

REVIEW JURNAL

Monitoring Software for IP-based Video Surveillance System



NAMA : ANDIKA ATMANEGARA PUTRA

NIM : 09011281419055

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

REVIEW JURNAL

International Conference on Computer Systems and Technologies -
CompSysTech'14

Monitoring Software for IP-based Video Surveillance System

Delyan Genkov

***Abstract:** Video surveillance systems become very popular in today's world. Some of them have operators that perform observation, but others rely on some alarm mechanisms for detection of events. There are sophisticated video surveillance software systems, that have video analytic functions, but simple video systems can detect only motion or loss of video signal. There are some vulnerabilities of such systems, including covering or spraying the camera's lenses. Present study presents a software system for detecting anomalies in an IP-based video surveillance, using network monitoring.*

***Key words:** Software system, Video surveillance, Monitoring, Traffic, SNMP.*

A. Pendahuluan

Objektif dari riset yang dilakukan adalah 'sistem pengawasan video' atau bahasa yang sering digunakan adalah sistem pengawasan video melalui CCTV. Alasan author atau penulis memilih objek ini untuk dilakukan riset dikarenakan ketidakadaannya review secara langsung sehingga beberapa kemungkinan terjadi serangan baik perusakan ataupun pembajakan untuk menetralkan penggunaan camera CCTV. Sebagai contoh, pandangan kamera dapat terhalang oleh benda asing, lensanya dapat disemprotkan cairan penghalang, atau bahkan dapat langsung memotong kabel power-nya. Terdapat beberapa software sistem pengawasan yang terbilang canggih, seperti: 'Milestone' dan 'Verint Nextiva', yang dapat mendeteksi event-event tertentu dengan fungsi analisisnya dan mengirimkan beberapa alarm via email, SMS, maupun Panggilan suara atau telepon. Umumnya, platform software-software ini sangatlah mahal. Sistem pengawasan video yang lebih murah biasanya dapat dikonfigurasi untuk memberikan alarm ketika suatu 'gerakan'

terdeteksi atau ketika sinyal video hilang, sehingga perangkat ini lebih cocok digunakan untuk tipe-tipe penyerangan ini.

Hampir keseluruhan sistem pengawasan video modern sudah berbasis IP, yang mana kamera terhubung ke jaringan komputer dan mengirimkan sinyal video dalam paket-paket melalui jaringan sistem komputer dan digunakan untuk perekaman saat melakukan pengawasan. Infrastruktur jaringan inipun dapat digunakan untuk mengirimkan data sekaligus pengawasan video secara terus-menerus. Dalam jurnal ini, diusulkan menggunakan pendekatan untuk memonitor sistem pengawasan video berbasis IP dengan menggunakan metode monitoring jaringan. Protokol monitoring jaringan yang paling populer adalah SNMP (Simple Network Management Protocol).

Dalam aplikasi SNMP secara umum menggunakan satu atau lebih sistem komputer dengan software khusus, yaitu 'manager installed'. Manager memonitor dan mengatur beberapa kelompok jaringan perangkat yang saling terhubung. Perangkat ini haruslah menjalankan modul software khusus yaitu 'Agent', yang merespin request dari software manager. Terdapat 7 jenis definisi pesan dalam SNMP:

- GetRequest: sebuah request dari manager ke agen untuk menerima nilai sebuah variabel atau grup
- SetRequest: sebuah request dari manager ke agen untuk merubah nilai sebuah variabel atau grup
- GetNextRequest: sebuah request dari manager ke agen untuk menemukan variabel-variabel yang bebas dan nilainya
- GetBulkRequest: pengoptimalan versi dari GetNextRequest
- Response: Jawaban dari agen, mengembalikan nilai atau mengkonfirmasi sebuah request
- Trap: Notifikasi asinkron dari agen ke manager terhadap event tertentu
- InformRequest: Mengkonfirmasi sebuah event trap dari manager ke agen

B. Metode

Seperti yang telah sedikit dijelaskan di bagian pendahuluan, metode yang digunakan adalah protokol SNMP. Pendekatan atau metode yang digunakan ini membutuhkan switch network yang mana kamera-kamera IP ini terhubung untuk mendukung protokol SNMP dan memiliki string komunitas read-only yang dikonfigurasi.

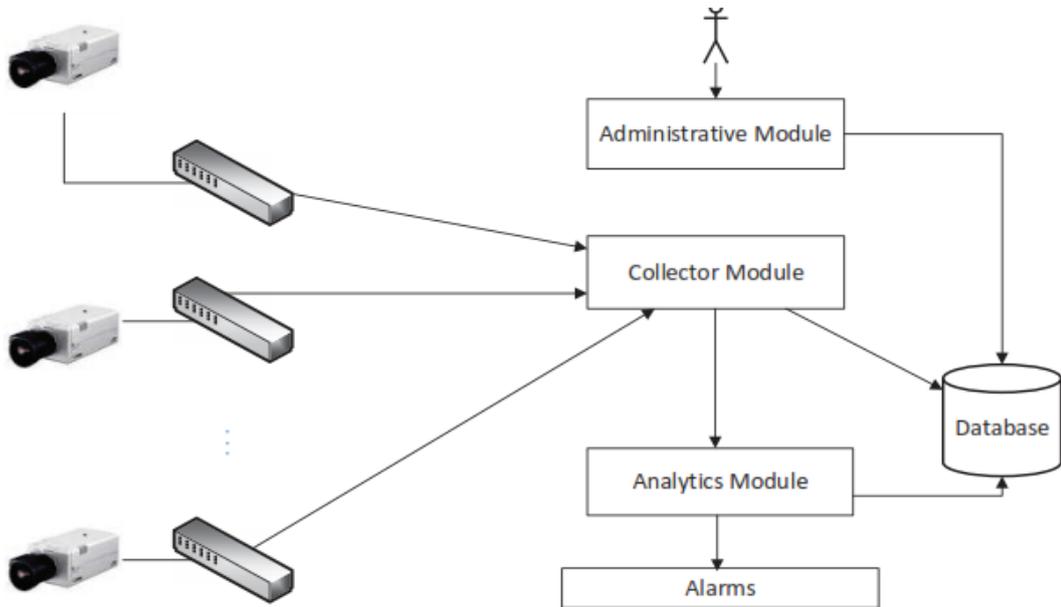
Pada siang hari, level traffic hampir selalu sama dan jika terdapat perubahan pada lingkungan seperti adanya cahaya matahari, awan, kabut, dan lainnya. Perubahan level traffic jaringan mencapai 10-15% dari traffic pada umumnya. Jika lensa kamera tertutup sepenuhnya, atau tertutup benda lainnya, traffic menurun secara signifikan ke level dimana tidak terlihatnya objek seperti di malam hari atau harus menggunakan cahaya inframerah untuk melihat. Jika kamera tertutup oleh benda semi-transparan, level traffic turun seketika sebesar 20-25%. Hal ini berarti perbedaan ini cukup untuk mendeteksi tipe-tipe serangan seperti ini.

Jika penyerang mengganti kabel listrik kamera, memutus kabel network kamera, port switch dimana kamera terhubung merubah statusnya dari up ke down. Perubahan ini dapat dengan mudah didapatkan dengan melalui SNMP. Aplikasi pengembangan untuk memonitor sistem pengawasan video berbasis IP memiliki 3 parameter untuk setiap kamera yang dikonfigurasi:

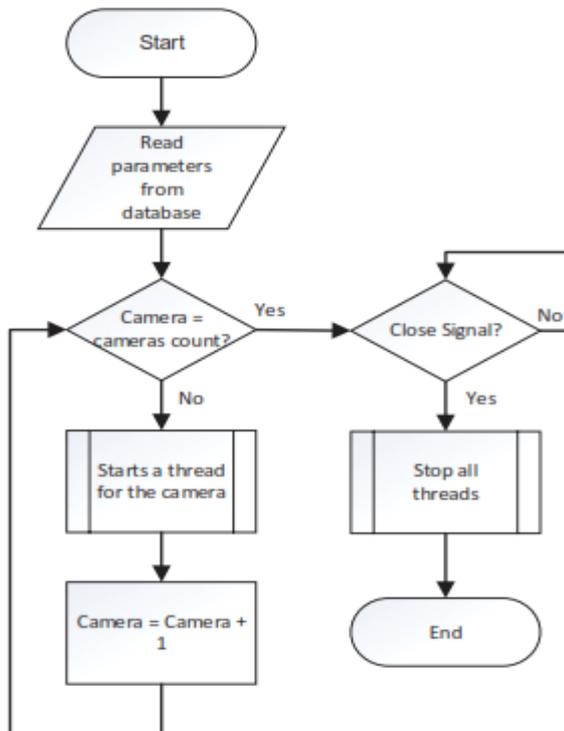
- Setiap kamera yang terhubung menggunakan ICMP (Internet Control Message Protocol). Sebuah paket ICMP dikirimkan ke alamat IP kamera per detik. Untuk setiap kamera sejumlah angka yang terus-menerus tidak terhitung dapat dijadikan penanda untuk berbunyinya alarm
- Status dari port switch (up atau down), dimana kamera terhubung. Ketika port ini down, alarm akan segera berbunyi.
- Level traffic yang masuk dari port ini akan selalu diukur per detik. Ketika sejumlah kecil data masuk diukur dan berbeda hasilnya dengan nilai rata-rata probe untuk satu waktu di hari tertentu akan memicu berbunyinya alarm

C. Struktur Aplikasi

Struktur aplikasi mengandung 4 modul berbeda dan ditunjukkan pada gambar dibawah ini:



Modul-modul bekerja dengan menggunakan algoritma berikut:



Ketika modul mulai membaca parameter-parameter yang dibutuhkan dari database, kamera monitoring, switch dan port yang terhubung, IP address switch, string komunitas SNMP. Kemudian, modul akan memulai urutan yang berbeda untuk setiap kamera monitoring, sehingga meminimalisir kebutuhan untuk menunggu proses selesainya kamera lain. Setelah proses awal ini selesai, layanan akan menjalankan closed loop sampai dengan sinyal close dikirimkan dari sistem operasi. Jika hal ini terjadi, modul akan memberhentikan semua urutan proses dan menyelesaikannya.

Peran utama dalam menghasilkan alarm diberikan ke modul analisis. Hal ini juga merupakan aplikasi layanan multi-threaded, yang mana mengkalkulasi nilai rata-rata untuk seluruh sampel di database dan membandingkannya dengan level traffic yang didapat. Karena penggunaan database yang intens, profil kamera dikalkulasikan dan dituliskan dalam tabel database yang berbeda. Pada tahap ini, kalkulasi ulang dari profil kamera dilakukan secara offline. Ketika beberapa parameter mencapai titik kritis, maka modul akan menghasilkan alarm. Implementasi alarm pada tahap ini adalah sebagai berikut:

- Alarm yang disebabkan kamera tidak terjangkau: ketika beberapa pesan berurut ICMP tidak mendapatkan jawaban
- Alarm yang disebabkan port down: Alarm dihasilkan secara langsung ketika kondisi ini terdeteksi
- Alarm yang disebabkan deviasi profil: Ketika traffic kamera sangat jauh berbeda dengan profil tersimpan
- Alarm untuk recorder: recorder tidak dapat merespon, ruang disk yang terlalu kecil, penggunaan CPU yang memakan banyak memori

Untuk saat ini alarm hanya terindikasi di layar monitor dan menghasilkan suara, namun sangat diharapkan kedepannya sistem dapat mengirimkan alarm via email, SMS, ataupun panggilan suara.

D. Kesimpulan

Pada tahap ini, sistem masih belum bisa mengumpulkan cukup data untuk meningkatkan presisi parameter kamera diantaranya: persentase 'nilai ambang' atau 'nilai batas' untuk menghasilkan sebuah alarm. Hal ini menyebabkan terjadinya beberapa alarm false-positive. Dan juga dimungkinkan untuk menggabungkan antara collector dan modul analisis sehingga menghasilkan pengurangan operasi database dalam satu waktu. Namun membagi modul, menjadi mungkin untuk menjalankan kedua aplikasi dalam komputer yang berbeda sehingga terjadi keseimbangan antara pemakaian CPU dan memori.