# Taksonomi Tinjauan Keamanan Pada Jaringan IP Camera

**Slamet Indriyanto[1], Budi Rahardjo[2]**
[1]Jurusan Teknik Elektro UIN Sunan Gunung Djati Bandung
Jl. A.H. Nasution No.105 Bandung, Jawa Barat, Indonesia
[2]Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung
Jl. Ganesha No. 10 Bandung, Jawa Barat, Indonesia
slamindriyanto@gmail.com[1], br@paume.itb.ac.id[2]

***Abstrak –*** *IP camera adalah jenis kamera video digital yang biasa digunakan untuk pemantauan keamanan dan dapat mengirim dan menerima data melalui jaringan komputer dan internet. Walaupun webcam juga dapat melakukan hal ini, namun istilah "IP Camera" atau "Network Camera" biasanya hanya digunakan untuk sistem pengawasan keamanan. IP ca-mera memanfaatkan jaringan network TCP/IP untuk mentransmisikan data nya. Berbeda dengan Web Cam (Web Camera) yang memerlukan PC/komputer dengan software untuk dapat digunakan, IP Camera dapat langsung terkoneksi dengan switch / hub dalam jaringan network TCP/IP dan dapat diakses online via internet melalui laptop, handphone, tablet dan mobile devices. Beberapa tahun terakhir, terdapat peningkatan jumlah penggunaan IP Camera yang signifikan di berbagai tempat, termasuk market, mall, farmasi, bioskop, sekolah dan tempat umum lainnya. Dengan penggunaan yang tersebar luas, keamanan dari IP camera ini muncul menjadi masalah yang penting dan perlu untuk dipelajari secara detail. Dengan terhubungnya kamera dengan internet maka meningkatkan resiko keamanan pada perangkat IP camera ini. Untuk itu tinjauan mengenai beberapa ancaman dan serangan yang mungkin terjadi pada jaringan IP camera perlu dilakukan. Pada paper ini secara umum akan membahas mengenai kerentanan pada jaringan IP camera dan ancaman yang mugkin terjadi.*

***Kata kunci****: IP Camera, Keamanan, Internet*

## 1. Pendahuluan

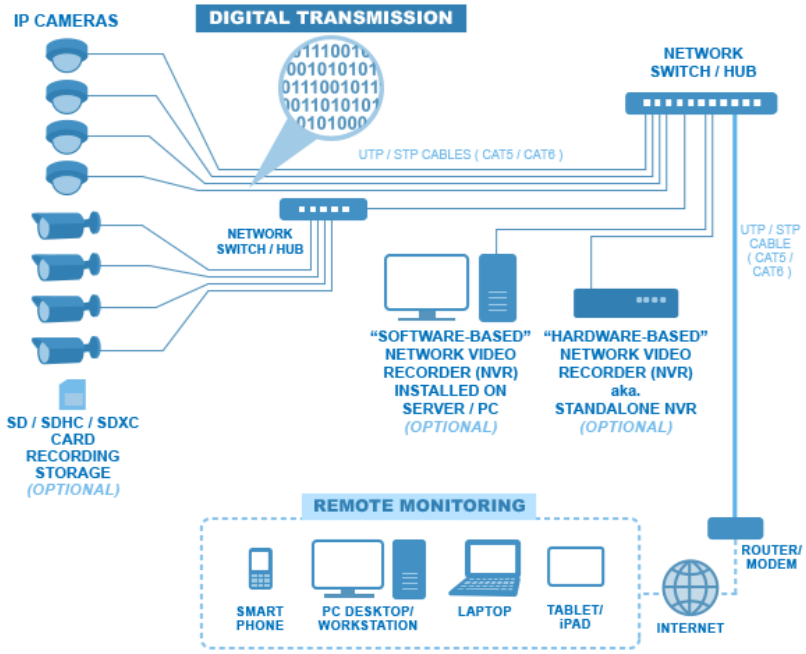
IP camera adalah jenis kamera video digital yang biasa digunakan untuk pemantauan keamanan yang dapat mengirim dan menerima data melalui jaringan komputer dan internet. Walaupun *webcam* juga dapat melakukan hal ini, namun istilah IP Camera atau *Network Camera* biasanya hanya digunakan untuk sistem pengawasan keamanan [1]. IP camera memanfaatkan jaringan/*network* TCP/IP untuk mentransmisikan datanya. Berbeda dengan *WebCam* (*Web Camera*) yang memerlukan PC/komputer dengan *software* untuk dapat digunakan, IP Camera dapat langsung terkoneksi dengan *switch / hub* dalam jaringan TCP/IP dan dapat diakses *online* via internet melalui *laptop, handphone, tablet* dan *mobile devices* [2].

IP Camera sebagai bagian dari sistem pemantauan CCTV atau *Video Surveillance* telah sangat luas digunakan untuk kebutuhan komersial, bisnis, perkantoran, industri, hingga pemantauan skala besar seperti *Traffic* dan *City-Wide Video Surveillance* yang merupakan komponen penting dari *Smart City* program. Secara garis besar terdapat dua teknologi yang biasa digunakan dalam sistem CCTV. Pertama adalah teknologi "*Analog Video Surveillance*" (Analog CCTV) yang menggunakan Analog CCTV Camera, dan kedua adalah teknologi "*Network Video Surveillance*" (IP CCTV) yang menggunakan IP Camera. Perbedaan Analog CCTV dengan IP CCTV atau IP camera adalah pada signal yang ditransmisikan dari kamera. Sistem CCTV Analog menggunakan transmisi sinyal analog via kabel coaxial, sedangkan sistem IP CCTV dengan IP camera menggunakan transmisi sinyal digital melalui jaringan TCP/IP (*Transmission Control Protocol / Internet Protocol*). Dengan penggunaan jaringan TCP/IP ini, sinyal video dan audio dari kamera dapat ditransmisikan melalui berbagai macam metode dan teknologi seperti *Fiber*

*Optic Networks*, jaringan kabel *Unshielded Twisted Pair* (UTP)/*Shielded Twisted Pair* (STP) *Category 5* (Cat5) atau *Category 6* (Cat6) dalam *Local Area Network* (LAN), hingga *Wireless Local Area Network* (WLAN) dengan *Point-to-Point* (P2P) dan *Point-to-Multipoint* (P2M) *Wireless Communication* [2].

## 2. Overview IP Camera

IP camera merupakan perangkat kunci untuk sistem video *surveillance*. *Security* dan *privacy* pada perangkat ini penting dan diperlukan untuk dipelajari secara detail. Dengan integrasi terbaru dari *cloud support* ke dalam IP camera *surveillance system*, transmisi video ke *remote cloud server* pihak ketiga meningkatkan resiko pada keamanan multimedia. Meskipun ditemukan beberapa kerentanan, kajian akademis dari masalah ini belum dipublikasikan untuk ilmu pengetahuan [3].




Gambar 1. *Network Video Surveillance System* (IP Camera) [2]

IP camera merupakan tipe kamera video digital yang digunakan untuk sistem pengawas (*surveillance system*), yang dapat mengirim dan menerima data via jaringan komputer. IP camera menawarkan banyak keuntungan yang berkontribusi untuk penggunaan yang luas. Perangkat ini mendukung audio dua arah dan *user* dapat berinteraksi dengan apa yang dilihat oleh kamera. Beberapa IP camera mendukung fungsi *pan, tilt* dan *zoom* (PTZ) dan untuk *wireless camera* dapat di pindah kemanapun dalam jaringan. IP camera memiliki *processing node* yang mengizinkan pemrosesan video dilakukan pada IP camera. *Remote access* dan *live* video dapat dilihat pada komputer, *smart phone* atau perangkat lain. IP camera menawarkan keamanan transmisi data melalui enkripsi dan autentikasi [3].

*Surveillance system* memiliki manfaat yang besar dan sangat diperlukan untuk kehidupan saat ini. Perangkat ini berfungsi untuk membantu mencegah pencuri dan *vandalisme* pada tempat publik maupun *private*, mencegah terjadinya tindak kekerasan dan kriminal, melindungi anak-anak dan bahkan meningkatkan *image* dari *customer* dan tingkat kepercayaan untuk para *vendor*.

Saat ini, semua *end-user* dapat membeli perangkat *surveillance* dengan harga yang cukup murah untuk menjamin keamanan di rumah maupun tempat bisnisnya. Namun, yang menjadi pertanyaan besar adalah bagaimana cara mengamankannya. *Security* dapat di karakterisasi dengan persamaan sederhana yaitu: adanya kemudahan/celah untuk diserang dan adanya musuh

ISBN: 978-623-7036-34-0

yang beresiko pada keamanan. Jadi pertanyaan pertama yang perlu dijawab adalah siapa musuh yang mungkin tertarik untuk berbuat jahat pada sistem. Musuh yang berpotensi untuk menyerang bisa bervariasi, dari pencuri sampai *hacker*. Terlihat jelas bahwa kombinasi antara jenis musuh ini akan sangat berbahaya. Jadi, suatu IP Camera secara tidak langsung dapat melindungi *user* untuk melawan pencuri. Tetapi jika pencuri bekerjasama dengan *hacker*, apakah kamera akan bisa melindungi dengan baik? Ketika terdapat dua jenis musuh, jika perangkat yang dimiliki juga memiliki kemudahan untuk diserang, maka terdapat resiko pada keamanan. Jadi pertanyaan selanjutnya yaitu apa kelemahan dari IP kamera? Dilihat dari perangkat yang mengirim informasi melalui Internet [4].

### 2.1. Jenis IP Camera

IP Camera terdiri dari dua jenis [1] yaitu:

1. IP Camera terpusat
   Jenis IP Camera ini memerlukan pusat *Network Video Recorder* (NVR) untuk merekam video dan manajemen alarm.
2. IP Camera desentralisasi
   Jenis IP kamera CCTV ini tidak memerlukan pusat NVR karena kamera telah memiliki fungsi perekam *built-in* sehingga dapat merekam langsung ke media penyimpanan seperti SD card, NAS (*Network Attached Storage*), komputer atau server.

IP Camera terpusat pertama dirilis pada tahun 1996 oleh Axis *Communications* dan dikembangkan oleh Martin Gren dan Carl-Axel Alm. IP Camera tersebut diberi nama Axis NetEye 200 dengan menggunakan *web server* kustom internal pada kamera. Pada akhir tahun 1999, Linux mulai digunakkan untuk mengoperasikan IP kamera tersebut. Axis juga merilis dokumentasi API tingkat rendah yang disebut "VAPIX", yang dibangun pada HTTP standar terbuka dan RTSP. Arsitektur terbuka ini dimaksudkan untuk mendorong produsen perangkat lunak pihak ketiga untuk mengembangkan *software* manajemen untuk merekam yang kompatibel. IP Camera desentralisasi pertama dirilis pada tahun 1999 oleh Mobotix dengan menggunakan sistem Linux. Sistem kamera ini tidak memerlukan lisensi software untuk mengatur perekaman video dan alarm. Kamera IP pertama dengan analisis konten video *onboard* (VCA) dirilis pada tahun 2005 oleh Intellio. Kamera CCTV ini mampu mendeteksi banyak *event* yang berbeda, seperti jika sesuatu barang dicuri, seseorang memasuki zona tertentu, atau sebuah mobil yang bergerak ke arah yang berlawanan. IP Camera tersedia dari resolusi 0,3 (VGA) hingga 29 megapiksel. Saat ini telah banyak digunakan IP camera dengan resolusi video HD (*high-definition*) 720p dan 1080p dengan format *widescreen* 16 : 9 [1].

### 2.2. Standar IP Camera

CCTV Analog menggunakan format siaran televisi seperti *Common Intermediate Format* (CIF), NTSC, PAL, dan SECAM. Setiap IP camera dapat memiliki fitur dan fungsi, skema *encoding* video kompresi, protokol jaringan yang tersedia, dan API yang berbeda. Untuk mengatasi masalah standarisasi IP camera ini dibentuklah dua institusi yaitu ONVIF dan PSIA. PSIA didirikan oleh 20 anggota perusahaan seperti Honeywell, GE dan Cisco. Sedangkan ONVIF didirikan oleh Axis Communications, Bosch dan Sony [1].

### 2.3. Perkembangan IP Camera

Pada awalnya IP camera menyimpan video yang ditangkap pada kamera atau lokal komputer yang lain, hal ini mengganggu penggunaan dari IP camera. User harus mengkonfigurasi *storage* dan mengatur *streaming server* untuk mengalirkan video. Sistem IP camera seperti ini cocok digunakan untuk aplikasi *home security* atau disebut UPnP *based Surveillance Camera System* (USCS) [5]. Produk terbaru yang ada dipasaran saat ini yaitu berbasis *cloud* dan *upload* video yang ditangkap oleh kamera dikirim ke *server cloud*. Video tersebut dapat diakses dimanapun melalui internet menggunakan komputer atau *smartphone*. IP camera berkomunikasi dengan *cloud server* dan user menghubungi *cloud server* untuk melihat video yang di *capture*. Pada

ISBN: 978-623-7036-34-0

kondisi normal, tidak ada komunikasi langsung antara user dan IP camera. User tidak perlu khawatir mengenai *storage* atau masalah *streaming* karena ditangani oleh *cloud* [3].

Dengan tersebarnya IP camera secara luas memunculkan persoalan penting yang berkaitan dengan keamanan dari perangkat ini. Banyak user sadar adanya potensi resiko keamanan dari IP camera. Disamping itu, belum cukup banyak pekerjaan dan penelitian yang berkaitan dengan keamanan dari perangkat ini, untuk itu perlu dilakukan penelitian pada *security* dan *privacy* pada perangkat [3].

## 3. Keamanan Pada IP Camera

Karena perangkat video pengawas berlokasi ditempat publik dan adanya interkoneksi berbasis IP diantaranya, menimbulkan meningkatnya ancaman keamanan. Sistem video pengawas (*video surveillance system*) berkaitan dengan informasi rahasia yang sensitif, dan informasi yang terkumpul dapat disalahgunakan oleh orang jahat. Ini dapat menimbulkan pelanggaran privasi yang serius dan ancaman keamanan lainnya. Dijelaskan oleh Chris Wampler [6] bahwa ditemukan kebocoran informasi pada video terenkripsi yang melalui trafik IP di beberapa *codec* yang telah diuji seperti MJPEG, H.264, VP8.

### 3.1. Ancaman Keamanan

Karena keterbukaan perangkat video pengawas dengan jaringan berbasis IP, maka jumlah ancaman keamanan yang muncul bervariasi dalam penyebaran *video surveillance system* [7].

1) *Eavesdropping/Disclosure/Interception*
   Perangkat video pengawas seperti IP Camera, CCTV, DVR, *Video Control Server* dan lainnya, berlokasi di tempat publik yang dapat dijangkau oleh siapapun, dan terhubung dengan jaringan IP. Video yang terkumpul oleh CCTV ditransmisikan ke DVR dan *control server* melalui jaringan IP publik. Pada proses transmisi video yang berisi informasi rahasia itu tidak terlindungi dari akses berbahaya. Jika disadap oleh orang yang tidak berhak dapat menyebabkan ancaman yang serius dan dapat juga digunakan dalam kejahatan lain. Ancaman keamanan ini harus dipertimbangkan dalam pengembangan sistem video pengawas.
2) *Interruption/Communication Jamming*
   Ancaman keamanan ini mengganggu dalam proses pengumpulan informasi video secara normal, hal ini menyebabkan *denial of service* (DoS) untuk respon yang efisien.
3) *Injection and Modification of Data*
   Ancaman keamanan ini memodifikasi data video yang ditransmisikan atau yang disimpan secara ilegal dan menginjeksi data yang tidak asli kedalamnya, hal ini menurunkan keandalan dari informasi video.
4) *Unauthorized Access*
   Akses yang tidak sah mungkin akan merusak keaslian dan validitas dari video yang terkumpul. Hal ini juga menyebabkan pelanggaran dan penyalahgunaan sumber daya dari sistem.
5) *Repudiation*
   CCTV/IP camera mungkin saja menolak pengumpulan/penyediaan video secara *real-time*, kecuali saluran komunikasi yang dipercaya antara perangkat pengawas yang mengumpulkan video dan perangkat penyimpanan video/*control server* tidak ada jaminan.
6) *Illegal Monitoring*
   Adanya orang lain yang bisa memonitor video yang ditransmisikan dari CCTV/IP camera secara ilegal merupakan pelanggaran. Meskipun *administrator* yang berwenang menjaga informasi video yang terkumpul, dia tidak diizinkan untuk memantau secara langsung dari tempat lain secara pribadi.

### 3.2 Fungsi Keamanan

Berikut ini merupakan tindakan pencegahan dari variasi ancaman yang terjadi:

1) *Privacy Masking*

ISBN: 978-623-7036-34-0

Sebagai video yang dikumpulkan oleh multiple IP camera untuk mengawasi baik itu orang, kendaraan, informasi tempat pribadi dan informasi *privacy-sensitif* lainnya, dibutuhkan sebuah teknologi tepat guna untuk melindungi informasi rahasia dan mencegah ekspos secara ilegal. Teknologi *privacy masking* dikategorikan kedalam dua metode yaitu metode statis dan metode dinamis. Metode *privacy masking statis* melindungi ROI (*Region of Interest*) tetap seperti jendela. Dengan kata lain, metode *privacy masking dinamis* digunakan untuk ROI bergerak termasuk orang, kendaraan bergerak.

2) *User/Device Authentication*
Sebagai perangkat pengumpul video, perangkat penyimpanan video, *video controller*, dan *video service provider* terdiri dari sistem pengawas video yang beroperasi berbasis pada jaringan IP publik, saluran komunikasi yang dipercaya diantara keduanya harus menjadi pertimbangan utama. Selanjutnya juga dibutuhkan metode autentikasi yang aman untuk meng-autentikasi *user* untuk mengakses sistem.

3) *Security Tunneling*
Informasi video ditransmisikan melalui jaringan IP publik, jadi mau tidak mau berpo-tensi terkena akses yang tidak sah. Untuk menyelesaikan masalah yang disebabkan oleh akses tidak sah, maka harus dibuat saluran yang bisa dipercaya antara entitas yang berkomunikasi, dan enkripsi informasi video perlu ditambahkan.

4) *Access Control*
Meskipun administrator terlibat dalam kelompok yang diizinkan untuk memelihara dan mengendalikan informasi video, setiap admin diberikan hak akses yang berbeda-beda. Itu menjamin keamanan dari informasi video dan menjamin keandalan.

5) *Intrusion Prevention*
Teknologi pencegahan gangguan memberikan deteksi gangguan secara *real-time* dan responnya wajib untuk melindungi informasi video dari percobaan akses dari internal/ eksternal, dan mencegah pelanggaran privasi. Teknologi pencegahan gangguan untuk *video surveillance system* dapat dikategorikan kedalam dua metode yaitu metode logikal dan metode fisik. Metode pencegahan gangguan logikal melindungi sumber daya sistem dari serangan yang menggunakan jaringan berbasis IP. Metode pencegahan gangguan fisik melindungi sumber daya sistem dari akses ilegal ke fisik.

6) *Prevention of Forgery*
Fungsi keamanan ini mendeteksi pemalsuan informasi video.

7) *Prevention of Misuse*
Informasi video yang terkumpul melibatkan banyak informasi yang signifikan. Itu berarti jika disalahgunakan dalam aplikasi yang salah, dapat mengakibatkan kerusakan yang tidak terduga [7].

Tabel 1 Hubungan antara ancaman keamanan dan fungsi keamanan [7]

| *Security Threats* / *Security Functions* | *Eavesdropping/ Disclosure/ Interception* | *Interruption/ Communication jamming* | *Forgery* | *Unauthorized access* | *Repudiation* | *Illegal Monitoring* |
|---|---|---|---|---|---|---|
| *Privacy Masking* | v | | v | v | v | |
| *Authentication* | | | v | v | v | |
| *Security Tunneling* | v | | v | v | v | |
| *Access Control* | | | v | v | | v |
| *Intrusion Prevention* | | v | v | v | | |
| *Forgery Prevention* | | | v | | | |
| *Misuse Prevention* | | | | | | v |

ISBN: 978-623-7036-34-0

## 4. Kerentanan Pada IP Camera

Lucian Constantin [8] telah menemukan kerentanan serius pada Foscam *wireless* IP camera yang terhubung dengan Internet. Dengan memanfaatkan kelemahan ini, *attacker* dapat membajak kamera dan merubah *firmware*. Meskipun kamera dipasang di jaringan rumah dan menggunakan alamat IP lokal, ini dapat diakses dari Internet setelah di setting *port-forwarding* pada *home-router*. Fitur ini memungkinkan pemilik kamera untuk terhubung dengan kamera dari manapun. Kenyamanan ini menunjukkan IP camera untuk terhubung ke internet dan ancaman dari luar.

Kerentanan yang lain yang memungkinkan *remote attacker* untuk mengakses *live-streaming* diungkapkan untuk Trendnet IP camera dalam [3]. Pada kasus ini, *firmware binary* Trendnet Wifi IP camera di download dan diuji dengan *binwalk* untuk mengambil jejak *file header* yang ada dalam *file firmware*. Ini memperlihatkan dua paket file terkompresi gzip kedalam *firmware*. Kemudian menggunakan tool linux dasar *dd*, isi dari *firmware* dipotong menjadi potongan kecil dan setelah diekstrak, skrip server pada *file system* minix diperlihatkan. ditemukan file pada folder server yang berisi skrip cgi-bin yang mendapatkan *live-stream* dari kamera. Ini normal, dan ditemukan bahwa meskipun telah menggunakan *password* untuk melindungi kamera untuk semua user, *live-stream* masih tersedia dengan skrip cgi-bin pada folder anony server kamera.

Populer *hack* IP camera yang lain terlihat pada konferensi DefCon'22 dalam [3]. Pada investigasinya, Dropcap IP camera dipisahkan untuk mendapatkan akses ke *root shell* dengan menyerang kabel ke *board* PCB melalui pin UART, memodifikasi dan me *reflash firmware* dengan kode *malicious*. Mereka menemukan bahwa *Dropcap* memiliki *vulnerable version* dari *library* OpenSSL dengan bug *heartbleed*, *busybox version* memiliki *vulnerability* untuk mengendalikan kode eksekusi dan iOS setup app *vulnerable* pada MitM *attack* disebab-kan oleh tidak dilakukannya pengecekan sertifikat SSL. Jenis serangan ini membutuhkan ak-ses langsung ke fisik kamera untuk di *hack*, untuk itu perlu mempertimbangkan lokasi dari IP camera yang dipasang.

Adapun Bogdan Groza [4], melakukan pengembangan keamanan video *surveillance system*, dalam penelitiannya yaitu *framework* untuk *video surveillance* yaitu: *availability*, *accessibility*, dan *authenticity*. Pada framework ini, dimana kamera dapat diakses melalui *remote device*, seperti *mobile phone*, PDA melalui alamat IP. Beberapa kekurangan *security* dari produk yang digunakan yaitu IP camera DCS-900 dan solusi yang diusulkan dengan menggunakan autentikasi kriptografi untuk gambar yang di-*broadcast*.

## 5. Security Model

*Video surveillance system* terdiri dari empat group [7]:

1) VGG (*Video Gathering Group*)
2) VSG (*Video Storage Group*)
3) VCG (*Video Control Group*)
4) VAG (*Video Application Group*)

VGG terdiri dari VGE (*Video Gathering Entity*) berfungsi untuk mengumpulkan informasi video. VSG terdiri dari VSE (*Video Strorage Group*) berfungsi untuk menyimpan infor-masi video yang terkumpul dari VGG. VCG terdiri dari VCE (*Video Control Entity*) berfungsi untuk mengendalikan entitas yang terlibat didalam VGG dan VSG. VAG ke terdiri dari VAE (*Video Application Entity*) untuk memberikan layanan video. Dari sini dapat didefinisikan VSS (*Video Surveillance System*) sebagai berikut:

$$VSS = \{VGG, VSG, VCG, VAG\} \quad (1)$$

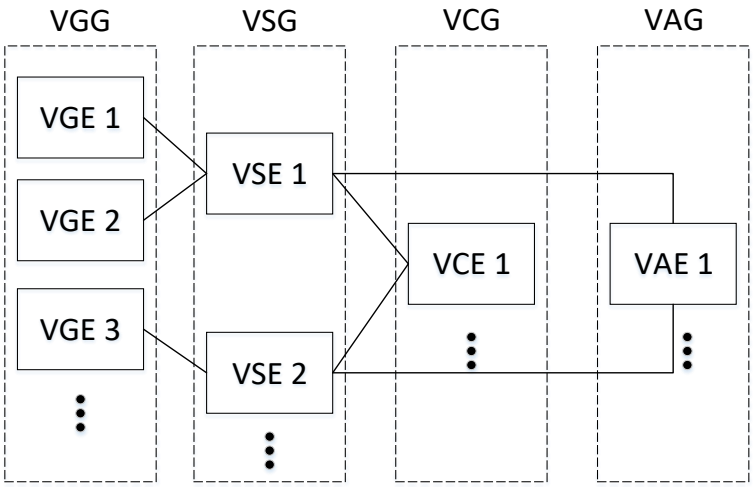
$$VGG = \sum VGE_i, dimana\ 1 \leq i \leq n, n: jumlah\ total\ VGE \quad (2)$$

$$VSG = \sum VSE_i, dimana\ 1 \leq i \leq m, m: jumlah\ total\ VSE \quad (3)$$

$$VCG = \sum VCE_i, dimana\ 1 \leq i \leq k, k: jumlah\ total\ VCE \quad (4)$$

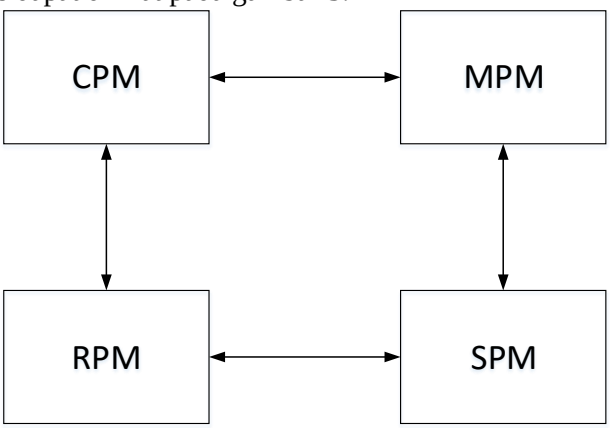
$$VAG = \sum VAE_i, dimana\ 1 \leq i \leq j, j: jumlah\ total\ VAE \quad (5)$$

ISBN: 978-623-7036-34-0




Gambar 2. Model untuk Video Surveillance System [7]

Berdasarkan model untuk sistem video pengawas pada gambar 2, model keamanan untuk sistem video pengawas dapat dilihat pada gambar 3.




Gambar 3. Model keamanan untuk sistem video pengawas [7]

Model keamanan untuk *video surveillance system* terdiri dari empat modul keamanan yaitu:

1) RPM (*Resource Protection Modules*)
2) CPM (*Channel Protection Modules*)
3) MPM (*Misuse Protection Module*)
4) SPM (*Service Protection Module*)

RPM (*Resource Protection Modules*) melindungi sumber daya sistem dari ancaman keamanan internal/eksternal. CPM (*Channel Protection Modules*) melindungi saluran komunikasi untuk pertukaran informasi video dengan aman. MPM (*Misuse Protection Module*) mencegah penyalahgunaan informasi video yang terkumpul. SPM (*Service Protection Module*) melindungi layanan yang disediakan oleh VAE.

Tabel 2 Identifikasi fungsi keamanan yang dijalankan oleh setiap modul keamanan [7]

| Security Modules | Security Function Provided |
|---|---|
| RPM | Privacy Masking<br>Authentication<br>Access Control<br>Intrusion Prevention<br>Misuse Prevention |
| CPM | Privacy Masking<br>Security Tunneling |

ISBN: 978-623-7036-34-0

| | |
|---|---|
| MPM | Access Control<br>Forgery Prevention<br>Misuse Prevention |
| SPM | Authentication<br>Intrusion Prevention<br>Forgery Prevention |

Sebagai perhatian utama dari RPM adalah informasi video dan *surveillance system*, fungsi keamanan oleh RPM harus melindungi sumber daya sistem. Fungsi ini termasuk *privacy masking, authentication, access control, intrusion prevention*, dan *misuse prevention*. Ketika CPM menarik hanya pada proteksi saluran, memberikan *privacy masking* dan *security tunneling*. MPM mencegah penyalahgunaan dari informasi video, itu memberikan *access control, forgery prevention,* dan *misuse prevention*. SPM juga berhubungan dengan penyediaan layanan pendukung *authentication, intrusion prevention* dan *forgery preven-tion.*

Tabel 3 Hubungan antara entitas dan security modules yang telah dijelaskan pada gambar 2 dan 3

| Security Modules / Entities | RPM | CPM | MPM | SPM |
|---|---|---|---|---|
| VGE | v | v | | |
| VSE | v | v | | |
| VCE | v | v | v | v |
| VAE | v | v | v | v |

Berdasarkan tabel 3, setiap entitas harus mengimplementasikan RPM dan CPM. Itu menjamin bahwa proteksi saluran sumber daya diwajibkan pada seluruh sistem. Dengan kata lain, MPM dan SPM diharapkan didukung oleh VCE dan VAE, sejak berhubungan dengan poin spesifik pada pengaplikasian layanan.

Tabel 4 Security functions yang harus dilakukan oleh setiap entitas [7]

| Entitas / Security Functions | VGE | VSE | VCE | VAE |
|---|---|---|---|---|
| Privacy Masking | v | v | v | |
| Authentication | v | v | v | v |
| Security Tunneling | v | v | v | v |
| Access Control | | v | v | v |
| Intrusion Prevention | v | v | v | v |
| Forgery Prevention | v | v | v | |
| Misuse Prevention | | v | v | v |

## 6. Kesimpulan

Pada paper ini telah dilakukan kajian berkaitan dengan tinjauan keamanan pada jaringan IP Camera dalam bentuk taksonomi. Berdasarkan kajian yang telah dilakukan, maka didapat kesimpulan sebagai berikut:

ISBN: 978-623-7036-34-0

- *Video surveillance system* dalam hal ini yaitu IP camera berkaitan dengan informasi rahasia yang sensitif, dan informasi video yang terkumpul dapat disalahgunakan oleh orang yang tidak berkepentingan.
- Variasi ancaman keamanan pada IP camera yang muncul yaitu: *Eavesdropping/ Disclosure/Interception, Interruption/Communication Jamming, Injection and modifycation of data, Unauthorized access* dan *Repudiation*
- Fungsi keamanan yang dapat dilakukan yaitu: *Security masking, User/Device Authentication, Security Tunneling, Access Control, Intrusion prevention, prevention of Forgery dan Prevention of Misuse.*

**Daftar Pustaka**

[1] Stealth.co.id. "*IP Camera"*. [Online]. Available: http://www.stealth.co.id/kamera-cctv/ip-camera/. [Accessed Desember 2016].

[2] Aetherica.com. "IP Camera". [Online]. Available: http://www.aetherica.com/ip_camera.html, [Accessed November 2016].

[3] A. Takeoglu and A.S. Tosun, "Investigating Security and Privacy of a Cloud-Based Wireless IP Camera: NetCam, " in *2015 24th International Conference on Computer Communication and Networks (ICCCN),* 2015, pp. 1-6.

[4] B. Groza, I. Silea, D. Pop, and V.-V. Patriciu, "Towards Developing Secure Video Surveillace System over IP," in *2009 4th International Conference on Internet Monitoring and Protection (ICIMP),* 2009, pp.27-33.

[5] Y. Gu *et al.,* "Design and Implementation of UPnP-Based Surveillance Camera System for Home Security," in 2013 *International Conference on Information Science and Applications (ICISA).* 2013, pp.1-4.

[6] C. Wampler, S. Uluagac, and R. Beyah, "Information Leakage in Encrypted IP Video Traffic, " in 2015 *IEEE Global Communication Conference (GLOBECOM),* 2015, pp. 1-7.

[7] G.W. Kim and J.W. Han, "Security Model for Video Surveillance system," in 2012 *International Conference on ICT Convergence (ICTC),* 2012, pp. 100-104.

[8] Lucian Constantin, "*Widely used wireless IP camera open to hijacking over the internet"*. [Online]. Available: http://www.pcworld.com/article/2033821/security/widely-used-wireless-ip-cameras-open-to-hijacking-over-the-internet-researchers-say.html. [Accessed Desember 201.

ISBN: 978-623-7036-34-0