E-ISSN : 2623-1700
P-ISSN : 1693-3672

Literature Review Mekanisme Pertahanan Terhadap Serangan Distributed Denial Of Service (DDOS)

[1]Muhammad Aditya Febriansyah Tanjung, [2] Muhammad Fadhli Ma'arif, [3]Jovic Luwis Tamaela
[1,2,3]Teknik Komputer, Ilmu Komputer, Universitas Amikom Yogyakarta
adityamuhammad497@students.amikom.ac.id, muhammadfadhli09@students.amikom.ac.id, joviccc24luizzz@students.amikom.ac.id

Abstrak

Serangan Distributed Denial of Service (DDoS), yang merupakan ancaman utama terhadap infrastruktur digital, menjadi tantangan besar bagi keamanan komputer di era digital saat ini. Dalam konteks keamanan jaringan komputer, penelitian ini menyelidiki berbagai pendekatan yang dapat digunakan untuk melindungi jaringan komputer dari serangan DDoS. Fokus utama adalah pendekatan untuk mencegah, mendeteksi, dan mengatasi serangan DDoS. Untuk mengurangi dampak serangan, teknik yang menggunakan filter protokol, deteksi tanda tangan, dan analisis lalu lintas jaringan sangat penting. Kesimpulannya, upaya pencegahan, deteksi, dan mitigasi serangan DDoS serta implementasi strategi keamanan yang efektif sangat diperlukan untuk melindungi infrastruktur digital dari ancaman tersebut
Kata kunci: Serangan Distributed Denial of Service (DDoS), Keamanan komputer, Pencegahan, deteksi, dan mitigasi

Abstract

Distributed Denial of Service (DDoS) attacks, which are a major threat to digital infrastructure, pose a major challenge to computer security in today's digital age. In the context of computer network security, this research investigates various approaches that can be used to protect computer networks from DDoS attacks. The main focus is on approaches to prevent, detect, and resolve DDoS attacks. To reduce the impact of the attack, techniques that use protocol filters, signature detection, and network traffic analysis are essential. In conclusion, efforts to prevent, detect and mitigate DDoS attacks and the implementation of effective security strategies are necessary to protect digital infrastructures from such threats
Keywords : Distributed Denial of Service (DDoS) Attacks, Computer security, Prevention, detection and mitigation.

PENDAHULUAN

Di abad ke-21, keamanan komputer adalah masalah utama. Seiring dengan kemajuan teknologi, Ancaman cyber telah meningkat pesat, mengubah keamanan dunia digital. Kita perlu memahami dan mengatasi bahaya yang menyertai komputer dan internet Jika kita ingin melindungi data pribadi, informasi bisnis, infrastruktur penting, dan bahkan kehidupan sehari-hari kita(1). Beberapa contoh kegagalan keamanan sistem digital yang digunakan oleh penjahat cyber yang semakin ahli termasuk serangan malware, peretasan, dan serangan jaringan yang kompleks. Ancaman terhadap objek penting dan keamanan file terus meningkat. Selain itu, semakin sulit untuk memastikan bahwa file tetap aman karena semakin banyak data yang dikirim dan disimpan secara elektronik(2).

Ada banyak masalah keamanan, ancaman, dan tantangan, salah satunya adalah serangan DDoS. Serangan DDoS bukan hal baru, tetapi mereka adalah masalah keamanan penting yang harus diperhatikan. Jumlah serangan DDoS yang dilaporkan sangat tinggi dan terus meningkat, membuat jenis serangan ini menjadi ancaman terbesar di antara yang lain(3)**.** Teknik DDoS ini melibatkan penyerang yang membuat komputer zombie dengan perangkat lunak berbahaya yang ditanamkan di komputer korban untuk mengirimkan paket besar, serangan DDoS meningkatkan lalu lintas jaringan dengan paket yang dikirim, membuat pengguna biasa yang

ingin menerima layanan tidak menerima permintaan mereka(4).

Studi mendalam tentang masalah ini dapat memberikan pemahaman yang lebih baik tentang cara mengatasi ancaman ini dan membuat kebijakan keamanan yang baik. Tujuan dari review paper ini adalah untuk menyelidiki dan menganalisis berbagai strategi dan mekanisme pertahanan terhadap ancaman keamanan komputer, terutama yang berkaitan dengan serangan DDoS (Distributed Denial of Service). Tujuan utama dari penelitian ini adalah untuk memberikan wawasan mendalam tentang cara menangani ancaman tersebut serta menganalisis mekanisme pertahanan terhadap serangan DDoS yang semakin meningkat

1.1 Keamanan Jaringan Komputer

Keamanan jaringan komputer merupakan masalah yang harus diperhatikan oleh setiap pengguna komputer. Karena sistem informasi jaringan sangat rentan terhadap serangan, penyusup dapat dengan mudah membobol dan mendapatkan data rahasia, karena sistem informasi jaringan sangat rentan terhadap serangan, penyusup dapat dengan mudah membobol dan mendapatkan data rahasia(5). Kejahatan cyber selalu terkait dengan penggunaan teknologi informasi dan komputer. Kejahatan cyber dilakukan dengan memasuki sistem jaringan komputer secara ilegal atau tanpa sepengetahuan pemilik sistem jaringan tersebut. Serangan dan kejahatan internet sangat umum, terutama serangan Distributed Denial of Service (DDoS), yang memiliki tujuan yang tidak baik, menghabiskan sumber daya server sehingga tidak dapat digunakan(1). Oleh karena itu, sistem keamanan jaringan komputer diperlukan untuk mencegah dan menemukan pelanggaran yang melanggar hukum, termasuk serangan DDoS

1.2 Serangan Distributed Denial of Service

Serangan DDoS adalah jenis serangan berbahaya yang mengirimkan lalu lintas berbahaya ke satu atau lebih node tertentu melalui berbagai komputer yang merupakan bagian dari suatu sistem, yang mungkin dikontrol secara sah oleh penyerang atau tidak. Serangan seperti itu membebani sumber daya target untuk memproses paket yang tidak sah dan membuatnya tidak mungkin mengirim permintaan layanan yang sah(6). Serangan DDoS (Denial of Service Distributed) merupakan jenis serangan yang digunakan untuk mengganggu akses pengguna secara signifikan(7). Karena jenis serangan kritis ini mengarahkan banyak node pada satu target, serangan ini pada awalnya sulit dideteksi dan dapat menyebabkan kerusakan besar pada korban dan jaringan(8).

1.3 Mekanisme Pertahanan

Serangan DDoS paling sering membuat sumber daya tidak dapat diakses daripada ancaman lainnya. Oleh karena itu, sistem pertahanan harus cukup kuat untuk menghadapi serangan tersebut.

a. Pencegahan Serangan DDoS (Prevention)

Arti pencegahan adalah secara proaktif melindungi sumber daya dan layanan cloud dari serangan DDoS. Manajemen lalu lintas jaringan, pemrograman ulang, dan server proxy/tersembunyi adalah komponen pencegahan serangan DdoS(9). Pemfilteran protokol, respons tantangan (CRP), dan pembatasan akses adalah beberapa metode pencegahan yang ditentukan(3).

b. Deteksi Serangan DDoS (Detection)

Untuk membedakan lalu lintas yang sah dari lalu lintas berbahaya, deteksi melibatkan pemeriksaan jaringan(9). Beberapa contoh deteksi termasuk deteksi berbasis tanda tangan, deteksi berbasis anomali, deteksi berbasis pemanfaatan sumber daya, dan deteksi berbasis asosiasi(3).

c. Mitigasi Serangan DDoS (Mitigation)

Mitigasi berarti menanggapi dampak serangan dengan cepat. Hasil dari tahap ini digunakan untuk memperbarui tahap pencegahan secara rutin(9). Beberapa metode mitigasi serangan DDoS yang disebutkan di sini adalah firewall perangkat lunak dan perangkat keras yang melindungi terhadap serangan DoS dan DDoS, penskalaan sumber daya, migrasi korban (VM), dan

mitigasi DDoS sebagai layanan (DMaaS)(3).

METODE

Dalam penelitian ini, Systematic Literature Review (SLR) digunakan. Studi kepustakaan dan penelitian kepustakaan berbeda. Studi kepustakaan adalah istilah lain untuk kajian kepustakaan, tinjauan kepustakaan, kajian teoritis, landasan teori, tinjauan literatur, dan tinjauan teoritis(10). Selain itu, metode SLR dapat membedakan data subjektif dan objektif. Hasil penelitian ini dapat digunakan untuk mempublikasikan literatur tentang penggunaan metode SLR di jurnal internasional.

Dalam proses pencarian, informasi tentang penelitian saat ini dikumpulkan untuk menjawab pertanyaan penelitian. Mesin pencari digunakan untuk melakukan pencarian. Pemilihan tinjauan literatur dilakukan berdasarkan topik yang dipilih, dan referensi yang relevan dipilih untuk memfokuskan pembuatan artikel pada topik utama yang dibahas. Kemudian, dilakukan review literatur terkait secara sistematis dan deskriptif, termasuk hasil penelitian, konsep, teori, dan konsekuensi dari mekanisme pertahanan.

Dalam penelitian ini, metode pengumpulan data yang digunakan adalah studi literatur. Dalam penelitian ini, teknik analisis data yang digunakan adalah deskriptif kualitatif. Metode ini digunakan karena dapat membantu mencapai tujuan penelitian, yaitu memberikan pemahaman yang lebih baik tentang penerapan mekanisme pertahanan terhadap keamanan.

HASIL DAN PEMBAHASAN

Tabel 1. Penentuan Mekanisme Pertahanan

Authors	Judul	Mekanisme Pertahanan		
		Prevention	*Detection*	*Mitigation*
(11)	Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment		√	√
(12)	Advanced Support Vector Machine-(ASVM-) Based Detection for Distributed Denial of Service (DDoS) Attack on Software Defined Networking (SDN)		√	
(13)	Distributed Denial of Service (DDoS) Attack in Cloud-Assisted Wireless Body Area Networks: A Systematic Literature Review		√	
(14)	A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks	√	√	
(15)	Real-Time Detection			√

Authors	Judul	Mekanisme Pertahanan		
		Prevention	*Detection*	*Mitigation*
	and Mitigation of Distributed Denial of Service (DDoS) Attacks in Software Defined Networking (SDN)			
(16)	Threat Analysis and Distributed Denial of Service (DDoS) Attack Recognition in the Internet of Things (IoT)		√	
(6)	An Effective Mechanism to Mitigate Real-Time DDoS Attack		√	
(17)	Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques	√	√	

Serangan Distributed Denial of Service (DDoS) dalam lingkungan komputasi awan berbasis software (SDN) menjadi tantangan yang semakin relevan dalam konteks keamanan jaringan saat ini. SDN menawarkan fleksibilitas dan kendali sentral dalam pengelolaan lalu lintas jaringan, yang membuatnya menjadi platform yang potensial untuk mengatasi serangan DDoS. Ancaman DDoS dapat menyebabkan penurunan layanan, kinerja yang buruk, dan kerugian moneter yang signifikan.

Salah satu manfaat utama SDN dalam mengurangi serangan DDoS adalah kemampuannya untuk mendeteksi lalu lintas yang mencurigakan, mengisolasi lalu lintas berbahaya, dan mengalihkan serangan ke pusat mitigasi atau layanan perlindungan DDoS berbasis awan. Selain itu, penggunaan teknologi pembelajaran mesin dan algoritma dalam mendeteksi serangan DDoS juga dapat membantu dalam mengurangi false positive, yang menghasilkan peningkatan efektivitas mitigasi.

Bermitra dengan penyedia layanan cloud juga penting dalam menjaga keamanan jaringan SDN dan melindungi layanan pelanggan dari serangan DDoS. Hal ini memastikan respons cepat terhadap serangan dan penggunaan sumber daya mitigasi secara efisien. Dengan SDN, kami memiliki alat potensial untuk mengatasi ancaman serangan DDoS yang semakin kompleks dan berbahaya, serta memastikan ketersediaan layanan jaringan penting.

Serangan Distributed Denial of Service (DDoS) telah menjadi ancaman yang signifikan dalam bidang keamanan komputer, terutama dalam konteks komputasi awan berbasis Software Defined Network (SDN). Kemampuan kontrol sentral yang diberikan oleh SDN memungkinkan administrator untuk mengatur lalu lintas jaringan dengan baik. Salah satu keuntungan menggunakan SDN dalam mengurangi serangan DDoS adalah kemampuan untuk mendeteksi lalu lintas mencurigakan, isolasi, dan redundansi, serta mengalihkan lalu lintas DDoS ke layanan mitigasi. Teknologi pembelajaran mesin seperti Advanced Support Vector Machine (ASVM) juga digunakan untuk meningkatkan deteksi serangan DDoS dalam SDN. Selain itu, ditekankan betapa pentingnya kerja sama antara organisasi dan penyedia layanan cloud untuk menjaga keamanan jaringan SDN dan mencegah serangan DDoS.

Serangan DDoS juga merupakan ancaman besar bagi Internet of Things (IoT). Oleh karena itu, sangat penting untuk mendeteksi dan mengatasi serangan DDoS dengan cepat. Analisis lalu lintas, pembelajaran mesin, dan pengenalan ancaman potensial adalah metode IoT untuk

mendeteksi serangan DDoS. Untuk melindungi perangkat Internet of Things dari serangan DDoS, desain perangkat IoT harus memiliki keamanan yang kuat, seperti enkripsi dan otentikasi. Terdapat tantangan yang perlu diatasi, seperti keterbatasan sumber daya perangkat IoT, dan diskusi akan membahas solusi deteksi yang tersedia dan konsekuensi untuk pengembangan kebijakan keamanan di masa depan. Ini terjadi meskipun ada solusi yang telah diusulkan. Oleh karena itu, untuk menjaga keamanan dan ketersediaan layanan di dunia yang semakin terhubung ini, mitigasi serangan DDoS menjadi sangat penting

KESIMPULAN

Dalam komputasi awan berbasis SDN, penerapan teknologi SDN membawa manfaat dalam hal pengelolaan awan, kemampuan program, dinamisme, dan skalabilitas. Namun, hal ini juga menimbulkan potensi kerentanan terhadap serangan DDoS pada cloud berbasis SDN. Beberapa masalah keamanan yang perlu dipertimbangkan dalam cloud berbasis SDN antara lain ketersediaan, skalabilitas, kontrol akses dan akuntabilitas, autentikasi dan otorisasi, ancaman yang berasal dari aplikasi, dan serangan DDoS.Untuk menangani serangan DDoS di lingkungan cloud berbasis SDN, beberapa metode dapat digunakan.Pendekatan ini mencakup metode pembaruan tambahan yang konsisten dan teknik pengoptimalan ruang aturan. Selain itu, ada teknik deteksi DDoS seperti deteksi berbasis tanda tangan dan deteksi berbasis anomali. Penggunaan SDN untuk memitigasi serangan DDoS mencakup membatasi kecepatan lalu lintas, mengalihkan aliran secara otomatis, memasukkan alamat IP berbahaya ke dalam daftar hitam, dan mengenali perilaku anomaly dengan menggunakan pembelajaran mesin. Dengan menerapkan metode dan teknik tersebut diharapkan dapat meningkatkan keamanan cloud berbasis SDN dan mengurangi risiko serangan DDoS. Namun, penting untuk diingat bahwa keamanan adalah proses yang terus berkembang. Oleh karena itu, pemantauan dan peningkatan keamanan berkelanjutan diperlukan untuk mengatasi ancaman baru dan yang terus berkembang

DAFTAR PUSTAKA

1. Sari I. KEAMANAN KOMPUTER DAN ANCAMAN CYBER DI ERA DIGITAL. Jurnal Teknologi Terkini. 2023;3(4).
2. Soesanto E, Romadhon A, Mardika BD, Setiawan MF. Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. Sammajiva: Jurnal Penelitian Bisnis dan Manajemen. 2023;1(2):172–91.
3. Radain D, Almalki S, Alsaadi H, Salama S. A Review on Defense Mechanisms Against Distributed Denial of Service (DDoS) Attacks on Cloud Computing. In: 2021 International Conference of Women in Data Science at Taif University (WiDSTaif). IEEE; 2021. p. 1–6.
4. Faiz MN, Somantri O, Supriyono AR, Muhammad AW. Impact of Feature Selection Methods on Machine Learning-based for Detecting DDoS Attacks : Literature Review. JOURNAL OF INFORMATICS AND TELECOMMUNICATION ENGINEERING. 2022 Jan 26;5(2):305–14.
5. Zukhruf A, Fatkhurrozi B, Kurniawan AA. COMPARATIVE STUDY OF DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK DETECTION IN COMPUTER NETWORKS. Jurnal Teknik Informatika (Jutif). 2023;4(5):1033–9.
6. Abubakar R, Aldegheishem A, Faran Majeed M, Mehmood A, Maryam H, Ali Alrajeh N, et al. An Effective Mechanism to Mitigate Real-Time DDoS Attack. IEEE Access. 2020;8:126215–27.
7. Hansen J, Sutabri T. Mendesain Cyber Security Untuk Mencegah Serangan DDoS Pada Website Menggunakan Metode Captcha. Digital Transformation Technology. 2023;3(1):289–98.

8. Khalaf BA, Mostafa SA, Mustapha A, Mohammed MA, Abduallah WM. Comprehensive Review of Artificial Intelligence and Statistical Approaches in Distributed Denial of Service Attack and Defense Methods. IEEE Access. 2019;7:51691–713.

9. Agrawal N, Tapaswi S. Defense mechanisms against DDoS attacks in a cloud computing environment: State-of-the-art and research challenges. IEEE Communications Surveys & Tutorials. 2019;21(4):3769–95.

10. Melfianora. Penulisan Karya Tulis Ilmiah dengan Studi Literatur. Open Science Framework. 2019;1–3.

11. Bhushan K, Gupta BB. Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment. J Ambient Intell Humaniz Comput. 2019 May 20;10(5):1985–97.

12. Myint Oo M, Kamolphiwong S, Kamolphiwong T, Vasupongayya S. Advanced Support Vector Machine-(ASVM-) Based Detection for Distributed Denial of Service (DDoS) Attack on Software Defined Networking (SDN). Journal of Computer Networks and Communications. 2019 Mar 4;2019:1–12.

13. Latif R, Abbas H, Assar S. Distributed Denial of Service (DDoS) Attack in Cloud-Assisted Wireless Body Area Networks: A Systematic Literature Review. J Med Syst. 2014 Nov 14;38(11):128.

14. Zargar ST, Joshi J, Tipper D. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. IEEE Communications Surveys & Tutorials. 2013;15(4):2046–69.

15. Lawal BH, Nuray AT. Real-time detection and mitigation of distributed denial of service (DDoS) attacks in software defined networking (SDN). In: 2018 26th Signal Processing and Communications Applications Conference (SIU). IEEE; 2018. p. 1–4.

16. Ali MH, Jaber MM, Abd SK, Rehman A, Awan MJ, Damaševičius R, et al. Threat Analysis and Distributed Denial of Service (DDoS) Attack Recognition in the Internet of Things (IoT). Electronics (Basel). 2022 Feb 8;11(3):494.

17. Sudar KM, Beulah M, Deepalakshmi P, Nagaraj P, Chinnasamy P. Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques. In: 2021 International Conference on Computer Communication and Informatics (ICCCI). IEEE; 2021. p. 1–5.