Privacy and Security Vulnerability of Smart Camera

Almyra Ramadhina

NIM 18217009

Program Studi Sistem dan Teknologi Informasi

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung

18217009@std.stei.itb.ac.id

Abstract—Sistem kamera pintar semakin banyak diimplementasi dalam berbagai jenis aplikasi. Tujuan dari adanya kamera pintar ini sangat bervariasi. Kamera pintar sering digunakan untuk hal-hal yang bersifat pribadi dan memiliki privasi tinggi. Sehingga informasi yang ada pada kamera pintar merupakan informasi sensitif. Untuk merancang kamera pintar ini dibutuhkan tingkat keamanan yang tinggi, agar menghindari dari berbagai kemungkinan serangan.

Index terms—Kamera pintar, jaringan, privasi, keamanan

I. PENDAHULUAN

Di era modern ini, semakin banyak komputer yang bisa dipakai tertempel pada tubuh manusia, misalnya pakaian, jam, peralatan olahraga, serta peralatan rumah tangga. Hal ini memiliki tujuannya masing-masing, diantaranya adalah untuk kepentingan pekerjaan, pemantauan keamanan, atau hanya sekadar hiburan. Hal-hal seperti ini disebut sebagai *Internet of Things* (IoT). Barang memiliki terkoneksi barang lainnya dengan internet. Tidak seperti internet pada konvensional sebelumnya, IoT dapat beroperasi di lingkungan yang sangat dinamis.

Salah satu pemanfaatan IoT ini adalah pada kamera. Kamera pintar banyak digunakan untuk keperluan pengawasan aplikasi. Kamera pintar memiliki keamanan yang cukup ketat dan ada persyaratan perlindungan privasi. Keamanan kamera pintar menjadi faktor kritis pada desain arsitektur secara keseluruhan. Desain dari sistem keamanan kamera pintar mempertimbangkan keamanan level *node* dan keamanan tingkat jaringan [1]. Persyaratan keamanan di kedua level harus menyediakan perlindungan data yang memadai. Sistem juga harus tahan terhadap segala macam kemungkinan serangan, termasuk serangan langsung, *side channel*, dan *denial of service* (DoS). Dengan meningkatnya sensor yang terhubung ke internet di seluruh dunia yang memonitor perilaku penggunanya secara pasif, privasi menjadi prioritas yang tinggi. Kamera yang terkoneksi internet popularitasnya semakin meningkat. Hal ini bisa dimanfaatkan penggunanya untuk mengawasi kantor-kantor, anak-anak mereka, binatang peliharaannya, serta keamanan rumah. IoT sering digambarkan sebagai kombinasi teknologi antara sensor, aktuator, dan perangkat pintar lainnya. Survei terbaru memperkirakan jumlah perangkat yang memanfaatkan IoT akan lebih dari 2 milyar pada tahun 20201. Namun, banyak perangkat IoT yang memiliki kerentanan keamanan, dan ini memungkinkan adanya ancaman kejahatan dan penyerangan pada kamera pintar. Keamanan kamera pintar bukanlah hal yang sangat baru untuk diteliti, dan sudah ada beberapa publikasi tulisan mengenai kerentanan IoT dan akses kamera.

Karena teknologi sudah berkembang pesat, semua orang terbiasa berbagi semua jenis informasi pribadi di media sosial. Kita tidak tahu mereka membagikannya walaupun peduli dengan privasi mereka sendiri atau tidak. Banyak orang yang secara sadar atau tidak sadar membagikan informasi pribadi mereka kepada publik. Tetapi mereka marah dan kesal ketika informasi yang mereka bagikan itu digunakan untuk iklan, atau yang lebih buruk lagi, informasi

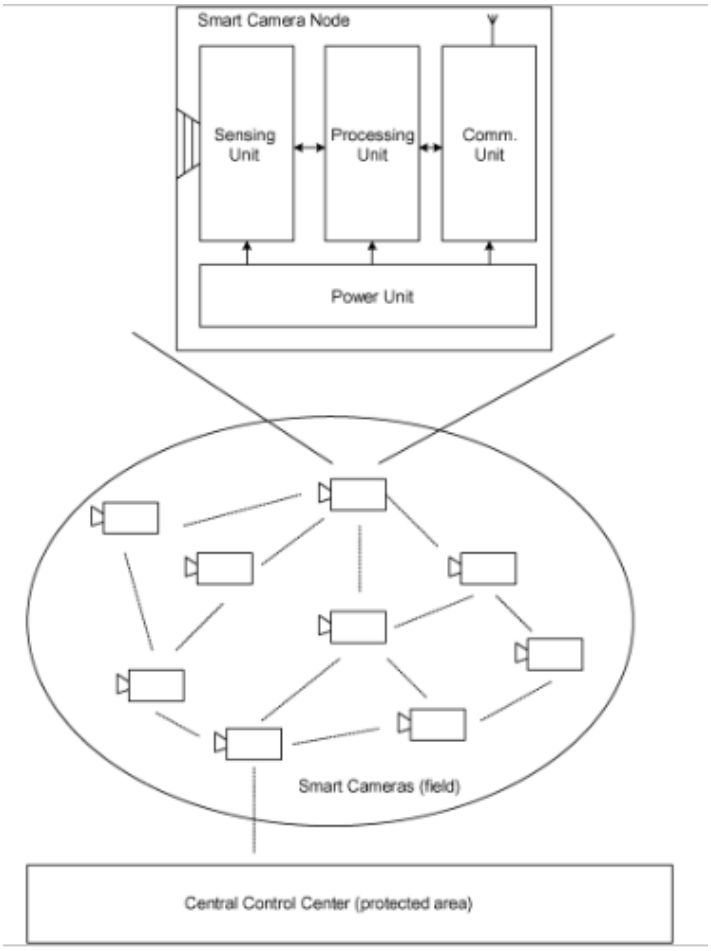
pribadi mereka digunakan untuk tindak kejahatan. Setiap perusahaan memberikan kebijakan tentang jenis data pengguna yang akan dibagikan dengan perusahaan pihak ketiga. Pengguna harus menyetujui syarat dan ketentuan sebelum membuat akun mereka. Mereka diberitahu tentang jenis data yang dikumpulkan dan kemungkinan itu akan dibagikan dengan vendor pihak ketiga. Sayangnya, masih sangat banyak yang tidak baca syarat dan ketentuan layanan yang mereka gunakan, hanya asal klik ‘saya menyetujui’ dan melanjutkan pembuatan akun mereka. Bahkan, beberapa di antara mereka tidak sepenuhnya memahami daftar istilah yang panjang dan kondisi yang ditulis dalam bahasa hukum. Jika kebocoran informasi data pribadi sudah bocor, pengguna tidak memiliki kendali lagi atas data yang bocor.

Dulu, keamanan kamera standar tidak diprioritaskan kecuali untuk urusan bisnis, tetapi saat ini perangkat *Internet of Things* (IoT) dibutuhkan banyak kepentingan. Misalnya di rumah mereka menggunakan untuk mengawasi dan mendeteksi pencurian rumah. Perangkat ini hanya merekam saat gerakan atau audio terdeteksi oleh pemilik rumah, sama seperti orang tua yang memantau bayi mereka. Tetapi kenyataannya adalah bahwa sebagian besar dari IP *address* kamera IoT ini diketahui memiliki mekanisme keamanan yang lemah [5]. Atau dapat dikatakan transmisi pengiriman data mereka tidak terenkripsi melalui internet dan datanya disimpan di *cloud*. Hal ini di luar kendali konsumen dan menimbulkan banyak masalah privasi serta keamanan.

II. SMART CAMERA

Kamera adalah perangkat digital yang dapat mengirimkan gambar, audio, dan video. Perangkat ini terdiri dari dua komponen, yaitu *hardware* dan *software*. Salah satu komponen *software* adalah HTTP *web server* untuk autentikasi dan konfigurasi pengaturan pada perangkat [3]. Kamera pintar dapat terhubung dengan *Wi-Fi* yang dapat diakses dari mana pun melalui koneksi internet, entah itu *software* komputer, *internet browser*, atau perangkat *mobile* Android/iOS. Kamera pintar memiliki beberapa fungsi seperti *video sensing*, pemrosesan dan komunikasi terletak pada satu perangkat. Tugas dari jaringan kamera pintar adalah untuk melacak objek yang berada pada pandangan beberapa node kamera. Dalam situasi seperti ini, node pada kamera perlu memproses data dalam jumlah besar dan berkomunikasi satu sama lain dengan batasan waktu. Selain itu, node kamera pintar biasanya diimplementasikan pada perangkat dengan sumber daya yang terbatas, di mana *task* komputasi dipetakan ke *hardware* dan *task controlling* dipetakan ke *software* [1].

Analisis keamanan yang detail dari sistem kamera pintar memerlukan spesifikasi dari karakteristik arsitektur utama mereka, terutama jika berkaitan dengan masalah keamanan. Sistem kamera pintar biasanya terdiri dari *node* kamera pintar itu sendiri yang saling terhubung. Untuk lebih jelasnya bisa dilihat pada ilustrasi berikut ini.



Gambar 1 Arsitektur kamera pintar

Sumber: https://ieeexplore.ieee.org/document/4653064

Gambar di atas menjelaskan bahwa kamera pintar terdiri dari beberapa *node*. Dan di dalam *node* tersebut terdapat *sensing unit, processing unit,* dan *communication unit* [1]. Kamera pintar yang terdiri dari *nodes* tersebut bisa dikontrol melalui *central control center*. Semua *unit* pada kamera pintar (*sensing, processing,* dan *communication*) dapat diimplementasikan ke sebuah *embedded device*. *Power unit* adalah sub-sistem yang menyediakan daya yang dibutuhkan oleh *node* untuk beroperasi. Daya operasional dapat berasal dari sumber daya dari pusat, atau dapat diperoleh dari lingkungan sekitar. Operasi *power unit* sangat penting, apalagi untuk aplikasi yang sumber daya energinya terbatas dan meemrlukan manajemen energi yang efisien. *Sensing unit* adalah sub-sistem yang mengambil gambar nyata dan menerjemahkannya ke dalam bentuk informasi digital, misalnya adalah sensor semi konduktor dan sistem lensa optik. Tujuannya adalah untuk mengambil *video stream* dari dunia nyata dan meneruskannya ke *processing unit. Processing unit* adalah sub-

sistem yang melakukan semua fungsi pemrosesan, atau *Digital Signal Processing* (DSP). Ini adalah komponen utama dari kamera pintar, karena disini dilakukan analisis dan pemrosesan video yang sudah diambil. Keluaran dari *processing unit* dapat berupa hasil dari fungsi DSP pada video yang diambil, atau sinyal dari video itu sendiri. *Communication unit* adalah sub-sistem yang melakukan semua fungsi komunikasi. Tujuan unit ini adalah menerima dan mengirimkan informasi yang diproses oleh kamera pintar (setelah dari *processing unit*), serta sinkronisasi dan sinyal kontrol.

Fungsi utama dari *software* kamera terdapat pada masing-masing *node*, yaitu *processing, communication*, dan *control*. Fungsi *processing* adalah semua fungsi dari *Digital Signal Processing* (DSP). Fungsi ini adalah fungsi utama dari keseluruhan sistem, dan ini terletak pada *processing unit*. Fungsi ini dapat didistribusikan ke *node* yang bekerja sama, karena kelompok *node* dapat bekerja pada area yang sama (*overlap*) dan memproses *task* yang sama. Fungsi *communication* adalah semua proses yang berhubungan dengan kebutuhan komunikasi antar *node* atau dengan pusat kontrol. Fungsi ini terdapat pada *communication unit*. Pendekatan untuk pembagian fungsi ini masuk akal dan didukung oleh fakta bahwa *controlling* dan *communication* memiliki sifat kurang terdistribusi.

Arsitektur jaringan sistem kamera pintar dapat menggunakan berbagai macam protokol. Secara umum, kamera pintar memiliki kesamaan dalam *ad hoc network*. Tidak semua *node* perlu terhubung dengan *node* yang lainnya, apalagi jika jaringannya sangat besar. *Protocol stack* pada *node* jaringan kamera pintar memiliki 4 lapisan, yaitu *physical, data link, network,* dan *application layer*. *Physical layer* dapat berupa jaringan kabel atau nirkabel. Pada kamera pintar konvensional masih menggunakan jaringan kabel, namun sekarang sudah banyak yang menggunakan jaringan nirkabel. Hal ini merupakan tantangan tersendiri dalam segi kerentanan keamanan. *Data link layer* sangat penting untuk mengamankan komunikasi kamera pintar. Bukan hanya mengontrol akses dan deteksi kesalahan, tapi juga dalam hal pengoperasian jaringan kamera pintar karena jumlah *node* semakin banyak, dan kebutuhan akses yang merata ke seluruh jaringan. *Network layer* dapat mengikuti beberapa teknik. *Node* selain berfungsi sebagai *end-device*, juga dapat berfungsi seperti *router* pada *multihop communication paths*. *Application layer* pada jaringan kamera pintar berkaitan dengan manajemen tugas dan distribusi, serta kolaborasi antar *node* yang ada.

III. SECURITY ANALYSIS

Perangkat apa pun yang memiliki koneksi internet rentan diretas, terutama perangkat IoT, karena ukurannya kecil sehingga kekurangan kekuatan pemrosesan yang cukup untuk menangani enkripsi yang besar. Peretas akan menargetkan perangkat itu sendiri, data, atau diam sampai perangkat terganggu. Ketika data kita disimpan di *cloud*, kita tidak memiliki kendali atas data kita sendiri, siapa yang menyimpannya atau di mana ia disimpan. Salah satu masalah privasi data *cloud* utama adalah siapa memiliki akses ke data. Kita mungkin melihatnya dari perangkat seluler, tetapi pusat penyimpanan cloud dapat ditemukan di negara lain seperti AS, Eropa atau Asia. Jika kita memutuskan untuk beralih penyedia *cloud*, tidak ada jaminan mereka akan memusnahkan data dengan baik atau membantu bermigrasi ke *cloud* baru. Berikut adalah jenis-jenis serangan yang memungkinkan untuk dilakukan pada kamera pintar.

A. Man In The Middle

Kerentanan yang paling sering ditemukan adalah kerentanan terhadap serangan *man-in-the-middle*. Protokol yang bernama *Address Resolution Protocol* (ARP) bisa digunakan sebagai langkah pertama untuk menghadapi serangan jenis seperti ini. Semua perangkat yang memiliki akses ke kamera memiliki tabel ARP. Isi dari tabel ARP adalah rekaman semua IP *address* dan MAC *address* yang ada. Pada kerentanan jenis ini tidak diperiksa lagi validasi MAC *address* yang dikirim kembali oleh alamat tujuan yang sebenarnya sudah benar [6].

B. Denial of Service

Komputer yang melakukan serangan dapat memposisikan diri sebagai *man-in-the-middle* dengan mudah. Ini merupakan masalah dalam potensi kebocoran data. Memang gambar yang dikirim dari kamera ke perangkat pasti terenkripsi, jadi mungkin orang berpendapat bahwa risiko ini tidak bahaya. Tapi saat ada *man-in-the-middle*, serangan apa pun dapat dilakukan. Serangan yang berhasil salah satunya adalah *Denial of Service* (DoS). Serangan ini bisa memblokir penerima pesan yang menerima gambar dari kamera. Serangan ini adalah serangan langsung setelah adanya *man-in-the-middle* [6].

Sistem jaringan secara umum terdapat beberapa persyaratan keamanan khusus. Informasi tidak hanya terdapat pada *end-device*, namun terdapat juga pada saat transmisi jaringan.

Kamera pintar yang baik adalah yang mampu menjaga kerahasiaan data penggunanya. Kerahasiaan data adalah kemempuan sistem untuk memastikan bahwa tidak ada pihak lain yang mengetahu informasi yang diperoleh, dalam hal ini berarti informasi yang terdapat pada masing-masing *node*. Untuk mencegah hal ini, terdapat beberapa cara yang bisa dilakukan. Kriptografi bisa membantu menjaga kerahasaian data dengan melakukan enkripsi data sebelum transmisi dan mendekripsinya kembali setelah penerimaan. Namun, enkripsi data ini membutuhkan banyak sumber daya dari masing-masing *node* pada kamera pintar. Biasanya tergantung kompleksitas dan sensitivitas informasi yang diperoleh.

Kamera pintar juga harus menjaga integritas data. Integritas data adalah data yang dikirimkan dari suatu *node* sama dengan yang diterima oleh *node* lainnya. Ada kemungkinan bahwa di tengah-tengah transmisi, data bisa berubah. Hal ini memungkinkan jika ada *middle-man-attack.* Jadi data yang dikirimkan dan yang diterima berbeda. Dalam kriptografi, kunci publik tidak dilindungi, berbeda dengan kunci *private*. Sehingga, mungkin bagi seseorang untuk memiliki kunci enkripsi publik, namun dia tidak memiliki akses ke informasi yang didekripsi pada informasi yang dikirimkan kecuali memiliki kunci *private*.

Kamera pintar juga dapat menjaga pembaruan data, artinya sistem dapat mendeteksi bahwa data yang dikirimkan bukan data lama yang diputar ulang kembali oleh orang jahat. Hal ini berbeda dengan integritas data, adanya serangan memungkinkan untuk memutar ulang kembali data yang pernah dikirimkan dengan cara yang tidak dapat dideteksi oleh mekanisme integritas data. Contohnya, ada serangan yang menghalangi komunikasi dan mengirimkan ulang data yang sebelumnya dari *node* yang sama, bisa melewati pemeriksaan integritas data karena datanya valid. Namun, data tersebut bukanlah data yang terbaru karena data tersebut sudah pernah dikirimkan sebelumnya.

Peer authentication adalah mengautentikasi setiap *node* yang terhubung. Hal ini penting untuk mencegah serangan dengan memasukkan *node* yang tidak valid. Kamera pintar biasanya beroperasi terus-menerus dan tidak terdapat *downtime* untuk penambahan *node* dan pemrograman ulang jaringan. Jadi dibutuhkan untuk menambahkan, menghapus, atau mengubah *node* dan topologi jaringan selama operasi sistem.

Serangan yang sangat umum dilakukan adalah DoS (*Denial of Service*). Serangan ini tidak bertujuan untuk mengakses atau mengubah informasi, namun untuk mencegah operasi jaringan yang biasa dilakukan. Serangan dilakukan dengan ketentuan *traffic* yang berlebihan atau permintaan layanan. Sistem kamera pintar memiliki persyaratan operasi *real-time* yang

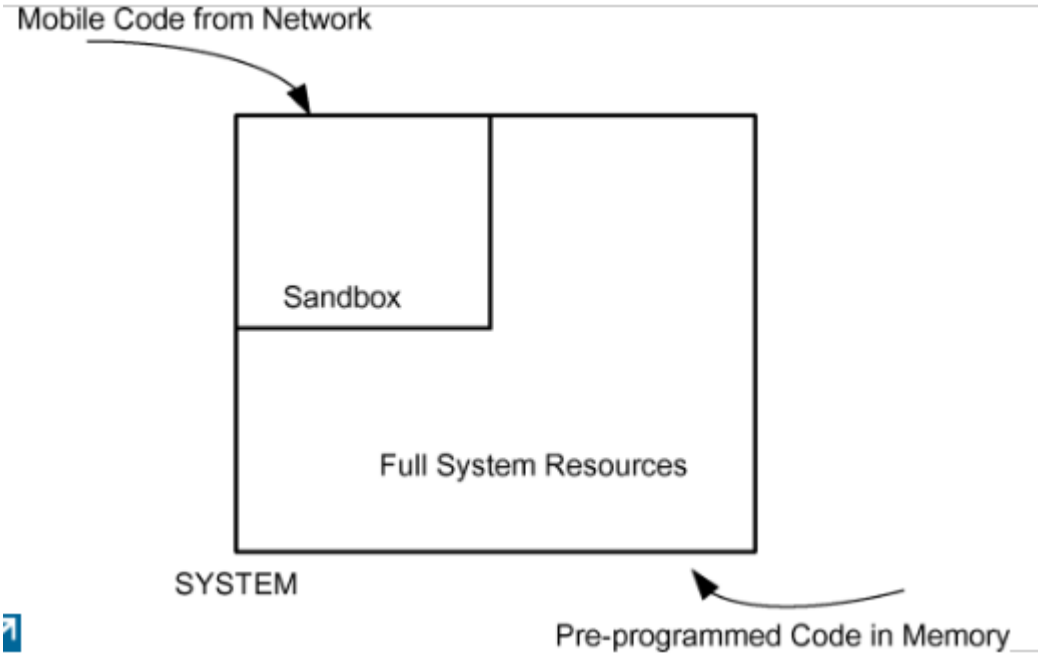
membuat mengarah ke diagnosis dan pencegahan serangan DoS, yang membuat sistem berhenti berfungsi atau menyebabkan masalah pada operasi yang sedang dijalankan [6]. Kita harus memperhatikan semua level, bukan hanya level tertentu. Karena serangan DoS sering ada pada kerentanan protokol jaringan yang muncul dari intensitas untuk memperkuat keamanan sistem. Mekanisme keamanan yang dibuat melibatkan enkripsi yang membutuhkan sumber daya yang besar. Serangan DoS kemungkinan akan menyerang di bagian enkripsi, dan operasi sistem akan terkena akibat yang sangat besar. Oleh karena itu, kita perlu mencegah serangan DoS. Hal ini dapat dicapai dengan implementasi protokol yang dilindungi dari serangan yang memiliki *demand* berlebih pada tahap enkripsi.

Pada umumnya, kamera pintar lebih sering menangkap dan merekam gambar. Penggunaannya biasanya untuk hal-hal sensitif seperti wajah orang, isi rumah, dan informasi sensitif lainnya. Maka, kita perlu untuk memastikan perlindungan informasi sensitif seperti di atas. Jika kerahasiaan data terletak pada sistem, kita juga harus memperhatikan perlindungan nilai aktual dari indormasi itu sendiri. Kebutuhan privasi berbeda dengan kebutuhan lainnya, yang data sering terdapat proteksi untuk melawan operator yang legal. Untuk itu, sebaiknya tidak langsung diizinkan informasi gambar apa pun untuk keluar dari *node* kamera. Hal ini sering terjadi pada kamera pintar yang sepenuhnya beroperasi sendiri, dan memiliki kebutuhan sumber daya yang minimal. Tapi, ini tidak selalu terjadi karena beberapa jaringan dari kamera pintar memungkinkan transmisi yang selektif dari video yang direkam. Jika kamera pintar menggunakan sumber daya dengan selektif, maka akan terlihat pada pilihan gambar yang memenuhi kriteria privasi untuk ditransmisikan. Enkripsi yang selektif dan memiliki banyak level dari data yang dienkripsikan adalah cara yang cukup tepat untuk menangani masalah privasi ini. Jadi, pengguna dengan tingkat masing-masing diberikan kemampuan yang berbeda untuk mengakses ke bagian informasi yang ditangkap atau direkam.

Node kamera pintar biasanya sering diletakkan di tempat publik. Maka dari itu, sangat rentan untuk menjadi target kejahatan. *Tamper resistance* adalah kemampuan sistem untuk mempertahankan sifat keamanannya jika sebagian atau keseluruhan diserang. Perlawanan terhadap serangan fisik dan *side-channel* merupakan kebutuhan yang cukup penting. Serangan *side-channel* tidak didasarkan pada kerentanan logis dan operasi algoritma, namun terhadap tingkat kebocoran informasi pada tingkat fisik sistem, contohnya informasi lokasi. Serangan fisik secara langsung, misalnya pada lensa kamera, dapat mempengaruhi kualitas video yang direkam. Serangan fisik dapat dimulai terhadap *node* yang mana saja. Manipulasi fisik sebuah *node* dapat mengakses bagian tertentu, mendapatkan informasinya, atau mempengaruhi operasi

kamera secara langsung. Serangan fisik dapat dideteksi menggunakan *hardware* yang dirancang khusus beserta *software*-nya. Saat *hardware* ini mendeteksi adanya serangan, maka akan membuat sistem tidak dapat dioperasikan secara keseluruhan. Ketika serangan fisik terdeteksi, lebih baik *node* berhenti beroperasi daripada terus beroperasi namun informasi yang dikirim terancam. Sebagian serangan fisik ditujukan ke sumber daya, misalnya pada baterai yang dilemahkan secara sengaja. *Sensing unit* juga memiliki kerentanan terhadap serangan fisik. Misalnya serangan kerusakan terhadap sensor cahaya. DSP yang ada pada *processing unit* harus bisa mendeteksi dan mengontrol pola yang tidak wajar pada gambar yang direkam, terutama dari *node* lain yang berdekatan namun masih sekelompok. Sedangkan, serangan *side-channel* biasanya digunakan untuk mengetahui kunci yang tersimpan pada sebuah *node*. Serangan analisis elektromagnetik juga dapat dilakukan, dengan cara mengungkapkan informasi rahasia dengan mengukur radiasi elektromagnetik yang dipancarkan oleh kamera pintar [1].

Semakin rumit *software* yang terdapat pada *node* kamera pintar, semakin besar kerentanan keamanannya. Hal ini disebabkan karena kamera pintar melakukan pemrosesan video, yang membutuhkan kompleksitas yang tinggi. Walaupun performansi adalah target utama, namun yang lain tidak dapat terabaikan begitu saja. Kita butuh memilih *software platform* yang menyediakan mekanisme kamanan yang efisien untuk menghindari serangan. Mayoritas dari *embedded system* menggunakan pemrograman C/C++, yang memiliki efisiensi tinggi namun perlindungan yang terbatas terhadap serangan. Pada level *network*, sangat memungkinkan adanya serangan *software* dengan virus yang dapat menyebar ke sebagian besar *node*. Maka dari itu, penting untuk mempertimbangkan pemrograman yang aman. Kerentanan dapat dibatasi dengan melakukan pemrograman ulang (memperbarui) *node* kamera pintar. Kenyataannya, *node* butuh kemampuan di-*upgrade* dan diprogram ulang saat operasi berlangsung. Ini dapat memodifikasi *task* tertentu pada *node* untuk dieksekusi, untuk membenarkan *bug*, atau untuk meng-*install* versi terbaru dari *software node*. Ini adalah kerentanan paling penting pada kamera pintar, karena kemungkinan serangan pada bagian ini akan membuat bagian penting dari sistem tidak dapat dioperasikan. Komunikasi *node* harus dikaitkan dengan protokol enkripsi yang kuat. Di dalam *node*, ada beberapa teknik untuk meningkatkan keamanan, misalnya *code-signing* [1]. Atau dengan *sandbox*, yaitu membatasi penggunaan *mobile code* hanya untuk bagian *software* yang tidak akan menimbulkan risiko keamanan yang serius, seperti gambar di bawah ini.



Gambar 2 Sandbox

Sumber: https://ieeexplore.ieee.org/document/4653064

Privasi pada kamera pintar juga sangat penting, karena kamera pintar biasanya digunakan untuk mengawasi orang atau mendapatkan informasi sensitif lainnya. Tingkatan perlindungan privasi ada dua level [1], yaitu:

1. Melindungi privasi dari penyerang yang memungkinkan
2. Melindungi privasi bahkan dari pengguna yang legal di dalam sistem

Dalam beberapa implementasi sistem, terkadang informasi video butuh untuk meninggalkan *node*. Jika transmisi ini dienkripsi, maka tetap akan ada risiko terkait privasi yang mengakses informasi video tersebut. Kita bisa melakukan pencegahan dengan pengenalan selektif dan enkripsi bagian gambar yang sesuai. Gambar bisa dienkripsi menggunakan kunci level satu, lalu kunci level dua digunakan untuk mengenkripsi seluruh sinyal. Jadi pengguna yang hanya memiliki kunci level dua tidak memiliki akses ke bagian sensitif gambar.

Komunikasi yang terenkripsi antar *node* memerlukan kunci enkripsi yang sesuai untuk masing-masing *node* tersebut. Penting untuk membentuk dasar komunikasi yang aman. Setelah kunci diatur dengan aman, sebagian besar kerahasiaan informasi dapat terjamin. Metode enkripsi yang digunakan ini menentukan tingkat keamanan. Kriptografi kunci publik adalah

yang paling efektif karena untuk mengenkripsi komunikasi antar *node* menuntut adanya komputasi. Namun, kriptografi kunci publik membutuhkan biaya yang tinggi.

Enkripsi *poit-to-point* lebih aman, namun membutuhkan memori yang lebih besar untuk menyimpan semua kunci. Pembaruan data biasanya dapat dicapai melalui komunikasi yang berhasil dienkripsi. *Watermarking digital* bisa digunakan untuk mencapai pembaruan data lebih lanjut, untuk peningkatan keamanan. Dengan menandai informasi gambar atau video menggunakan data waktu, tanggal, tempat, maka semakin sulit bagi penyerang untuk membuat sinyal video yang valid.

Serangan DoS bisa terdapat pada berbagai lapisan protokol (*physical, link, network*) dari hubungan antar *node*. Serangan DoS secara fisik ini sulit untuk sistem kamera pintar dengan kabel, namun merupakan ancaman besar untuk jaringan nirkabel. Oleh karena itu, jaringan kamera pintar lebih aman dengan menggunakan sambungan kabel daripada nirkabel. Serangan yang paling memungkinkan untuk sistem jaringan nirkabel adalah gangguan pada frekuensi komunikasi. Serangan ini akan membatasi transmisi radio, sehingga komunikasi menjadi lebih sulit. Kerentanan tinggi terdapat pada komunikasi di frekuensi tetap. Namun, bisa dicegah dengan *spread-spectrum* untuk komunikasi, yang menyebarkan sinyal komunikasi di berbagai frekuensi. Jadi gangguan frekuensi akan lebih tahan. Pada *link layer* juga biasa ditargetkan oleh serangan DoS. Serangan akan mencoba mengeksploitasi kerentanan protokol pada *link layer* dan dapat menyebabkan kesulitan komunikasi. Misalnya adanya tabrakan karena *frame* yang sama dikirim secara bersamaan. Hal ini akan menyebabkan transmisi yang dilakukan berulang kali, dan akan menyebabkan terbuangnya energi. Serangan DoS pada *network layer* menargetkan setiap node pada jaringan, karena semua *node* berfungsi sebagai *routing*. Sementara pada jaringan terpusat, fungsi *routing* hanya dilakukan oleh beberapa *node* tertentu. Serangan mungkin untuk memaksa *node* melakukan *routing* yang salah. *Misrouting* dapar digunakan untuk menyebabkan *flooding* dengan mengarahkan paket ke tujuan tertentu [6].

IV. KESIMPULAN

Keamanan jaringan kamera pintar sangat penting untuk dipertimbangkan, karena informasi-informasi yang terdapat pada kamera pintar biasanya bersifat sensitif. Keamanan harus sangat dipertimbangkan saat tahap perancangan dan desain kamera pintar ini. Kemaanan tidak bisa dengan mudah ditambahkan di tengah-tengah pembuatan, atau ditambahkan ke sistem dan protokol sebelumnya. Keamanan ini harus dirancang dari awal. Sistem keamanan dengan kerentanan performansi rendah itu memungkinkan. *Node* pada kamera pintar lebih bisa diandalkan daripada *sensor node*. Kebutuhan keamanan pada *node* dan *network* saling melengkapi, namun pasti ada perbedaan mana yang lebih kuat antara keamanan *node* atau *network*. Oleh karena itu, privasi dan keamanan ini merupakan bagian yang sangat penting untuk kamera pintar karena melibatkan informasi pribadi para penggunanya.

REFERENSI

[1] D. N. Serpanos and A. Papalambrou, "Security and Privacy in Distributed Smart Cameras," in Proceedings of the IEEE, vol. 96, no. 10, pp. 1678-1687, Oct. 2008.

[2] A. A. Zarezadeh and C. Bobda, "Enabling communication infrastructure and protocol on embedded distributed smart cameras," 2011 Fifth ACM/IEEE International Conference on Distributed Smart Cameras, Ghent, 2011, pp. 1-6.

[3] N. Ozay, U. Topcu, R. M. Murray and T. Wongpiromsarn, "Distributed Synthesis of Control Protocols for Smart Camera Networks," 2011 IEEE/ACM Second International Conference on Cyber-Physical Systems, Chicago, IL, 2011, pp. 45-54.

[4] M. Happe, Y. Huang and A. Keller, "Dynamic protocol stacks in smart camera networks," 2014 International Conference on ReConFigurable Computing and FPGAs (ReConFig14), Cancun, 2014, pp. 1-6.

[5] J. Liranzo and T. Hayajneh, "Security and privacy issues affecting cloud-based IP camera," 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, NY, 2017, pp. 458-465.

[6] K. Boyarinov and A. Hunter, "Security and trust for surveillance cameras," 2017 IEEE Conference on Communications and Network Security (CNS), Las Vegas, NV, 2017, pp. 384-385.

[7] J. Bugeja, D. Jönsson and A. Jacobsson, "An Investigation of Vulnerabilities in Smart Connected Cameras," 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Athens, 2018, pp. 537-542.

[8] J. Valente, K. Koneru and A. Cardenas, "Privacy and Security in Internet-Connected Cameras," 2019 IEEE International Congress on Internet of Things (ICIOT), Milan, Italy, 2019, pp. 173-180.

[9] James Pierce and CITRIS. 2019. Smart Home Security Cameras and Shifting Lines of Creepiness: A Design-Led Inquiry. In *Proceedings of CHI '19: CHI Conference on Human Factors in Computing Systems (CHI '19), May 04, 2019, Glasgow, Scotland UK*. ACM, New York, NY, USA.