PERTEMUAN 2
PHYSICAL SECURITY & BIOMETRICS

A. TUJUAN PEMBELAJARAN

Pada Pertemuan ini akan dijelaskan mengenai keamanan fisik dan biometrik. Setelah mempelajari materi ini mahasiswa diharapkan mampu untuk:

1. Menjelaskan konsep perlindungan aset fisik.
2. Memahami hubungan antara cyber dan physical security
3. Mendeskripsikan biometrik beserta jenis cirinya.

B. URAIAN MATERI

1. Menjelaskan konsep keamanan fisik

Kita hidup di dunia fisik. Tentu ini adalah fakta yang jelas, tetapi secara mengejutkan mudah terlewatkan saat membahas keamanan informasi digital. Kecenderungan yang kita alami mempertimbangkan keamanan komputer secara ketat dalam konteks digital, di mana komputer hanya diakses melalui jaringan atau melalui antarmuka digital yang ditentukan dengan baik dan tidak pernah diakses secara langsung atau dengan alat fisik, seperti palu, obeng, atau wadah nitrogen cair. Pada akhirnya, informasi digital harus berada di suatu tempat secara fisik, media magnetik, atau perangkat optic. Mengakses informasi ini memerlukan penggunaan antarmuka antara dunia fisik dan digital. Dengan demikian, perlindungan informasi digital harus mencakup metode untuk melindungi antarmuka ini secara fisik.

Keamanan fisik (*physical security*) secara luas didefinisikan sebagai penggunaan tindakan fisik untuk melindungi barang berharga, informasi, atau akses ke sumber daya yang dibatasi. Serangannya dapat memengaruhi kerahasiaan (*confidentiality*) dan integritas (*integrity*), dan kondisi lingkungan dapat memengaruhi ketersediaan (*availability*).

a. Perencanaan Terhadap Bencana

Melindungi organisasi dari bencana adalah perencanaan terhadap bencana tersebut. Rencana pemulihan terhadap bencana adalah rencana untuk menyediakan peralatan komputer dan informasi kita jika terjadi keadaan

darurat. Perencanaan bencana dapat menunjukkan perbedaan antara masalah dan bencana yang mungkin mengancam bisnis.

Rencana pemulihan bencana organisasi kita akan melibatkan aktivitas seperti mencadangkan data untuk penyimpanan di fasilitas aman jarak jauh dan mengatur penggunaan fasilitas atau peralatan komputer lain jika terjadi keadaan darurat. Pengaturan semacam itu mungkin informal (misalnya, kita mungkin membuat perjanjian timbal balik dengan departemen atau organisasi lain untuk menggunakan peralatan satu sama lain jika terjadi bencana), atau mungkin formal (misalnya, kita mungkin menyiapkan situs atau kontrak darurat terpisah. dengan organisasi yang menangani kesiapsiagaan bencana).

Tempat darurat biasanya ditandai sebagai dingin, hangat, atau panas. Tempat dingin adalah fasilitas darurat yang berisi AC dan kabel, tetapi tidak ada komputer. kita dapat mempercepat beberapa server dan desktop, memindahkan peralatan pengganti lainnya ke tempat ini, dan melanjutkan pemrosesan. Tempat panas adalah fasilitas darurat yang berisi komputer, data cadangan berfungsi. Tempat hangat, hibrida, adalah situs di mana komputer dan peralatan telah diinstal sebelumnya, tetapi bukan program atau data cadangan. Dengan meningkatnya kesadaran akan kelemahan jaringan listrik yang saling berhubungan, semakin banyak perusahaan yang memasukkan persyaratan tambahan ke dalam jarak geografis tempat cadangan mereka.

Selain melindungi peralatan dan informasi organisasi kita, rencana pemulihan bencana dapat sangat meningkatkan kepercayaan publik serta kepercayaan karyawan dan manajer terhadap kemampuan kita untuk melindungi data dan terus memberikan layanan. Ingatlah bahwa backup adalah kunci perencanaan bencana. Jika terjadi bencana dan kita telah mencadangkan sistem, dan akan dapat memulihkannya pada akhirnya.

b. Tindakan Perlindungan terhadap Bencana Alam

Pembahasan risiko keamanan informasi difokuskan pada bencana buatan manusia seperti sabotase, peretasan, dan kesalahan manusia. Tetapi jangan lupa bahwa komputer dan jaringan dipengaruhi oleh jenis bahaya yang sama yang membahayakan semua peralatan organisasi kita, seperti api/ kebakaran, banjir, petir, getaran/ gempa, dan bencana alam lainnya.

Faktanya, banyak ancaman alam sebenarnya lebih merupakan masalah bagi komputer daripada jenis peralatan lainnya karena komputer dan peralatan terkait sangat sensitif terhadap perubahan suhu, kelembapan, kehilangan daya, dan lonjakan arus listrik. Poin pentingnya sementara komputer mudah diganti, namun informasi yang dikandungnya mungkin tidak. Saran yang diberikan berikut ini sangat singkat dan mendasar.

c. Api dan Asap
   1) Pasang detektor asap di dekat peralatan kita dan periksa secara berkala.
   2) Simpan alat pemadam kebakaran di dalam dan di dekat ruang server, ruang telekomunikasi, dan area kerja kita, dan pastikan semua orang tahu bahwa mereka ada di sana.
   3) Pastikan alat pemadam kebakaran diperiksa secara teratur dan memiliki jenis dan peringkat yang benar (kode ABCD).
   4) Menegakkan hukum dan kebijakan dilarang merokok, ini juga penting untuk mengendalikan asap, bahaya lain bagi komputer.
   5) Pastikan bahwa sistem gas khusus untuk pengendalian kebakaran, seperti Halon dan karbon dioksida, dapat digunakan, tidak dapat dilepaskan secara tidak sengaja atau sembarangan, dan sesuai dengan undang-undang lingkungan.
   6) Bergantung pada kode lokal, mungkin ide yang baik untuk memiliki antarmuka sistem AC dengan sistem alarm kebakaran, sehingga AC dapat dimatikan jika kebakaran di bagian lain dari bangunan mengancam untuk menyemprotkan asap ke ruang server melalui saluran AC.

d. Iklim
   1) Simpan semua ruangan yang berisi komputer pada suhu yang wajar (sekitar 50-80 derajat Farenheit atau 10-26 derajat Celcius).
   2) Jaga agar ruang telekomunikasi dan ruang server tetap sejuk; jika diperlukan pakailah sweter saat mengerjakannya.
   3) Jaga tingkat kelembaban pada 20-80 persen.
   4) Pasang alat pengukur dan alarm yang memperingatkan kita jika suhu atau kelembapan di luar kisaran.
   5) Lengkapi sistem pemanas dan pendingin dengan filter udara untuk melindungi dari debu (bahaya lain bagi komputer dan terutama kaset dan paket disk lama, dan media optik tertentu).

e. Gempa Bumi dan Getaran

1) Jauhkan komputer dan peralatan telekomunikasi dari jendela kaca dan permukaan tinggi, terutama jika kita berada di area tinggi yang berisiko.
2) Pemasangan rack-mount jika memungkinkan, dengan mengingat untuk mengamankan pelat lantai. Gunakan standar ANSI / TIA / EIA-569-A pada jalur dan ruang telekomunikasi, dengan variasi seismik lokal sebagai panduan kita.
3) Pastikan bahwa jika terjadi getaran kuat (karena gempa bumi, konstruksi, atau sumber lain), benda tidak akan mudah jatuh ke komputer dan peralatan jaringan Anda.

f. Air
1) Ada berbagai macam jenis kerusakan dari air. Banjir dapat disebabkan oleh hujan atau penumpukan es di luar, toilet atau wastafel yang meluap di dalam, atau air dari alat penyiram yang digunakan untuk memadamkan api. AC dan unit pendingin lainnya dapat menghasilkan air karena kondensasi. Ini biasanya disimpan di baki, tetapi ini bisa berkarat atau meluap. Pastikan kita terlindungi dari semua jenis kelembapan.
2) Jika komputer kita basah, biarkan komputer benar-benar kering sebelum mencoba menyalakannya kembali.
3) Pasang sensor air jika diperlukan.
4) Ingatlah bahwa keberadaan air meningkatkan kemungkinan sengatan listrik. Lebih berhati-hati dalam kasus darurat banjir di area peralatan.

g. Listrik
1) Komputer kita akan menderita jika listriknya terlalu banyak atau terlalu sedikit.
2) Untuk hasil terbaik, pasang pemasok daya yang tidak pernah terputus. Ini akan menyerap lonjakan dan memberikan tegangan ekstra selama pemutusan arus listrik, dan jika daya mati sepenuhnya, itu akan memberi daya sampai kita dapat mematikan sistem. Kehilangan daya yang tidak terlindungi dapat menyebabkan kerusakan serius. Perhatikan bahwa pelindung lonjakan tidak akan berfungsi kecuali sistem kelistrikan kita digrounding dengan baik.
3) Pasang line filter pada pemasok daya komputer kita. Lonjakan tegangan yang disebabkan oleh petir atau gangguan daya dapat merusak komputer kita.

4) Pastikan pelindung sistem grounding memadai. Ini mungkin memerlukan ahli listrik atau spesialis grounding. Standar lokal yang berlaku harus menjadi panduan kita, bersama dengan kode kelistrikan setempat.
5) Jika perlu, pasang sirkuit listrik khusus dengan pemutus sirkuit berlabel jelas untuk setiap sistem kita.
6) Pasang karpet antistatis di fasilitas kita. Karpet ini mengandung filamen khusus yang menghilangkan listrik statis.
7) Minta spesialis telekomunikasi dan teknisi listrik untuk memverifikasi keefektifan peralatan atau sistem pentanahan sinyal Anda. Dalam kebanyakan kasus, pentanahan sinyal harus diikat secara elektrik ke sistem pentanahan listrik atau pelindung.

h. Petir
1) Jika badai petir melanda, coba matikan komputer kita dan cabut kabelnya. Petir menghasilkan lonjakan daya yang sangat besar yang dapat merusak komputer bahkan jika kita memiliki pelindung lonjakan arus pada komputer.
2) Jika kita menggunakan media magnetis sebagai pendukung, lindungi dari medan magnet yang tercipta jika petir menyambar bangunan kita. Simpan media sejauh mungkin dari penyangga baja bangunan. Bahkan rak logam bisa menimbulkan bahaya.

2. Memahami hubungan antara cyber dan physical security

Penting untuk diingat bahwa ada hubungan yang pasti antara keamanan dunia maya dan keamanan fisik komputer dan peralatan komunikasi, yang paling jelas adalah bahwa jika seseorang yang tidak berwenang mendapatkan akses ke ruang kantor dengan komputer yang masuk ke jaringan, individu tersebut akan memiliki akses yang sama atau lebih besar ke sistem daripada yang dapat dicapai oleh banyak peretas. Akses tersebut memungkinkan individu untuk berpotensi membuat akun pengguna yang tidak sah, menempatkan Trojan atau spyware pada sistem, mengakses data yang dilindungi, atau mencuri data kepemilikan. Intinya di sini adalah bahwa tidak peduli seberapa bagus keamanan dunia maya, jika seseorang dapat masuk ke fasilitas dan mendapatkan akses ke sistem, individu tersebut sebenarnya telah menghindari pertahanan keamanan dunia maya.

Selain itu, laptop yang hilang atau dicuri sering kali dilengkapi dengan perangkat lunak yang dikonfigurasi untuk mengakses sistem host. Dengan demikian keamanan fisik perangkat komputasi bergerak merupakan kelemahan yang perlu dibenahi.

Hubungan lain antara keamanan fisik dan cyber terjadi ketika pelanggan, pemasok, atau penyedia layanan memiliki akses jarak jauh ke sistem komputer organisasi terkait. Jika keamanan fisik di fasilitas tempat komputer tersebut berada tidak memadai, keamanan dunia maya dari komputer induk dapat dikompromikan dengan cara yang mirip dengan yang dijelaskan saat pelanggar masuk ke kantor dan mengakses sistem komputer. Oleh karena itu, disarankan untuk merancang mekanisme keamanan cyber yang tidak mengasumsikan bahwa komputer jarak jauh telah diamankan secara fisik.

a. Prosedur Keamanan Data Center

Menetapkan prosedur untuk keamanan pusat data fisik adalah salah satu prioritas utama saat mengembangkan rencana keamanan fisik TI. Kompleksitas bagian ini akan bergantung pada beberapa karakteristik pusat data yang berbeda, termasuk apakah pusat data tersebut menempati seluruh bangunan atau hanya sebagian dari suatu bangunan. Jenis prosedur yang dibutuhkan terkait pengamanan data center ditunjukkan pada tabel berikut:

Tabel 1. Jenis Prosedur Pengamanan Data Center

Jika data center menempati seluruh gedung, maka perencanaan perlu memperhatikan keamanan untuk ruang eksterior gedung, area lobi, area utilitas, dermaga pemuatan, kantor, dan setiap subarea ruangan yang memiliki peralatan IT.
Jika pusat data hanya menempati sebagian bangunan, maka rencana tersebut perlu menangani keamanan untuk kantor staf TI dan setiap subarea ruangan yang memiliki peralatan TI.
Kontrol akses dan manajemen akses adalah elemen kunci dari rencana keamanan pusat data dan harus menunjukkan siapa yang memiliki akses, bagaimana akses diberikan, bagaimana pengunjung dan vendor dikelola, dan bagaimana menangani pelanggaran kebijakan akses.

Bagaimana dan kapan seharusnya seorang pimpinan atau manajer keamanan secara teratur meninjau laporan akses?
Apa prosedur untuk mengamankan peralatan tertentu, sistem kabel, peralatan enkripsi, ruang media, dan lemari penyimpanan atau area yang berisi jenis informasi paling sensitif?
Buat daftar metode keamanan untuk sistem utilitas, termasuk AC, pasokan daya, koneksi jaringan, dan sistem daya darurat.
Buat daftar prosedur keamanan untuk operasi jam kerja, operasi setelah jam kerja, dan operasi darurat.
Bagaimana log terbaru dari semua peralatan dikelola, yang mencakup nomor seri dan informasi konfigurasi?
Bagaimana daftar terbaru personel yang diberi wewenang untuk mengakses area sensitif dikelola?
Bagaimana pengaturan lingkungan di ruang peralatan dipertahankan?
Bagaimana cara masuk dan keluar peralatan, dokumen, dan persediaan?
Bagaimana dan di mana paket yang masuk diperiksa dan dibuka sebelum isinya dibawa ke pusat data?
Bagaimana dan di mana sistem pemadam kebakaran dipasang?
Jenis wadah pelindung apa yang harus digunakan untuk bahan sensitif, termasuk standar tahan api atau tahan pencuri?
Bagaimana cara membuang bahan cetakan dan media magnet bekas dan siapa yang bertanggung jawab atas pembuangannya?
Jika monitor sirkuit tertutup digunakan, prosedur diperlukan untuk penggunaan dan pemeliharaannya.

Seperti semua area di mana prosedur dikembangkan, prosedur keamanan TI fisik untuk pusat data (data center) harus mendukung rencana

terkait termasuk keamanan cyber, pemulihan bencana, atau kelangsungan bisnis, atau membantu mematuhi hukum dan peraturan terkait. Selain langkah-langkah yang diuraikan di bagian sebelumnya untuk mengembangkan prosedur, ada beberapa hal yang perlu diingat saat mengembangkan prosedur khusus untuk pusat data.

1) Prosedur keamanan pusat data mungkin jauh lebih kompleks daripada prosedur untuk area lain seperti pemasangan kabel dan pemasangan kabel yang terletak di luar pusat data.
2) Prosedur keamanan pusat data biasanya berisi terminologi teknis yang perlu diperiksa keakuratannya.
3) Mungkin lebih bijaksana untuk memasukkan prosedur keamanan fisik untuk pusat data sebagai sub-bagian dari manual prosedur pusat data daripada membuat dokumen terpisah yang berdiri sendiri.
4) Karena prosedur keamanan pusat data sedang dikembangkan, disarankan agar berbagai orang di dalam pusat data meninjau prosedur tersebut. Memilih staf yang akan terpengaruh oleh suatu prosedur karena bidang kerja atau jenis keahlian khusus mereka.
5) Kita tidak boleh berasumsi bahwa karena pusat data memiliki kontrol akses, tingkat keamanan tambahan tidak diperlukan untuk dokumen sensitif atau jenis peralatan penting di dalam pusat data.

b. Locks & Keys

Garis pertahanan pertama melawan penyusup adalah dengan menjauhkan mereka dari gedung, keluar dari ruang server, dari lemari telekomunikasi kita. Dulu ini lebih mudah. Ruang komputer yang dikunci atau dijaga secara historis menjadi sarana utama untuk melindungi peralatan komputer dan informasi organisasi dari gangguan fisik dan akses yang tidak dibatasi. Sebagian besar organisasi saat ini, setiap orang memiliki *workstation*, di mana informasi dapat dihapus dengan mudah pada memory stick USB atau floppy disk, misalnya. Printer, dari mana dokumen dapat dikumpulkan, didistribusikan di sekitar kantor.

Untuk mendapatkan akses ke fasilitas terkunci, pengguna harus lulus tes otentikasi. Ada tiga cara klasik untuk mengidentifikasi diri kita:

1) Yang kita ketahui misalnya, kata sandi.
2) Apa yang kita miliki misalnya, kunci, token, lencana, atau kartu pintar.

3) Apa yang menjadi identitas/ciri kita misalnya, sidik jari di jari (yang cocok dengan yang ada di file).

Semua teknik otentikasi ini dapat digunakan untuk keamanan fisik (misalnya, akses gedung atau ruang komputer) serta untuk kontrol akses sistem. Ketika kartu pintar atau sidik jari digunakan untuk akses komputer, biasanya itu hanya langkah pertama. Kata sandi biasanya diperlukan juga. Ketika dua teknik berbeda digunakan untuk otentikasi dengan cara ini, itu disebut otentikasi dua faktor. Satu faktor adalah sesuatu yang kita miliki; misalnya, menunjukkan kartu pintar kita atau sidik jari atau cetak suara dipindai. Faktor lainnya adalah sesuatu yang kita ketahui; misalnya, mengetik nomor identifikasi pribadi (PIN) atau kata sandi ke dalam sistem. Sistem identifikasi multifaktor mempromosikan lingkungan "pertahanan mendalam".

c. Jenis Pengaman / Kunci

Selain mengunci gedung dan ruang komputer, kita juga dapat mengamankan komputer, jaringan, drive disk, dan disk. Berikut dua contoh jenis kunci yang dapat digunakan:

1) Kunci peralatan (*equipment locks*)
Cara termudah untuk mencegah seseorang keluar dengan PC, router, sakelar, atau perangkat jaringan lainnya adalah dengan menguncinya. Komputer, *workstation*, dan kabel mungkin juga dilengkapi dengan kunci yang hanya dapat dibuka dengan kunci khusus, token elektronik, atau kartu pintar.
2) Kunci kriptografi (*cryptographic locks*)
Beberapa produk ultra-aman dilengkapi dengan perangkat elektronik yang dikenal sebagai kunci pintar. Kunci ini digunakan untuk memuat informasi kunci kriptografi awal (biasanya dipasok oleh lembaga pemerintah) ke dalam produk. Mereka biasanya memiliki sirkuit deteksi gangguan, yang menghapus penyimpanan kunci aman jika sirkuit rusak.

3. Mendeskripsikan biometrik beserta jenis cirinya

Kemampuan untuk mengidentifikasi individu secara unik dan untuk mengasosiasikan atribut pribadi (misalnya, nama, kebangsaan, dll.) dengan individu sangat penting untuk struktur masyarakat manusia. Karakeristik tubuh seperti wajah, suara, gaya berjalan juga bersamaan dengan informasi

kontekstual lainnya (misalnya lokasi dan pakaian) ialah suatu yang biasanya manusia gunakan untuk saling mengenali. Himpunan atribut yang terkait dengan seseorang merupakan identitas pribadinya. Pada masa awal peradaban, orang hidup dalam komunitas kecil di mana individu dapat dengan mudah mengenali satu sama lain. Namun, ledakan pertumbuhan penduduk yang disertai peningkatan pergerakan dalam masyarakat modern mengharuskan pengembangan sistem manajemen identitas yang canggih yang mampu merekam, memelihara, dan menghapus identitas individu secara efisien.

Cara ketiga dalam menetapkan identitas orang berdasarkan sifat fisik atau perilaku yang melekat dan dikenal sebagai pengenalan biometric (*biometric recognition*). Secara formal, pengenalan biometrik dapat didefinisikan sebagai ilmu untuk menetapkan identitas individu berdasarkan karakteristik fisik dan / atau perilaku orang tersebut baik secara otomatis atau semi-otomatis.

Pengenalan orang berbasis pengetahuan dan token bergantung pada representasi identitas pengganti seperti kata sandi atau kartu ID, yang dapat dengan mudah dilupakan / hilang, ditebak / dicuri, atau dibagikan. Selain itu, mereka tidak dapat menyediakan fungsi manajemen identitas penting seperti tanpa penyangkalan dan mendeteksi banyak pendaftaran oleh orang yang sama dengan identitas yang berbeda. Misalnya, individu dapat dengan mudah menolak (menolak) menggunakan layanan dengan mengklaim bahwa kata sandi mereka telah dicuri atau ditebak. Individu juga dapat menyembunyikan identitas aslinya dengan menunjukkan dokumen identitas palsu atau duplikat. Selain itu, mekanisme tradisional seperti sandi dan token tidak memberikan bukti kuat untuk pengenalan orang pasca-acara, seperti identifikasi tersangka di TKP. Oleh karena itu, menjadi semakin jelas bahwa mekanisme berbasis pengetahuan dan berbasis token saja tidak cukup untuk manajemen identitas yang andal.

Pengenalan biometrik, atau *simply biometrics*, menawarkan solusi alami dan lebih andal untuk masalah pengenalan orang. Karena pengenal biometrik melekat pada individu, lebih sulit untuk memanipulasi, membagikan, atau melupakan ciri-ciri ini. Karenanya, ciri-ciri biometrik merupakan hubungan yang kuat dan cukup permanen antara seseorang dan identitasnya.

a. Fingerprint

Gambar 2. *Finger Print*

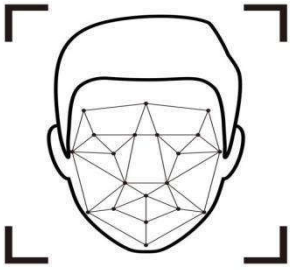
Tidak seperti kulit di sebagian besar bagian tubuh kita, yang halus dan mengandung rambut dan kelenjar minyak, kulit di telapak tangan dan telapak kaki menunjukkan pola pegunungan dan lembah yang mengalir (kadang-kadang disebut sebagai alur), dan tidak memiliki rambut atau kelenjar minyak. Tonjolan papiler pada jari ini, yang disebut punggung gesekan, membantu tangan untuk menggenggam objek dengan meningkatkan gesekan dan meningkatkan penginderaan sentuhan pada tekstur permukaan. Kulit punggungan gesekan terdiri dari dua lapisan utama: dermis (lapisan dalam) dan epidermis (lapisan luar). Tonjolan muncul di epidermis untuk meningkatkan gesekan antara volar (telapak tangan atau telapak kaki) dan permukaan kontak. Laki-laki muda rata-rata memiliki rata-rata 20,7 tonjolan per sentimeter sedangkan betina memiliki 23,4 punggung per sentimeter.

Nilai penting lainnya dari gesekan adalah penggunaannya dalam pengenalan biometrik. Pola lekukan gesekan pada setiap jari diklaim unik dan tidak berubah, memungkinkan penggunaannya sebagai tanda identitas. Bahkan, saudara kembar identik pun bisa dibedakan berdasarkan sidik jarinya. Cedera superfisial seperti luka dan memar pada permukaan jari mengubah pola di daerah yang rusak hanya untuk sementara. Memang, struktur punggung bukit telah diamati muncul kembali setelah cedera sembuh. Namun, jika cedera meluas ke lapisan basal epidermis, itu dapat melenyapkan kemampuan lapisan basal untuk meregenerasi sel di daerah yang rusak. Sel-sel basal di sekitarnya akan berusaha untuk memperbaiki cedera tersebut,

namun proses ini akan menghasilkan bekas luka permanen pada permukaan kulit gesekan.

Faktanya, sistem biometrik berbasis sidik jari sangat populer dan sukses sehingga menjadi identik dengan gagasan pengenalan biometrik di benak masyarakat umum.

b. Face Recognition



Gambar 3. *Face Recognition*

Wajah merupakan bagian depan kepala manusia, memanjang dari dahi ke dagu dan meliputi mulut, hidung, pipi, dan mata. Menjadi bagian terpenting dalam interaksi seseorang dengan dunia luar, wajah menampung sebagian besar organ sensorik fundamental yang dibutuhkan untuk memahami dunia sekitar. Wajah dianggap sebagai ciri biometrik yang paling umum digunakan oleh manusia; kami mengenali satu sama lain dan, dalam banyak kasus, menetapkan identitas kami berdasarkan wajah. Oleh karena itu, telah menjadi praktik standar untuk memasukkan foto wajah dalam berbagai token otentikasi seperti KTP, paspor, dan SIM.

Pengenalan wajah dapat diartikan sebagai proses pembentukan identitas seseorang berdasarkan ciri-ciri wajahnya. Dalam bentuknya yang paling sederhana, masalah pengenalan wajah melibatkan perbandingan dua gambar wajah dan menentukan apakah mereka adalah orang yang sama. Sementara manusia tampaknya mahir dalam menentukan kemiripan antara dua gambar wajah yang diperoleh dalam berbagai kondisi, proses pengenalan wajah otomatis menghadapi beberapa tantangan. Gambar wajah seseorang mungkin memiliki variasi dalam usia, pose, iluminasi, dan ekspresi wajah serta menunjukkan perubahan penampilan karena make-up, rambut wajah, atau aksesori (misalnya kacamata hitam). Selain itu, mungkin ada kesamaan

antara gambar wajah orang yang berbeda, terutama jika mereka terkait secara genetik (misalnya, kembar identik, ayah dan anak, dll.). Kemiripan antar kelas seperti itu semakin memperparah kesulitan untuk mengenali orang berdasarkan wajah mereka. Terlepas dari tantangan ini, kemajuan signifikan telah dicapai di bidang pengenalan wajah otomatis selama dua dekade terakhir. Teknik pengenalan wajah otomatis telah dikembangkan untuk tujuan pengenalan orang dari gambar diam 2 dimensi (2D), video (urutan gambar 2D), dan gambar rentang 3D (kedalaman).

Meskipun ada peningkatan yang stabil dalam kinerja pengenalan wajah selama dua dekade terakhir, beberapa tantangan tetap ada karena variasi intra-kelas yang besar dan variasi antar-kelas yang kecil yang disebabkan oleh variasi pose dan pencahayaan, ekspresi, oklusi, penuaan, dan non-representasi yang kuat dari data citra wajah. Sementara sistem pengenalan wajah 3D telah dikembangkan untuk mengatasi masalah pose dan iluminasi, sejumlah faktor (misalnya, biaya tinggi dan keberadaan database wajah lama yang besar dalam domain 2D) telah menghambat penerapan praktis sistem pengenalan wajah 3D. Teknik penginderaan canggih untuk menangkap gambar beresolusi lebih tinggi dalam berbagai spektrum, teknik deteksi wajah yang dapat menangani perubahan pose, dan representasi yang kuat serta skema pencocokan sangat penting untuk lebih meningkatkan akurasi sistem pengenalan wajah.

c. Iris Recognition

Gambar 4. *Iris Recognition*

Penggunaan daerah okuler sebagai ciri biometrik telah mendapatkan dorongan, terutama karena kemajuan signifikan yang dibuat dalam

pengenalan iris sejak 1993. Daerah mata pada wajah manusia terdiri dari mata dan struktur sekitarnya seperti kulit wajah, alis, dan hidung jembatan. Sementara berbagai komponen mata telah diusulkan sebagai indikator biometrik (yaitu, iris, retina, dan pembuluh darah konjungtiva), irislah yang telah dipelajari secara ekstensif dalam literatur biometrik dan digunakan dalam sistem biometrik skala besar.

Iris adalah organ dalam mata yang terletak tepat di belakang kornea dan di depan lensa. Kegunaan prinsipil iris mata adalah untuk mengatur kuantitas cahaya yang masuk pada mata dengan melebarkan atau mengontrak lubang kecil di dalamnya yang disebut pupil. Iris berkontraksi pada pupil saat iluminasi ambien tinggi dan melebar saat iluminasi rendah.

Menurut literatur biometrik, tekstur struktural pada iris sangat beragam di seluruh populasi. Seperti yang dinyatakan sebelumnya, bahkan perjalanan kembar monozigot menunjukkan perbedaan struktural. Pengujian skala besar telah mengkonfirmasi potensi pola iris untuk mengidentifikasi individu dalam basis data subjek yang besar. Eksperimen yang dilakukan oleh Daugman pada database 632.500 gambar iris (316.250 orang dari 152 kebangsaan) menunjukkan kemungkinan kebijakan keputusan yang dapat menghasilkan tingkat kesalahan nol. Namun, kecepatan ini didasarkan pada kualitas gambar iris, yang harus dipantau secara ketat untuk memastikan kejernihan tekstur yang wajar. Pengujian yang dilakukan pada tahun 2006 oleh National Institute of Standards and Technology yang melibatkan berbagai kualitas gambar menunjukkan bahwa tingkat ketidakcocokan palsu dari algoritme pengenalan iris yang berkinerja terbaik dapat bervariasi antara 1,1 hingga 1,4 persen dengan tingkat kecocokan palsu 0,1 persen. Kemajuan luar biasa dalam sistem pengenalan iris mata telah menghasilkan beberapa tantangan dan peluang baru, yang menjadi fokus dari upaya penelitian terbaru.

d. Biometrics Lainnya

Berbagai macam sifat biometrik telah diusulkan dan dipelajari dalam literatur. Dalam beberapa kasus, keingintahuan akademis tentang keunikan dan keabadian sifat biologis tertentu telah mendorong penelitian eksplorasi (misalnya iris). Dalam kasus lain, domain aplikasi baru telah menghasilkan eksplorasi ciri-ciri biometrik baru (misalnya, biometrik periokular). Selain itu, ciri-ciri biometrik tertentu secara unik cocok untuk beberapa aplikasi dan

skenario. Misalnya, suara mungkin lebih praktis dalam aplikasi telekomunikasi. Telinga mungkin berguna dalam aplikasi pengawasan di mana hanya profil samping wajah manusia yang tersedia; pola gaya berjalan mungkin relevan dalam skenario identifikasi-pada-jarak-jauh. Geometri tangan mungkin sesuai untuk digunakan dalam sistem yang memerlukan verifikasi (sebagai lawan dari identifikasi) dari beberapa identitas terdaftar sehingga mengurangi beberapa masalah yang terkait dengan penggunaan isyarat biometrik yang kuat seperti sidik jari. Lalu iris atau sidik jari dapat dipilih dalam aplikasi di mana subjeknya kooperatif dan dekat dengan sensor.

Gambar 5. Biometrik lainnya

Terlepas dari ciri-ciri tersebut di atas, informasi tambahan seperti jenis kelamin, etnis, usia, tinggi badan, dan warna mata juga dapat digunakan untuk meningkatkan akurasi pencocokan sistem biometrik.

C. SOAL LATIHAN/ TUGAS

1. Jelaskan definsi keamanan fisik yang Anda ketahui!
2. Bagaimana tindakan perlindungan aset fisik terhadap bencana alam?
3. Jelaskan metode-metode identifikasi/otentikasi diri!
4. Sebutkan dan jelaskan *biometrics recognition* serta cirinya!
5. Ketika Anda menjadi staff sebuah data center. Menurut Anda, bagaimana cara Anda meyakinkan manajer perusahaan agar perusahaan tersebut menerapkan perlindungan yang standart !

D. REFERENSI

Bishop, M. (2019). *Computer Security Art and Science*. 2nd Edition. Boston: Pearson Education Inc.

Goodrich, M., & Tamassia, R. (2014). Introduction to Computer Security. Harlow: Pearson Education Ltd.

Pfleeger, P. C., Pfleeger, S. L., & Margulies, J. (2015). Security in Computing. 5th Edition. Westford: Pearson Education Inc.

Salomon, D. (2006). Foundations of Computer Security. Springer Science+Business Media

Jain, A. K., Ross, A. A., & Nandakumar, K. (2011). Introduction to Biometrics Foreword by James Wayman. Springer Science+Business Media

Land, M., Ricks, T., & Ricks, B. (2014). Security Management A Critical Thinking Approach. London: CRC Press Taylor & Francis Group.

Peltier, T. R. (2014). Information Security Fundamentals Second Edition. London: CRC Press Taylor & Francis Group.

Lincke, S. (2015). Security Planning An Applied Approach. London: Springer International Publishing Switzerland.

Erbschloe, M. (2005). Physical Security for IT. Amsterdam: Elsevier Inc.

Lehtinen, R. (2006). *Computer Security Basics 2nd Edition*. O'Reilly Media.

Paulsen, C., & Byers, R. D. *Glossary of Key Information Security Terms* [Internet]. Juli 2019. NIST Pubs. Tersedia pada: https://www.nist.gov/publications/glossary-key-information-security-terms-2, https://csrc.nist.gov/glossary