SISTEM KEKEBALAN DIGITAL UNTUK PERLINDUNGAN DATA DAN PRIVASI MASYARAKAT AWAM DI MASYARAKAT 5.0

UNIVERSITAS GADJAH MADA

Pidato Pengukuhan Jabatan Guru Besar
dalam Bidang Teknologi Informasi
pada Fakultas Teknik
Universitas Gadjah Mada

Disampaikan pada Pengukuhan Guru Besar
Universitas Gadjah Mada
pada Tanggal 6 Juli 2023

Oleh:
Prof. Ir. Paulus Insap Santosa, M.Sc., Ph.D., IPU

Yang terhormat
Ketua, Sekretaris, dan Anggota Majelis Wali Amanat Universitas Gadjah Mada;
Rektor dan para Wakil Rektor Universitas Gadjah Mada;
Ketua, Sekretaris, dan Anggota Dewan Guru Besar Universitas Gadjah Mada;
Ketua, Sekretaris, dan Anggota Senat Akademik Universitas Gadjah Mada;
Dekan dan para Wakil Dekan di lingkungan Universitas Gadjah Mada;
Ketua, Sekretaris, dan seluruh Anggota Senat Fakultas Teknik;
Rekan-rekan sejawat, para dosen, tenaga kependidikan, dan seluruh sivitas akademika Universitas Gadjah Mada;
Seluruh tamu undangan, mahasiswa, alumni, mitra kerja, keluarga, dan seluruh hadirin yang berbahagia.

Assalaamu'alaikum wa Rahmatullaahi wa Barokaatuh
Shalom
Om Swastiastu
Namo Buddhaya
Salam Kebajikan
Salam sejahtera bagi kita semua

Pertama kali, saya mengajak hadirin sekalian untuk memanjatkan segala puji syukur ke hadirat Tuhan YME atas segala berkat, karunia, dan rahmat-Nya yang selalu dilimpahkan untuk kita semua sehingga kita bisa hadir dan berkumpul di Balai Senat ini dalam keadaan sehat walafiat, tanpa kurang suatu apa pun. Sebuah kehormatan dan kebanggaan bagi saya bahwa sejak 1 November 2022 diberi amanah untuk menjadi salah satu Guru Besar di Universitas Gadjah Mada. Sebagai salah satu kewajiban sebagai Guru Besar Universitas Gadjah Mada, izinkan saya menyampaikan pidato pengukuhan dengan judul:

SISTEM KEKEBALAN DIGITAL UNTUK PERLINDUNGAN DATA DAN PRIVASI MASYARAKAT AWAM DI MASYARAKAT 5

Para hadirin dan tamu undangan yang saya hormati,

Pidato ini saya awali dengan sedikit menyinggung data statistik penggunaan internet. Penggunaan internet sebagai media untuk mencari dan bertukar informasi saat ini bertumbuh sangat pesat. Data yang dipublikasikan oleh Statista menunjukkan bahwa pengguna internet di seluruh dunia sampai dengan awal tahun 2023 mencapai 5,18 miliar. Pengguna sosial media merupakan pengguna terbesar dalam akses informasi menggunakan internet, yaitu sebanyak 4,8 miliar. Pengguna internet yang paling banyak menghabiskan waktu adalah mereka yang berusia 15–24 tahun (Statista, 2023). Meningkatnya penggunaan internet ini disebabkan oleh perkembangan teknologi dan infrastruktur yang makin luas dan merata ke berbagai belahan dunia serta akses ke berbagai media yang makin mudah dan merata.

Pandemi Covid-19 berdampak pada berbagai bidang, tidak terkecuali dalam hal pemanfaatan teknologi, khususnya yang berkaitan dengan penggunaan internet sebagai sarana komunikasi global yang murah, bahkan dalam situasi dan kondisi tertentu bisa diperoleh layanan internat secara gratis. Di era sebelum pandemi, sudah banyak aktivitas yang memanfaatkan internet untuk berbagai transaksi. Pada saat pandemi, pemanfaatan internet seperti mendapat momentum yang tepat sehingga makin banyak bidang kehidupan yang memanfaatkan internet. Transformasi digital di hampir semua bidang kehidupan menjadi sebuah keniscayaan.

Di satu sisi, teknologi membawa manfaat yang sangat besar di masyarakat. Namun, di sisi lain, perkembangan penggunaan internet dalam kehidupan sehari-hari juga menimbulkan isu privasi dan keamanan data yang signifikan. Berbagai kasus yang terkait dengan privasi dan keamanan data seperti pencurian informasi, kebocoran data, penipuan daring, pemerasan (baik kepada individu maupun institusi), penyebaran *ransomware* yang penyebarnya meminta sejumlah uang tebusan, dan sejumlah kasus lainnya. Kasus terbaru di tanah air dialami oleh salah satu bank di Indonesia (Laucereno, 2023; Helmi, 2023; Arini, 2023). Kasus di atas berkaitan dengan salah satu virus komputer berjenis *ransomware*. Pemilik atau penyebar

ransomware ini akan meminta uang tebusan kepada korban sebelum mereka memberikan antidotnya. Pada kasus ini, memang yang diserang adalah sebuah organisasi keuangan, tetapi karena melibatkan banyak nasabah, yang masing-masing nasabah perlu dilindungi data dan privasinya, maka urusannya menjadi lebih rumit dan makin kompleks ketika, misalnya, data memang benar-benar bocor sehingga ada kemungkinan nasabah-lah yang akan menjadi korban terbesarnya.

Para hadirin dan tamu undangan yang berbahagia,

Socio-Technical System

Sebelum saya membahas tentang sistem *socio-technical*, terlebih dahulu kita melihat definisi sistem. Sebuah sistem adalah sekelompok elemen otonom yang saling berinteraksi menurut aturan tertentu untuk membentuk satu kesatuan yang lebih besar dan utuh (Webster, 2023). Dalam dunia komputer, kita mengenal, antara lain, sistem operasi, sistem informasi, sistem cerdas, sistem perangkat lunak, sistem basis data, dan lain-lain. Dalam sosial kemasyarakatan, kita mengenal sistem sosial, sistem pemerintahan, sistem penggajian, dan lain-lain. Sesuai dengan definisi di atas, sistem informasi, sebagai contoh, merupakan sekumpulan elemen yang bersifat otonom. Elemen-elemen yang ada di dalam sebuah sistem informasi, antara lain, perangkat keras, perangkat lunak, data, manusia, dan aturan atau prosedur yang harus ditaati agar sistem informasi dapat bekerja sesuai dengan tujuannya.

Sebagai makhluk sosial, setiap individu perlu berkomunikasi dengan individu lain atau sekelompok anggota masyarakat untuk mencapai tujuan tertentu, dari sekadar bercanda, bertukar pikiran, sampai membahas hal-hal yang sangat serius. Cara manusia berkomunikasi berkembang dari zaman prasejarah hingga era Masyarakat 5.0 (*Society 5.0*), terutama dengan adanya perkembangan teknologi komunikasi yang sangat pesat. Cara berkomunikasi yang di zaman prasejarah dilakukan dengan memanfaatkan yang tersedia di alam, misalnya asap, kentongan, dan burung merpati pos, pada saat ini digantikan dengan media sosial berbasis pada internet. Pendek kata, komunikasi sebagai salah satu kebutuhan manusia sekarang banyak

dibantu dengan perangkat teknologi. Kolaborasi inilah merupakan salah satu dari yang disebut dengan sistem *socio-technical*. Secara sederhana, sistem *socio-technical* dapat disajikan seperti terlihat pada Gambar 1 (adaptasi Rettig, 2017).

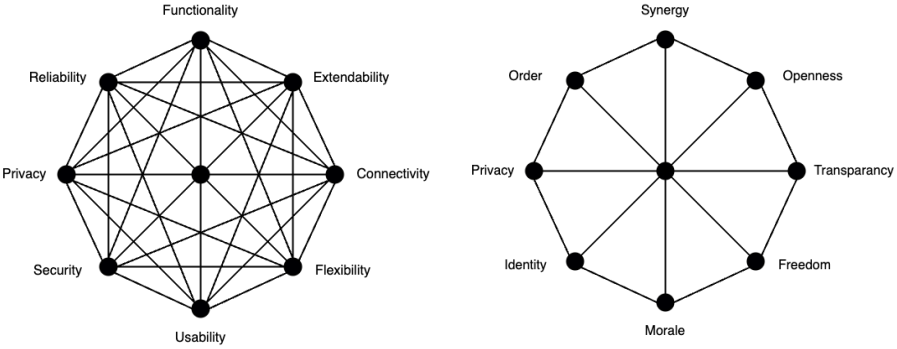
Aras	Bidang Ilmu	Sistem	Kombinasi	Contoh
Komunitas	Sosiologi, Politik, Bisnis	Sosial	Sistem *socio-technical*	Budaya, hukum, aturan, sanksi
Individu	Psikologi, Biologi	Kognitif	Interaksi Manusia-Komputer	Sikap, *believe*, ide, opini
Informasi	Ilmu Komputer, Sains Informasi	Perangkat Lunak (*software*)	Teknologi (*software* dan *hardware*)	Program, data, memori, *bandwidth*
Fisik	Teknik, Fisika, Kimia	Fisik	Perangkat keras (*hardware*)	Komputer, *mouse*, *printer*

Gambar 1. Aras sistem *socio-technical* (adaptasi Rettig, 2017)

Gambar 1 menunjukkan bahwa secara sederhana, sistem *socio-technical* terdiri atas empat aras, yakni aras fisik, aras informasi, aras manusia sebagai individu, dan yang tertinggi adalah aras komunitas. Aras fisik berfokus pada perangkat keras, baik secara terpisah maupun secara terintegrasi. Aras informasi berfokus pada data, aplikasi, dan pengiriman data dari satu tempat ke tempat lain sehingga data dapat dimanfaatkan untuk berbagai keperluan di tempat yang berbeda. Aras individu berkaitan dengan aspek kognitif, sikap, keyakinan, opini, emosi, dan pengalaman pengguna ketika memanfaatkan sebuah teknologi. Aras komunitas berkaitan, antara lain, dengan pengaruh, budaya, hukum, aturan, dan risiko penggunaan aplikasi komputer di masyarakat luas.

Kinerja setiap aras pada sistem *socio-technical* ditentukan oleh sejumlah kriteria. Gambar 2 menyajikan jejaring beberapa kriteria untuk mengukur kinerja pada dua aras yang berbeda. Gambar 2.a (Whitworth et al., 2006) menunjukkan jejaring beberapa kriteria untuk mengukur kinerja pada aras aplikasi. Gambar 2.b (Whitworth, 2009)

menunjukkan jejaring beberapa kriteria untuk mengukur kinerja pada aras komunitas. Semua pengguna aplikasi pasti menginginkan aplikasi yang memenuhi semua kriteria seperti terbaca dari Gambar 2a secara melingkar. Pertanyaan yang kemudian timbul adalah apakah semua kriteria dapat dimaksimalkan? Jawabannya adalah tidak. Dua kriteria yang saling berseberangan, misalnya fungsionalitas dan kebergunaan (*usability*), bersifat saling membatasi. Fungsionalitas memang bisa dirancang selengkap mungkin, tetapi akan berakibat pada menurunnya kebergunaan aplikasi. Contoh lain, privasi dan konektivitas tidak mungkin keduanya dimaksimalkan. Aras privasi berbanding terbalik dengan jumlah konektivitas. Makin banyak seseorang terkoneksi dengan berbagai aplikasi, aras privasinya akan menurun.



a. b.

Gambar 2.
a. Jejaring kriteria kinerja pada aras aplikasi (Whitworth et al., 2006)
b. Jejaring kriteria kinerja pada aras komunitas (Whitworth, 2009)

Setiap aras pada sistem *sosio-technical* seperti disajikan pada Gambar 1 mempunyai sejumlah kriteria yang berbeda untuk setiap arasnya. Kriteria untuk menentukan kinerja aras perangkat keras tentu berbeda dengan kriteria kinerja aras informasi; berbeda juga dengan

kriteria kinerja aras individu maupun dengan aras komunitas, tetapi pada dasarnya menganut mekanisme yang sama dengan yang dijelaskan sebelumnya. Pada aras komunitas (Gambar 2b), anggota komunitas pasti menginginkan adanya kesempatan bersinergi, bersikap terbuka, bebas berkomunikasi dengan semua anggota komunitas. Akan tetapi, sekali lagi, perlu disadari bahwa dua kriteria yang berseberangan merupakan dua kriteria yang saling berlawanan. Jika salah satu ingin ditingkatkan maka yang lainnya harus dikorbankan. Contoh sederhana, jika kita aktif di sejumlah media sosial, di satu sisi kita bisa terkoneksi ke banyak teman, namun di sisi lain, secara disadari atau tidak, privasi kita akan berkurang, apalagi bagi kita yang gemar berbagi kegembiraan lewat *posting* berupa foto atau cerita naratif.

Para hadirin dan tamu undangan yang saya hormati,

Industri 4.0 dan Masyarakat 5.0

Saat ini, kita berada pada suatu era yang sering disebut sebagai era Industri 4.0. Industri 4.0 adalah nama yang diberikan pada tren saat ini tentang otomasi dan pertukaran data pada teknologi manufaktur. Nama Industri 4.0 terinspirasi oleh *Industrie 4.0* yang merupakan inisiatif pemerintah Jerman untuk mempromosikan *connected manufacturing* dan konvergensi digital antara industri, bisnis, dan proses lainnya (Daniel, 2023). Industri 4.0, terutama, melibatkan sistem siber-fisik (*cyber-physical system* atau CPS), IoT, dan komputasi awan. IoT pada dasarnya mengacu pada kemampuan untuk menghubungkan perangkat komputasi non- tradisional ke internet atau ke jaringan pribadi. Berbagai layanan, baik kepada individu maupun organisasi, memanfaatkan beberapa komponen di atas. Sebagai contoh, terdapat berbagai layanan di bidang pelayanan kesehatan, sistem keuangan, turisme, pertanian, dan berbagai sistem yang mendukung kota cerdas atau *smart city* (Tussyadiah et al., 2019).

Industri 4.0 lebih berfokus pada sisi teknologi. Bagaimana dengan masyarakat penggunanya? Pemerintah Jepang mengusulkan bahwa masyarakat pengguna berbagai teknologi di Industri 4.0 disebut dengan Masyarakat 5.0 atau *Society 5.0*. Pada dasarnya, Masyarakat 5.0 adalah masyarakat yang “memanfaatkan integrasi ruang fisik dan

ruang siber tingkat tinggi agar mampu mengimbangi kemajuan ekonomi dengan penyelesaian masalah sosial dengan menyediakan barang dan jasa dalam berbagai tingkatan layanan untuk mengatasi berbagai kebutuhan segera tak gayut terhadap lokasi, usia, jenis kelamin, suku, ras, atau bahasa" (Deguchi et al., 2020). Pandangan tentang Masyarakat 5.0 ini memerlukan pemikiran ulang terkait dua hubungan: hubungan antara teknologi dengan masyarakat dan hubungan termediasi teknologi antara individu dengan masyarakat.

Industri 4.0 sangat mengandalkan ketersediaan dan keandalan jaringan komunikasi data, terutama internet. Ketersediaan dan keandalan jaringan komunikasi data dan internet dipengaruhi oleh keamanannya terhadap ancaman siber. Oleh karena itu, salah satu dimensi penting dalam Industri 4.0 adalah keamanan siber (*cyber security*). Konektivitas antara berbagai perangkat keras dan sumber daya TI meningkatkan ancaman terhadap berbagai perangkat yang ada. Sistem TI yang rentan dapat memberi jalan bagi penyerang untuk melakukan serangan terhadap sumber daya yang ada. Keamanan siber merupakan upaya untuk melindungi sistem informasi, jaringan komunikasi data, dan sumber daya lainnya dari serangan siber dan ancaman lainnya. Aspek penting dalam keamanan siber meliputi aspek teknis dan non-teknis, antara lain, penggunaan teknologi, prosedur, dan praktik keamanan untuk melindungi data pribadi dan aset penting lainnya dari peretas, virus, dan serangan lainnya.

Para hadirin dan tamu undangan yang saya hormati,

Privasi dan Keamanan Data

Salah satu aspek penting dalam kriteria kinerja sistem *socio-technical*, khususnya pada aras komunitas, adalah privasi. Privasi adalah hak asasi manusia mendasar yang mendasari kebebasan berserikat, berpikir dan berekspresi, serta kebebasan dari diskriminasi. Negara yang berbeda menawarkan pandangan yang berbeda, seperti halnya individu yang juga mempunyai pandangan berbeda terkait privasi (Australian Government, 2023). Meskipun demikian, ada tiga aspek kunci privasi: bebas dari gangguan (intrusi), mempunyai kendali terhadap informasi tentang dirinya sendiri, dan bebas dari pengawasan (diikuti, dilacak, diawasi, dan disadap) (Basse, 2013).

Privasi menjadi salah satu kebutuhan setiap orang, terutama dalam kaitannya dalam kehidupan bermasyarakat, terlebih lagi saat keterhubungan antar-anggota masyarakat menjadi sebuah keniscayaan.

Ancaman terhadap privasi bisa datang dari individu yang bersangkutan maupun dari lingkungannya. Keteledoran seorang yang sedang menggunakan komputer di area publik ketika dia lupa untuk *logout* atau ketidakhati-hatian ketika membaca dan membalas pesan singkat dari seseorang yang tidak dikenal bisa menjadi sumber malapetaka baginya. Dari lingkungannya, ancaman terhadap privasi seseorang bisa berasal dari penggunaan informasi personal yang dilakukan oleh orang lain tanpa seizin empunya, pencurian informasi, dan kebocoran informasi karena keteledoran operator. Gambar 2.a dan 2.b menunjukkan bahwa ancaman terhadap privasi bisa disebabkan oleh makin banyaknya seseorang terkoneksi ke jaringan komunikasi publik seperti internet.

Privasi terkait erat dengan keamanan data yang dimiliki oleh setiap orang. Keamanan data adalah usaha untuk memproteksi data dan informasi digital terhadap akses yang tidak sah, kerusakan, dan pencurian data sepanjang siklus hidup data tersebut. Keamanan data merupakan sebuah konsep yang menekankan pada setiap aspek keamanan data dan informasi, mulai dari keamanan fisik (perangkat keras dan peranti penyimpan) sampai ke pengendalian administratif dan akses; dan yang tidak kalah pentingnya adalah keamanan perangkat lunak aplikasi. Keamanan data juga melibatkan kebijakan dan prosedur yang berlaku dalam sebuah organisasi (IBM, 2023). Pada dasarnya, keamanan data untuk menjaga kerahasiaan data (C*onfidentiality*), integritas data (I*ntegrity*), dan ketersediaan data (A*vailability*) yang dalam bahasa teknis disebut dengan CIA Triad. Kerahasiaan data berkaitan dengan proteksi untuk mencegah akses yang tidak sah dan untuk menjaga privasi data. Integritas data berkaitan dengan kualitas dan validitas data sehingga data selalu dapat dipercaya. Ketersediaan data berkaitan dengan data yang selalu dapat diakses oleh mereka yang setiap saat membutuhkannya (SecurityScorecard, 2023).

Berdasar sifatnya, ancaman terhadap keamanan data dapat dikategorikan menjadi ancaman pasif dan ancaman aktif. Ancaman pasif, antara lain, berasal dari bencana alam (gempa bumi, banjir, kebakaran, perang), kesalahan dan kelalaian manusia (kesalahan memasukkan data, kesalahan menghapus data, kesalahan memberi label pada tempat penyimpanan data), dan kegagalan perangkat keras dan perangkat lunak yang disebabkan oleh gangguan listrik, rusaknya perangkat keras, dan fungsionalitas perangkat lunak yang tidak sesuai dengan yang diharapkan. Ancaman aktif adalah ancaman yang berasal dari individu atau sekelompok orang yang memang berniat tidak baik terhadap individu atau sekelompok orang lain, organisasi, bahkan pemerintahan negara. Beberapa bentuk ancaman aktif, antara lain, kecurangan dan kejahatan menggunakan komputer (penyelewengan aktivitas, penyalahgunaan kartu kredit, sabotase, pelanggaran hak akses) dan program jahat yang sering disebut dengan virus. Ada berbagai sebutan dan jenis virus, misalnya *malware*, *worm*, *ransomware*, kuda troya, dan lain-lain.

Pemanfaatan *Big Data,* Kecerdasan Buatan, dan Kerentanan Privasi

Dua dari beberapa bidang penting dalam Industri 4.0 adalah *Big Data* dan Kecerdasan Buatan atau *Artificial Intelligence*. Berbagai penelitian dan penerapan kedua bidang di atas menunjukkan bahwa penggunaan keduanya dapat membantu meningkatkan kinerja dan efisiensi sistem siber fisik. Berikut adalah beberapa contoh penerapan *Big Data* dan Kecerdasan Buatan (untuk seterusnya disingkat dengan BDKB). Dalam bidang transportasi, BDKB digunakan untuk menganalisis kondisi lalu lintas secara *real time* guna mengurangi kemacetan. Hal ini dilakukan dengan mengombinasikan data pengguna terkait rute yang akan dilakukan dengan data yang berasal dari media sosial (Xiong, et al., 2021). Dalam bidang industri kesehatan, BDKB digunakan untuk mengumpulkan dan menganalisis data yang dihasilkan oleh perangkat pemantau, perangkat *wearable*, dan sensor medis yang dipasang pada tubuh pasien (Özdemir, 2019; Sreedevi et al., 2022). Hal ini memungkinkan dilakukannya deteksi dini dan prediksi terhadap perubahan kondisi pasien, seperti deteksi

detak jantung yang tidak normal, fluktuasi tekanan darah, atau gejala lain yang memerlukan perhatian medis dengan segera. Dengan demikian, tindakan cepat dan tepat segera dilakukan untuk menghindari memburuknya kondisi pasien (Ramasamy et al., 2022; Wang dan Alexander 2019). Dalam bidang pendidikan, salah satu pemanfaatan Kecerdasan Buatan adalah untuk menentukan efektivitas kuliah daring menggunakan sejumlah kriteria, seperti pilihan jadwal belajar, mode pembelajaran, dan jenis pembelajaran (Santosa dan Rianto, 2022).

BDKB dapat dimanfaatkan untuk mengembangkan pengalaman belajar yang dipersonalisasi sesuai kebutuhan siswa lewat *Intelligent Tutoring System* (Zhou, et al., 2020). Dengan menganalisis data individu siswa, termasuk kinerja akademik, preferensi belajar, serta kekuatan dan kelemahan mereka, algoritma Kecerdasan Buatan dapat menghasilkan jalur pembelajaran dan konten sesuai kebutuhan mereka. Metode ini memungkinkan siswa untuk belajar sesuai dengan kecepatan dan kebutuhan mereka sehingga menghasilkan peningkatan keterlibatan dan pencapaian akademik. BDKB juga dapat diterapkan dalam perancangan kurikulum dan pembagian sumber daya pada suatu lembaga pendidikan (Brahma et al., 2021) sehingga area perbaikan dan optimalisasi alokasi sumber daya dapat dilakukan (Song dan Zhu, 2017). Alhasil, hal tersebut dapat meningkatkan hasil pendidikan secara keseluruhan (Jin et al., 2022).

Contoh-contoh yang disajikan di atas menunjukkan hanya sebagian kecil dari pemanfaatan BDKB. Di sisi lain, pengambilan keputusan yang memanfaatkan penerapan BDKB sering melibatkan data personal sehingga meningkatkan risiko terhadap privasi dan keamanan data personal (Wachter dan Mittelstadt, 2019). Integrasi Kecerdasan Buatan di berbagai domain secara signifikan meningkatkan kekhawatiran tentang privasi dan keamanan data. Data yang menggerakkan Kecerdasan Buatan mencakup berbagai informasi sensitif, khususnya informasi individu, termasuk gambar, ucapan, komentar, catatan medis, dan unggahan di media sosial (Chen et al., 2013; Hu dan Min, 2023).

Pada hakikatnya, setiap kerentanan memiliki potensi terhadap dampak bencana yang berkaitan dengan aspek privasi dan keamanan

data. Beberapa penelitian sejauh ini difokuskan untuk mengidentifikasi berbagai macam ancaman BDKB pada sistem siber-fisik dan memberikan solusi tindakan pencegahan untuk mengurangi risiko yang disebabkan oleh serangan. Pada proses pengumpulan dan penggunaan data pribadi dalam lingkup sistem siber-fisik, keterbukaan dan transparansi sangat penting untuk diperhatikan. Pengguna layanan harus diberi tahu dengan jelas tentang jenis dan macam data yang dikumpulkan dan cara data tersebut digunakan. Hal ini biasanya tertuang dalam *privacy policy* atau *disclaimer* dari penyedia layanan. Pengguna layanan harus memiliki kendali atas data pribadi mereka dan memastikan bahwa data tersebut tidak disalahgunakan atau digunakan secara tidak sah. Akan tetapi, berapa banyak di antara kita yang menyempatkan diri untuk membaca *privacy policy* yang diberikan oleh penyedia layanan yang kita butuhkan? Ini menjadi bahan renungan bersama.

Para hadirin dan tamu undangan yang berbahagia,

Sistem Kekebalan Digital

Sistem kekebalan digital, untuk seterusnya disingkat dengan SKD, adalah sistem keamanan yang diterapkan pada sistem berbasis komputer untuk memantau aktivitas digital dan melindungi pengguna dari berbagai *malicious code*, seperti *malware*, virus, dan serangan *hacker*. SKD berprinsip mirip dengan sistem kekebalan tubuh manusia yang dapat mengidentifikasi ancaman, merespons, dan melakukan tindakan preventif yang diperlukan (Termanini, 2016). Tujuan utamanya adalah untuk menjaga CIA Triad, yakni menjaga kerahasiaan informasi, integritas, dan ketersediaan layanan digital yang diperlukan (Schatz dan Phillippy, 2012). SKD memainkan peran penting dalam melindungi privasi, terutama untuk memastikan bahwa data atau informasi pribadi tidak terbuka untuk ancaman keamanan, seperti pencurian identitas atau penyalahgunaan informasi (Forrest et al., 1997). Di sisi lain, implementasi SKD juga harus mempertimbangkan privasi pribadi dan hak-hak privasi pengguna. SKD yang terlalu agresif dalam memantau aktivitas digital justru bisa kontra produktif karena dapat membahayakan privasi pribadi (Said dan Mostafa, 2020). Sejumlah risiko tinggi berkaitan dengan terlalu

agresifnya sistem kekebalan digital, antara lain, adalah pengaturan parameter keamanan yang kurang tepat, pemblokiran aplikasi atau aktivitas yang tidak tepat, pengumpulan informasi dari pengguna aplikasi tanpa izin, penggunaan sumber daya yang boros, dan ketergantungan pada perangkat lain yang justru meningkatkan risiko keamanan.

SKD dan keamanan siber memiliki korelasi yang erat. SKD bekerja untuk mengidentifikasi dan memblokir ancaman potensial seperti virus dan *malware*, namun di sisi lain, keamanan siber bertanggung jawab untuk melindungi jaringan, sistem, dan data dari serangan dan ancaman siber. Dengan demikian, SKD dapat diterapkan sebagai bagian dari strategi keamanan siber untuk membantu mencegah serangan dan memastikan bahwa sistem dan data tetap aman. Di lain pihak, perlu diingat bahwa sistem kekebalan digital tidak dapat mengatasi semua ancaman siber dan harus digunakan sebagai bagian dari strategi keamanan siber yang lebih luas yang meliputi tindakan preventif dan pemantauan aktif (Igbe et al., 2016).

Pengembangan teknologi keamanan dalam lingkup sistem siber-fisik menjadi makin penting karena keterkaitannya dengan BDKB. Hal ini termasuk pengembangan algoritma proteksi untuk melindungi data personal dan mencegah serangan siber. Pada prinsipnya, BDKB pada sistem siber-fisik merupakan integrasi sistem yang sangat kompleks. Sistem siber-fisik pada dasarnya mengejar bentuk baru interaksi terintegrasi dengan manusia melalui komputasi dan kemampuan fisik yang mencakup sistem yang kompleks, cerdas, dan otonom (Kim dan Ben-Othman, 2020). Oleh karena itu, proteksi data menjadi sangat penting untuk menjaga keamanan dan privasi data pengguna. Ada sejumlah algoritma proteksi data yang dikembangkan dan digunakan pada lingkup sistem siber-fisik berbasis BDKB, di antaranya: *Secure Multiparty Computation* (Du dan Atallah, 2001); *Homomorphic Encryption* (Kocabas dan Soyata, 2015); *Differential Privacy* (Hassan et al., 2020); *Blockchain* (Wang et al., 2019); *Temper Detection* (Kim dan Ben- Othman, 2020); dan *Explanability* (Hussein dan El-Dosuky, 2023).

Fokus terbesar dari penggunaan algoritma proteksi data adalah untuk memastikan bahwa sistem dapat beroperasi secara aman dan

efektif (Giraldo et al., 2017). Data yang dikumpulkan dan diproses dapat digunakan untuk mengambil keputusan kritis sesuai dengan tujuan diterapkannya sistem siber-fisik. Oleh karena itu, proteksi data harus memastikan bahwa sistem dapat beroperasi dengan aman dan efektif dalam mengambil keputusan yang tepat (Chong et al., 2019).

Ancaman siber terus berkembang dan menjadi lebih kompleks sehingga perlu dilakukan tindakan pencegahan dan pemantauan yang berkelanjutan untuk memastikan bahwa sistem dan data tetap aman (Kaur dan Ramkumar, 2022). Di lain pihak, tidak ada jaminan bahwa sistem kekebalan digital terbaik akan memastikan keamanan organisasi secara total. SKD yang diterapkan di organisasi atau industri hanya merupakan bagian dari strategi keamanan siber yang lebih luas dan harus digunakan bersama dengan tindakan preventif dan pemantauan aktif lainnya. Selain itu, kebijakan yang lebih bersifat non-teknis juga perlu diterapkan, misalnya pengendalian akses, pengelolaan kata sandi, jenis enkripsi data, segmentasi jaringan, *disaster plan recovery*, keberkalaan *backup* data, keberkalaan pemantauan, dan yang tidak kalah pentingnya adalah pelatihan staf yang diberi tugas untuk mengawasi jaringan dengan berbagai dinamikanya.

Dari perspektif pengguna, penggunaan algoritma proteksi data sangat penting untuk memastikan bahwa data personal yang diberikan untuk digunakan dalam sistem tersebut tetap aman dan terjaga privasinya. Ketika pengguna memberikan data pribadinya, mereka seharusnya sudah memastikan bahwa data tersebut tidak akan disalahgunakan atau digunakan untuk tujuan yang tidak sesuai tanpa kekhawatiran akan kebocoran data atau penyalahgunaan data (Rani et al., 2022). Dengan proteksi data personal pengguna yang baik, pengguna akan yakin bahwa keputusan yang dihasilkan oleh sistem tersebut didasarkan pada data yang valid dan dapat dipercaya.

Selain dari sisi teknis, SKD perlu juga dilengkapi bantuan bagi pengguna internet dengan menanamkan kemampuan berpikir pada sistem yang mampu melakukan arahan edukasi pada pengguna sehingga dapat secara efektif membantu pengguna dalam memahami perilaku penggunaan internet dan perangkat siber-fisik lain dengan aman tanpa mengurangi rasa kenyamanan mereka. Kelompok

pengguna tertentu, yakni remaja dan masyarakat awam yang belum mempunyai tingkat literasi terkait privasi dan keamanan data yang cukup tinggi, perlu disadarkan bahwa berselancar di internet tidak selamanya aman. Mereka perlu diberi pengertian dan pengarahan tentang bahaya yang mengancam privasi dan keamanan data mereka. Oleh karena itu, kepada mereka dan sesungguhnya juga kita semua, perlu ditumbuhkan kesadaran tentang adanya ancaman siber dan memahami konsekuensi dari tindakan yang mereka ambil. Kepada mereka perlu diajarkan aspek tertentu dari keamanan siber dengan mengenali sejumlah tautan dan lampiran yang berbahaya serta tidak mudah berinteraksi dan berbagi informasi kepada pihak yang belum atau tidak dikenal. Selain itu, mereka juga perlu dibekali dengan literasi keamanan siber seperti pengaturan privasi pada aplikasi yang digunakan, responsif terhadap ancaman dengan cara mengembangkan kemampuan untuk mengenali tanda-tanda ancaman dan meresponsnya dengan tepat pada diri sendiri, serta membentuk perilaku digital yang bertanggung jawab.

Para hadirin dan tamu undangan yang saya hormati,

Pada bagian akhir dari pidato ini, saya ingin menggarisbawahi, saat ini penggunaan teknologi digital makin luas dan makin kompleks yang kemudian menimbulkan tantangan baru dalam hal keamanan digital, tidak saja bagi organisasi, pemerintahan, maupun industri, tetapi juga bagi individu, terutama bagi pengguna awam dan remaja yang saat ini menjadi pengguna aktif dan termasuk dalam jumlah pengguna internet yang besar. Penyediaan fasilitas keamanan oleh platform teknologi yang digunakan sudah menjadi keharusan. Di sisi lain, perilaku pengguna teknologi digital yang tidak tepat atau kurang mengikuti praktik keamanan yang sesuai dapat meningkatkan risiko terhadap serangan dan ancaman digital, seperti pencurian identitas, kebocoran data, *malware*, dan sebagainya. Jika kita memandang ancaman terhadap privasi dan keamanan data merupakan ancaman penyakit maka kita perlu membangun SKD, khususnya bagi pengguna awam dan remaja, untuk melindungi kita semua dari berbagai ancaman privasi dan keamanan data yang makin lama juga makin canggih dan bervariatif, baik cara maupun metodenya.

Peran yang harus kita mainkan dalam hal keamanan atau sekuriti data dan privasi yang kita miliki tercermin dari kata "sekuriti" dan "privasi" itu sendiri. Kata "sekUrItI" mengandung huruf U dan dua huruf I. Huruf U, yang dalam bahasa Inggris dibaca *you* (atau 'kamu'), kita artikan sebagai peran pemerintah, organisasi keamanan siber, lembaga lainnya, maupun berbagai *tool* untuk menjaga privasi dan keamanan data kita, seperti anti-virus, *firewall*, dan lainnya. Huruf I, yang dalam bahasa Inggris dibaca *ai* (atau 'saya'), menunjuk ke diri kita masing-masing untuk berperan aktif dalam menjaga privasi dan keamanan data kita masing-masing. Dengan demikian, untuk menjaga keamanan data, kita tidak boleh hanya mengandalkan pihak lain, tetapi kita juga harus dan wajib berperan aktif untuk menjaga keamanan data kita dengan cara yang kita pahami dan benar. Kata "prIvasI" yang mengandung dua buah huruf I mencerminkan bahwa urusan privasi harus menjadi tanggung jawab kita pribadi. Kita harus paham bahwa data yang kita sediakan, misalnya untuk meminta email baru, bisa digunakan untuk tujuan-tujuan tertentu sesuai *privacy policy* penyedia layanan. Dengan demikian, kita sebaiknya atau bahkan seharusnya membaca dan memahami isi *privacy policy* sebelum memberikan persetujuan. Hal paling akhir yang ingin saya sampaikan dari pidato ini saya ambil dari cuplikan dialog pada film serial *The Night Agent*, "Episode 1: The Call", yakni "Dalam keamanan siber, orang baik dan jahat sulit dibedakan. Tantangan yang utama adalah menghentikan orang yang melanggar privasi dan mencuri data kita," dan pada "Episode 2: Redial", yakni "Perusahaan besar harus melindungi informasi sensitif, tetapi privasi juga penting bagi perusahaan kecil dan individu." Hal ini bermakna bahwa privasi dan keamanan data tidak bisa diabaikan oleh siapa pun.

Para hadirin dan tamu undangan yang saya hormati,

Saya akan menutup pidato ini dengan pertama kali dan yang utama mengucap syukur kepada Tuhan Yang Maha Pengasih dan Pemurah dan memuji nama-Nya atas karunia-Nya yang sangat besar bahwa setelah berjuang selama lebih dari 10 tahun, pada akhirnya saya diberi kepercayaan untuk menjadi salah satu Guru Besar di Departemen Teknik Elektro dan Teknologi Informasi, Fakultas

Teknik, Universitas Gadjah Mada. Semoga alam semesta pun ikut bersorak dan bersukacita atas karunia-Nya yang membahagiakan.

Ucapan terima kasih dan penghargaan setinggi-tingginya saya sampaikan kepada Rektor Universitas Gadjah Mada beserta jajarannya, Pimpinan dan Anggota Senat Akademik, Pimpinan dan Anggota Dewan Guru Besar, Dekan Fakultas Teknik beserta jajarannya, Ketua dan Anggota Senat Fakultas Teknik, Tim Penilai Kenaikan Jabatan Guru Besar Fakultas Teknik, Ketua dan Sekretaris Departemen Teknik Elektro dan Teknologi Informasi yang sudah mengizinkan dan mengusulkan jabatan akademik, serta kepada Pemerintah Republik Indonesia melalui Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi yang menyetujui usulan jabatan akademik Guru Besar saya. Ucapan terima kasih juga saya sampaikan kepada Tim SDM di tingkat Universitas, Fakultas, dan Departemen: Dr. Ratminto, Bu Kenok, Pak Slamet, Pak Juwari, Pak Eka Firmansyah, ST., M.Eng., Ph.D., Mbak Ratna Endah, serta tim pengelola dokumen di departemen yang telah memberikan bantuannya untuk menyiapkan berbagai dokumen yang diperlukan dan dengan sigap menginformasikan kekurangan dokumen yang harus dilengkapi.

Dalam kesempatan ini, saya juga ingin mengucapkan terima kasih kepada semua guru dan mentor saya sejak di SD Kanisius II Klaten, SMP Pangudi Luhur Bruderan Klaten, dan SMA Negeri I Klaten yang telah mendidik, membentuk, dan membekali saya dengan berbagai ilmu dasar dan sikap mental untuk selalu tekun bekerja dan belajar dengan sungguh-sungguh. Kepada Prof. F. Soesianto (alm.), dosen pembimbing skripsi sekaligus pembimbing spiritual saya; Ir. Soetarno (alm.) yang mengusulkan saya menjadi dosen; Prof. Adhi Susanto (alm.); Ir. Soedjatmiko, M.Sc. (alm.); Ir. Surjono, M.Phil. (alm.); Ir. Litasari, M.Sc. (alm.); Prof. Dr. Ir. T. Harjono, M.Sc.; Dr. Ir. Wahyuni Reksoatmodjo, dosen pembimbing akademik saya; Ir. A. Rida Ismu; Ir. Bambang Sutopo, M.Phil.; Ir. I Nengah Sumerti; Drs. HC. Yohanes; teman seangkatan saya Prof. Tumiran dan Ir. Wahyu Dewanto, M.T. yang banyak memberi motivasi dan semangat untuk terus bekerja sebaik-baiknya, saya mengucapkan terima kasih yang sebesar-besarnya. Pada kesempatan ini, saya juga mengucapkan terima kasih kepada seluruh dosen dan karyawan Departemen Teknik

Elektro dan Teknologi Informasi, Fakultas Teknik, Universitas Gadjah Mada. Kepada Prof. Ir. Panut Mulyono, M.Eng., D.Eng.; Prof. Dr. Ir. Bambang Agus Kironoto; Prof. Ir. I Made Bendiyasa, M.Sc., Ph.D.; Prof. Dr. Ir. Indarto, DEA., IPM, ASEAN Eng.; dan Prof. Dr.Eng. Ir. Arief Budiman, M.S., IPU, saya mengucapkan banyak terima kasih atas motivasi dan sarannya untuk terus berjuang mencapai asa. Kepada Prof. Dr. Ir. Sasongko Pramono Hadi, DEA. dan Prof. Ir. Selo, S.T., M.T., M.Sc., Ph.D., IPU, ASEAN Eng., saya mengucapkan banyak terima kasih dan penghargaan setinggi-tingginya atas kesediaannya mereviu naskah pidato ini.

Ucapan terima kasih dan hormat saya haturkan kepada Prof. Dr. Partini, S.U. yang selalu memberikan petuah, nasihat, saran, motivasi, semangat, maupun kritik yang sangat saya butuhkan untuk terus maju meraih cita-cita saya. Terima kasih yang sebesar-besarnya kepada Bapak Gondowijoyo dan Bapak Joko Irawan Mumpuni dari Penerbit Andi yang memberi kesempatan saya untuk menerbitkan sejumlah buku pemrograman komputer, Bapak Yosep Edyanto dari Graha Ilmu, Dr. Ir. Eko Nugroho, M.Sc. (alm), dr. Hawa Mustika, Sofyan Lukmanfiandy, S.Kom., M.Kom., dan Pak Bambang Cahyo yang selalu menguatkan dalam berbagai kesulitan saya. Kepada Prof. Zainal A. Hasibuan, Ph.D. (Universitas Dian Nuswantoro), Prof. Dr.rer.nat Achmad Benny Mutiara, S.Si., S.Kom. (Universitas Gunadarma), Prof. Dr. Ir. Mauridhi Hery Purnomo, M.Eng. (Institut Teknologi Sepuluh November), Prof. Dr. Ir. Yanuarsyah Haroen (Institut Teknologi Bandung), Prof. Ir. Suyoto, M.Sc., Ph.D. (Universitas Atma Jaya Yogyakarta), teman-teman di APTIKOM, IndoCEISS, AISINDO, dan LAM INFOKOM yang tidak bisa saya sebutkan satu per satu, saya mengucapkan banyak terima kasih atas dorongan semangat dan motivasi yang selalu diberikan kepada saya.

Ucapan terima kasih dan sungkem saya haturkan kepada kedua orang tua saya, Bapak Yohanes Suyekno (alm.) dan Ibu Yuliana Isdwiyati (alm.) dan kedua mertua saya, Bapak Harjowiryono (alm.) dan Ibu Harjowiryono (alm.) yang dengan tekun dan penuh kasih sayang mendidik, membimbing, dan selalu mendoakan untuk kesehatan dan kesuksesan saya. Semoga beliau-beliau tersenyum dan bahagia di surga melihat putra dan menantunya berdiri di podium

yang terhormat ini. Kepada semua saudara kandung dan ipar yang tidak bisa saya sebut satu per satu, terima kasih atas dorongan semangat dan doanya yang tulus.

Kepada belahan jiwaku, Dra. Istiyati, yang dengan setia, sabar, penuh pengertian, dan kasih sayang selalu mendampingi, mengingatkan, dan memberikan dorongan semangat, motivasi, dan doa yang tulus dalam setiap langkah yang saya lakukan. Tidak ada kata yang tepat untuk mewakili semua perasaanku, kecuali ucapan terima kasih dan penghargaan setinggi-tingginya padamu. Hasil yang saya peroleh ini juga tidak lepas dari doa tulus putra semata wayang, Okky Wisnu Murti Santosa, S.T. yang setiap saat menanyakan "kapan pengukuhannya". Terima kasih untuk doamu, Nak. Kepada menantuku, Irna Transista, S.T., terima kasih untuk doamu. Kepada cucuku, Aldrich Ranoedirdja Santosa tersayang, kau-lah sumber kebahagiaan, sumber tawa yang senantiasa memberi warna ceria di hari-hari penuh kesibukan Akung. Kupersembahkan keberhasilan ini untuk kalian semua dan semoga Ranoe bisa mengikuti jejak Akung. Semoga kita semua dilindungi dan diberkati oleh Tuhan YME.

Para hadirin yang berbahagia,

Dengan mengucapkan puji syukur kepada Tuhan YME, saya mengakhiri Pidato Pengukuhan Guru Besar saya. Atas nama pribadi dan seluruh anggota keluarga, saya mengucapkan terima kasih yang tak terhingga serta apresiasi yang sebesar-besarnya atas kesabaran dan keikhlasan para hadirin sekalian dalam mendengarkan pidato saya. Seperti pepatah mengatakan, "tiada gading yang tak retak", maka saya mohon maaf yang sebesar-besarnya atas kesalahan-kesalahan yang mungkin saya perbuat selama saya menyampaikan pidato, baik dari perkataan, kalimat yang kurang mengena, maupun tingkah laku saya yang tidak baik. Kepada para hadirin sekalian, saya mohon doa restu serta kritik dan saran agar saya dapat mengemban amanah jabatan akademik ini dengan sebaik-baiknya sehingga saya dapat berkontribusi sesuai dengan ilmu, pengetahuan, dan kompetensi yang saya miliki, serta tugas dan fungsi jabatan akademik yang diamanahkan kepada saya. Semoga Tuhan Yang Maha Pengampun, Maha Pengasih, dan Maha Penyayang senantiasa melimpahkan

berkat-Nya kepada kita semua, dan kita selalu diberi kesehatan yang baik dan senantiasa berbahagia. Amin.

Wassalaamu'alaikum wa Rahmatullaahi wa Barokaatuh
Shalom
Om Swastiastu
Namo Buddhaya
Salam Kebajikan
Salam sejahtera bagi kita semua

DAFTAR PUSTAKA

Arini, S.C. (2023). "BSI Jamin Data dan Dana Nasabah Aman Meski Ada Isi Data Bocor," *Dokumen Web*, https://finance.detik.com/moneter/d-6724196/bsi-jamin-data-dan-dana-nasabah-aman- meski-ada-isu-data-bocor, diakses 18 Mei 2023, pukul 13.00.

Australian Government, Office of the Australian Information Commissioner. (2023). "What is privacy?" *Dokumen Web*, https://www.oaic.gov.au/privacy/your-privacy-rights/what-is-privacy, diakses 28 Januari 2023, pukul 07.45.

Baase, S. (2013). *A Gift of Fire, Social, Legal, and Ethical Issues for Computing Technology*, 4th Edition, Pearson Education, Inc.

Brahma, M., Tripathi, S. S., dan Sahay, A. (2021). "Developing curriculum for industry 4.0: digital workplaces". *Higher Education, Skills and Work-Based Learning, 11*(1):144–163. https://doi.org/10.1108/HESWBL-08-2019-0103.

Chen, J., Brust, M. R., Kiremire, A. R., dan Phoha, V. V. (2013). "Modeling Privacy Settings of an Online Social Network from a Game-Theoretical Perspective". *9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, 20-23 October 2013, Austin, TX, USA, https://ieeexplore-ieee-org.ezproxy.ugm.ac.id/stamp/stamp.jsp?tp=&arnumber=6679987

Chong, M. S., Sandberg, H., dan Teixeira, A. M. H. (2019). "A tutorial introduction to security and privacy for cyber-physical systems," *18th European Control Conference, ECC 2019*, 968–978. https://doi.org/10.23919/ECC.2019.8795652

Daniel, D. (2023). “Industry 4.0,” *Dokumen Web*, https://www.techtarget.com/searcherp/ definition/Industry-40, diakses 28 Januari 2023 pukul 10.00.

Deguchi, A., Hirai, C., Matsuoka, H., Nakano, T., Oshima, K., Tai, M., dan Tani, S. (2020). “What is Society 5.0?” dalam Hitachi-UTokyo-Laboratory (H-UTokyo Lab.) (Ed.), *Society 5.0, A People-centric Super-smart Society*, Hitachi and The University of Tokyo Joint Research Laboratory. https://doi.org/10.1007/978-981-15-2989-4.

Du, W. dan Atallah, M.J. (2001). “Secure Multi-Party Computation Problems and Their Applications: A Review and Open Problems”. *Electrical Engineering and Computer Science*, *11*. https://surface.syr.edu/eecs/11

Forrest, S., Hofmeyr, S. A., dan Somayaji, A. (1997). “Analogies with immunology represent an important step toward the vision of robust, distributed protection for computers”. *Communication of The ACM*, *40*(10):88–96. https://people.scs.carleton.ca/~soma/id-2006w/readings/forrest-immunology.pdf.

Giraldo, J., Sarkar, E., Cardenas, A. A., Maniatakos, M., dan Kantarcioglu, M. (2017). “Security and Privacy in Cyber-Physical Systems: A Survey of Surveys”. *IEEE Design and Test*, *34*(4):7–17. https://doi.org/10.1109/MDAT.2017.2709310.

Hassan, M. U., Rehmani, M. H., dan Chen, J. (2020). “Differential Privacy Techniques for Cyber Physical Systems: A Survey”. *IEEE Communications Surveys and Tutorials*, *22*(1):746–789. https://doi.org/10.1109/COMST.2019.2944748.

Helmi, I. (2023). “Ransomware Lokbit 3.0 Ancam BSI, Beri Tenggat Waktu 72 Jam untuk Negosiasi”, *Dokumen Web*, https://www.kompas.tv/article/406330/ransomware-lockbit-3-0-ancam-bsi-beri-tenggat-waktu-72-jam-untuk-negosiasi, diakses 15 Mei 2023.

Hu, Y. dan Min, H. (Kelly). (2023). “The dark side of artificial intelligence in service: The “watching-eye” effect and privacy

concerns". *International Journal of Hospitality Management*, *110*, April. https://doi.org/10.1016/j.ijhm.2023.103437.

Hussein, S.K. dan El-Dosuky, M. A. (2023). "Anomaly Detection in Cyber-Physical Systems using Explainable Artificial Intelligence and Machine Learning". *Journal of Theoretical and Applied Information Technology*, *101*(8):3138–3151. http://www.jatit.org /volumes/Vol101No8/28Vol101No8.pdf

IBM (2023). "Why is data security important?" *Dokumen Web*, https://www.ibm.com/id-en/topics/data-security, diakses 10 Mei 2023, pukul 19.15.

Igbe, O., Darwish, I., dan Saadawi, T. (2016). "Distributed Network Intrusion Detection Systems: An Artificial Immune System Approach." *Proceedings - 2016 IEEE 1st International Conference on Connected Health: Applications, Systems and Engineering Technologies, CHASE 2016*, pp. 101–106, 27-29 June 2016, Washington DC, USA, https://doi.org/10.1109/CHASE.2016.36.

Jin, S. J., Abdullah, A. H., Mokhtar, M., dan Abdul Kohar, U. H. (2022). "The Potential of Big Data Application in Mathematics Education in Malaysia". *Sustainability (Switzerland)*, *14*(21). https://doi.org/10.3390/su142113725.

Kaur, J. dan Ramkumar, K. R. (2022). "The recent trends in cyber security: A review". *Journal of King Saud University – Computer and Information Sciences*, *34*(8):5766–5781. https://doi.org/10.1016/J.JKSUCI.2021.01.018.

Kim, H., dan Ben-Othman, J. (2020). "Toward Integrated Virtual Emotion System with AI Applicability for Secure CPS-Enabled Smart Cities: AI-Based Research Challenges and Security Issues". *IEEE Network*, *34*(3):30–36. https://doi.org/10.1109/ MNET.011. 1900299.

Kocabas, O. dan Soyata, T. (2015). "Utilizing Homomorphic Encryption to Implement Secure and Private Medical Cloud Computing". *Proceedings - 2015 IEEE 8th International Conference on Cloud Computing, CLOUD 2015*, pp. 540–547, 27 June–2 July 2015, New York, USA, https://doi.org/10.1109/CLOUD.2015.78.

Laucereno, S.F. (2023). “Heboh Lockbit Ngaku Retas BSI, Dirut Jamin Data Nasabah Aman”, https://finance.detik.com/moneter/d-6718799/heboh-lockbit-ngaku-retas-bsi-dirut-jamin-data-nasabah-aman, diakses 15 Mei 2023.

Özdemir, V. (2019). “The big picture on the ‘AI Turn’ for digital health: The internet of things and cyber-physical systems”. *OMICS A Journal of Integrative Biology*, *23*(6):308–311. https://doi.org/10.1089/omi.2019.0069.

Ramasamy, L. K., Khan, F., Shah, M., Prasad, B. V. V. S., Iwendi, C., dan Biamba, C. (2022). “Secure Smart Wearable Computing through Artificial Intelligence-Enabled Internet of Things and Cyber-Physical Systems for Health Monitoring”. *Sensors*, *22*(3). https://doi.org/10.3390/s22031076.

Rani, S., Kataria, A., Chauhan, M., Rattan, P., Kumar, R., dan Kumar Sivaraman, A. (2022). “Security and Privacy Challenges in the Deployment of Cyber-Physical Systems in Smart City Applications: State-of-Art Work”. *Materials Today: Proceedings*, *62*:4671–4676. https://doi.org/ 10.1016/j.matpr.2022.03.123.

Rettig, M. (2017). “Notes on sociotechnical systems design,” *Dokumen Web*, https://medium.com/rettigs-notes/notes-on-sociotechnical-systems-design-178f161bc9e8, diakses 15 Mei 2013, pukul 21.00.

Said, W. dan Mostafa, A. M. (2020). “Towards a Hybrid Immune Algorithm Based on Danger Theory for Database Security”. *IEEE Access*, *8*:145332–145362. https://doi.org/10. 1109/ACCESS.2020.3015399.

Santosa, P.I. dan Rianto. (2022). “Modeling the Classifier of Online Learning Effectiveness Using Machine Learning”. *ICIC Express Letters*, *16*(10):1079–1086. https://doi. org/10.24507/icicel.16.10.1079.

Schatz, M. C. dan Phillippy, A. M. (2012). “The rise of a digital immune system”. *GigaScience*, *1*(4):1–3. https://doi.org/10.1186/2047-217X-1-4

SecurityScorecard (2023), “What is the CIA Triad? Definisition, Importance, & Examples,” *Dokumen Web*.

https://securityscorecard.com/blog/what-is-the-cia-triad/, diakses 10 Mei 2023, pukul 19.30.

Song, I. Y. dan Zhu, Y. (2017). "Big Data and Data Science: Opportunities and Challenges of iSchools". *Journal of Data and Information Science*, *2*(3):1–18. https://doi.org/10.1515/jdis-2017-0011.

Sreedevi, A. G., Nitya Harshitha, T., Sugumaran, V., dan Shankar, P. (2022). "Application of cognitive computing in healthcare, cybersecurity, big data and IoT: A literature review". *Information Processing and Management*, *59*(2). https://doi.org/10.1016/j.ipm.2022.102888.

Statista (2023). "Number of internet and social media users worldwide as of April 2023," *Dokumen Web*, https://www.statista.com/statistics/617136/digital-population-worldwide/, diakses 13 Mei 2023.

Termanini, R. (2016). *The Cognitive Early Warning Predictive System using The Smart Vaccine*, CRC Press Taylor & Francis Group.

Tussyadiah, I., Li, S., dan Miller, G. (2019). "Privacy Protection in Tourism: Where We Are and Where We Should Be Heading For". *Information and Communication Technologies in Tourism 2019*: 278–290, Springer International Publishing. https://doi.org/10.1007/978-3-030-05940-8_22.

Wachter, S. dan Mittelstadt, B. (2019). "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI". *Columbia Business Law*, 2019(2), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829.

Wang, K., Dong, J., Wang, Y., dan Yin, H. (2019). "Securing Data with Blockchain and AI". *IEEE Access*, *7*:77981–77989. https://doi.org/10.1109/ACCESS.2019.2921555.

Wang, L. dan Alexander, C. A. (2019). "Big Data Analytics in Healthcare Systems". *International Journal of Mathematical, Engineering and Management Sciences*, *4*(1):17–26. https://doi.org/10.33889/ijmems.2019.4.1-002

Webster, M. (2023). “Definisi System”, *Dokumen Web*, https://www.merriamwebster.com /dictionary/system, diakses 26 Januari 2023, pukul 21.00.

Whitworth, B. (2009). “The Social Requirements of Technical Systems,” dalam Whitworth dan de Moor, A. (Eds.), *Handbook of Research on Socio-Technical Design and Social Networking Systems*, Volume I, IGI Global.

Whitworth, B., Fjermestad, J., dan Mahinda, E. (2006). “The Web of System Performance”. *Communication of the ACM*, *49*(5):92–99. https://doi.org/10.1145/1125944.1125947.

Xiong, G., Li, Z., Wu, H., Chen, S., Dong, X., Zhu, F., & Lv, Y. (2021). “Building Urban Public Traffic Dynamic Network Based on CPSS: An Integrated Approach of Big Data and AI”. *Applied Sciences (Switzerland)*, *11*(3):1–14. https://doi.org/10.3390/app11031109.

Zhou, G., Yang, X., Azizsoltani, H., Barnes, T., dan Chi, M. (2020). “Improving Student-System Interaction Through Data-driven Explanations of Hierarchical Reinforcement Learning Induced Pedagogical Policies”. *UMAP 2020 - Proceedings of the 28th ACM Conference on User Modeling, Adaptation and Personalization*, July, 284–292. https://doi.org/10.1145/3340631.3394848.

DAFTAR RIWAYAT HIDUP

Nama	: Prof. Ir. Paulus Insap Santosa, M.Sc., Ph.D., IPU
Tempat/Tangal lahir	: Klaten, 8 Januari 1961
NIP	: 196101081985031002
Jabatan Akademik	: Guru Besar, TMT 1 Nov. 2022
Pangkat/Golongan	: Pembina Utama Madya / IVd
Alamat Kantor	: Departemen Teknik Elektro & Teknologi Informasi, Fakultas Teknik UGM, Jalan Grafika, Yogyakarta 55281

Alamat Rumah : Perumahan Nandan Griya Idaman No. 30, Sleman, Yogyakarta 55281
Email : *insap@ugm.ac.id*

DATA KELUARGA

Istri : Dra. Istiyati
Anak : Okky Wisnu Murti Santosa, S.T.
Menantu : Irna Transista, S.T.
Cucu : Aldrich Ranoedirdja Santosa

PENDIDIKAN

1984 S-1 Jurusan Teknik Elektro, Fakultas Teknik, Universitas Gadjah Mada
1991 S-2 Department of Computer Science, University of Colorado at Boulder

2006 S-3 Department of Information Systems, School of Computing, National University of Singapore

PENGALAMAN KERJA DI UGM

2022–2023 Ketua Unit Penjaminan Mutu Program Studi Magister Manajemen Perguruan Tinggi, Sekolah Pascasarjana, UGM.
2017–2021 Sekretaris Program Studi Magister Manajemen Perguruan Tinggi, Sekolah Pascasarjana, UGM.
2017–2018 Kepala Divisi Sistem Informasi dan Pendukung, Kantor Jaminan Mutu, UGM.
2009–2013 Kaprodi Pascasarjana (S-2 dan S-3) Departemen Teknik Elektro & Teknologi Informasi, Fakultas Teknik UGM.
2009–2011 Kepala Laboratorium Informatika dan Komputer, Departemen Teknik Elektro & Teknologi Informasi, Fakultas Teknik UGM.
Sejak 1985 Staf Pengajar di Departemen Teknik Elektro & Teknologi Informasi, Fakultas Teknik UGM.

PENGALAMAN KERJA DI LUAR UGM

2020–2025 Anggota Dewan Eksekutif LAM INFOKOM, Divisi Penjaminan Mutu
2021–2024 Dewan Pembina Badan Kejuruan Informatika Persatuan Insinyur Indonesia
2018–2019 Bendahara ACM Nusantara Chapter
2018 Anggota Tim Pengembang Rencana Induk Jogjakarta Smart Province
2017–2021 Ketua Bidang Pendidikan dan Pelatihan DPP IndoCEISS
2015–2017 Ketua ACM Yogyakarta Chapter
2014–2015 Wakil Ketua ACM SIGCHI Indonesia Chapter
2014–2018 Wakil Ketua Bidang Pengembangan Pembelajaran dan Materi Ajar DPP APTIKOM
2011–2017 Anggota Tim Technical Support GCI-O DEPKOMINFO
Sejak 2018 Ketua Bidang SPMI dan Akreditasi DPP APTIKOM
Sejak 2022 Asesor LAM INFOKOM

Sejak 2021 Asesor Smart City KOMINFO
Sejak 2018 Asesor Sistem Pemerintahan Berbasis Elektronik KEMENPAN-RB
Sejak 2011 Asesor BAN-PT

PENGHARGAAN

Penghargaan "Satya Lencana Karya Satya 30 Tahun", Presiden Joko Widodo, 2017.
Penghargaan "Kesetiaan 25 Tahun Mengabdi" Fakultas Teknik UGM, 2011.

PUBLIKASI JURNAL ENAM TAHUN TERAKHIR (2017–2022)

- **Santosa, P.I**. dan Pramunendar, R. A. (2022) "A Robust Feature Construction for Fish Classification Using Grey Wolf Optimizer", (will be published in) *Cybernetics and Information Technologies*, Vol. 22, No. 4, Desember 2022
- **Santosa, P.I.** dan Rianto (2022) "Modeling the Classifier of Online Learning Effectiveness Using Machine Learning", *ICIC Express Letters*, Vol. 16, No. 10, Oktober, pp. 1079-1086
- **Santosa, P.I.**, Risyah, M. M, Auliasari, M. M., dan Pratama, A. D. (2022) "Modeling Literacy-based Self-Efficacy in Digital Humanities: An Exploratory Study," *Hong Kong Journal of Social Sciences*, Vol. 59, Spring/Summer, Juli, pp. 181-190
- **Santosa, P.I.** (2022), "Student Satisfaction with Online Learning: A Multigroup Analysis," *Register*, Vol. 8. No. 2, Juli 2022, pp. 122-132
- Perdana, I., **Santosa, P.I.**, Setiawan, N.A., dan Wimbarti, S. (2022), "A Proposed User Interface Design as a Stimulus for Personality Types Confirmation", *Advances in Science and Technology*, Vol. 112, pp. 145-152
- Liliana, L., **Santosa, P.I.**, Kusumawardani, S.S. (2022), "Completion Factor in Massive Open Online Course in Developing Countries: A Literature Review in 2015-2021)," *World Journal on Educational Technology*, Vol. 14, No. 2, Maret, pp. 456-472

- Wasilah, Nugroho, L.E., **Santosa, P.I.**, dan Sorour, S.E. (2021), "Study on the Influencing Factors of the Flexibility of University IT Management in Education 4.0," *International Journal of Innovation and Learning*, Vol. 30, No. 2, Agistus, pp. 132-153
- Rianto, Mutiara, A.B., Wibowo, E.P., dan **Santosa, P.I.** (2021), "Improving the accuracy of text classification using stemming method, a case of non-formal Indonesian conversation," *Journal of Big Data*, Vol. 8, No. 1, Januari, pp. 1-16
- Chandra, A.Y., Prasetyaningrum, P.T., Suria, O., **Santosa, P.I.**, dan Nugroho, L.E. (2021), "Virtual Reality Mobile Application Development with Scrum Framework as a New Media in Learning English," *International Journal of Interactive Mobile Technologies*, Vol. 15, No. 8, pp. 31-49
- Rianto, Mutiara, A.B., Wibowo, E.P., dan **Santosa, P.I.** (2021), "Improving Stemming Techniques for Non-formal Indonesian Sentenses Using INCORBIZ," *ICIC Express Letters*, Vol. 15, No. 1, Januari, pp. 67-74
- Hantono, B.S., Nugroho, L.E., dan **Santosa, P.I.** (2020), "Mental Stress Detection via Heart Rate Variability using Machine Learning," *International Journal on Electrical Engineering and Informatics*, Vol. 12, No. 3, September, pp. 431-444
- Sabariah, M.K., **Santosa, P.I.**, dan Ferdiana, R. (2020), "A Proposed User Requirements Document for Children's Learning Application," *International Journal of Advanced Computer Science and Applications (IJACSA)*, Vol. 11, No. 9., September, pp. 317-324
- Ibnugraha, P.D., Nugroho, L.E., dan **Santosa, P.I.** (2020), "Reliability Analysis od Risk Model Metrics Based on Business Approach in Information Security," *Ingénierie des Systèmes d'Information*, Vol. 25, No. 4, Agustus, pp. 475-480
- Soe, Y.N., Feng, Y., **Santosa, P.I.**, Hartanto, R., dan Sakurai, K. (2020), "Machine Learning-Based IoT-Botnet Attach Detection with Sequential Architecture*," Sensor*, Vol 20, 4372, Agustus, pp. 1-15

- Sabariah, M.K., **Santosa, P.I.**, dan Ferdiana, R. (2020), "Identification of Children Learning Styles using Elicitation Application," *Journal of Computer Science*, Vol. 16, No. 6, Juli
- Sabariah, M.K., **Santosa, P.I.**, dan Ferdiana, R. (2020), "Model of Tools Requirements Elicitation Process for Children's Learning Applications," *International Journal of Advanced Computer Science and Applications (IJACSA)*, Vol. 11, No. 3, Maret, pp. 322-228
- Soe, Y.N., Feng, Y., **Santosa, P.I.**, Hartanto, R., dan Sakurai, K. (2020), "Towards a Lightweight Detection System for Cyber Attacks in the IoT Environment Using Corresponding Features*," Sensor*, Vol. 9, 144, Januari, pp. 1-19
- Soe, Y.N., Feng, Y., **Santosa, P.I.**, Hartanto, R., dan Sakurai, K. (2019), "Rule Generation for Signature Based Detection Systems of Cyber Attack in IoT Environments*," Bulletin of Networking, Computing, Systems, and Software*, Vol. 8, No. 2, Juli, pp. 93-97
- Pramunendar, R.A., Wibirama, S., **Santosa, P.I.**, Andono, P.N,, dan Soeleman, M.A. (2019), "A Robust Image Enhancement Techniques for Underwater Fish Classification in Marine Environment," *International Journal of Intelligent Engineering & Systems*, Vol. 12, No. 5, Maret, pp. 116-129
- Hasibuan, M.S., Nugroho, L.E., dan **Santosa, P.I.** (2019), "Model Detecting Learning Styles with Artificial Neural Network," *Journal of Technology and Science Education*, Vol. 9, No. 1, pp. 85-95
- Pramunendar, R.A., Wibirama, S., **Santosa, P.I. (2018)**, "A Novel Approach for Underwater Image Enhancement Based on Improved Dark Channel Prior with Colour Correction," *Journal of Engineering Science and Tehnology*, Vol. 13, No. 10, pp. 3220-3237
- Wasilah, Nugroho, L.E., dan **Santosa, P.I.** (2018), "IT-Based Change Resistance in Higher Education," *International Journal of Engineering & Technology*, Vol. 7 (4.40), pp. 98-103
- Hasibuan, M.S., Nugroho, L.E., dan **Santosa, P.I.** (2018), "Model E-learning MDP for Learning Style Detection using Prior

Knowledge," *International Journal of Engineering & Technology*, Vol. 7 (4.40), pp. 118-122

- Nurmasari, J., Nugroho, L.E., **Santosa, P.I.**, dan Ferdiana, R. (2018), "The Measurement of Consumer Interest and Prediction of product Selection in E-commerce using Eye Tracking Method," *International Journal of Intelligent Engineering & Systems*, Vol. 11, No. 1, Agustus, 30-40
- Sahid, D.S.S., Nugroho, L.E., dan **Santosa, P.I.** (2018), "A Model of Personalized Context Aware E-Leaning Based on Psychological Experience," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, Vol. 10 (1-5), pp .137–143
- Sahid, D.S.S., Nugroho, L.E., dan **Santosa, P.I.** (2017), "Integrated Stochastic and Literate Based Driven Approaches in Learning Style Identification dor Personalized E-Learning Purpose," *International Journal on Advanced Science Engineering Information Technology*, Vol. 7, No. 5., pp 1708-1715

BUKU INTERNASIONAL

- Yeo, G.K., Kankahali, A.M., Oh, L.B., Koh, C.H, Santosa, P.I., ***ICT and Our Society***, Second Edition, Asia Customized Edition, McGraw Hill, 2003.

BOOK CHAPTER

- Santosa, P.I. (2022), "Quality of interaction and Environment support as perceived by first- year students in Indonesia," in Coates, H., Gao, X., Guo, F., and Shi, J. (Eds.) *Global Student Engagement, Policy Insights and International Research Perspectives*, Asian Higher Education Outlook, Routledge, Taylor & Francis Group.
- Santosa, P.I. (2006), "Helping Users, Mentally: A Lesson Learnt from Hypertext Navigation," in Guah, M.W., and Currie, W.L. (Eds.) *Internet Strategy: The Road to Web Services*," Publisher Idea Group Inc.

BUKU NASIONAL

- *Metodologi Penelitian*, Penerbit Universitas Terbuka, 2021
- *Interaksi Manusia dan Komputer*, Penerbit Universitas Terbuka, 2020
- *Metode Penelitian Kuantitatif, Pengembangan Hipotesis dan Pengujiannya Menggunakan SmartPLS*, Penerbit Andi, Juni 2018.
- *Interaksi Manusia dan Komputer, Edisi 2*, Penerbit Andi, 2009
- *Interaksi Manusia dan Komputer, Teori dan Praktek*, Penerbit Andi, 1998
- *Grafika Komputer dan Antarmuka Grafis*, Penerbit Andi, 1997
- *Struktur Data Menggunakan Turbo Pascal 6.0*, Penerbit Andi, 1995
- *Pemrograman Pascal Lanjut*, Penerbit Andi, 1994
- *dBASE II dan Komunikasi dBASE II dengan BASIC*, Penerbit Liberty, 1992
- *Dasar-dasar Pemrograman Pascal, Teori dan Program Terapan*, Penerbit Andi, 1988
- *Teori dan Program Terapan Menggunakan QuickBasic*, Penerbit Andi, 1987
- *Pemrograman Fraktal Resolusi Tinggi untuk Kartu Trident SVGA*, Penerbit Andi. Coauthor Kusumantoro, R.T., 1997.
- *Mendayagunakan Sepasang Komputer*, Penerbit Andi Offset, Yogyakarta. Coauthor Cahyono. N., 1995
- *Pemrograman BASIC*, Penerbit Andi Offset. Coauthor Soesianto, F. dan Nugroho, E., 1985