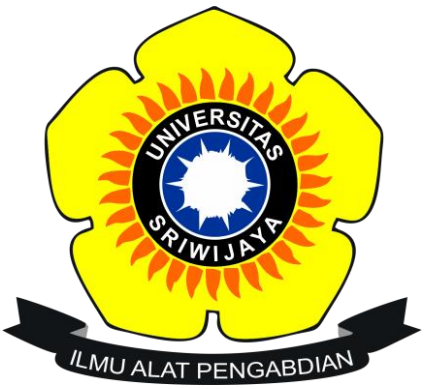
DETEKSI SERANGAN *DDOS* PADA *SMART HOME* DENGAN METODE *K-NEAREST NEIGHBOR (KNN)*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer



Oleh:

MUHAMMAD REZKY

09011281924064

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

LEMBAR PENGESAHAN

DETEKSI SERANGAN *DDOS* PADA *SMART HOME* DENGAN METODE *K-NEAREST NEIGHBOR (KNN)*

TUGAS AKHIR

Program Studi Sistem Komputer

Jenjang S1

Oleh:

Muhammad Rezky

09011281924064

Palembang, Agustus 2024

Pembimbing I	Pembimbing II
Prof. Deris Stiawan, M.T., Ph.D.	**Kemahyanto Exaudi, S. KOM, M.T.**
NIP. 197806172006041002	**NIP. 198405252023211018**

Mengetahui, 4/8/24

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

AUTHENTICATION PAGE

DETECTION OF DDOS ATTACKS ON SMART HOME USING THE K-NEAREST NEIGHBOR (KNN) METHOD

FINAL PROJECT

Computer System Study Program

Bachelor's Degree

By:

Muhammad Rezky

09011281924064

Palembang, Agustus 2024

Final Project Advisor I	**Final Project Advisor II**
Prof. Deris Stiawan, M.T., Ph.D.	**Kemahyanto Exaudi, S. KOM, M.T.**
NIP. 197806172006041002	**NIP. 198405252023211018**

Acknowledged,

Head of Computer System Department

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

LEMBAR PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Selasa

Tanggal : 30 Juli 2024

Tim Penguji :

1. Ketua : Aditya Putra Perdana Prasetyo, S.Kom., M.T.
2. Sekretaris : Nurul Afifah, M.Kom.
3. Penguji : Dr. Ahmad Zarkasi, M.T.
4. Pembimbing I : Prof Deris Stiawan, M.T., Ph.D.
5. Pembimbing II : Kemahyanto Exaudi, M.T.

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr.Ir.H.Sukemi.M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Muhammad Rezky

NIM : 09011281924064

Judul : Deteksi Serangan *DDoS* pada *Smart Home* dengan Metode *K-Nearest Neighbor (KNN)*

Hasil Pengecekan Plagiat/Turnitin: 2%

Menyatakan bahwa laporan tugas akhir ini adalah hasil karya saya sendiri dan tidak mengandung unsur penjiplakan atau plagiat. Saya sepenuhnya menyadari bahwa jika terbukti adanya penjiplakan atau plagiat dalam laporan tugas akhir ini, saya siap menerima sanksi akademik dari Universitas Sriwijaya. Pernyataan ini saya buat dengan kesadaran penuh dan tanpa adanya paksaan dari pihak manapun.

Palembang, Agustus 2024

Muhammad Rezky

NIM. 09011281924064

KATA PENGANTAR

Segala Puji dan syukur atas kehadiran Allah Subhanahu wa Ta'ala, karena berkat Rahmat dan Karunia-Nya, sehingga penulis dapat menyelesaikan Proposal Tugas Akhir ini yang berjudul "Deteksi Serangan *DDoS* pada *Smart Home* Dengan Metode *K-Nearest Neighbor (KNN)"* Shalawat serta salam tak lupa kita curahkan kepada junjungan kita Nabi Muhammad SAW beserta keluarga, sahabat dan para pengikutnya yang insyaallah istiqomah hingga akhir zaman.

Dalam kesempatan ini penulis mengucapkan terima kasih kepada pihak yang telah memberikan bantuan serta motivasi sehingga penulis dapat menyelesaikan penulisan Proposal Tugas Akhir ini:

1. Allah Subhanahu wa Ta'ala, yang telah melimpahkan Berkat dan Rahmatnya.
2. Keluarga yang selalu mendukung dan memotivasi penulis.
3. Bapak Prof. Dr. Erwin, S.Si, M.Si. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
5. Bapak Huda Ubaya, M.T. selaku Sekretaris Jurusan Sistem Komputer Universitas Sriwijaya.
6. Bapak Deris Stiawan, M.T., Ph.D. selaku Dosen Pembimbing I Tugas Akhir yang telah berkenan meluangkan waktunya guna membimbing, memberikan saran dan motivasi serta bimbingan terbaik untuk penulis dalam menyelesaikan Tugas Akhir ini.
7. Bapak Kemahyanto Exaudi, S. KOM, M.T. selaku Dosen Pembimbing II Tugas Akhir yang telah berkenan meluangkan waktunya guna membimbing dan memberikan saran terbaik untuk penulis dalam menyelesaikan Tugas Akhir ini.
8. Bapak Abdurahman, S. KOM., M. HAN. Selaku Dosen Pembimbing Akademik Jurusan Sistem Komputer.
9. Mbak Sari selaku admin Jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas administrasi selama perkuliahan.

10. Bapak, Ibu dosen jurusan Sistem Komputer yang telah memberikan ilmunya serta pengalamannya kepada penulis
11. Seluruh pihak yang tergabung dalam COMNETS.
12. Teman-teman seperjuangan Jurusan Sistem Komputer Angkatan 2019, yang selalu memberikan dukungan kepada penulis.
13. Teman-teman saya yang tergabung dalam Grup baCOD Mobile yang selalu memberikan dukungan kepada penulis.
14. Seluruh pihak yang tidak dapat penulis sebutkan satu persatu yang telah memberikan semangat serta doa.
15. Jurusan Sistem Komputer dan Almamater.

Penulis menyadari bahwa dalam penyusunan laporan ini masih sangat jauh dari kata sempurna. Oleh karena itu penulis mengharapkan kritik dan saran dari semua pihak yang berkenan agar laporan ini dapat lebih baik. Akhir kata penulis mengucapkan terima kasih banyak kepada semua pihak yang telah membantu penulis dalam proses penyelesaian serta penyusunan Proposal Tugas Akhir ini. Penulis juga berharap agar Proposal Tugas Akhir ini dapat bermanfaat dan berguna bagi siapa saja yang membacanya.

Palembang, Mei 2024

Penulis,

Muhammad Rezky

NIM. 09011281924064

DETEKSI SERANGAN *DDOS* PADA *SMART HOME* DENGAN METODE *K-NEAREST NEIGHBOR (KNN)*

MUHAMMAD REZKY (09011281924064)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
Email: rezkymfl@gmail.com

ABSTRAK

Serangan *Distributed Denial of Service* merupakan jenis serangan *cyber* yang di mana penyerang membuat layanan atau jaringan menjadi tidak tersedia bagi pengguna dengan cara sejumlah besar *traffic* palsu menuju *server* sehingga target terbebani dengan tujuan untuk menghentikan layanan. Pada penelitian ini, digunakan metode *K-Nearest Neighbor (KNN)* untuk mendeteksi serangan dalam dataset. Dataset yang digunakan pada penelitian ini merupakan dataset dari COMNETS *Smart Home* yang terdiri dari data *benign* dan serangan. Dataset diseimbangkan menggunakan Teknik oversampling SMOTE. Pada metode *K-Nearest Neighbor (KNN)* dengan perbandingan data 80:20 mendapatkan hasil parameter nilai K-5 dengan *accuracy* 97,32%, *precision* 98,91%, *recall* 95,78%, dan *f1 score* 97,32%.

Kata Kunci : *Distributed Denial of Service*, Deteksi Serangan, *K-Nearest Neighbor*

DETECTION OF DDOS ATTACKS ON SMART HOME USING THE K-NEAREST NEIGHBOR (KNN) METHOD

MUHAMMAD REZKY (09011281924064)
Department of Computer Systems, Faculty of Computer Science
Sriwijaya University
Email: rezkymfl@gmail.com

ABSTRACT

A Distributed Denial of Service (DDoS) attack is a type of cyber attack where the attacker makes a service or network unavailable to users by sending a large amount of fake traffic to the server, overloading the target with the intent to stop the service. In this research, the K-Nearest Neighbor (KNN) method is used to detect attacks in the dataset. The dataset used in this study is from the COMNETS Smart Home, consisting of benign and attack data. The dataset is balanced using the SMOTE oversampling technique. Using the K-Nearest Neighbor (KNN) method with an 80:20 data split, the results showed a K-5 with an accuracy of 97.32%, precision of 98.91%, recall of 95.78%, and an F1 score of 97.32%.

Keywords : *Distributed Denial of Service,* Deteksi Serangan, *K-Nearest Neighbor*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi yang maju menjadikan aktivitas bermasyarakat bertambah mudah, apalagi dibantu dengan perangkat seluler untuk menunjang kebutuhan sehari-hari. Seringkali ditemui kegiatan manusia yang tidak bisa lepas dari perangkat seluler seperti berselancar di sosial media, melakukan pekerjaan sampai sebatas membaca berita, yang dimana biasanya sudah di sisipkan dengan sensor Internet of Things (IoT) yang dapat memudahkan bagi para pengguna perangkat sesuler tersebut[1].

Pemanfaatan *gadget* semakin meningkat di era digital saat ini, terutama dengan munculnya perangkat-perangkat yang terhubung dengan internet seperti smart speaker, smart TV, dan smart lock. Penggunaan sistem *smart home* dan IoT menyediakan kemudahan dan kenyamanan bagi *user*, tetapi membawa risiko terhadap keamanan dan privasi. Serangan *cyber attack* merupakan salah satu ancaman yang sering dihadapi oleh sistem *smart home* dan IoT.[2]

Serangan *cyber attack* dapat menyebabkan perangkat IoT dalam *smart home* yang terinfeksi botnet dapat mengganggu layanan yang penting, kerusakan pada perangkat, kehilangan data, atau pencurian informasi pribadi. Selain itu, serangan *cyber attack* juga dapat menyebabkan gangguan pada jaringan, seperti penurunan kinerja atau kegagalan dalam komunikasi antar perangkat.[3] Serangan *cyber attack* pada sistem *smart home* dapat menyebabkan kerugian yang signifikan bagi pengguna, sehingga penting untuk mendeteksi serangan *cyber attack* pada sistem *smart home* secepat mungkin untuk mencegah kerugian yang lebih besar.

Penelitian ini penting untuk dilakukan dikarenakan masih terdapat kerentanan yang tinggi terhadap serangan *cyber attack* pada sistem *smart home*. Walaupun telah banyak penelitian yang dilakukan sebelumnya untuk mendeteksi serangan *cyber attack* pada sistem *smart home*, masih terdapat kelemahan dan kekurangan dari metode yang sudah ada.

Penelitian ini bertujuan untuk mengevaluasi kemampuan metode *K-Nearest Neighbors (K-NN)* dalam mendeteksi serangan *cyber attack* pada sistem *smart home* secara efektif dan akurat.

Sistem *smart home* rentan terhadap serangan *cyber attack* karena terhubung dengan *IoT* yang merupakan media yang mudah diakses oleh siapapun. Penggunaan perangkat-perangkat yang terhubung dengan internet tanpa proteksi yang memadai juga dapat meningkatkan risiko serangan *cyber attack* pada sistem *smart home*. Penelitian yang dilakukan oleh Kim, Park, dan Lee[4], menunjukkan bahwa sistem *smart home* yang terhubung dengan internet tanpa proteksi yang memadai lebih rentan terhadap serangan *cyber attack*. Selain itu, perangkat-perangkat yang terhubung dengan internet juga dapat menjadi sumber serangan *cyber attack* jika tidak dilakukan pembaruan sistem secara berkala.

Salah satu pemecahan yang bisa dipakai untuk melewati kejadian ini yakni dengan mengklasifikasi dataset menerapkan metode KNN. Dalam jurnal penelitian [5] disebutkan bahwa metode KNN merupakan salah satu metode umum yang digunakan untuk mendeteksi serangan *cyber attack*. KNN adalah satu dari sekian metode klasifikasi yang amat dasar dan mudah manfaatkan. Metode ini merupakan sistem klasifikasi non-parametrik yang kuat yang mengatasi masalah kepadatan probabilitas sepenuhnya.

Sehingga dari latar belakang tersebut yang telah disebutkan sebelumnya, peneliti ingin mengambil judul "Deteksi Serangan *DDoS* Pada *Smart Home* Dengan Metode *K-Nearest Neighbor (KNN)"*. Penelitian ini diharapkan dapat memberikan informasi untuk menghindari gangguan pada sistem *smart home*.

1.2. Rumusan Masalah

Rumusan masalah berikut terbentuk dari latar belakang yang sudah disebutkan sebelumnya:

1. Apakah metode KNN adalah metode yang tepat untuk mengklasifikasi serangan *cyber attack*?
2. Bagaimana efektivitas metode KNN dalam mengklasifikasi serangan *cyber attack*?
3. Bagaimana *machine learning* dapat mendeteksi serangan *cyber attack* pada system *smart home*?

1.3. Batasan Masalah

Batasan masalah ini berniat untuk memusatkan pada penelitian sehingga tidak terlalu luas dan tidak terlalu sempit, sehingga hasil penelitian yang didapatkan lebih tepat dan konkret. Batasan masalah yang ditetapkan untuk batasan penelitian ini adalah sebagai berikut:

1. Studi hanya mengutamakan pada klasifikasi serangan cyber attack pada sistem *smart home* yang menggunakan metode KNN.
2. Penelitian ini ini hanya akan membahas klasifikasi serangan *cyber attack* dengan menggunakan dataset yang dibuat kelompok *smarthome* comnets.

1.4. Tujuan

Tujuan penelitian ini dibentuk beralaskan rumusan masalah, yang mencakup hal-hal berikut:

1. Untuk mengetahui kemampuan metode KNN dalam mengklasifikasi serangan *cyber attack*.
2. Untuk membedakan data normal dan data serangan pada dataset comnets.
3. Untuk menemukan serangan *Distributed Denial-of-Service (DDoS)* di *smart home* yang mungkin merupakan tindakan penyerangan system.

1.5. Manfaat

Adapun beberapa manfaat dari studi ini adalah sebagai berikut:

1. Dapat menyeleksi antar data *benign* dan data serangan didalam dataset comnets.
2. Memanfaatkan metode KNN dapat mendeteksi data *benign* dan data serangan pada system *smart home.*

1.6. Metode Penelitian

Metodologi yang dipakai dalam studi ini ialah mencari, serta mengumpulkan referensi dari buku, jurnal, tesis, dan sumber lain yang relevan tentang “Deteksi Serangan *DDoS* pada Smart *Home* dengan Metode *K-Nearest Neighbor (KNN)”* bersama referensi lainnya.

1.6.1 Metode Studi Pustaka Literatur

Metode ini memungkinkan peneliti untuk menemukan dan mengumpulkan literatur seperti artikel, jurnal, dan sumber online yang signifikan dengan tema penelitian yang dibuat.

1.6.2 Metode Konsultasi

Dengan menggunakan metode ini, penulis dapat berbicara langsung dengan setiap orang yang mempunyai keterampilan dan keahlian yang diperlukan untuk menyelesaikan masalah penelitian ini.

1.7. Sistematika Penulisan

Sistematika yang dipakai dalam penulisan studi ini adalah:

BAB I PENDAHULUAN

Berisikan latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, metode penelitian, serta sistematika penulisan yang digunakan dalam penulisan tugas akhir ini.

BAB II TINJAUAN PUSTAKA

Berisikan konsep dari *Smart home, Cyber attack, DDoS*, dataset, Algoritma *K-Nearest Neighbors (K-NN)*.

BAB III METODOLOGI PENELITIAN

Berisikan desain penelitian, kerangka kerja penelitian, dan perancangan model yang akan digunakan pada penelitian untuk mendeteksi serangan *Distributed Denial-of-Service (DDoS).*

BAB IV HASIL DAN ANALISA

Berisikan hasil studi yang dilakukan dan pengkajian dari studi yang digunakan.

BAB V KESIMPULAN DAN SARAN

Dalam BAB V berisikan pendapat dari hasil studi yang dilakukan dan juga masukan untuk studi selanjutnya.

DAFTAR PUSTAKA

[1] by Yahya Sulaiman Al-hadhrami and F. Khadeer Hussain, “Intelligent Machine Learning Architecture for Detecting DDoS attacks in IoT networks,” 2020.

[2] Y. Alshboul, A. A. R. Bsoul, M. AL Zamil, and S. Samarah, “Cybersecurity of Smart Home Systems: Sensor Identity Protection,” *J. Netw. Syst. Manag.*, vol. 29, no. 3, pp. 1–27, 2021, doi: 10.1007/s10922-021-09586-9.

[3] N. M. A. Huijts *et al.*, “User experiences with simulated cyber-physical attacks on smart home IoT,” *Pers. Ubiquitous Comput.*, vol. 27, no. 6, pp. 2243–2266, 2023, doi: 10.1007/s00779-023-01774-5.

[4] S. Kim, M. Park, S. Lee, and J. Kim, “Smart home forensics—data analysis of iot devices,” *Electron.*, vol. 9, no. 8, pp. 1–13, 2020, doi: 10.3390/electronics9081215.

[5] H. Parvin, H. Alizadeh, and B. Minati, “A Modification on K-Nearest Neighbor Classifier,” *Glob. J. Comput. Sci. Technol.*, vol. 10, no. 14, pp. 37–41, 2010.

[6] V. Hnamte and J. Hussain, “Dependable intrusion detection system using deep convolutional neural network: A Novel framework and performance evaluation approach,” *Telemat. Informatics Reports*, vol. 11, no. July, p. 100077, 2023, doi: 10.1016/j.teler.2023.100077.

[7] K. Alissa, T. Alyas, K. Zafar, Q. Abbas, N. Tabassum, and S. Sakib, “Botnet Attack Detection in IoT Using Machine Learning,” *Comput. Intell. Neurosci.*, vol. 2022, 2022, doi: 10.1155/2022/4515642.

[8] A. Prasad and S. Chandra, “VMFCVD: An Optimized Framework to Combat Volumetric DDoS Attacks using Machine Learning,” *Arab. J. Sci. Eng.*, vol. 47, no. 8, pp. 9965–9983, 2022, doi: 10.1007/s13369-021-06484-9.

[9] A. L. Yaser, H. M. Mousa, and M. Hussein, “Improved DDoS Detection Utilizing Deep Neural Networks and Feedforward Neural Networks as Autoencoder,” *Futur. Internet*, vol. 14, no. 8, 2022, doi: 10.3390/fi14080240.

[10] L. G. Fahad and S. F. Tahir, “Activity recognition and anomaly detection in smart homes,” *Neurocomputing*, vol. 423, pp. 362–372, 2021, doi: 10.1016/j.neucom.2020.10.102.

[11] R. Hanipah and H. Dhika, “Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Dengan Wireshark,” *DoubleClick J. Comput. Inf. Technol.*, vol. 4, no. 1, p. 11, 2020, doi: 10.25273/doubleclick.v4i1.5668.

[12] C. Douligeris and A. Mitrokotsa, “DDoS attacks and defense mechanisms: Classification and state-of-the-art,” *Comput. Networks*, vol. 44, no. 5, pp. 643–666, 2004, doi: 10.1016/j.comnet.2003.10.003.

[13] A. Haditsah, “Klasifikasi Masyarakat Miskin menggunakan Metode Naïve Bayes,” *Ilk. J. Ilm.*, vol. 10, no. 2, pp. 160–165, 2018.

[14] Y. Mardi, “Data Mining : Klasifikasi Menggunakan Algoritma C4.5,” *Edik Inform.*, vol. 2, no. 2, pp. 213–219, 2017, doi: 10.22202/ei.2016.v2i2.1465.

[15] Jumaidi, “Sistem Pendukung Keputusan Untuk Menentukan,” *J. Istek*, vol. VI, no. 1, pp. 40–42, 2013.

[16] V. N. G. Raju, K. P. Lakshmi, V. M. Jain, A. Kalidindi, and V. Padma, “Study the Influence of Normalization/Transformation process on the Accuracy of Supervised Classification,” *Proc. 3rd Int. Conf. Smart Syst. Inven. Technol. ICSSIT 2020*, no. Icssit, pp. 729–735, 2020, doi: 10.1109/ICSSIT48917.2020.9214160.

[17] S. Nalcin, “StandardScaler vs. MinMaxScaler vs. RobustScaler: Which one to use for your next ML project?”

[18] D. Andrianto Iskandar and A. Salam, “JURNAL MEDIA INFORMATIKA BUDIDARMA Evaluasi Performa Oversampling dan Augmentasi pada Klasifikasi Penyakit Kulit Menerapkan Convolutional Neural Network,” vol. 8, pp. 240–250, 2024, doi: 10.30865/mib.v8i1.7119.

[19] K. Octavianus, “Oversampling Method SMOTE for Imbalanced Data.”

[20] A. A. Arifiyanti and E. D. Wahyuni, “Smote: Metode Penyeimbang Kelas Pada Klasifikasi Data Mining,” *SCAN - J. Teknol. Inf. dan Komun.*, vol. 15, no. 1, pp. 34–39, 2020, doi: 10.33005/scan.v15i1.1850.

[21] T. R. Shultz and S. E. Fahlman, *Encyclopedia of Machine Learning and Data Mining*. 2017. doi: 10.1007/978-1-4899-7687-1.

[22] R. Susmaga, “Confusion Matrix Visualization,” *Intell. Inf. Process. Web Min.*, pp. 107–116, 2004, doi: 10.1007/978-3-540-39985-8_12.

[23] J. Xu, Y. Zhang, and D. Miao, “Three-way confusion matrix for classification: A measure driven view,” *Inf. Sci. (Ny).*, vol. 507, pp. 772–794, 2020, doi: 10.1016/j.ins.2019.06.064.

[24] D. Chicco and G. Jurman, “The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation,” *BMC Genomics*, vol. 21, no. 1, pp. 1–13, 2020, doi: 10.1186/s12864-019-6413-7.

[25] M. Mimura, “Impact of benign sample size on binary classification accuracy,” *Expert Syst. Appl.*, vol. 211, no. November 2021, p. 118630, Jan. 2023, doi: 10.1016/j.eswa.2022.118630.

[26] E. Ropelewska, V. Slavova, K. Sabanci, M. Fatih Aslan, X. Cai, and S. Genova, “Discrimination of onion subjected to drought and normal watering mode based on fluorescence spectroscopic data,” *Comput. Electron. Agric.*, vol. 196, no. March, p. 106916, May 2022, doi: 10.1016/j.compag.2022.106916.

[27] Z. Meng, H. Huo, Z. Pan, L. Cao, J. Li, and F. Fan, “A gear fault diagnosis method based on improved accommodative random weighting algorithm and BB-1D-TP,” *Measurement*, vol. 195, no. March, p. 111169, May 2022, doi: 10.1016/j.measurement.2022.111169.

[28] M. Boubaris, A. Cameron, J. Manakil, and R. George, “Artificial intelligence vs. semi-automated segmentation for assessment of dental periapical lesion volume index score: A cone-beam CT study,” *Comput. Biol. Med.*, vol. 175, no. April, p. 108527, Jun. 2024, doi: 10.1016/j.compbiomed.2024.108527.