Informasi". Seminar Nasional Informatika. 2008.

[28] Supriyanto, Aji. "Prinsip dan Siklus Hidup Keamanan Informasi". Jurnal Teknologi Informasi DINAMIK:101-108. 2007

[29] Triantono, Henricus Bambang. "Kebijakan Keamanan Dengan Standar BS 7799/ ISO 17799 Pada Sistem Manajemen Keamanan Informasi Organisasi". Seminar Nasional Aplikasi Teknologi Informasi. 2007.

[30] Murti, Hari. "Implementasi Keamanan Pemanfaatan Teknologi Informasi untuk Usaha Kecil dan Menengah". Jurnal Teknologi Informasi DINAMIK:08-15.2006