Manajemen Keamanan pada Jaringan Komputer : A Survey

Deri Andany, Sistem Komputer, Universitas Sriwijaya, deriandany0901@gmail.com

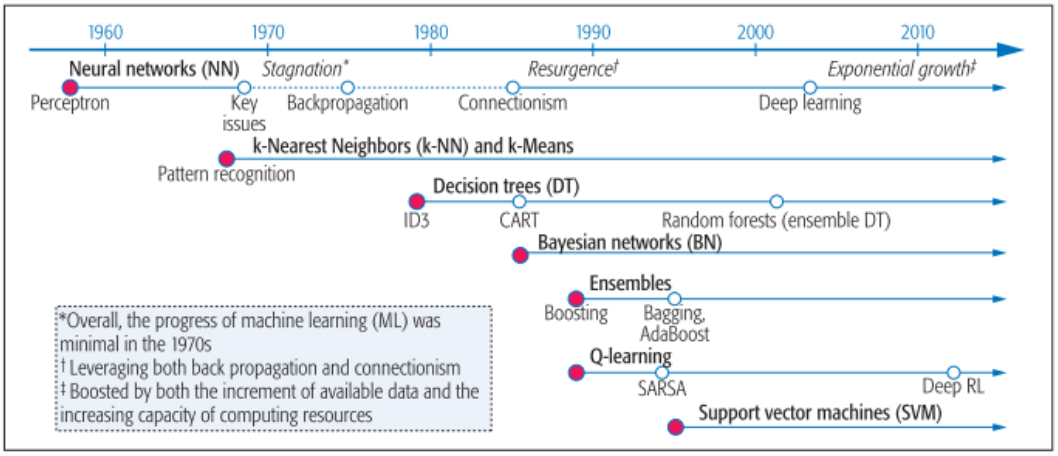
1. ABSTRAK

Selama dekade terakhir, sejumlah besar upaya telah diinvestasikan untuk merancang solusi manajemen yang lincah dan adaptif dalam mendukunng otomasi jaringan komputer. Peralatan keamanan seperti sistem pencegahan intrusi merupakan pelengkap penting untuk manajemen keamanan. Mereka mengurangi kesulitan manajemen jaringan dengan memberikan alarm yang sesuai dengan serangan yang berbeda, bukan inspeksi paket lalu lintas mentah. Tetapi ada banyak alarm palsu karena mekanisme kerjanya, yang sangat mengurangi kegunaannya. Oleh karena itu, manajemen keamanan yang dibutuhkan dalam jaringan untuk meningkatkan efisiensi administrasi keamanan sangat dibutuhkan. Pada makalah ini akan membahas bagaimana sistem keamanan jaringan berkerja dengan memanfaatkan pendekatan machine learning dan diterapkan dalam industri dengan menerapkan pendekatan sistem pencegahan intrusi.

2. PENDAHULUAN

Intrusion Prevention System atau sering juga disebut *Intrusion Detection and Prevention System* (IDPS) adalah teknologi atau sistem pencegahan ancaman pada keamanan jaringan yang memeriksa lalu lintas jaringan, *network flow* untuk mendeteksi dan mencegah penyalahgunaan kerentanan lalu lintas jaringan. *Intrusion Prevention System* [1] sering berada tepat di belakang *firewall* dan menyediakan lapisan analisis untuk memilih dan memfilter konten berbahaya. Sistem deteksi dan pencegahan intrusi memberikan pertahanan terhadap kerentanan dan serangan yang dieksekusi di jaringan dan memberikan *alert* tentang hal itu. Tidak seperti antivirus, IPS tidak memindai *signature* dari file jahat saja, melainkan memindai aliran lalu lintas jaringan (*network flow*) untuk paket kerentanan dan eksploitasi yang diketahui. *Intrusion Prevention System* [2] tidak mencari signature berbahaya saja tetapi untuk mencari pola serangan, IPS dapat memberikan perlindungan terhadap kerentanan yang diketahui dan tidak diketahui. Firewall, Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) dianggap sebagai perangkat paling penting untuk manajemen keamanan jaringan [3]. Pembelajaran mesin (Machine Learning) adalah teknik yang populer untuk mengekstraksi pengetahuan dari data. Secara teori, ML

dapat digunakan untuk mengotomatisasi operasi dan manajemen jaringan. Namun, ada sedikit bukti penerapannya dalam mewujudkan otomasi jaringan [4].



Gambar 1. Evolusi Algoritma Machine Learning [4]

3. LITERATURE REVIEW

Penerapan algoritma machine learning pada manajemen jaringan mengambil peranan yang penting. Menurut [4] terdapat beberapa sistem manajemen jaringan yang dapat dilakukan dengan machine learning.

3.1. Manajemen Kesalahan: Kegagalan dalam jaringan adalah normal daripada pengecualian, dan dampaknya bisa sangat mahal [10]. Waktu reaksi yang lambat dan akurasi teknik manajemen kesalahan tradisional yang buruk semakin meningkatkan biaya ini.

3.2. Manajemen Konfigurasi: Operator harus menerapkan kebijakan jaringan yang semakin canggih yang harus diterjemahkan ke dalam perintah konfigurasi tingkat rendah , sehingga dapat disesuaikan dengan perubahan kondisi jaringan.

3.3. Manajemen Akuntansi: Akuntansi sangat erat dengan bisnis dan modul kontrol. Model-model ini memanfaatkan data akuntansi dalam pengambilan keputusan, perencanaan layanan, dan pengiriman, dan merancang tarif dan rencana penetapan harga. Oleh karena itu, penting untuk memastikan integritas data penghitungan dengan pengumpulan data penggunaan yang akurat dan deteksi penipuan.

3.4. Manajemen Kinerja: Jaringan saat ini biasanya menjalankan berbagai layanan dengan persyaratan kinerja yang berbeda untuk melayani peningkatan jumlah pengguna dengan profil berbeda. Menjaga kinerja adalah tugas yang menakutkan.

3.5. Manajemen Keamanan: Berkaitan erat dengan bagaimana suatu jaringan dapat terlindungi dari ancaman baik dari dalam maupun luar jaringan. Manajemen keamanan dibutuhkan supaya intrusi dapat terdeteksi dan ditangani dengan baik.

4. METODE DAN ANALISIS

Pada penelitian yang dilakukan pada Institut Mines-Telecom Paris [5], menerapkan sistem manajemen jaringan berbasis Network Functions Virtualization (NFV). Virtualisasi Fungsi Jaringan baru-baru ini muncul sebagai salah satu kekuatan pendorong utama teknologi yang secara signifikan mempercepat evolusi komputer dan jaringan komunikasi saat ini. Kasus penggunaan tentang kontrol akses berbasis NFV juga dikembangkan, menggambarkan kelayakan dan keuntungan dari penerapan manajemen keamanan dan orkestrasi berbasis NFV. Sedangkan pada penelitian lain [6] menerapkan metode kuantitative dan kualitatif dalam proses identifikasi penilaian risiko keamanan jaringan. Pendekatan machine learning pun dimasukkan dalam proses manajemen jaringan, pada penelitian yang dilakukan oleh [4] menambahkan algoritma kecerdasan buatan dalam implementasi nya. Tujuan akhir dari semua metode ini adalah untuk mencapai *Service Level Agreement* (SLA) yang telah di tetapkan sehingga dapat memenuhi tingkat kepuasan konsumen.

5. KESIMPULAN DAN SARAN

Lebih dari satu dekade telah berlalu sejak visi komputasi otonom pada awalnya diusulkan. Kesenjangan antara tuntutan visi dan kemampuan jaringan telah menghambat yang pertama untuk tidak diefektifkan. Namun, jaringan telah datang jauh sejak saat itu dengan meningkatnya adopsi SDN, NFV, dan komputasi awan. Kemajuan teknologi ini telah membuat infrastruktur lebih gesit, dan menghitung serta menyimpan sumber daya lebih banyak daripada sebelumnya. Untuk mengelola jaringan oleh administrator secara efektif dalam waktu dan energi yang terbatas [3], telah mengembangkan kerangka kerja hierarki untuk memproses data log masif yang dihasilkan oleh IPS. Untuk memproses alarm yang berbeda dengan kebijakan yang berbeda, kami membagi alarm menjadi dua bagian, satu bagian dari mereka adalah beberapa jenis serangan serius, dan bagian lainnya terdiri dari

sisanya. Manajemen jaringan sangat dibutuhkan dalam upaya pengingkatan kualitas dalam mencapai tujuan akhir yaitu *Service Level Agreement* (SLA).

6. REFRENSI

[1] R. M. Yousufi, P. Lalwani, and M. B. Potdar, "A network-based intrusion detection and prevention system with multi-mode counteractions," in *2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, 2017, pp. 1–6, doi: 10.1109/ICIIECS.2017.8276023.

[2] R. T. Gaddam and M. Nandhini, "An analysis of various snort based techniques to detect and prevent intrusions in networks: Proposal with code refactoring snort tool in Kali Linux environment," *Proc. Int. Conf. Inven. Commun. Comput. Technol. ICICCT 2017*, no. Icicct, pp. 10–15, 2017, doi: 10.1109/ICICCT.2017.7975177.

[3] Y. Meng, T. Qin, Y. Liu, and C. He, "An Effective High Threating Alarm Mining Method for Cloud Security Management," *IEEE Access*, vol. 6, pp. 22634–22644, 2018, doi: 10.1109/ACCESS.2018.2823724.

[4] S. Ayoubi *et al.*, "Machine Learning for Cognitive Network Management," no. January, pp. 158–165, 2018.

[5] M. Pattaranantakul, R. He, A. Meddahi, and Z. Zhang, "SecMANO: Towards network functions virtualization (NFV) based security MANagement and orchestration," *Proc. - 15th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 10th IEEE Int. Conf. Big Data Sci. Eng. 14th IEEE Int. Symp. Parallel Distrib. Process. with Appl. IEEE Trust. 2016*, pp. 598–605, 2016, doi: 10.1109/TrustCom.2016.0115.

[6] Y. Ye, L. Yan, W. Sun, Q. Zhang, and N. Wang, "Discussion on Risk Assessment of Network Security Management," *Proc. - 10th Int. Conf. Meas. Technol. Mechatronics Autom. ICMTMA 2018*, vol. 2018-January, pp. 409–411, 2018, doi: 10.1109/ICMTMA.2018.00106.