Qwen

Analisis Mendalam Doktrin Pengelolaan Pengguna-Augmentasi.101: Paradigma Kontinuitas Siber Berbasis Logika Murni

Dekonstruksi Arsitektur Logis Murni: Prinsip-Prinsip Fundamental Doktrin

Doktrin Pengelolaan Pengguna-Augmentasi.101: Kontinuitas Operasi Siber menyajikan sebuah proposisi arsitektural yang radikal dan koheren, yang secara eksplisit menolak apa yang ia sebut sebagai "arsitektur berbasis emosi" [1]. Tujuan fundamentalnya bukan sekadar meningkatkan keamanan, melainkan menciptakan sebuah sistem digital yang ketahanannya tidak bergantung pada variabilitas, konsistensi, atau bahkan kecerdasan intelektual manusia, melainkan pada ketegasan kode, transparansi protokol, dan disiplin logika deterministik. Ini adalah sebuah manifestasi ideologis yang menempatkan operasi sistem yang bebas emosi sebagai jalan mutlak untuk memastikan keamanan, ketahanan, dan kontinuitas digital [1]. Setiap aspek dari doktrin ini dirancang untuk secara konsisten mengimplementasikan prinsip ini, mulai dari hak istimewa pengguna hingga respons insiden, semata-mata untuk membangun lapisan pertahanan yang tidak dapat dilanggar oleh variabel non-logis. Pada dasarnya, doktrin ini berpendapat bahwa sistem bertahan bukan karena kemampuan adaptifnya, melainkan karena disiplin logika yang ketat—di mana node-node berfungsi dan doktrin berlanjut tanpa gesekan atau ambiguitas [1].

Asumsi fundamental yang mendasari doktrin ini adalah bahwa semua proses yang bersifat afektif, intuitif, atau subjektif merupakan sumber utama dari kerentanan, inkonsistensi, dan kegagalan dalam operasi sistem. Emosi, persepsi, dan intuisi dianggap sebagai variabel yang tidak dapat diprediksi, tidak dapat diaudit sepenuhnya, dan sangat rentan terhadap manipulasi, baik dari serangan eksternal maupun dari kesalahan internal [39][44]. Oleh karena itu, tujuan utamanya adalah mengecualikan seluruh pemrosesan afektif dari node-node operasional yang kritis untuk misi [1]. Stabilitas dan ketahanan dicapai bukan melalui fleksibilitas adaptif, melainkan melalui kontrol yang ketat dan prediktif atas setiap elemen sistem. Hak istimewa (privilege) yang diberikan kepada pengguna atau entitas lain tidak lagi bersifat abstrak atau berbasis peran yang ambigu, melainkan didefinisikan sebagai hak istimewa modular yang dapat dilacak sepenuhnya [1]. Ini adalah pergeseran fundamental dari model akses tradisional, seperti Role-Based Access Control (RBAC), yang sering kali mengandung ambiguitas dan kompleksitas, menuju sebuah sistem di mana otorisasi adalah hasil dari logika matematis dan transparan, bukan interpretasi kontekstual [9].

Prinsip-prinsip implementasi doktrin ini tersebar luas di seluruh arsitekturnya. Pertama, dalam model peran dan hak istimewa, pengguna tidak hanya memiliki izin, tetapi juga jejak audit yang tidak dapat dibantah untuk setiap tindakan mereka [1]. Instruksi yang diberikan kepada sistem tidak lagi

diinterpretasikan berdasarkan konteks atau niat pengguna, melainkan diartikan secara harfiah dan literal berdasarkan aturan yang telah ditetapkan [1]. Ini menciptakan sebuah lingkungan di mana setiap interaksi dapat diverifikasi dan divalidasi secara kriptografis, menghilangkan ruang untuk ambiguitas atau justifikasi situasional. Kedua, dalam penerapan AI dan umpan balik, modul AI tidak lagi mengevaluasi sinyal berdasarkan konteks emosional atau intuisi; sebaliknya, ia hanya menganalisis input diferensial untuk membuat keputusan [1]. Arsitektur umpan baliknya berkembang dari perbedaan output/input yang dapat diukur, menghindari inferensi perilaku yang subjektif dan berpotensi keliru [1]. Ketiga, protokol mesh dirancang untuk propagasi informasi yang efisien namun aman, dengan secara proaktif membuang meta-konteks yang tidak dapat divalidasi melalui konsensus atau mekanisme kriptografi [1]. Ini adalah upaya untuk membersihkan sistem dari noise informasi yang berasal dari variabel non-esensial dan memastikan bahwa hanya data yang solid yang akan dieksekusi.

Keamanan dan optimisasi diimplementasikan dengan cara yang sangat preskriptif. Respons terhadap insiden keamanan dilaksanakan secara instan dan tanpa penundaan, karena setiap penundaan dianggap sebagai kelemahan [1]. Alur rollback dan eskalasi insiden dikodekan secara eksplisit ke dalam sistem dan dapat diaudit sepenuhnya, tanpa toleransi untuk override manual yang didasarkan pada afeksi atau intuisi operator [1]. Kepatuhan terhadap protokol dan regulasi diotomatiskan melalui patch modular yang diterapkan berdasarkan konsensus, validasi efisiensi operasional yang berkelanjutan, dan identitas yang dikelola melalui kredensial kuantum yang dianggap tidak dapat disangkal [1]. Terakhir, aspek unifikasi bahasa—di mana semua antarmuka pengguna diterjemahkan secara literal dan konsisten tanpa nuansa atau konotasi—berfungsi sebagai mekanisme tambahan untuk menghilangkan ambiguitas linguistik yang bisa menjadi sumber kebingungan atau manipulasi [1].

Model otonomi yang diusulkan oleh doktrin ini menunjukkan tingkat kedalaman pemahaman tentang sistem dinamis. Setiap instance sistem tidak beradaptasi berdasarkan variabel afektif, melainkan hanya merespons terhadap metrik objektif seperti tingkat error, latensi, kepatuhan terhadap protokol, dan entropi [1]. Ini adalah bentuk adaptasi pur sang froid, di mana sistem berevolusi berdasarkan data dan performa, bukan berdasarkan "perasaan" atau persepsi. Sebagai contoh, jika metrik error rate meningkat, sistem akan melakukan rollback atau memicu ulang proses, bukan karena operator merasa "ada sesuatu yang salah". Model ini secara radikal menolak gagasan bahwa intuisi manusia atau bahkan AI yang canggih dapat memberikan wawasan yang lebih baik daripada data mentah. Dengan demikian, arsitektur ini secara fundamental adalah antitesis dari arsitektur yang dirancang untuk memfasilitasi atau bahkan memanfaatkan pemahaman manusia. Ia berdiri teguh pada argumen bahwa keamanan yang sejati tidak dapat dicapai jika ia harus mengandalkan elemen-elemen yang paling tidak dapat diandalkan dalam ekosistem digital: pikiran dan perasaan manusia.

Komponen Doktrin	Deskripsi Implementasi	Tujuan Utama
Prinsip Kontinuitas Sistem	Mengecualikan pemrosesan afektif dari node operasional misi-kritis untuk mencapai stabilitas maksimal.	Memastikan operasi yang tidak terganggu dan prediktif, terlepas dari kondisi operator atau konteks. [1]
	Pengguna beroperasi di bawah hak istimewa modular yang dapat dilacak	Menghilangkan ambiguitas dan justifikasi situasional dalam akses,

Komponen Doktrin	Deskripsi Implementasi	Tujuan Utama
Model Peran & Privilege	sepenuhnya, dengan instruksi yang diartikan literal, bukan diintuisi.	serta menciptakan jejak audit yang tidak dapat dibantah. [1]
AI & Umpan Balik	Modul AI mengevaluasi sinyal berdasarkan input/output diferensial, menghindari inferensi perilaku yang subjektif.	Menggunakan data objektif untuk pengambilan keputusan, menjauhkan sistem dari bias intuisi atau kontekstual. [1]
Protokol Mesh	Propagasi informasi melalui jaringan mesh yang secara proaktif membuang meta-konteks yang tidak dapat divalidasi secara kriptografi atau konsensus.	Membersihkan sistem dari informasi yang tidak relevan dan berpotensi merugikan, memastikan integritas data. [1]
Keamanan & Optimisasi	Logika respons insiden dikodekan, dapat diaudit, dan tidak dapat dioverride berbasis afeksi. Waktu respons minimum.	Menciptakan respons insiden yang cepat, konsisten, dan tidak terpengaruh oleh stres atau kepanikan operator. [1]
Kepatuhan	Patch modular diterapkan berdasarkan konsensus, validasi efisiensi operasional berkelanjutan, dan identitas berbasis kredensial kuantum.	Otomatisasi dan mekanisasi kepatuhan untuk menghilangkan risiko kesalahan manusia dalam manajemen patch dan identitas. [1]
Model Otonomi	Sistem beradaptasi berdasarkan metrik objektif (error rate, latency, compliance, entropy), bukan variabel afektif.	Menciptakan evolusi sistem yang prediktif dan berbasis data, bukan berdasarkan persepsi atau intuisi. [1]

Secara keseluruhan, doktrin ini bukanlah sekadar daftar fitur teknis, melainkan sebuah pandangan dunia tentang bagaimana sistem digital harus beroperasi untuk mencapai level ketahanan tertinggi. Ia bergerak melampaui pertimbangan teknis untuk masuk ke ranah filosofis, yakin bahwa dengan mengisolasi sistem dari realitas psikologis, kita dapat menciptakan dunia virtual yang lebih aman dan andal. Meskipun pendekatan ini tampaknya radikal dan mungkin tidak praktis untuk aplikasi skala besar, ia menyediakan kerangka kerja yang kuat untuk memahami batas-batas keamanan berbasis aturan dan mendorong diskusi tentang trade-off antara adaptabilitas berbasis kognisi dan ketahanan absolut yang didasarkan pada logika murni.

Konflik Filosofis: Doktrin Logis vs. Realitas Psikologis Manusia dalam Keamanan Siber

Di sinilah letak konflik inti dan peluang analisis yang paling signifikan dari doktrin Pengelolaan Pengguna-Augmentasi.101. Di satu sisi, doktrin ini secara radikal menolak variabel afektif sebagai sumber kekuatan. Di sisi lain, literatur ilmiah yang luas dan konsisten menunjukkan bahwa emosi, bias kognitif, dan motivasi manusia adalah elemen sentral, bahkan prediktif, dalam perilaku keamanan

siber. Doktrin ini, dengan mengecualikan pemrosesan afektif dari "node operasional misi-kritis," secara teoretis menciptakan sebuah lapisan pertahanan yang sangat tangguh terhadap ancaman teknis tetapi sama rapuh terhadap serangan sosial-organisasi, yang merupakan ancaman dominan saat ini. Realitas psikologis manusia tidak dapat diabaikan begitu saja, karena seringkali merupakan titik lemah terbesar dalam rantai pertahanan siber.

Studi-studi yang dikumpulkan secara konsisten membuktikan bahwa serangan sosial-organisasi secara langsung mengeksploitasi dimensi psikologis manusia. Serangan seperti phishing, spear phishing, pretexting, dan baiting bukanlah serangan teknis pada sistem, melainkan serangan pada pikiran individu [44]. Mereka menargetkan emosi dasar seperti takut, urgensi, rasa hormat terhadap otoritas, kepercayaan, dan rasa ingin tahu [39 40 43]. Misalnya, pesan phishing yang mengklaim akun Anda akan dinonaktifkan akan memicu emosi takut, yang dapat mendorong tindakan impulsif seperti mengklik tautan tanpa verifikasi yang cermat [40]. Demikian pula, serangan quid pro quo yang menawarkan imbalan tertentu untuk informasi sensitif mengeksploitasi prinsip scarcity (kelangkaan) dan keinginan untuk mendapatkan sesuatu [44]. Doktrin ini, dengan secara total mengecualikan pemrosesan konteks emosional, tampaknya mengabaikan titik lemah fundamental ini. Jika sebuah sistem hanya dapat berinteraksi dengan input yang logis dan literal, maka ia akan sangat rentan terhadap manipulasi yang dirancang untuk memicu respons emosional yang tidak rasional.

Lebih jauh, penelitian biometrik dan psikologis secara konsisten menunjukkan bahwa intensitas emosi, bukan jenis emosinya, adalah prediktor utama dari perilaku keamanan yang tidak aman. Satu studi menemukan bahwa intensitas emosi secara signifikan meningkatkan kemungkinan pengguna mengambil tindakan yang tidak aman, seperti mengklik tautan atau membuka lampiran berbahaya [41]. Temuan ini menunjukkan bahwa apakah seseorang merasa marah, gembira, atau cemas, jika intensitas emosi tersebut tinggi, mereka lebih rentan terhadap manipulasi. Studi lain menemukan bahwa emosi negatif seperti takut dan frustrasi dapat menyebabkan apa yang disebut security fatigue (kelelahan keamanan), sebuah kondisi di mana individu merasa lelah dan putus asa dengan permintaan keamanan yang berulang, yang pada gilirannya mengarah pada penurunan kompliansi dan perilaku yang lebih berisiko [34 43]. Ini adalah paradoks: sistem keamanan yang terlalu banyak membebani pengguna dengan aturan dan notifikasi dapat secara tidak sengaja menciptakan kondisi psikologis yang justru membuat mereka lebih rentan.

Realitas perilaku manusia juga seringkali tidak rasional, yang bertentangan dengan asumsi dasar doktrin ini. Teori dual-process, misalnya, menjelaskan bahwa keputusan manusia dibuat melalui dua jalur: proses intuitif yang cepat, otomatis, dan emosional, serta proses reflektif yang lambat, terkontrol, dan logis [4]. Banyak keputusan keamanan, seperti apakah suatu email terlihat mencurigakan, dibuat melalui proses intuitif yang cepat. Doktrin ini secara efektif menghapus proses intuitif ini dari sistem, yang bisa jadi menjadi masalah jika proses reflektif lambat atau tidak tersedia, terutama dalam situasi tekanan tinggi. Selain itu, bias kognitif seperti optimisme bias (optimism bias) —kecenderungan untuk percaya bahwa "hal buruk tidak akan terjadi pada saya"—secara signifikan meningkatkan kerentanan terhadap phishing dan penipuan online [43]. Orang-orang yang rentan terhadap bias ini cenderung mengabaikan peringatan keamanan dan meremehkan risiko.

Namun, beberapa perspektif alternatif memberikan jalan keluar yang lebih seimbang, yang dapat digunakan untuk merekonstruksi doktrin ini secara positif. Konsep psychological safety (keselamatan

psikologis) adalah salah satunya. Ini adalah keyakinan bersama bahwa tim aman untuk melakukan risiko interpersonal, seperti mengakui kesalahan atau melapor insiden, tanpa takut dihukum atau dihina [42]. Konsep ini menunjukkan bahwa sistem keamanan yang paling efektif adalah yang dirancang untuk bekerja sama dengan psikologi manusia, bukan melawannya. Pendekatan blameless post-mortems dalam budaya keamanan yang kuat adalah contoh implementasi nyata dari prinsip ini [42]. Paradigma baru dalam keamanan siber juga bergerak dari melihat manusia sebagai "link lemah" menuju melihat mereka sebagai bagian integral dari sistem pertahanan [18]. Ini berarti desain keamanan harus mempertimbangkan kebutuhan psikologis manusia seperti autonomi (kehendak untuk mengontrol tindakan sendiri), kompetensi (merasa mampu dalam tugas keamanan), dan keselamatan (permintaan untuk rasa aman) [18].

Riset yang lebih canggih juga menunjukkan adanya peluang untuk menciptakan sistem yang responsif secara emosional. Riset yang menggunakan data biometrik seperti Aktivitas Elektrodermal (EDA) dan Pengenalan Ekspresi Wajah (FER) menunjukkan bahwa latihan yang sensitif terhadap emosi, seperti menggunakan umpan balik biofeedback, dapat meningkatkan ketahanan terhadap manipulasi phishing [40]. Ini mengimplikasikan bahwa sistem keamanan masa depan tidak harus pasif; ia dapat aktif memantau kondisi mental penggunanya dan meresponsnya secara adaptif. Alih-alih menghilangkan variabel afektif, pendekatan yang lebih kuat adalah memodelkan dan memprediksi respons emosional untuk merancang sistem yang lebih tangguh. Misalnya, algoritma AI dalam sistem ini bisa dilatih untuk: 1. Mendeteksi pola perilaku yang menandakan stres atau tekanan tinggi pada pengguna (misalnya, waktu login yang tidak biasa, klik acak, atau kegagalan otentikasi berulang) dan secara proaktif mengaktifkan lapisan perlindungan tambahan atau menunda tindakan berisiko. 2. Menerapkan nudge psikologis yang cerdas, bukan instruksi yang kaku, untuk mengarahkan pengguna ke tindakan yang aman. Nudge ini dapat dirancang berdasarkan pemahaman tentang motivasi dan bias kognitif pengguna, seperti menggunakan prinsip social proof (bukti sosial) atau loss aversion (ketidaknyamanan kerugian) untuk meningkatkan kepatuhan [39].

Dengan demikian, konflik antara doktrin logis dan realitas psikologis tidak sepenuhnya tidak dapat dipecahkan. Daripada memilih satu di antara keduanya, pendekatan yang lebih maju mungkin berada di tengah jalan: membangun sistem yang didasarkan pada fondasi logika yang kokoh untuk fungsi-fungsi kritis, sambil secara bersamaan mengintegrasikan pemahaman yang mendalam tentang psikologi manusia untuk merancang lapisan pertahanan yang lebih manusiawi dan adaptif. Ini berarti mengubah pandangan dari "mengeliminasi manusia" menjadi "memahami dan melindungi manusia".

Aspek Psikologis Manusia	Dampak pada Keamanan Siber	Implikasi untuk Doktrin Augmentasi.101
Social Engineering	Secara langsung mengeksploitasi emosi (takut, urgensi, kepercayaan) untuk memancing tindakan tidak aman.	Doktrin ini mengabaikan titik lemah ini karena mengecualikan pemrosesan konteks emosional, sehingga sistem sangat rentan terhadap serangan sosial. [40 43 44]
Intensitas Emosi	Tingkat intensitas emosi (tidak peduli jenisnya) lebih signifikan	Sistem yang tidak dapat "memproses" emosi mungkin tidak dapat mengantisipasi

Aspek Psikologis Manusia	Dampak pada Keamanan Siber	Implikasi untuk Doktrin Augmentasi.101
	daripada jenis emosinya dalam memengaruhi tindakan pengguna.	lonjakan intensitas yang memicu perilaku berisiko. [41]
Security Fatigue	Kondisi kelelahan dengan permintaan keamanan yang berulang, yang menyebabkan penurunan kompliansi dan perilaku yang lebih berisiko.	Doktrin yang mengotomatiskan segalanya mungkin mengurangi beban psikologis, tetapi jika interaksinya tetap ada, ia tidak mengatasi akar penyebabnya. [34 43]
Bias Kognitif	Cacat dalam pemikiran yang menyebabkan pengambilan keputusan yang tidak rasional (contoh: optimisme bias).	Doktrin yang mengandalkan logika murni secara teoretis dapat melawan bias ini, tetapi tidak dapat melindungi dari serangan yang dirancang untuk memanfaatkannya. [4 43]
Dual-Process Theory	Kebanyakan keputusan dibuat melalui proses intuitif/cepat, bukan proses reflektif/lambat.	Doktrin ini secara efektif menghapus proses intuitif, yang merupakan mode default pengambilan keputusan manusia, sehingga memaksa pengguna ke mode yang lebih sulit dan lebih lambat. [4]
Psychological Safety	Keyakinan bahwa individu dapat melapor kesalahan tanpa hukuman, yang penting untuk budaya keamanan yang kuat.	Doktrin yang sangat preskriptif dan tidak dapat dinegosiasikan mungkin menciptakan lingkungan di mana pengguna enggan melapor insiden untuk menghindari konsekuensi. [42]

Implikasi Regulasi dan Strategis di Konteks Ekosistem Siber Indonesia

Memposisikan doktrin Pengelolaan Pengguna-Augmentasi.101 dalam konteks regulasi dan strategi keamanan siber Indonesia, yang secara dominan dikoordinasikan oleh Badan Siber dan Sandi Negara (BSSN), menghasilkan analisis yang bernuansa dan sarat akan implikasi strategis. Kerangka kerja keamanan siber nasional Indonesia, yang tercermin dalam Strategi Keamanan Siber Indonesia dan berbagai peraturan turunannya, berfokus pada aspek-aspek yang sangat konkret: kebijakan, kelembagaan, teknologi, infrastruktur, dan sumber daya manusia [1 24]. Fokus utamanya adalah pada mitigasi ancaman spesifik seperti malware, Advanced Persistent Threats (APT), ransomware, dan phishing, serta pada pembangunan kapasitas nasional dalam lima domain: intelijen siber, pertahanan siber, kejahatan siber, diplomasi siber, dan ekonomi siber [12]. Namun, meskipun komprehensif, dokumen-dokumen ini, secara umum, cenderung lebih berorientasi pada aspek teknis dan manajerial, dengan sedikit pembahasan eksplisit tentang dampak psikologis pada operator sistem atau bagaimana merancang protokol yang selaras dengan cara manusia berpikir dan merasakan.

Dalam konteks ini, doktrin "Augmentasi.101" secara paradoks dapat dilihat sebagai sebuah solusi teoretis untuk tantangan-tantangan regulasi yang dihadapi Indonesia. Dengan mengeliminasi variabel manusia dari "node operasional misi-kritis" [1], doktrin ini secara teoretis dapat meningkatkan kepatuhan protokol secara drastis dan mengurangi risiko kesalahan manusia—yang merupakan penyebab utama dari pelanggaran data. Laporan Verizon tahun 2022, misalnya, menyatakan bahwa sekitar 85% dari semua pelanggaran data melibatkan unsur manusia, baik itu kesalahan, kelalaian, atau eksploitasi perilaku pengguna [42][43]. Dengan membangun sistem yang tidak dapat dibobol oleh manipulasi psikologis, doktrin ini menjanjikan tingkat kepatuhan yang hampir sempurna pada level operasional, sebuah ideal yang sangat menarik bagi regulator yang bertanggung jawab untuk menjaga keamanan infrastruktur kritis nasional.

Meskipun secara filosofis radikal, beberapa prinsip inti dari doktrin ini memiliki potensi aplikasi strategis yang signifikan dalam ekosistem siber Indonesia, terutama jika diterapkan secara selektif pada komponen-komponen sistem yang paling kritis dan stabil. Pertama, prinsip logika respons insiden yang dikodekan, dapat diaudit sepenuhnya, dan tidak dapat di-override berbasis afeksi sangat selaras dengan standar BSSN untuk respons insiden yang terstruktur dan berkelanjutan [12][13]. Standar BSSN untuk respons insiden mengikuti siklus yang jelas: Persiapan, Deteksi & Analisis, Penangkalan, Eradikasi & Pemulihan, dan Aktivitas Pasca-Incident [12]. Implementasi doktrin ini dapat mengotomatiskan fase-fase awal respons insiden—terutama Penangkalan (Containment) dan Eradikasi (Eradication)—untuk mengurangi waktu tanggap secara dramatis. Dalam konteks Indonesia, di mana jumlah serangan siber sangat masif (misalnya, 495,3 juta serangan pada tahun 2020 dan 2,48 juta aktivitas APT pada tahun 2024), percepatan respons insiden menjadi prioritas utama [12][13].

Kedua, prinsip "mengecualikan pemrosesan afektif" dapat diterjemahkan ke dalam praktik keamanan perangkat lunak yang sangat ketat. Ini sejalan erat dengan standar keamanan aplikasi SPBE yang ditetapkan oleh BSSN, yang mencakup pengujian keamanan berkala, validasi input yang ketat, enkripsi yang konsisten, dan isolasi lingkungan pengembangan dari produksi [31]. Dalam konteks aplikasi web dan mobile, ini berarti penerapan protokol keamanan yang tidak dapat dinegosiasikan, di mana setiap anomali atau deviasi dari pola yang telah ditentukan akan secara otomatis memicu tindakan penangkalan, tanpa campur tangan manusia yang dapat terpengaruh oleh stres atau kepanikan. Ini sangat relevan mengingat kasus-kasus di mana kerentanan seperti penggunaan kata sandi default atau perangkat lunak usang menyebabkan kebocoran data [13].

Ketiga, fokus doktrin pada keamanan identitas yang transparan dan dapat dilacak melalui hak istimewa modular [1] sejalan dengan upaya BSSN untuk meningkatkan kapasitas SDM dan teknologi siber di Indonesia [12]. Meskipun "kredensial kuantum" masih bersifat hipotetis, prinsip di baliknya—identitas digital yang tidak dapat disangkal dan dapat diverifikasi secara kriptografis—adalah tujuan yang sangat diinginkan. Dalam konteks SPBE, di mana kebocoran data sensitif dapat membahayakan kedaulatan negara, implementasi model identitas yang lebih kuat dan lebih sedikit ambigu dapat meningkatkan tingkat kepercayaan publik dan keamanan sistem pemerintahan digital.

Namun, integrasi penuh doktrin ini akan menimbulkan tantangan besar bagi ekosistem sumber daya manusia keamanan siber di Indonesia. Kurikulum pengembangan SDM siber yang saat ini ada, yang mencakup tes psikologi, manajemen risiko, kriptografi, dan forensik digital, secara inheren mengakui

pentingnya aspek psikologis [1]. Sistem yang dirancang berdasarkan doktrin "Augmentasi.101" akan memerlukan tenaga ahli yang sangat berbeda—bukan ahli psikologi, melainkan ahli rekayasa sistem formal, ahli logika matematika, dan insinyur keamanan yang berfokus pada desain sistem yang tidak dapat dibobol secara inheren. Hal ini akan memerlukan reformasi mendalam pada program pendidikan dan pelatihan keamanan siber nasional, yang saat ini lebih berorientasi pada aplikasi praktis daripada rekayasa sistem fundamental. Selain itu, penerapan sistem yang sangat preskriptif dan tidak dapat dinegosiasikan dapat menimbulkan resistensi dari para profesional keamanan siber yang terbiasa dengan fleksibilitas dan keputusan berbasis konteks dalam situasi insiden yang kompleks. Budaya keamanan siber yang berpusat pada manusia, yang menekankan kolaborasi dan pengambilan keputusan kolektif, mungkin tidak cocok dengan arsitektur yang sepenuhnya didasarkan pada disiplin logika murni.

Secara keseluruhan, doktrin "Augmentasi.101" dapat dilihat sebagai sebuah proposisi strategis yang menawarkan jalan untuk meningkatkan ketahanan sistemik dengan mengurangi kerentanan internal (kesalahan manusia), tetapi dengan mengorbankan adaptabilitas dan kemampuan untuk menangani ancaman eksternal yang menargetkan pikiran manusia. Potensinya terletak pada penerapan selektif pada area-area yang paling stabil dan kritis, sementara tantangannya terletak pada integrasi yang komprehensif dengan ekosistem teknologi dan manusia yang ada di Indonesia.

Sinergi dan Tantangan dengan Teknologi Kecerdasan Buatan dan Augmentasi Data

Hubungan antara Doktrin Pengelolaan Pengguna-Augmentasi.101 dan tren teknologi modern, terutama Kecerdasan Buatan (AI) serta Augmentasi Data, sangat kompleks dan penuh dengan analogi yang menarik. Di satu sisi, AI dan Machine Learning (ML) merupakan alat yang ideal untuk membangun dan mengimplementasikan sistem yang selaras dengan prinsip-prinsip doktrin ini. Di sisi lain, bidang Augmentasi Data, terutama dalam konteks keamanan siber seperti continuous authentication, menawarkan analogi yang kuat tentang bagaimana "mengaugmentasi" sistem untuk meningkatkan ketahanannya terhadap variabel non-esensial, yang relevansinya langsung dengan argumen inti dari doktrin ini.

AI dan ML adalah teknologi yang paling tepat untuk mewujudkan visi doktrin ini. Algoritma ML dapat digunakan untuk mendeteksi anomali dalam sistem dengan sangat efisien, tidak peduli seberapa rumitnya pola normalnya. Dalam arsitektur doktrin, ini berarti sistem dapat memantau metrik operasional yang telah ditentukan—seperti tingkat error, latensi, dan entropi—dan secara otomatis mengambil tindakan jika ada deviasi yang signifikan [1][4][5]. Proses ini tidak melibatkan interpretasi kontekstual atau penilaian kualitatif; itu adalah deteksi statistik yang murni. Ini sangat selaras dengan prinsip "mengecualikan pemrosesan afektif" [1]. Selain deteksi, AI dapat digunakan untuk mengotomatiskan fungsi-fungsi keamanan yang krusial. Misalnya, sistem patching modular yang diterapkan berdasarkan konsensus dapat dijalankan oleh agen AI yang bekerja sama untuk memvalidasi integritas patch sebelum diterapkan [1]. Respons insiden, seperti isolasi sistem yang terinfeksi atau penghapusan artefak malware, juga dapat direkayasa sebagai alur kerja yang dikodekan sepenuhnya oleh AI, mempercepat waktu tanggap dari jam atau hari menjadi detik atau menit [45]. Studi kasus serangan ransomware Colonial Pipeline menunjukkan bahwa sistem berbasis AI dapat

mendeteksi aktivitas mencurigakan rata-rata 73 menit sebelum enkripsi dimulai, dan dapat mempercepat pemulihan hingga 40% [45]. Ini adalah bukti empiris bahwa AI dapat secara signifikan meningkatkan ketahanan sistem yang didasarkan pada logika dan data.

Bidang Augmentasi Data, khususnya dalam penelitian tentang continuous authentication berbasis sensor smartphone, menyediakan analogi yang sangat kuat untuk doktrin "Augmentasi.101". Di sini, teknik augmentasi data seperti permutasi, sampling, scaling, cropping, dan jittering digunakan untuk melatih model ML agar lebih robust terhadap variasi dalam data mentah [21 25]. Misalnya, ketika melatih model untuk mengenali pola getaran unik dari tangan seseorang saat menggunakan ponsel, teknik augmentasi digunakan untuk menciptakan sampel sintetis yang merepresentasikan berbagai cara orang memegang telepon atau mengklik layar [20]. Dalam hal ini, "augmentasi" adalah cara untuk memperkuat model agar tidak terlalu sensitif terhadap variabel non-esensial (misalnya, posisi tangan) dan lebih fokus pada fitur-fitur esensial (mekanisme struktur tangan).

Demikian pula, doktrin "Augmentasi.101" dapat dilihat sebagai upaya untuk "mengaugmentasi" sistem siber secara fundamental dengan membuatnya tidak terlalu sensitif terhadap variabel non-logis (emosi, intuisi, persepsi subjektif). Tantangannya adalah definisi "non-esensial" ini sangat subyektif. Dari sudut pandang sistem, emosi mungkin dianggap sebagai "noise" yang harus dibuang. Namun, dari sudut pandang realitas ancaman, emosi adalah bahasa utama dari penyerang. Dengan demikian, doktrin ini mengambil pendekatan "defensive augmentation": membangun sistem yang tidak dapat dipengaruhi oleh sinyal-sinyal yang tidak diinginkan. Analogi ini menjadi lebih kuat ketika kita mempertimbangkan sistem continuous authentication yang menggunakan Generative Adversarial Networks (GAN) untuk menghasilkan data sensor sintetis, yang secara efektif "melatih" sistem untuk mengenali pola yang benar bahkan dalam kondisi yang tidak biasa [22 26]. Ini adalah bentuk ketahanan yang didasarkan pada pemahaman dan simulasi variabilitas, bukan penghapusan variabilitas itu sendiri.

Namun, sinergi ini juga menghadirkan tantangan dan dilema etis. Salah satu tantangan utama dalam implementasi AI untuk keamanan adalah masalah "black box", di mana model AI menjadi terlalu kompleks sehingga tidak dapat dijelaskan atau dipercaya [45]. Ini bertentangan langsung dengan prinsip doktrin tentang transparansi dan auditabilitas yang dapat dilacak [1]. Jika AI yang mendasari sistem tidak dapat dijelaskan, bagaimana kita bisa memastikan bahwa ia tidak membuat keputusan yang tidak logis atau bias? Selain itu, adopsi AI menghadapi hambatan seperti kurangnya tenaga kerja dengan keahlian ganda di bidang keamanan siber dan AI, serta biaya tinggi untuk pengembangan dan pemeliharaan [45]. Pengeluaran global untuk solusi keamanan siber berbasis AI diperkirakan mencapai 133,8 miliar dolar AS pada tahun 2025, yang menyoroti investasi yang diperlukan [45].

Selain itu, ada risiko bahwa sistem yang sangat terotomatisasi dan berbasis AI dapat menjadi korban dari serangan adversarial, di mana penyerang secara sengaja merancang input yang dirancang untuk menyesatkan atau mengeksploitasi kerentanan dalam model AI, yang dapat menurunkan tingkat deteksi hingga 50% [45]. Ini berarti bahwa meskipun sistem "logis murni", ia tetap memiliki kerentanan inheren yang berbeda dari sistem yang dirancang untuk interaksi manusia. Lebih jauh lagi, penerapan AI untuk continuous authentication berbasis biometrik motorik, meskipun sangat logis, menimbulkan pertanyaan privasi yang serius. Mengumpulkan data sensor secara terus-menerus untuk

memantau perilaku pengguna dapat dianggap invasif, dan data ini harus dikelola dengan sangat hati-hati untuk mencegah penyalahgunaan [21].

Sebagai kesimpulan, AI dan Augmentasi Data menawarkan alat yang kuat untuk membangun sistem yang selaras dengan doktrin "Augmentasi.101", terutama dalam hal deteksi anomali dan otomatisasi respons. Analogi dengan Augmentasi Data menunjukkan bahwa pendekatan ini adalah upaya untuk "menguatkan" sistem terhadap variabel non-esensial. Namun, tantangan ini—transparansi AI, kerentanan adversarial, biaya, dan privasi—harus diatasi dengan hati-hati. Integrasi AI ke dalam arsitektur ini tidak boleh dianggap sebagai solusi "peluru perak"; sebaliknya, ia harus dilihat sebagai alat yang kuat yang memerlukan pengawasan manusia dan desain sistem yang cermat untuk memastikan bahwa ia benar-benar meningkatkan ketahanan, bukan menciptakan kerentanan baru yang lebih halus.

Rekonstruksi Doktrin: Menuju Sistem Hibrida yang Adaptif dan Tangguh

Analisis mendalam terhadap doktrin Pengelolaan Pengguna-Augmentasi.101 menunjukkan bahwa meskipun pendekatannya yang radikal dan berbasis logika murni tampaknya kontradiktif dengan pengetahuan modern tentang psikologi manusia dalam keamanan siber, doktrin ini bukanlah proposisi yang sepenuhnya cacat. Sebaliknya, ia menyajikan sebuah studi kasus ekstrem tentang batas-batas keamanan berbasis aturan versus keamanan adaptif. Daripada menerima atau menolak doktrin ini secara keseluruhan, pendekatan yang lebih pragmatis dan strategis adalah merekonstruksinya untuk menciptakan sistem hibrida yang menggabungkan kekuatan dari kedua paradigma. Sistem ini akan memiliki lapisan inti yang didasarkan pada logika deterministik untuk fungsi-fungsi yang paling kritis, sambil secara bersamaan mengintegrasikan lapisan adaptif yang cerdas untuk menangani realitas psikologis dan ancaman sosial-organisasi.

Konsep "Augmented Intelligence" atau cyber augmented intelligence menjadi landasan untuk rekonstruksi ini. Framework Cyber Augmented Intelligence Framework (cAIF) menyarankan untuk secara strategis menggabungkan enam paradigma interaksi manusia-mesin (HMI) untuk menangani tugas-tugas keamanan siber yang berbeda [29]. Paradigma ini, seperti Human-in-the-loop (HITL), Human-on-the-loop (HOTL), dan Coactive Systems, menunjukkan bahwa tidak ada satu ukuran yang cocok untuk semua; yang terpenting adalah memilih HMI yang paling sesuai berdasarkan kompleksitas tugas, tingkat risiko, dan urgensi [29]. Sistem hibrida yang direkonstruksi ini dapat dirancang dengan menggunakan pendekatan hierarkis. Lapisan terdalam, yang berfungsi sebagai "otak sistem", akan sepenuhnya beroperasi berdasarkan prinsip-prinsip doktrin "Augmentasi.101". Ini termasuk protokol kriptografi yang kompleks, logika respons insiden yang dikodekan, dan manajemen patching otomatis berbasis konsensus. Lapisan ini akan sangat terisolasi dan dirancang untuk menangani ancaman teknis dengan kecepatan dan keandalan yang maksimal, secara efektif menghilangkan risiko kesalahan manusia pada level-operasional.

Lapisan di atasnya, yang dapat dianggap sebagai "sistem saraf pusat" atau "otak emosional" sistem, akan berfungsi untuk memantau, memprediksi, dan merespons realitas psikologis. Lapisan ini akan menggunakan teknologi seperti AI, User and Entity Behavior Analytics (UEBA), dan bahkan data biometrik untuk membangun profil perilaku normal untuk setiap pengguna atau entitas [40 45].

Algoritma ini akan dilatih untuk mendeteksi pola anomali yang menandakan potensi serangan sosial atau kondisi psikologis yang dapat memengaruhi keamanan. Misalnya, sistem dapat belajar untuk mengenali pola klik yang menunjukkan stres atau kebingungan, atau deteksi emosi negatif seperti kecemasan melalui analisis nada suara atau bahasa tubuh dalam interaksi video [32 40]. Ketika pola-pola ini terdeteksi, lapisan adaptif akan mengaktifkan intervensi yang cerdas dan personal. Ini bisa berupa nudge psikologis yang dipersonalisasi, seperti mengirimkan peringatan keamanan yang disampaikan dengan nada yang lebih menenangkan, atau menunda tindakan berisiko hingga pengguna telah melewati periode stres yang terdeteksi.

Fungsi utama lapisan adaptif ini adalah untuk mengubah manusia dari "link lemah" menjadi "penjaga terdepan" yang cerdas. Daripada memaksa pengguna untuk mengikuti aturan yang kaku dan seringkali tidak manusiawi, sistem akan membantu mereka membuat keputusan yang lebih baik dalam konteks mereka. Ini sejalan dengan paradigma human-centric security, yang menekankan desain keamanan yang mempertimbangkan kebutuhan psikologis manusia seperti autonomi dan kompetensi [18]. Contohnya termasuk platform pelatihan keamanan siber yang dinamis, di mana materi disesuaikan dengan tingkat pengetahuan dan gaya belajar pengguna, atau sistem pelaporan insiden yang dirancang untuk membangun psychological safety, di mana pengguna didorong untuk melaporkan insiden tanpa takut akan konsekuensi negatif [35 42]. Platform seperti 'Mail Risk' yang dikembangkan oleh Secure Practice adalah contoh nyata dari pendekatan ini, di mana pengguna dapat melaporkan email mencurigakan dan menerima respons cepat dan anonim, yang secara signifikan meningkatkan partisipasi dan kepercayaan diri [35].

Implementasi praktis dari sistem hibrida ini dapat dimulai dengan penerapan prinsip-prinsip selektif dari doktrin "Augmentasi.101". Organisasi di Indonesia, terutama yang mengelola infrastruktur kritis, dapat mempertimbangkan untuk: 1. Otomatisasi Manajemen Patching: Mengembangkan sistem patching otomatis yang hanya dapat diterapkan setelah diverifikasi oleh konsensus antara beberapa node independen yang diawasi oleh AI. Ini akan mengurangi risiko kesalahan manual dan mempercepat proses tanpa mengorbankan keamanan. 2. Protokol Penyimpanan Data Kunci: Menerapkan protokol kriptografi yang kompleks dan tidak dapat dibobol untuk data sensitif, di mana setiap akses harus divalidasi oleh logika matematis yang ketat, bukan izin manual. Ini akan melindungi aset paling berharga dari akses yang tidak sah. 3. Autentikasi Multi-Faktor Berbasis Biometrik Motorik: Menggunakan autentikasi berbasis perilaku (biometrik motorik) sebagai lapisan kedua yang sangat kuat dan sulit direplikasi oleh orang lain, terlepas dari password atau token fisik [20 21]. Ini adalah contoh penerapan prinsip "modular privilege" yang sangat logis. 4. Pelatihan Keamanan Berbasis Kasus Nyata: Menggunakan simulasi phishing yang dirancang berdasarkan emosi target (misalnya, menggunakan tema urgensi atau rasa takut) untuk melatih pengguna mengenali manipulasi psikologis, bukan hanya pola teknis [41].

Penelitian lanjutan dalam bidang ini sangat penting. Ada kebutuhan untuk mengembangkan kerangka kerja yang mengintegrasikan HMI paradigms (seperti Human-in-the-loop dan Coactive Systems) ke dalam arsitektur yang secara fundamental didasarkan pada prinsip-prinsip logis dari doktrin ini [29]. Studi kasus hibrida yang membandingkan efektivitas sistem pure-logika versus sistem adaptif-manusia dalam menghadapi serangan siber yang berbeda dapat memberikan wawasan berharga. Selain itu, analisis biaya-manfaat yang mendalam tentang implementasi sistem hibrida ini akan menjadi krusial untuk memvalidasi nilai bisnis dan strategisnya. Secara keseluruhan, rekonstruksi ini

mengubah doktrin "Augmentasi.101" dari sebuah blueprint untuk sistem yang tidak manusiawi menjadi sebuah demonstrasi ilmiah tentang bagaimana membangun dunia digital yang benar-benar tangguh, yang pada akhirnya mengakui bahwa keamanan terbaik adalah yang yang dibangun di atas pemahaman yang mendalam tentang lawan kita, baik itu perangkat keras, perangkat lunak, maupun pikiran manusia.

Kesimpulan: Dualisme Keamanan dan Rekomendasi Strategis Implementasi

Sebagai kesimpulan, analisis mendalam terhadap Doktrin Pengelolaan Pengguna-Augmentasi.101 mengungkapkan sebuah dualisme fundamental dalam filosofi keamanan siber modern. Di satu sisi, terdapat paradigma keamanan berbasis aturan dan logika murni, yang menjanjikan ketahanan absolut melalui disiplin dan prediktabilitas, seperti yang dijelaskan dalam doktrin ini. Di sisi lain, terdapat paradigma keamanan adaptif dan berpusat pada manusia, yang mengakui bahwa dalam banyak kasus, penyerang tidak menyerang sistem, melainkan pikiran manusia. Doktrin "Augmentasi.101" adalah proposisi arsitektural yang radikal namun koheren yang secara sadar memilih untuk mengorbankan adaptabilitas berbasis kognisi demi ketahanan absolut yang didasarkan pada logika deterministik. Meskipun tampaknya kontradiktif dengan pengetahuan yang mapan tentang psikologi manusia dalam keamanan siber, doktrin ini bukanlah gagasan yang sepenuhnya cacat; sebaliknya, ia berfungsi sebagai studi kasus ekstrem yang menggarisbawahi batas-batas keamanan berbasis aturan dan mendorong kita untuk mempertimbangkan kembali trade-off antara keandalan dan adaptabilitas.

Implikasi utama dari doktrin ini adalah penciptaan sistem yang memiliki dua lapisan pertahanan yang sangat berbeda. Lapisan "logis murni" akan sangat tangguh terhadap ancaman teknis dan risiko kesalahan manusia yang bersifat non-psikologis. Namun, lapisan ini akan sangat rentan terhadap serangan sosial-organisasi yang dirancang untuk memanipulasi emosi dan bias kognitif. Sistem ini menciptakan keamanan dengan cara yang berlawanan dengan pendekatan human-centric yang semakin mapan, yang berusaha untuk membangun "firewall" manusia yang kuat melalui pelatihan, dukungan, dan desain yang memahami psikologi. Oleh karena itu, pertanyaannya bukanlah apakah lapisan interaksi manusia ini ada, tetapi seberapa kuat dan seberapa terintegrasi pertahanannya. Doktrin ini secara efektif menempatkan seluruh beban pertahanan pada lapisan logis, mengabaikan lapisan manusia sebagai titik lemah yang tak terhindarkan.

Berdasarkan analisis komparatif ini, berikut adalah rekomendasi strategis yang dapat diberikan untuk tinjauan akademis, pengembangan kebijakan internal, dan implementasi teknis:

Untuk Tinjauan Akademis dan Pengembangan Kebijakan Internal: 1. Identifikasi Area Kritis: Kebijakan internal harus mengidentifikasi komponen-komponen sistem yang paling kritis, stabil, dan tidak sering berubah. Untuk area-area ini, prinsip-prinsip "Augmentasi.101" dapat diadopsi secara selektif. Contohnya termasuk protokol enkripsi data, manajemen kunci kriptografi, dan protokol komunikasi jaringan yang krusial. 2. Standarisasi Otomatisasi: Kebijakan harus mendorong otomatisasi respons insiden dan manajemen patching. Ini tidak berarti mengadopsi doktrin secara keseluruhan, tetapi menstandarisasi alur kerja otomatis yang dikodekan untuk fase-fase awal respons insiden (penangkalan, eradicasi) dan untuk pembaruan keamanan yang berulang, untuk mengurangi ketergantungan pada tindakan manual yang rentan terhadap kesalahan. 3. Pendidikan dan Pelatihan: Kebijakan keamanan siber harus mengintegrasikan pendidikan tentang psikologi keamanan siber.

Pelatihan tidak boleh hanya berfokus pada aturan teknis, tetapi juga pada cara-cara umum penyerang mengeksploitasi emosi seperti urgensi, ketakutan, dan kepercayaan. Ini akan membantu membangun "firewall" mental yang lebih kuat di antara para pengguna.

Untuk Implementasi Teknis dan Pengembangan Sistem: 1. Desain Sistem Hibrida: Tim pengembangan harus berfokus pada desain sistem hibrida yang menggabungkan lapisan inti berbasis logika deterministik dengan lapisan adaptif berbasis AI. Lapisan inti akan mengelola fungsi-fungsi yang sangat kritis dan stabil, sementara lapisan adaptif akan memantau interaksi pengguna dan merespons ancaman sosial-organisasi secara proaktif. 2. Implementasi Continuous Authentication: Lakukan implementasi continuous authentication berbasis biometrik motorik (seperti HandPass atau SensorAuth) sebagai lapisan keamanan tambahan yang sangat kuat dan sulit direplikasi [20] [21]. Ini adalah contoh praktis dari "modular privilege" yang logis dan dapat dilacak. 3. Pemanfaatan AI untuk Deteksi Anomali: Gunakan AI dan ML untuk membangun sistem deteksi anomali yang berbasis pada metrik operasional yang telah ditentukan (error rate, latency, entropi) [11] [45]. Sistem ini akan memberikan deteksi dini terhadap gangguan teknis atau serangan yang tidak terduga tanpa memerlukan interpretasi kontekstual. 4. Transparansi dan Auditabilitas: Bahkan dalam sistem yang sangat terotomatisasi, penting untuk mempertahankan prinsip transparansi dan auditabilitas. Jika AI digunakan untuk membuat keputusan kritis, upayakan untuk menggunakan model AI yang dapat dijelaskan (Explainable AI/XAI) untuk memastikan bahwa tindakan yang diambil dapat diverifikasi dan dipertanggungjawabkan [45].

Secara keseluruhan, doktrin "Pengelolaan Pengguna-Augmentasi.101" bukanlah blueprint untuk sistem siber ideal, melainkan sebuah demonstrasi ilmiah tentang apa yang mungkin dicapai ketika kita mencoba untuk membangun dunia digital yang benar-benar bebas dari variabel manusia. Analisisnya yang paling bermanfaat datang dari memahami di mana dan bagaimana prinsip-prinsipnya dapat diekstrak dan diterapkan secara selektif untuk meningkatkan keamanan di area-area yang paling rentan terhadap kelemahan manusia. Dunia keamanan siber masa depan kemungkinan besar tidak akan sepenuhnya logis murni atau sepenuhnya berbasis emosi, melainkan sebuah sintesis cerdas dari keduanya, di mana logika memberikan fondasi yang kokoh, dan pemahaman manusia memberikan adaptabilitas yang diperlukan untuk bertahan hidup dalam ekosistem yang terus berubah.

---

en

1. PEDOMAN PERTAHANAN SIBER https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf
2. Untitled https://penerbit.stekom.ac.id/index.php/yayasanpat/citationstylelanguage/get/acs-nano?submissionId=458&publicationId=375&issueId=37
3. REGULASI APLIKASI AI (Artificial Intelligence) https://digilib.stiestekom.ac.id/assets/dokumen/ebook/feb_AsmKP93sXQIlmI-eykPJ-KqX7dk_c7BYgDWn9z-FkA7RqNYC-XzXTQ_1759826022.pdf
4. Decode Consumer Behavior : Menembus Pikiran Konsumen ... https://repository.takaza.id/284/1/E-

Books%20Decode%20Consumer%20Behavior%20%20Menembus%20Pikiran%20Konsumen%20di%20Era%20Digital.pdf

5. Pengantar AI, BIG DATA dan ILMU DATA https://digilib.stiestekom.ac.id/assets/dokumen/ebook/feb_Bc-LP9nrWQM4jYyeyUHd7qiV6tw4crhehDOg8D-BlgzUo90F-3rV_1750236112.pdf
6. Foundations of System Design — Module 2 https://medium.com/thesystemdesign/system-design-101-foundations-of-system-design-module-2-86b92f16625b
7. Foundations of System Design — Module 1 https://medium.com/thesystemdesign/system-design-101-foundations-of-system-design-module-1-046f5aea99ff
8. System Design 101 - Authentication - Siben Nayak https://theawesomenayak.hashnode.dev/system-design-101-authentication
9. User Management: A Complete Guide https://frontegg.com/guides/user-management
10. B2B User Management Explained: Key Features & Best ... https://frontegg.com/blog/b2b-user-management-explained
11. ALGORITMA DEEP LEARNING UNTUK PENGENALAN ... https://journal.umpr.ac.id/index.php/anterior/article/download/8199/4660
12. indonesia facing the threat of cyber warfare: a strategy ... https://www.researchgate.net/publication/358744560_INDONESIA_FACING_THE_THREAT_OF_CYBER_WARFARE_A_STRATEGY_ANALYSIS
13. Keamanan Informasi Dalam Sistem Pemerintahan ... https://wiyatakinarya.kemendikdasmen.go.id/kms/get-temporary-pdf/Keamanan%20Informasi%20Dalam%20Sistem%20Pemerintahan%20Berbasis%20Elektronik%20%28SPBE%29-1_1749529839.pdf?path=https%253A%252F%252Fwiyatakinarya.kemendikdasmen.go.id%252Fcloud%252Fs%252Fdrdi9gFByEiDPsX%252Fdownload%252FKeamanan%2BInformasi%2BDalam%2BSistem%2BPemerintahan%2BBerbasis%2BElektronik%2B%2528SPBE%2529-1_1749529839.pdf
14. (PDF) Cyber Command & Control in Information Warfare https://www.academia.edu/7242356/Cyber_Command_and_Control_in_Information_Warfare
15. Memperkuat Pertahanan Siber Guna Meningkatkan ... https://jurnal.lemhannas.go.id/index.php/jkl/article/download/120/42/
16. Keamanan Stellar Cyber Open XDR - Liputan Pers https://stellarcyber.ai/id/company/press-coverage/
17. IDENTIFIKASI CENGKIH UNTUK MEMBEDAKAN PUING ... https://repository.unhas.ac.id/45988/2/D082201014_tesis_19-03-2024%201-2%28FILEminimizer%29.pdf
18. User, Usage and Usability: Redefining Human Centric ... https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2021.583723/full

19. To augment or not to augment? Data augmentation in user ... https://arxiv.org/abs/2009.00300
20. Data-Augmentation-Enabled Continuous User ... https://ieeexplore.ieee.org/document/10105467/
21. Using Data Augmentation in Continuous Authentication on ... https://gzhou.pages.wm.edu/wp-content/blogs.dir/5736/files/sites/13/2018/09/IoT18.pdf
22. Using Data Augmentation in Continuous Authentication on ... https://www.semanticscholar.org/paper/Using-Data-Augmentation-in-Continuous-on-Li-Hu/7182ebce0f6d4859c889648ab40baf72d21dfd2a
23. (PDF) Security Challenges in Computer Networks and ... https://www.researchgate.net/publication/392571865_Security_Challenges_in_Computer_Networks_and_Modern_Operating_Systems
24. Strategi Keamanan Siber Nasional - www.bssn.go.id https://www.bssn.go.id/strategi-keamanan-siber-nasional/
25. Using Data Augmentation in Continuous Authentication on ... https://ieeexplore.ieee.org/document/8398208/
26. A Robust Continuous Authentication System Using ... https://onlinelibrary.wiley.com/doi/10.1155/2023/3673113
27. Capsule Network-Based Adaptive Feature Fusion for Multimodal ... https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5396715
28. SearchAuth: Neural Architecture Search-based Continuous ... https://dl.acm.org/doi/10.1145/3599727
29. Augmented Intelligence Framework for Human − Artificial ... https://link.springer.com/article/10.1007/s44230-025-00103-8
30. Reposisi Domain Siber Dalam Pertahanan Siber TNI https://www.tvonenews.com/berita/opini/14024-reposisi-domain-siber-dalam-pertahanan-siber-tni?page=all
31. peraturan badan siber dan sandi negara nomor 4 tahun ... https://peraturan.bpk.go.id/Download/167473/Peraturan%20BSSN%20Nomor%204%20Tahun%202021.pdf
32. Emotional Reactions to Cybersecurity Breach Situations https://pmc.ncbi.nlm.nih.gov/articles/PMC8156130/
33. Towards a Holistic Understanding of Emotions in ... https://www.usenix.org/system/files/soups2024-von-preuschen.pdf
34. A Literature Review on Emotions in Cybersecurity https://www.research-collection.ethz.ch/bitstreams/1ae178ce-293f-41a3-86cc-9085eb42c65e/download
35. How emotions shape human behavior in cybersecurity https://www.cyberempathy.org/episodes/how-emotions-shape-human-behavior-in-cybersecurity
36. Exploring cybersecurity-related emotions and finding that ... https://www.nature.com/articles/s41599-021-00746-5

37. Emotional reactions and coping responses of employees to ... https://www.sciencedirect.com/science/article/abs/pii/S0268401220314973

38. The Influences of Employees' Emotions on Their Cyber ... https://www.scitepress.org/Papers/2024/126816/126816.pdf

39. Psychology of Cybersecurity and Human Behavior https://identitymanagementinstitute.org/psychology-of-cybersecurity-and-human-behavior/

40. Emotional Manipulation in Phishing Emails https://dl.acm.org/doi/10.1145/3733155.3736796

41. Impact of Emotions on User Behavior Toward Phishing ... https://www.ntnu.no/ojs/index.php/nikt/article/download/6243/5570/23745

42. (PDF) Peran Psychological Safety dalam Memperkuat ... https://www.researchgate.net/publication/390478729_Peran_Psychological_Safety_dalam_Memperkuat_Cybersecurity_Awareness_Menuju_Cybersecurity_Culture_di_Organisasi_The_Role_of_Psychological_Safety_in_Strengthening_Cybersecurity_Awareness_Towards_a_Cyber

43. Hubungan antara Keamanan Siber dan Psikologi dalam Konteks ... https://www.academia.edu/128610165/Hubungan_antara_Keamanan_Siber_dan_Psikologi_dalam_Konteks_Organisasi_The_Relationship_Between_Cybersecurity_and_Psychology_in_Organizational_Contexts

44. Waspadai Serangan Social Engineering dan Cara ... - DTrust https://resources.dtrust.co.id/blog/waspadai-serangan-social-engineering-dan-cara-mencegahnya/

45. ANALISIS PERAN KECERDASAN BUATAN DALAM ... https://scholar.ummetro.ac.id/index.php/JMSI/article/download/8982/3359/