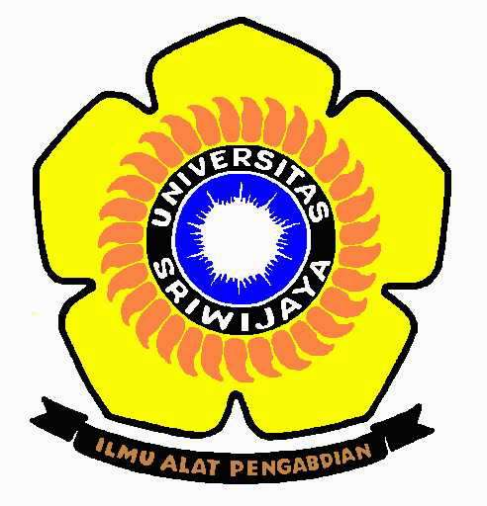
SISTEM PENCEGAHAN SERANGAN DDoS SYN FLOODING MENGGUNAKAN METODE ARTIFICIAL IMUNE SYSTEM

TUGAS AKHIR



OLEH :

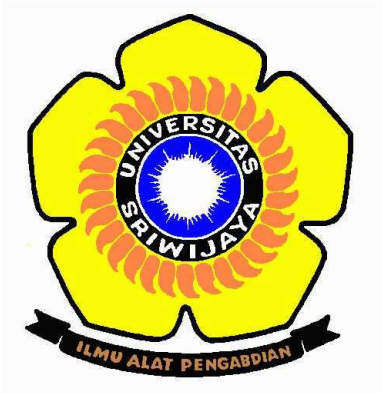
AHMAD ILHAM ARISMAWAN
09011381621064

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2021

SISTEM PENCEGAHAN SERANGAN DDoS SYN FLOODING MENGGUNAKAN METODE ARTIFICIAL IMUNE SYSTEM

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer



OLEH :

AHMAD ILHAM ARISMAWAN
09011381621064

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2021

HALAMAN PENGESAHAN

SISTEM PENCEGAHAN SERANGAN DDoS SYN FLOODING MENGGUNAKAN METODE ARTIFICIAL IMMUNE SYSTEM

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

AHMAD ILHAM ARISMAWAN
09011381621064

Indralaya, Maret 2022

Mengetahui,

Pembimbing I Tugas Akhir	**Pembimbing II Tugas Akhir**
Deris Stiawan, Ph. D.	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 197806172006041002	**NIP. 198701222015041002**

Ketua Jurusan Sistem Komputer

Ir., Dr., Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada

Hari : Jum'at

Tanggal : 24 Desember 2021

Tim Penguji:

1. **Ketua** : **Ahmad Zarkasi, M.T.**
2. **Sekretaris** : **Iman Saladin, S.Kom., M.MSI.**
3. **Pembimbing I** : **Deris Stiawan, M.T., Ph.D.**
4. **Pembimbing II** : **Ahmad Heryanto, M.T.**
5. **Penguji** : **Huda Ubaya, M.T.**

Mengetahui
Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP. 19661203200641001

HALAMAN PERNYATAAN

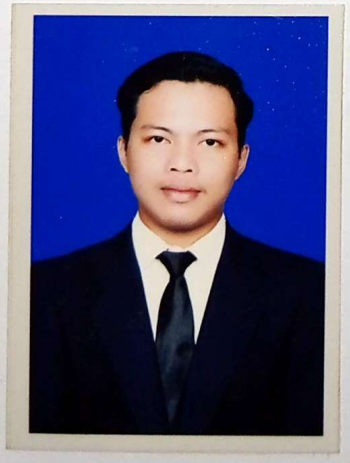
Yang bertanda tangan dibawah ini:

Nama : Ahmad Ilham Arismawan
NIM : 09011381621064
Judul : Sistem Pencegahan *DDoS SYN Flooding* Menggunakan Metode *Artificial Immune System*

Hasil Pengecekan *Software iThenticate Turnitin : 1 %*

Menyatakan bahwa laporan skripsi saya merupakan hasil karya sendiri dan bukan hasil penjiplakan / *Plagiat*. Apabila ditemukan unsur penjiplakan / *plagiat* dalam laporan skripsi ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian Pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan



Palembang, Maret 2022

Ahmad Ilham Arismawan

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Allah SWT, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan proposal tugas akhir dengan judul **"Sistem Pencegahan Serangan DDoS SYN Flooding Menggunakan Metode Artificial Immune System"**.

Penulisan Proposal Tugas Akhir ini dilakukan untuk melengkapi salah satu syarat memperoleh gelar Sarjana Komputer di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya. Adapun sebagai bahan penulisan, penulis mengambil berdasarkan hasil penelitian, observasi dan beberapa sumber literatur yang mendukung dalam penulisan proposal ini. Pada kesempatan ini juga, penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu baik dari segi moril ataupun materil serta memberikan kemudahan, dorongan, saran dan kritik selama dalam proses penulisan Proposal Tugas Akhir ini.

Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Allah SWT. dan mengucapkan terima kasih kepada yang terhormat :

1. Orang Tua serta keluarga penulis tercinta, yang telah memberikan doa dan restu serta dukungan yang sangat besar selama mengikuti dan melaksanakan perkuliahan di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya hingga dapat menyelesaikan Proposal Tugas Akhir ini.
2. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Ir., Dr., Sukemi M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Deris Stiawan, M.T., Ph. D., selaku Dosen Pembimbing I Tugas Akhir penulis.
5. Bapak Ahmad Heryanto S.Kom, M.T., selaku Dosen Pembimbing II Tugas Akhir penulis.

6. Bapak Ahmad Fali Oklilas, M.T selaku Dosen Akademik di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Seluruh dosen, staff, serta karyawan Fakultas Ilmu Komputer Universitas Sriwijaya.
8. Seluruh teman-teman seperjuangan angkatan 2016 Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
9. Teman-teman yang mau di sebutkan nama-namanya M. Nawwar Athalaza S.Kom, Tasya Yoandhita S.Kom, Sri Retno Rahayu S.Kom, Fachrudin Abdau S.Kom, M. Cahyadi S.Kom, M. Ikhsan S.Kom, Dio Azmi Saputra S.Kom, dan lain-lain.
10. Diri Sendiri
11. Almamater

Penulis menyadari bahwa masih banyak kekurangan dalam penulisan Proposal Tugas Akhir ini. Karena sesungguhnya tak ada yang sempurna didunia ini. Untuk itu, segala saran dan kritik sangatlah penting bagi penulis. Akhir kata, semoga Proposal Tugas Akhir ini dapat bermanfaat dan berguna bagi khalayak.

Palembang, Maret 2022

Penulis

Ahmad Ilham Arismawan

NIM. 09011381621064

SISTEM PENCEGAHAN SERANGAN DDoS SYN FLOODING MENGGUNAKAN METODE ARTIFICIAL IMMUNE SYSTEM

Ahmad Ilham Arismawan (09011381621064)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya

ABSTRAK

Intrusion Prevention System merupakan sistem yang menggabungkan antara sistem deteksi serta pencegahan dini terhadap suatu serangan. *DDoS Syn Flooding* merupakan aktifitas serangan *DDoS* yang memanfaatkan paket *Syn* dalam proses *Three Way Handsake* untuk membanjiri resource korban dalam protocol *TCP*. *Negative Selection Algorithm* atau dikenal dengan NSA merupakan algoritma turunan dari *Artificial Immune System* (AIS) yang di rancang untuk dapat mendeteksi anomaly pada traffic jaringan. Dengan menggunakan *Hping3* sebagai tools untuk membuat traffic data dirancang 3 skenario pembuatan dataset yang bersifat *homogen*. Pada penelitian ini, dengan menggunakan metode *Artificial Immune System* (AIS) serta pemanfaatan *Negative Selection Algorithm* serangan berhasil untuk dideteksi dan dicegah dengan tingkat Akurasi 88%, Presisi 100% dan TPR 81%.

Kata Kunci *– Artificial Immune System, DDoS SYN Flooding, Intrusion Prevention System*.

DDoS SYN FLOODING INTRUSION PREVENTION SYSTEM BASED ON ARTIFICIAL IMMUNE SYSTEM METHOD

Ahmad Ilham Arismawan (09011381621064)

Department of Computer Engineering, Faculty of Computer Science
Sriwijaya University

ABSTRACT

Intrusion Prevention System is a system that combines early detection and pro active prevention system. *DDoS SYN Flooding* is a *DDoS* attack activity which utilizes *Syn* Packet in the *Three Way Handshake* process to flood victim resource in the *TCP* Protocol. *Negative Selection Algorithm* known as NSA is an algorithm from *Artificial Immune System* (AIS) method which is designed to detect network traffic anomalies. Using *Hping3* as a tool to create traffic data, 3 scenarios for create *homogeneus* dataset are designed. In this case, using *Artificial Immune System* (AIS) by utilizing the *Negative Selection Algorithm*, attacks were successfully detected and prevented with an Accuracy rate of 88%, Precision 100% and TPR 81%.

Keyword *– Artificial Immune System, DDoS SYN Flooding, Intrusion Prevention System*.

DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1.Latar Belakang

Keamanan informasi selama ini telah menjadi prioritas tertinggi untuk individu maupun sebuah organisasi atau perusahaan. Keamanan informasi menjamin keamanan dan ketersediaan informasi selama perpindahannya dari pengirim hingga penerima [1]. Berdasarkan data penelitian yang telah dilakukan oleh [2], hampir 69% perusahaan menggunakan pencegahan *intrusi* (serangan) untuk mencegah berbagai ancaman dan serangan terhadap keamanan informasi yang dimiliki. Berdasarkan hal tersebut, maka di butuhkan sebuah sistem yang mampu untuk mendeteksi dan mencegahnya secara cepat sehingga layanan tetap terjaga ketersediaan informasinya.

Salah satu ancaman terhadap keamanan informasi yang masih banyak terjadi adalah serangan *Denial of Service* (DoS). Serangan DoS dapat melumpuhkan akses terhadap penggunaan layanan yang sedang diserang. Serangan yang lebih berbahaya lagi adalah serangan DoS yang terdistribusi, atau sering disebut *Distributed Denial of Service* (*DDoS*). *DDoS* melakukan serangan dengan menggunakan botnet yang di kontrol untuk menyerang secara simultan, sehingga sumber daya target yang diserang akan habis dengan membebani permintaannya [3]. Serangan *DDoS* saat ini dapat di klasifikasikan dalam beberapa faktor, salah satunya yaitu berdasarkan *Volume based*, *Protocol based*, maupun *Application layer based* [4].

SYN Flooding merupakan salah satu serangan *DDoS* yang masih menjadi ancaman serius bagi keamanan jaringan. Dengan memanfaatkan mekanisme koneksi didalam protokol TCP yang dinamakan dengan *Three-way handshake* , penyerang akan membanjiri paket SYN pada korban [5] sehingga dinamakan serangan *SYN Flooding*.

Dalam beberapa penelitian yang dilakukan sebelumnya serangan *SYN Flooding* ini telah berhasil dideteksi dengan menggunakan beberapa metode.

Seperti menggunakan analisis *Payload* [6], *Super Vector Machine* (SVM) [7] serta *Artificial Immune System* [8][9].

Intrusion Prevention System (IPS) merupakan sebuah sistem yang menggabungkan antara *Intrusion Detection System* (IDS) dengan sistem pencegahan yang menjadikan sistem IPS menjadi sistem yang pro-aktif [2]. IPS dapat melakukan deteksi terhadap ancaman yang ada layaknya cara kerja sistem IDS, dan berusaha menghentikan ancaman tersebut secara langsung [10]. Hal tersebut membuat sistem IPS menjadi salah satu langkah paling efektif [11] dalam pencegahan keamanan jaringan. Dengan melakukan trigger pada IPS baik karena adanya akfititas mencurigakan maupun normal, maka IPS dapat melakukan respon *Log*, *Block*, *Allow* ataupun *Deny [2]*.

Berdasarkan pada beberapa ulasan sebelumnya, bahwa banyaknya permintaan penggunaan sistem keamanan intrusi saat ini salah satunya terhadap serangan *SYN Flooding*, serta serangan *SYN Flooding* yang tidak hanya cukup untuk di deteksi saja. Oleh karena itu pada penelitian ini akan difokuskan untuk membahas tentang sistem IPS terhadap serangan *SYN Flooding* menggunakan metode *Artificial Immune System*.

1.2.Tujuan

Tujuan yang diharapkan dapat dicapai pada penelitian ini ialah:

1. Mendapatkan hasil deteksi paket serangan *SYN Flooding* dengan paket normal.
2. Merancang sistem pencegahan serangan *SYN Flooding* menggunakan metode *Artificial Immune System.*
3. Menganalisa hasil akurasi deteksi dan pencegahan pada serangan *SYN Flooding* menggunakan metode *Artificial Immune System.*

1.3.Manfaat

Manfaat yang diharapkan didapatkan pada penelitian ini ialah:

1. Menghasilkan rancangan sistem pencegahan serangan *SYN Flooding* menggunakan metode *Artificial Immune System.*
2. Bisa untuk membedakan paket data serangan *SYN Flooding* dengan paket data normal.

1.4.Rumusan Masalah

Dari latar belakang serta tujuan penelitian di atas, maka permasalahan yang dibahas pada penelitian kali ini ialah bagaimana cara mencegah paket serangan *SYN Flooding* dengan menggunakan metode *Artificial Immune System.*

1.5.Batasan Masalah

Beberapa Batasan masalah dalam penelitian ini ialah :

1. Menggunakan data dari pengambilan dengan skenario serangan *SYN Flooding*.
2. Mekanisme pendeteksian serangan *SYN Flooding* adalah dengan metode menggunakan metode *Artificial Immune System*.
3. Paket yang dideteksi hanyalah paket serangan *SYN Flooding.*
4. Tidak untuk diuji pada lalu lintas jaringan terenkripsi.

1.6.Metodologi Penelitian

Pada penulisan Tugas Akhir ini peneliti akan melalui beberapa tahap metodologi :

1. Metode Literatur

   Pada fase ini penulis menggali informasi yang dibutuhkan melalui jurnal akademik, internet, buku, dan kemungkinan artikel yang bersangkutan dalam berbagai media untuk membantu dalam penulisan.

2. Metode Konsultasi

   Dalam Fase kedua, peneliti akan berkonsultasi dengan berbagai sumber yang diyakini punya akan pengetahuan serta wawasan tentang masalah yang mungkin timbul dalam pengerjaan tugas akhir.

3. Metode Perancangan Sistem

   Fase ketiga ini adalah fase di mana proses dibahas, bagaimana membuat metode ataupun pendekatan khusus, "software" atau "hardware" apa yang yang mungkin akan dipakai, serta bebagai pengaturan dalam sistem dan aplikasi.

4. Metode Pengujian

   Fase keempat ini ialah tahap selanjutnya untuk pengujiann sistem, sistem akan diuji berdasarkan pada metode penelitian serta serta penelitian sebelumnya agar menghasilkan hasil yang di inginkan serta sesuai dengan konseptual atau praktis.

5. Metode Analisa dan Kesimpulan

   Hasil pemeriksaan prosedur pengujian lalu dianalisa yang dimaksudkan agar peneliti tahu dan sadar akan kekurangan-kekurangan hasil rancangan serta faktor-faktor yang menyebabkannya sehingga dapat dijadikan acuan untuk penelitian berikutnya lalu dapat ditarik kesimpulan pada akhirnya.

1.7.Sistematika Penulisan

Adapun sistematika penulisan dalam Project Tugas Akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab I akan berisi latar belakang penelitian, tujuan, manfaat, rumusan masalah, batasan penelitian serta metodologi penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada Bab II berisikan dasar pengetahuan mengenai "*Intrusion Detection System*" (IDS), "*Intrusion Prevention System*" (IPS), "*Distributed Denial of Service*" (*DDoS*), *SYN Flooding,* metode *Artificial Immune System* serta berbagai kegiatan yang terkait.

BAB III METODOLOGI

Pada Bab III di bahas metodologi maupun perancangan implementasi sistem pencegahan serangan *SYN Flooding* menggunakan metode *Artificial Immune System.*

BAB IV HASIL DAN ANALISA

Pada Bab IV merupakan isi dari hasil dan pembahasan mengenai perancangan sistem pencegahan serangan *SYN Flooding* menggunakan metode *Artificial Immune System.*

BAB V KESIMPULAN

Terakhir Bab V akan ditarik berbagai macam kesimpulan terkait hasil dan analisa dari implementasi metode *Artificial Immune System* dalam merancang sistem pencegahan serangan *SYN Flooding*. Pada bab ini juga akan berisi saran dari peneliti yang mungkin dapat digunakan dalam penelitian yang akan dilakukan oleh peneliti selanjutnya

DAFTAR PUSTAKA

[1] M. Baykara and R. Das, "A novel honeypot based security approach for real-time intrusion detection and prevention systems," *J. Inf. Secur. Appl.*, vol. 41, pp. 103–116, 2018, doi: 10.1016/j.jisa.2018.06.004.

[2] D. Stiawan, A. H. Abdullah, and M. Y. Idris, "The trends of Intrusion Prevention System network," *ICETC 2010 - 2010 2nd Int. Conf. Educ. Technol. Comput.*, vol. 4, pp. 217–221, 2010, doi: 10.1109/ICETC.2010.5529697.

[3] J. Nyman, "Evaluating the mitigating effect on HTTP flood attacks using an application layer Challenge-response approach," 2018.

[4] M. Malik and Y. Singh, "International Journal of Computer Science and Mobile Computing A Review: DoS and DDoS Attacks," *Int. J. Comput. Sci. Mob. Comput.*, vol. 4, no. 6, pp. 260–265, 2015, [Online]. Available: www.ijcsmc.com.

[5] M. Bogdanoski, T. Shuminoski, and A. Risteski, "Analysis of the SYN Flood DoS Attack," *Int. J. Comput. Netw. Inf. Secur.*, vol. 5, no. 8, pp. 15–11, 2013, doi: 10.5815/ijcnis.2013.08.01.

[6] S. H. C. Haris, R. B. Ahmad, M. A. H. A. Ghani, and G. M. Waleed, "TCP SYN flood detection based on payload analysis," *Proceeding, 2010 IEEE Student Conf. Res. Dev. - Eng. Innov. Beyond, SCOReD 2010*, no. May, pp. 149–153, 2010, doi: 10.1109/SCORED.2010.5703991.

[7] Z. Mašetić, D. Kečo, N. Doğru, and K. Hajdarević, "SYN flood attack detection in cloud computing using support vector machine," *TEM J.*, vol. 6, no. 4, pp. 752–759, 2017, doi: 10.18421/TEM64-15.

[8] Candra Adi Winanto, "Deteksi Serangan Denial of Service Menggunakan Artificial Immune System," vol. 2, no. 1, pp. 456–459, 2016.

[9] G. Ramadhan, Y. Kurniawan, and C. S. Kim, "Design of TCP SYN Flood DDoS attack detection using artificial immune systems," *Proc. 2016 6th Int. Conf. Syst. Eng. Technol. ICSET 2016*, pp. 72–76, 2017, doi: 10.1109/FIT.2016.7857541.

[10] B. MaqboolBeigh, U. Bashir, and M. Chahcoo, "Intrusion Detection and

Prevention System: Issues and Challenges," *Int. J. Comput. Appl.*, vol. 76, no. 17, pp. 26–30, 2013, doi: 10.5120/13340-0701.

[11] Y. Farhaoui, "Design and implementation of an intrusion prevention system," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 675–683, 2017, doi: 10.6633/IJNS.201709.19(5).04.

[12] H. J. Liao, C. H. Richard Lin, Y. C. Lin, and K. Y. Tung, "Intrusion detection system: A comprehensive review," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 16–24, 2013, doi: 10.1016/j.jnca.2012.09.004.

[13] C. Constantinides, S. Shiaeles, B. Ghita, and N. Kolokotronis, "A novel online incremental learning intrusion prevention system," *2019 10th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2019 - Proc. Work.*, pp. 1–6, 2019, doi: 10.1109/NTMS.2019.8763842.

[14] C. L. Schuba *et al.*, "Analysis of a Denial of Service Attack on TCP 1398 Department of Computer Sciences."

[15] P. Mishra, V. Varadharajan, S. Member, and U. Tupakula, "A Detailed Investigation and Analysis of using Machine Learning Techniques for Intrusion Detection," *IEEE Commun. Surv. Tutorials*, vol. PP, no. c, p. 1, 2018, doi: 10.1109/COMST.2018.2847722.

[16] N. Bergerak, A. I. Tranport, and S. Its, "Analisis Kinerja TCP/IP untuk Jaringan Nirkabel Bergerak 3G di Surabaya," vol. 5, no. 2, 2016.

[17] L. Dokumen and C. Seluruh, "Muhamad Husni Lafif," 2007.

[18] M. Tabatabaefar, M. Miriestahbanati, and J. C. Gregoire, "Network intrusion detection through artificial immune system," *11th Annu. IEEE Int. Syst. Conf. SysCon 2017 - Proc.*, 2017, doi: 10.1109/SYSCON.2017.7934751.

[19] J. Al-Enezi, M. Abbod, and S. Alsharhan, "Artificial Immune Systems-models, algorithms and applications," *Int. J. Res. Rev. Appl. Sci.*, vol. 3, no. May, pp. 118–131, 2010, [Online]. Available: http://bura.brunel.ac.uk/handle/2438/4643.

[20] U. Aickelin and D. Dasgupta, "Search Methodologies : Introductory Tutorials in

Optimization and Decision Support Techniques Edmund K . Burke (Editor), Graham Kendall (Editor) ARTIFICIAL IMMUNE SYSTEMS," pp. 1–29.

[21] J. Greensmith, U. Aickelin, and S. Cayzer, "Detecting danger: The dendritic cell algorithm," *Robust Intell. Syst.*, pp. 89–112, 2008, doi: 10.1007/978-1-84800-261-6_5.

[22] E. K. Burke and G. Kendall, *Search methodologies: Introductory tutorials in optimization and decision support techniques*, no. March. 2005.

[23] O. Igbe and T. Saadawi, "Insider Threat Detection using an Artificial Immune system Algorithm," *2018 9th IEEE Annu. Ubiquitous Comput. Electron. Mob. Commun. Conf. UEMCON 2018*, no. November, pp. 297–302, 2018, doi: 10.1109/UEMCON.2018.8796583.