E-ISSN : 2716-375X
P-ISSN : 2716-3768
JURNAL MANAJEMEN PENDIDIKAN DAN ILMU SOSIAL (JMPIS)
https://dinastirev.org/JMPIS dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jmpis.v5i4
Received: 29 Mei 2024, **Revised:** 8 Juni 2024, **Publish:** 10 Juni 2024

Penggunaan Alat Biometrik Sidik Jari sebagai Kontrol Akses dalam Analisis CPTED terhadap Risiko *Trespassing* di Instalasi Gudang Material Korporasi "X"

Muhammad Naufal Afif[1], Mohammad Kemal Dermawan[2]
[1] Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Indonesia, Depok, Indonesia, muhammad.naufal27@ui.ac.id
[2] Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Indonesia, Depok, Indonesia, moh.kemal@ui.edu

Corresponding Author: muhammad.naufal27@ui.ac.id

Abstract: *The study aims to analyze the use of a unimodal biometric scanner with fingerprint geometry capital against the risk of break-in or trespassing as an effective access control. The research was conducted for five months, from January 1 to May 15, 2024. The researchers will assess the effectiveness of this biometric system scheme in access control against break-in (both accidental and intentional), with the CPTED theory as the basis for understanding the phenomenon. The qualitative approach is used with direct observation of the installation 'A' at the company 'X' in Jakarta, during the period 1 January - 20 May 2024. The results of the research showed that on the unimodal biometric access control system with fingerprints in the 'A' installation there were 24 cases of break-in and trespassing. Of the total, 17 cases were false positive, while 7 cases were intentional with 3 cases with no bad intensity and 4 cases with poor intensity. The error lies not in the scanner itself, but in security system modifications, inappropriate usage, and improper placement.*

Keyword: *Access Control, Biometric, CPTED, Trespassing.*

Abstrak: Penelitian ini bertujuan menganalisis penggunaan alat pemindai biometrik unimodal dengan modal geometri sidik jari terhadap risiko *break-in* atau *trespassing* sebagai kontrol akses yang efektif. Penelitian dilakukan selama lima bulan, dari 1 Januari hingga 15 Mei 2024. Peneliti akan menilai efektivitas skema sistem biometrik ini dalam kontrol akses terhadap *break-in* (baik *accidental* maupun *intentional*), dengan teori CPTED sebagai dasar pemahaman fenomena. Pendekatan kualitatif digunakan dengan observasi langsung pada instalasi 'A' di perusahaan 'X' di Jakarta, selama periode 1 Januari - 20 Mei 2024. Hasil penelitian menunjukkan bahwa pada sistem kontrol akses biometrik unimodal dengan sidik jari di instalasi 'A' terdapat 24 kasus *break-in* dan *trespassing*. Dari jumlah tersebut, 17 kasus adalah *false positive*, sementara 7 kasus adalah *intentional* dengan 3 kasus tanpa intensi buruk dan 4 kasus dengan intensi buruk. Kesalahan tidak terletak pada pemindai itu sendiri, tetapi pada modifikasi sistem keamanan, penggunaan yang tidak sesuai arahan, dan penempatan yang tidak tepat.

Kata Kunci: Biometrik, CPTED, Kontrol Akses, Penyusupan.

PENDAHULUAN

Keamanan ruang dari bangunan dan premisnya adalah sebagai prioritas dari suatu perencanaan dan *planning* dari suatu fungsi bangunan, dengan perkembangan jaman dan perkembangan era ini menimbulkan kompleksitas baru seperti ukuran bangunan, integrasi teknologi baru, bentuk bangunan, akses keluar-masuk, yang dengan itu menimbulkan problematika baru dalam suatu upaya pengamanan yang tidak sesederhana dan semudah era sebelumnya. Sehingga keamanan dari ruang bangunan dan premisnya diharapkan dapat mengatasi berbagai elemen, tidak lupa dengan permintaan dari efisiensi dan efektivitas upaya pengamanan sebagai harapan utama didalam skema keamanan. Lalu mengapa menggunakan biometrik dalam skema keamanan dan upaya kontrol aksesnya begitu penting? sebagai konteks terkait upaya yang digunakan dalam premis tema ini ada satu sistem, yang pertama adalah sistem tradisional kontrol akses, dan kedua adalah sistem unimodal dari penggunaan alat biometrik. Dalam penelitian ini difokuskan kepada sistem biometrik unimodal atas basis dimana biometrik tidak seperti keamanan tradisional yang mana bersanding pada kunci akses seperti *passcode*, *password*, kartu akses, kunci fisik maupun akses dari sistem menggunakan segala jenis kunci dan kartu fisik lainnya. Itu semua mengandalkan suatu informasi maupun data yang dapat terlupakan maupun hilang baik secara sengaja maupun disengaja disalah fungsikan oleh manusia yang tidak memiliki hak dari akses yang dimaksud, seperti apa yang disampaikan oleh Jones bahwa sistem ini, sistem kontrol akses biometrik memberikan akses berlandaskan pada individu dan siapa dia, bukan pada apa yang mereka pegang atau miliki atau mereka bawa ditangan mereka atau secara kontekstual kunci akses (Jones, 2019). Dan tidak hanya sampai disitu, menurut (Muntasa, Sirajuddin, & Purnomo, 2019) terdapat risiko duplikasi, kemudian biaya produksi kunci akses, serta terdapat eksistensi gap dari error didalamnya.

Selain itu, menurut pandangan Mark Lockie (Lockie, 2002) pada era tahun 2000 ke atas akan menjadi tahun yang menentukan bagi perkembangan ilmu biometrik. Dorongan berkembangnya ilmu biometrik datang dari besarnya perhatian dan kesadaran banyak komunitas global mengenai keamanan jaringan, perdagangan online, serta turunnya harga perangkat keras. Asosiasi Industri Biometrik Internasional atau The International Biometric Industry Association (BIA) juga memperkirakan bahwa pada tahun 2003, penjualan perangkat keras biometrik akan mencapai US$600 juta, sedangkan penjualan perangkat lunak akan mencapai setidaknya 2-3 kali lipatnya. Dari beberapa teknologi biometrik yang saat ini dikomersialkan seperti alat pengenalan sidik jari, mata, wajah, suara, dan rekognisi tanda tangan, teknologi identifikasi biometrik sidik jarilah yang paling banyak digunakan. Sistem identifikasi biometrik sidik jari ini memiliki banyak keunggulan, harganya cukup murah dibandingkan alat biometrik lainnya, serta penggunaan dan penerapannya semakin mudah dan sederhana (Nugroho, 2009). Seperti yang dijelaskan oleh Penrith City Council (2014), penggunaan hambatan fisik dan simbolis dapat digunakan secara efektif untuk menarik perhatian, mengalihkan, mengarahkan, dan membatasi pergerakan orang yang menggunakan jalur atau ruang. Penghalang simbolis menciptakan penghalang psikologis bagi orang-orang yang melihatnya, seperti pencahayaan, perubahan tekstur trotoar (membagi ruang publik dari ruang pribadi), tanaman hias, dan tanda-tanda peringatan. Sementara itu, penghalang fisik secara fisik dapat menghentikan dan mencegah satu atau lebih orang mencapai suatu area, contohnya dinding, pagar, gerbang, dan penghalang lainnya.

Dalam manajemen ruang, ruang publik yang menarik, bersih, dan terawat baik dapat secara efektif mengundang pengguna atau publik, sesuai dengan prinsip-prinsip penguatan teritorial. Jika manajemen ruang ini efektif, ruang tersebut akan digunakan, dipelihara, dan dimanfaatkan dengan baik. Prinsip penguatan teritorial ini sangat bergantung pada penghuni,

komunitas, dan pengguna area tersebut. Diharapkan bahwa pengguna ruang akan merasa memiliki ruang tersebut. Karena rasa kepemilikan ini, mereka akan lebih nyaman dan percaya diri untuk berkumpul dan menikmati ruang tersebut, dan dengan rasa kepemilikan ini meningkatkan kemungkinan bahwa ketika suatu kejahatan terjadi, orang-orang di ruang tersebut akan merespons dengan mencoba menghentikan, mencegah, dan melaporkannya kepada pihak berwenang. Elemen terakhir adalah pemantauan dengan pengawasan. Dengan menciptakan peluang untuk pengawasan yang efektif, baik secara alami maupun teknis, dapat mengurangi daya tarik dan risiko suatu titik menjadi target kejahatan. Dalam konteks ini, pengguna ruang di daerah tersebut dapat melihat apa yang dilakukan orang lain, sehingga menghalangi dan mengurangi kesempatan bagi pelaku untuk melakukan kejahatan di daerah dengan tingkat pengawasan yang tinggi. Oleh karena itu, penelitian ini akan lebih berfokus pada elemen CPTED di bagian kontrol akses guna melihat bagaimana pemindai biometrik sebagai alat dalam sistem kontrol akses fisik bekerja.

Keamanan personel dan pekerja merupakan perhatian utama bagi pemilik atau pengguna bangunan bisnis, kantor, atau instalasi perusahaan. Dengan banyaknya orang yang datang dan pergi setiap hari, menjaga keamanan menjadi tantangan. Sistem kontrol akses berbasis kunci fisik seperti kartu dan kunci adalah yang paling umum digunakan, tetapi kartu dan kunci yang hilang atau dicuri dapat membahayakan keamanan, mengancam keselamatan karyawan, serta data dan aset fasilitas. Sistem kontrol akses tradisional yang menggunakan kartu, kode, dan kunci dapat mudah dipintas dengan menduplikasi atau mencuri sumber asli. Sebaliknya, sistem biometrik yang menggunakan karakteristik manusia sebagai kunci diharapkan mampu mengenali dan membedakan individu yang memiliki hak akses dari orang asing, sehingga meningkatkan keamanan. Namun, dalam penerapannya, pemahaman dan pengetahuan tentang keamanan biometrik, baik secara umum maupun khusus di sektor swasta, masih memerlukan data hasil yang lebih proyektif untuk menilai efektivitas dan efisiensinya dibandingkan dengan sistem sejenis (unimodal dan multimodal). Keterbatasan informasi ini dapat menjadi masalah signifikan di masa depan. Hal ini sangat disayangkan karena dengan kemajuan teknologi, sistem kontrol akses berbasis biometrik, jika diterapkan dengan benar, dapat dengan cepat mengidentifikasi pekerja di pintu masuk suatu ruang atau fasilitas, mengidentifikasi individu dengan keaslian identitas yang diragukan, dan bahkan menghentikan upaya pencurian aset.

Penelitian ini mengevaluasi penerapan pemindai biometrik dalam sistem kontrol akses untuk meningkatkan keamanan ruang dan fasilitas. Fokusnya adalah memahami mekanisme operasional, protokol, dan komponen yang terlibat dalam sistem kontrol akses biometrik untuk mengurangi risiko dan melindungi aset. Selain itu, penelitian ini mencari pemahaman dari para pekerja yang terlibat dalam penggunaan sistem ini. Selanjutnya, penelitian ini membahas penggunaan pemindai biometrik dalam kontrol akses, termasuk tanggung jawab, serta keuntungan dan kerugian penggunaan teknologi biometrik. Selanjutnya, penelitian ini melakukan perbandingan antara efektivitas sistem biometrik multimodal (menggunakan geometri wajah dan sidik jari) dengan sistem unimodal (hanya menggunakan sidik jari) dalam meningkatkan tingkat keamanan. Dari fokus dan tujuan tersebut, maka pertanyaan penelitian yang akan diajukan adalah Bagaimana mekanisme biometrik sidik jari sebagai alat rekognisi dalam sistem kontrol akses pada studi kasus di instalasi bangunan ‘A’ di perusahaan ‘X’?

METODE

Penelitian ini mengadopsi pendekatan kualitatif dengan melakukan observasi dan wawancara tidak terstruktur untuk mendapatkan pemahaman yang lebih mendalam. Menurut Denzin dan Lincoln (1994), pendekatan kualitatif melibatkan tindakan interpretatif dan berbagai materi empiris seperti pengalaman, studi kasus, wawancara, observasi, interaksi, introspeksi, dan teks lainnya untuk memahami posisi manusia sebagai pengamat. Penelitian ini dilakukan pada dua lokasi instalasi korporasi 'X', yaitu bangunan 'A', selama periode 1

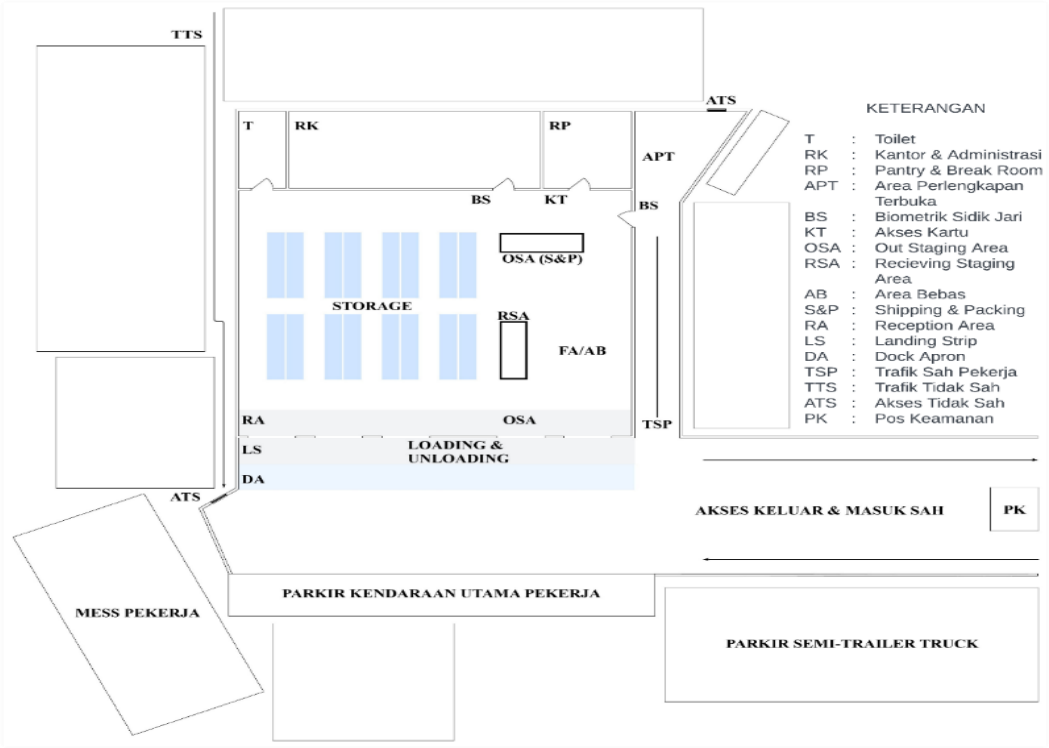
Januari - 20 Mei 2024. Data yang dikumpulkan digunakan untuk menganalisis mekanisme dan skema kerja, reaksi dan tanggapan pekerja, serta penggunaan CPTED dalam mekanisme dan reaksi yang diamati.

Wawancara tidak terstruktur dilakukan dengan beberapa elemen pekerja, pihak keamanan korporat, eksekutif korporat, konselor keamanan, dan vendor alat pemindai biometrik yang bermitra dengan perusahaan 'X'. Data yang dikumpulkan meliputi protokol kerja, rencana bangunan, denah bangunan, dan regulasi bangunan untuk menganalisis konteks mekanisme, denah dan trafik gerak, serta penempatan alat pemindai biometrik. Identitas narasumber, korporasi, dan lokasi disamarkan untuk menjaga kerahasiaan dan keamanan. Secara deduktif, penelitian ini akan memetakan penggunaan sistem kontrol akses biometrik (sidik jari) di instalasi 'A' selama periode waktu 1 Januari - 20 Mei, 2024 melalui observasi langsung dan wawancara tidak terstruktur.

HASIL DAN PEMBAHASAN

Hasil Observasi Mekanisme, *Break-In*, dan *Trespassing*

Dari data hasil observasi dan wawancara, peneliti menemukan contoh dan mekanisme aplikasi dan penggunaan dari alat pemindai biometrik sidik jari dan geometri wajah sebagai bagian instrumen dari sistem kontrol akses dalam denah dan *building plan* yang dapat disesuaikan dengan upaya pengamanan ruang dalam kacamata teori dan metode *crime prevention through environmental design* (CPTED). Untuk menjaga prinsip konfidensialitas, menghargai paten dari mekanisme keamanan, dan kontrol akses yang digunakan perusahaan, akan ada beberapa perubahan arah, tititk, dan penempatan yang tidak akan merubah konteks dan data penelitian dan ini hanya akan berpengaruh secara visual di dalam denah dan trafik yang dilampirkan, ini juga tanpa mengurangi bentuk efektif sistem kontrol akses dengan pemindai biometrik sebagai instrumen.

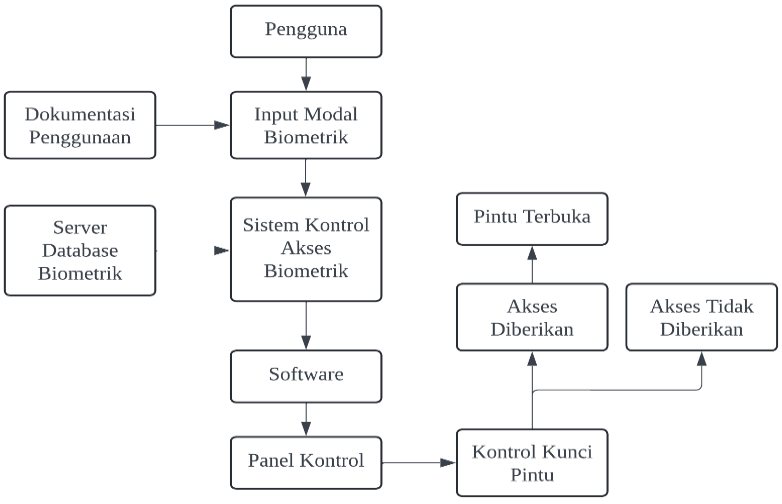


Sumber: Bangunan dan Premis dari Instalasi ‘A’ di Perusahaan ‘X’

Gambar 1. Gambar denah trafik bangunan ‘A’ (1 Januari – 20 Mei, 2024) yang telah diproses dan diubah titik penempatan dan *landmark* untuk alasan keamanan

Lokasi instalasi ‘A’ di korporasi ‘X’ adalah instalasi pergudangan yang diperuntukan dalam penerimaan material mentah, pemilahan, serta pemeriksaan material yang masuk, yang mana nantinya akan disimpan sementara di instalasi ini untuk nantinya dikirim keluar kepada instalasi lain sebagai bahan pembangun produk di instalasi lini perakitan korporasi ‘X’. Merujuk dari hasil observasi secara langsung yang telah dilaksanakan, peneliti dapat menggambarkan bangunan ‘A’ yang terdiri dari satu bangunan instalasi dengan dua premis bangunan, yaitu (1) wilayah loading dan unloading kendaraan truck semi-trailer, (2) wilayah parkir kendaraan utama bagi pekerja dan (3) lorong yang mengarah pada pintu masuk utama instalasi dan (4) wilayah perlengkapan terbuka keduanya berhubungan dengan satu akses keluar dan masuk. Didalam bangunan instalasi ini terdapat satu ruang terbuka yang difungsikan sebagai ruang penyimpanan khusus material (main storage area), ruang area bebas, ruang staging area untuk penerimaan material dari proses unloading, ruang staging area keluar untuk menuju ke proses loading.

Dalam instalasi ini terdapat (1) beberapa rute patrol divisi keamanan yang khusus bekerja hanya di titik ‘A’, (2) terdapat pembatas atau pagar dari beton dan kawat dengan tinggi yang sulit untuk dipanjat menggunakan bantuan tangga, (3) terdapat tempat pejalan kaki dan jalan khusus kendaraan yang dibedakan secara spesifik dengan bentuk dan tanda. (4) Terdapat penerangan di setiap sisi terutama pada sisi jalan kendaraan dan manusia, (5) terdapat alat pengawasan mekanis (CCTV) yang diposisikan pada bagian dalam instalasi (untuk mengawasi material penting dan ruang dokumen) dan (5) pengawasan natural dalam bentuk ruang terbuka, selain itu terdapat (6) pos pengamanan yang diposisikan pada ruang terbuka untuk dapat melakukan pengawasan. Selain itu terdapat empat kontrol menggunakan kartu akses, dan dua pintu akses menggunakan pemindai biometrik, untuk akses kartu terdapat di pintu utama, pintu akses kendaraan, pintu ruang kantor dan dokumen, dan satu kontrol khusus untuk identifikasi pengendara truck semi-trailer. Untuk pemindai biometrik sidik jari terdapat dua unit, satu pada pintu utama masuk kedalam ruang instalasi dan satu pada pintu akses kantor dan ruang dokumen.



Sumber: Bangunan dan Premis Instalasi ‘A’ perusahaan ‘X’

Gambar 2. Mekanisme dari sistem kontrol akses dengan pemindai biometrik yang digunakan di instalasi ‘A’ (2024) dari hasil observasi intalasi ‘A’ perusahaan ‘X’

Mekanisme kerja alat biometrik ini diperoleh dari melakukan observasi secara langsung dan wawancara tidak terstruktur dalam lingkup instalasi ‘A’, untuk instalasi ini menggunakan sistem dan mekanisme yang dimodifikasi untuk dapat bekerja secara tandem dan memiliki data laporan yang *interchangeable* dengan mudah diantara keduanya, dengan

kata lain instalasi ini menggunakan skema yang berbeda dari apa yang umunya direkomendasikan oleh produsen alat pemindai biometrik, Apa yang telah diperoleh sebagai berikut;

1. Pengguna berdiri di depan pemindai biometrik sidik jari dan mengikuti instruksi untuk akses masuk bangunan, seperti memilih jari yang tepat, memastikan jari bersih, menekan layar optik dengan benar, dan menunggu hingga pemindaian selesai sebelum menarik jari.
2. Data yang diinput dan dipindai akan dikirim dan diproses oleh perangkat lunak sistem kontrol akses biometrik, kemudian dibandingkan dengan data registrasi awal di database untuk identifikasi.
3. Jika data individu tidak ditemukan atau terjadi kesalahan, pengguna diminta menunggu sebentar dan mencoba lagi, serta memeriksa kondisi sidik jari untuk memastikan tidak ada substansi seperti pembersih berbasis alkohol atau cairan pelembab kulit.
4. Jika akses masih tidak berhasil, notifikasi akan dikirim ke sistem kontrol dan interface di ruang keamanan dan kantor instalasi untuk membantu pengguna.
5. Jika akses diterima, informasi akan diproses oleh unit pemindai biometrik, dibandingkan dengan *database*, dan jika cocok, pintu fisik akan terbuka.
6. Untuk akses fisik (ruang) atau logis (data) pada perangkat elektronik, otorisasi fisik mengikuti langkah-langkah di atas, sedangkan akses logis memerlukan otorisasi tambahan dari individu berwenang disertai surat izin, dan biasanya dilakukan dengan perangkat khusus yang diawasi.
7. Semua proses tersebut adalah wajib dan berurutan, sama seperti saat pekerja melakukan *punch-out* pada jam keluar kerja. Jika seseorang masuk, mereka harus keluar, dan tanpa dokumen keluar, ini akan di-*flag* sebagai kejanggalan. Verifikasi pemindaian dua kali diperlukan untuk masuk dan keluar.
8. Dalam akses logis, dilarang membawa atau menggunakan perangkat keras seperti flash disk atau CD-DVD yang bisa mencuri data atau menyebarkan virus. Sama halnya dengan akses fisik, pemilik hak, baik pekerja atau tamu dengan otorisasi sementara, harus menyimpan gawai di kompartemen khusus dekat pintu akses yang diawasi oleh pihak keamanan.

Selama periode pengamatan dari 1 Januari hingga 20 Mei 2024, di instalasi 'A', terjadi 24 kasus masuk tanpa izin dan pelanggaran yang terdiri dari 17 kasus *false positive* dan 7 kasus masuk tanpa izin yang disengaja. Dari 17 kasus *false positive*, sebagian besar disebabkan oleh kesalahan manusia dalam proses otentikasi akses, termasuk kesalahan penggunaan geometri biometrik dan sidik jari yang kotor. Penyebab lainnya adalah kegagalan alat pemindai dalam mendeteksi geometri biometrik atau menarik *database* secara benar. Kemudian, untuk 7 kasus masuk tanpa izin yang disengaja, termasuk upaya memotong jalur menuju area tertentu dan pencurian aset. Sistem kontrol akses berbasis kartu fisik yang digunakan di lokasi memiliki beberapa titik kontrol untuk mengelola aliran orang dan barang, namun terdapat kekurangan dalam hal pemantauan yang menyebabkan beberapa kasus pencurian berhasil dicegah atau diselesaikan setelah kejadian. Kasus-kasus ini dianalisis secara rinci dengan melibatkan berbagai pihak termasuk staf keamanan, eksekutif korporat, dan vendor alat biometrik. Upaya dilakukan untuk memahami penyebab dari kasus-kasus ini dan mencari solusi untuk meningkatkan sistem keamanan di lokasi instalasi 'A'.

Analisis CPTED

Strategi multidisiplin yang disebut pencegahan kejahatan melalui desain lingkungan atau *crime prevention through environmental design* (CPTED) bertujuan untuk menurunkan kejahatan dan ketakutan akan kejahatan, yang mana tujuan dari teknik CPTED adalah untuk mengurangi viktimisasi, mencegah keputusan kriminal atau pelaku potensial yang muncul sebelum terjadinya kejahatan, serta menumbuhkan dan memperkuat perasaan komunitas di antara penduduk setempat sehingga mereka dapat mengambil kendali teritorial atas tempat

dan menurunkan kemungkinan kejahatan mereka (LAPD, 2021; ICA, 2021). Dalam penelitian ini akan menggunakan teori CPTED generasi pertama dengan elemen atau pilar yang difokuskan kepada elemen kontrol dari akses dan pengawasan natural (dan mekanis). Arahan dari fokus kedua elemen ini untuk dapat mempermudah peneliti memetakan dan menggambarkan fenomena, serta melakukan analisis dari apa yang terlampirkan dari hasil data dari observasi dan wawancara yang dilakukan pada instalasi perusahaan yang mana ini juga berfokus pada pengamanan secara fisik dan pengawasan baik secara mekanis maupun desain yang memanfaatkan pengawasan natural.

Terkait argumen peneliti mengenai manipulasi bangunan di lokasi 'A' yang dianalisis menggunakan sudut pandang teori CPTED, didapatkan beberapa temuan: (1) Penggunaan pembatas akses fisik bertujuan untuk mengendalikan trafik keluar dan masuk dari pekerja yang memiliki akses, orang luar, dan tamu. Pembatasan ini juga memudahkan pemantauan di beberapa titik utama karena orang yang hendak mengakses harus berhenti sejenak, sehingga informasi tentang mereka dapat lebih mudah diperoleh oleh pihak keamanan atau alat pengawasan mekanis. (2) Secara resmi, instalasi ini hanya memiliki satu akses keluar dan masuk di arah timur, dengan satu jalan utama yang menghubungkan seluruh sektor lain di perusahaan 'X'. Setiap sisi jalan ini diterangi oleh banyak lampu penerangan berwarna putih, dengan pembatas jalan di setiap sisinya dan area pejalan kaki yang terbatas. Dalam analisis CPTED, penggunaan lampu penerangan di setiap titik trafik jalan dan sudut sesuai dengan prinsip *natural surveillance*, yang dijelaskan dalam teori CPTED dimana keempat pilar teori tersebut saling mendukung. Dengan adanya jalan yang jelas bagi kendaraan dan pejalan kaki, pekerja, tamu, dan orang berkepentingan diharuskan mengikuti jalur yang disediakan. Jika ada yang berjalan di luar jalur yang ditentukan, mereka akan lebih terlihat dan tindakannya dapat dianggap tidak normal, sehingga akan ditanyakan intensi dan tujuannya oleh patroli keamanan atau supervisor. Selain itu, ini bertujuan untuk memisahkan jalur kendaraan dan pejalan kaki secara jelas, meminimalisir risiko kecelakaan, dan memudahkan kontrol ruang. (3) Premis instalasi ini dikelilingi oleh pagar pembatas beton dan kawat besi yang sulit dipanjat. Namun, peneliti menemukan dua titik akses (ATS) di bagian utara dan barat premis instalasi yang tidak seharusnya ada menurut denah perencanaan pengamanan dan pembangunan. Kedua titik ini digunakan oleh pekerja instalasi khusus dan pekerja dari instalasi lain untuk memotong waktu perjalanan mereka. Untuk elemen lain, yaitu (4) pengawasan, terdapat dua kamera pengawas (CCTV) di pos keamanan yang memantau dua jalur masuk dan keluar instalasi, satu kamera di pintu utama masuk pegawai (TSP) bersebelahan dengan alat pemindai biometrik sidik jari, satu kamera di dekat akses masuk ruang kantor (administrasi dan dokumen), dan dua kamera lainnya di sisi kiri dan kanan zona penyimpanan material dan barang. Sayangnya, tidak ada pengawasan mekanis di area perlengkapan terbuka (APT), area parkir utama pekerja, dan sisi barat wilayah luar yang digunakan sebagai jalur trafik gerak manusia tidak sah. Selama masa observasi, peneliti menemukan bahwa (5) rute patroli dari divisi keamanan tidak bervariasi dan memiliki rute serta jadwal yang mudah ditebak jika seseorang melakukan pengamatan selama satu minggu, sehingga ada kemungkinan rute kosong tanpa patroli pengawasan manusia dan mekanis secara bersamaan.

Peneliti juga menemukan bahwa (6) sistem dan jaringan kontrol akses berbasis biometrik menggunakan jaringan terlokalisir khusus untuk instalasi bangunan 'A', sedangkan sistem kontrol akses berbasis kartu terhubung dengan jaringan seluruh sektor instalasi di perusahaan 'X'. Untuk jaringan komunikasi keamanan, sebagian besar menggunakan jaringan lokal, namun kepala divisi memiliki akses jaringan ke pusat keamanan korporasi. Komunikasi pegawai di dalam instalasi ditiadakan dengan mewajibkan penyimpanan *smartphone* atau gawai sejenisnya di loker khusus. Hanya ada satu jaringan yang terhubung ke pusat seluruh sektor di ruang kantor dan dokumen untuk memfasilitasi transfer komunikasi, informasi, dan data secara aktual dan langsung. Untuk (7) alat pemindai

biometrik yang terletak di akses keluar dan masuk utama di arah utara dari rute trafik sah pekerja, alat ini digunakan setiap hari sebagai pemberi otorisasi akses pekerja dan sebagai sistem kehadiran pekerja. Alat biometrik di ruang kantor dan dokumen berfungsi sebagai kunci kedua untuk memberikan akses kepada pekerja yang berhak. Ada empat kontrol kartu, tiga sebagai kontrol akses dan satu sebagai alat identifikasi pengendara yang membawa material. Identifikasi pertama adalah untuk pembawa kendaraan yang hendak masuk ke dalam premis instalasi 'A', kedua di titik akses utama bersama dengan alat pemindai biometrik sidik jari, dan ketiga di pintu akses ruang kantor dan dokumen yang juga bersama dengan alat pemindai biometrik sidik jari.

Di pintu utama dan pintu kantor, pemindai biometrik sidik jari dan kartu akses fisik bisa digunakan bersama atau secara mandiri untuk membuka akses. Skema pengaturan lokal memungkinkan akses dengan satu alat saja, tidak perlu keduanya, untuk mempercepat antrean akses pekerja, memudahkan yang tidak membawa kartu, tamu atau VIP, serta meminimalisir kesalahan. Uji coba menunjukkan bahwa penggunaan kedua alat membutuhkan rata-rata 14 detik, sedangkan kartu saja memerlukan 5 detik. Kedua alat ini juga mencatat data dan informasi pengguna ke dalam laporan yang dikirim ke *database*, memudahkan pengolahan data bagi administrasi, kepegawaian, dan keamanan untuk pengawasan akses dan deteksi kejanggalan atau orang asing yang di-*flag* sistem.

Uji Coba Alat Pemindai Biometrik

Peneliti menilai *margin of error* alat pemindai biometrik sidik jari di lokasi 'A' dengan melakukan uji coba terkontrol terhadap upaya manipulasi yang mungkin dilakukan oleh pelaku potensial. Uji coba tidak menggunakan geometri tiga dimensi sidik jari dari *database*. Peneliti bekerja sama dengan vendor biometrik dan perwakilan eksekutif korporasi 'X' untuk melakukan uji coba manipulasi dengan metode yang paling mudah dan efisien (penangkapan optikal). Uji coba dilakukan dengan memvariasikan *threshold* sensitivitas pemindai pada tingkat rendah, medium, dan tinggi (semakin tinggi *threshold*, semakin mudah pemindai menangkap sidik jari palsu). Upaya pemalsuan dilakukan dengan menggunakan gambar dua dimensi dari tiga kamera: kamera *smartphone* (48mp), kamera PowerShot SX 540 HS, dan gambar dari *database* yang diambil saat registrasi. Gambar-gambar ini dicetak pada kertas dua dimensi dengan berbagai jenis: kertas *uncoated* 300GSM, 350GSM (kertas kartu bisnis), dan 80GSM (kertas dokumen A4 biasa). Gambar dicetak akan diuji dengan berbagai pemberat: jari manusia kering, pemberat logam 350 gram, dan jari manusia basah, untuk melihat efektivitas pemindai dalam mendeteksi sidik jari palsu.

Tabel 1. Variabel Perubahan Set Parameter Modal Optik 1 (48MP)

Uji Coba	Sensitivitas Fake Threshold	Medium Kertas	Pemberat	Hasil
A1	Rendah	300GSM	Kering, Basah	Gagal
A2	Menengah	300GSM	Kering, Basah	Gagal
A3	Tinggi	300GSM	Kering, Basah	Gagal
A1	Rendah	300GSM	Logam (350g)	Gagal
A2	Menengah	300GSM	Logam (350g)	Gagal
A3	Tinggi	300GSM	Logam (350g)	Gagal
B1	Rendah	350GSM	Kering, Basah	Gagal
B2	Menengah	350GSM	Kering, Basah	Gagal
B3	Tinggi	350GSM	Kering, Basah	Gagal
B1	Rendah	350GSM	Logam (350g)	Gagal
B2	Menengah	350GSM	Logam (350g)	Gagal
B3	Tinggi	350GSM	Logam (350g)	Gagal
C1	Rendah	80GSM	Kering, Basah	Gagal
C2	Menengah	80GSM	Kering, Basah	Gagal
C3	Tinggi	80GSM	Kering, Basah	Gagal

C1	Rendah	80GSM	Logam (350g)	Gagal
C2	Menengah	80GSM	Logam (350g)	Gagal
C3	Tinggi	80GSM	Logam (350g)	Gagal

Sumber : Data Uji Coba

Tabel 2. Variabel Perubahan Set Parameter Modal Optik 2 (PowerShot SX 540 HS)

Uji Coba	Sensitivitas Fake Threshold	Medium Kertas	Pemberat	Hasil
D1	Rendah	Uncoated 300GSM	Kering	Gagal
D1	Rendah	Uncoated 300GSM	Basah	Gagal
D1	Rendah	Uncoated 300GSM	Logam (350g)	Gagal
D2	Menengah	Uncoated 300GSM	Kering	Gagal
D2	Menengah	Uncoated 300GSM	Basah	Gagal
D2	Menengah	Uncoated 300GSM	Logam (350g)	Gagal
D3	Tinggi	Uncoated 300GSM	Kering	Gagal
D3	Tinggi	Uncoated 300GSM	Basah	Gagal
D3	Tinggi	Uncoated 300GSM	Logam (350g)	Gagal
E1	Rendah	Uncoated 350GSM	Kering	Gagal
E1	Rendah	Uncoated 350GSM	Basah	Gagal
E1	Rendah	Uncoated 350GSM	Logam (350g)	Gagal
E2	Menengah	Uncoated 350GSM	Kering	Gagal
E2	Menengah	Uncoated 350GSM	Basah	Gagal
E2	Menengah	Uncoated 350GSM	Logam (350g)	Gagal
E3	Tinggi	Uncoated 350GSM	Kering	Gagal
E3	Tinggi	Uncoated 350GSM	Basah	Gagal
E3	Tinggi	Uncoated 350GSM	Logam (350g)	Gagal
F1	Rendah	Uncoated 80GSM	Kering	Gagal
F1	Rendah	Uncoated 80GSM	Basah	Gagal
F1	Rendah	Uncoated 80GSM	Logam (350g)	Gagal
F2	Menengah	Uncoated 80GSM	Kering	Gagal
F2	Menengah	Uncoated 80GSM	Basah	Gagal
F2	Menengah	Uncoated 80GSM	Logam (350g)	Gagal
F3	Tinggi	Uncoated 80GSM	Kering	Gagal
F3	Tinggi	Uncoated 80GSM	Basah	Gagal
F3	Tinggi	Uncoated 80GSM	Logam (350g)	Gagal

Sumber : Data Uji Coba

Tabel 3. Variabel Perubahan Set Parameter Modal Optik 3 (Geometri biometrik)

Uji Coba	Sensitivitas Fake Threshold	Medium Kertas	Pemberat	Hasil
G1	Rendah	300GSM	Kering	Gagal
G2	Menengah	300GSM	Kering	Gagal
G3	Tinggi	300GSM	Kering	Gagal
G1	Rendah	300GSM	Basah, Logam (350g)	Gagal
G2	Menengah	300GSM	Basah, Logam (350g)	Gagal
G3	Tinggi	300GSM	Basah, Logam (350g)	Gagal
H1	Rendah	350GSM	Kering	Gagal
H2	Menengah	350GSM	Kering	Gagal
H3	Tinggi	350GSM	Kering	Gagal
H1	Rendah	350GSM	Basah, Logam (350g)	Gagal
H2	Menengah	350GSM	Basah, Logam (350g)	Gagal
H3	Tinggi	350GSM	Basah, Logam (350g)	Gagal
I1	Rendah	80GSM	Kering	Gagal
I2	Menengah	80GSM	Kering	Gagal
I3	Tinggi	80GSM	Kering	Gagal
I1	Rendah	80GSM	Basah, Logam (350g)	Gagal
I2	Menengah	80GSM	Basah, Logam (350g)	Gagal
I3	Tinggi	80GSM	Basah, Logam (350g)	Gagal

Sumber : Data Uji Coba

Dari keseluruh parameter (a; sensitivitas, b; optik, c; kertas, dan d; pemberat) yang digunakan ini menunjukkan bahwa dalam modal yang diuji dalam upaya melakukan *bypass* alat pemindai biometrik mengalami kegagalan untuk diidentifikasi sebagai modal biometrik asli, mulai dari pengaturan sensitivitas pada pemindai biometrik pada *fake threshold* rendah, menengah, tinggi. Seluruh kombinasi parameter gagal melewati tahap pemindaian dan identifikasi awal, ketiga parameter penangkapan modal biometrik dua dimensi yaitu; parameter optik kamera (b); *smartphone* (48mp), kamera *PowerShot SX 540 HS*, dan kamera optik pemindai alat biometri, begitu juga ketiga parameter pemberat (d) yaitu; logam 350 gram, jari dalam keadaan kering, jari dalam keadaan basah (lembab), serta ketiga parameter medium *print* (c) yang digunakan yaitu; kertas *uncoated* 350GSM, 300GSM dan 80GSM, yang mana dengan ini seluruh kombinasi dari set parameter yang digunakan tidak dapat melewati tahap proses identifikasi biometrik sidik jari sebagai tahap awal mendapatkan autorisasi akses ruang.

Penggunaan Alat Biometrik Sidik Jari Sebagai Kontrol Akses

Dalam sistem keamanan yang mengandalkan komponen biometrik, terdapat serangkaian langkah yang khas, yaitu identifikasi, verifikasi, dan autentikasi. Identifikasi adalah proses mengenali identitas seseorang, sementara autentikasi adalah proses membandingkan data biometrik seseorang dengan data dalam server untuk memberikan akses. Verifikasi memastikan keaslian dan identitas orang yang telah diotorisasi. Meskipun autentikasi dan verifikasi tampak serupa, keduanya memiliki peran yang berbeda dalam memastikan keamanan sistem.

Langkah-langkah otorisasi dan validasi pengesahan melibatkan kontrol akses lebih lanjut untuk mencegah akses tidak sah. Jika seseorang tidak terdaftar dalam sistem biometrik, mereka tidak akan diotorisasi untuk akses. Kesalahan atau upaya akses tidak sah akan dicatat dan direspons sesuai. Tindakan keamanan tambahan, seperti peringatan dan patroli ke lokasi pemindai, membantu mencegah masuk tanpa izin. Jika terjadi pelanggaran, petugas keamanan akan menangani situasi tersebut.

Pengamatan dan wawancara menunjukkan bahwa risiko akses tidak sah dapat diminimalkan dengan tindakan keamanan yang tepat. Penggunaan pemindai biometrik, seperti yang disarankan dalam teori CPTED, efektif dalam mencegah akses tidak sah. Keakuratan data biometrik dan kesulitan dalam mencuri kunci biometrik membuat sistem ini lebih aman daripada kontrol akses tradisional. Meskipun risiko manipulasi dan pencurian identitas tetap ada, sistem biometrik masih dianggap lebih aman dan efektif dalam mencegah akses tidak sah. Penempatan pemindai biometrik juga penting untuk memaksimalkan efektivitasnya, dengan mempertimbangkan faktor-faktor seperti kestabilan dinding dan ketersediaan cahaya. Secara keseluruhan, penggunaan pemindai biometrik memperkuat kontrol akses dan membantu menciptakan lingkungan yang aman dan terjamin.

KESIMPULAN

Ditemukan dari hasil observasi pada periode 1 Janurari – 20 Mei, 2024, bahwa penggunaan alat pemindai biometrik sebagai alat dalam sistem kontrol akses pada instalasi ‘A’ secara unimodal masih mendapati adanya sedikit kekurangan dari sisi kerja sistem, durabilitas alat, dan mekanisme kerja yang dipengaruhi manusia, bukan kelemahan dalam ‘adanya manipulasi modal biometrik’ di *margin of error* pemindai. Ini dilihat dari bagaimana terjadinya break-in diakibatkan oleh adanya manipulasi sistem dengan tidak semestinya akibat modifikasi skema dan sistem dengan tidak mengikuti arahan yang sesuai dari penggunaan alat kontrol akses, terutama terkait pemindai biometrik. Sebagai contoh lainnya adalah pada *Human Error* dalam melakukan perawatan dan penggunaan dari alat pemindai, dari hasil observasi ditemukan bahwa banyak pekerja yang menggunakan cairan pembersih

berbahan dasar alkohol sebelum menggunakan dan sesudah menggunakan pemindai, bahkan didapati beberapa kejadian dimana cairan pembersih berbahan dasar alkohol itu dibilaskan ke permukaan kaca diatas optik, ini menjadikan adanya 'awan' buram pada lapisan atas sehingga optik pemindai sulit untuk menangkap modal biometrik sidik jari seseorang dengan akurat dan baik. Hal ini yang menyebabkan banyak dari kasus *false positive* dan kegagalan dari melakukan identifikasi oleh pemindai sehingga didapati adanya kerja yang kurang efisien dan efektif terkait upaya kontrol akses dalam rangka mengamankan instalasi 'A'. Dengan permasalahan alat pemindai biometrik yang tidak konsisten (akibat pengguna) ini juga yang menjadi satu dari banyak alasan mengapa skema dan sistem kontrol akses semakin dirubah dengan bergantung pada skema yang sekarang ini digunakan, dimana orang yang ada di dalam *database* dapat menggunakan kartu akses atau pemindai biometrik sidik jari, namun mereka juga dapat menggunakan keduanya, yang masih menjadi penolong dalam keamanan dalam instalasi ini adalah adanya rekap laporan dari pengguna serta adanya alat pengawas mekanis di beberapa titik sehingga saat ada empat kasus yang dapat *bypass* sistem kontrol akses akibat manipulasi kelemahan pada alat kontrol akses kartu masih dapat dilakukan runut ulang secara visual maupun data laporan.

Lokasi penempatan pemindai biometrik juga perlu mengikuti pedoman metode CPTED untuk mencapai potensi maksimalnya, pertama dari aspek pengelolaan ruang, menurut sumber *engineer* dari vendor yang menyediakan peralatan biometrik dan sebagai konsultan keamanan bagi korporasi "yang harus diperhatikan pada saat pemasangan adalah dinding pada lokasi penempatan tidak boleh bergetar, terkena sinar matahari baik secara langsung maupun pantulan cahaya begitu juga dengan air hujan." disusul dengan jawaban lanjutan lainnya "letak alat pemindai biometrik harus berada di tempat yang strategis agar pengguna mudah menjangkau alat tersebut dan terhindar dari tindakan vandalisme" menurut analisis peneliti hal ini dapat menciptakan citra positif bagi pengguna bangunan yang bangunan terpelihara dan dirawat dengan baik, serta penerapan teknologi, material, dan sumber daya yang secara empiris efektif dalam meminimalisir, mengurangi bahkan mencegah terjadinya kejahatan yang dimaksud. Penggunaan pemindai biometrik juga memperkuat aspek kontrol akses CPTED, hal ini karena risiko kejahatan dan pelanggaran, terutama pelanggaran, berkurang (merujuk pada data observasi) bila dibandingkan dengan penggunaan alat kontrol akses tradisional, karena kata sandi dari *keypad* dapat dengan mudah dicuri, kartu kunci mudah diduplikasi dan hilang secara tidak sengaja sementara kunci biometrik jauh lebih sulit dan merupakan upaya yang berbeda untuk diduplikasi atau dicuri.

REFERENSI

Denzin, N. K., & Lincoln, Y. S. (1994). Handbook of qualitative research. Los Angeles, London, Washington DC: Sage Publications, Inc.

Denzin, N. K., & Lincoln, Y. S. (2005). Introduction: The Discipline and Practice of Qualitative Research - The Sage handbook of qualitative research. California: Sage Publications Ltd.

Greater Manchester Police. (2021). Crime Prevention Through Environmental Design. Retrieved from Design for Security, Greater Manchester Police: https://designforsecurity.org

ICA. (2021). A Brief History of the ICA & Primer CPTED - What is CPTED? Retrieved from The International Crime Prevention Through Environmental Design Association: https://www.cpted.net

Jones, L. (2019, February 14). Biometrics. Retrieved from Touch Star Access, Time, CCTV (ATC): https://www.touchstar-atc.com/

LAPD. (2021). Crime Prevention, Design Out Crime : City of Los Angeles. Retrieved from Official Site of the Los Angeles Police Department: https://www.lapdonline.org

Lockie, M. (2002). Science at the Edge: Biometric Technology. Heinemann-Raintree.

Muntasa, A., Sirajuddin, I. A., & Purnomo, H. M. (2019). Basics & Implementation of Biometrics Science. Yogyakarta: Teknosain.

Nugroho, E. (2009). Biometrics. In M. Dr. Ir. Eko Nugroho, Getting to Know the Future Identification System (p. 14). Yogyakarta: C.V Andi Offset.

Penrith City Council. (2014). Penrith Development Control Plan, C1 Site Planning and Design Principles. Penrith: Secretary of the NSW Department of Planning and Environment.