Deteksi Serangan *SQL Injection* Menggunakan *Deep Neural Networks*

Diajukan Sebagai Syarat Untuk Menyelesaikan
Pendidikan Program Strata-1 Pada
Jurusan Teknik Informatika Fakultas Ilmu Komputer
Universitas Sriwijaya

Oleh :

M. Friza Dwi Aditya Frinison
NIM : 09021181924018

Jurusan Teknik Informatika
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA
2024

LEMBAR PENGESAHAN SKRIPSI

Deteksi Serangan *SQL Injection* Menggunakan *Deep Neural Networks*

Oleh :

M. Friza Dwi Aditya Frinison
NIM : 09021181924018

Palembang 26 Juni 2024

Pembimbing I	Pembimbing II
Mastura Diana Marieska, M.T.	**Annisa Darmawahyuni, M.Kom.**
NIP. 198603212018032001	**NIP. 199006302023212044**

Mengetahui,
Ketua Jurusan Teknik Informatika

Dr. M. Fachrurozi, S.Si., M.T.
NIP. 198005222008121002

TANDA LULUS UJIAN KOMPREHENSIF SKRIPSI

Pada hari Kamis tanggal 20 Juni 2024 telah dilaksanakan ujian komprehensif oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya

Nama : M. Friza Dwi Aditya Frinison

NIM : 09021181924018

Judul : Deteksi Serangan *SQL Injection* Menggunakan *Deep Neural Networks*

dan dinyatakan LULUS

1. **Ketua**

   Osvari Arsalan, M.T. .....
   NIP. 198806282018031001
2. **Penguji**

   Samsuryadi, M.Kom., Ph.D. .....
   NIP. 197102041997021003
3. **Pembimbing I**

   Mastura Diana Marieska, M.T. .....
   NIP. 198603212018032001
4. **Pembimbing II**

   Annisa Darmawahyuni, M.Kom. .....
   NIP. 199006302023212044

Mengetahui,
Ketua Jurusan Teknik Informatika

Dr. M. Fachrurrozi, S.Si., M.T.
NIP. 198005222008121002

HALAMAN PERNYATAAN

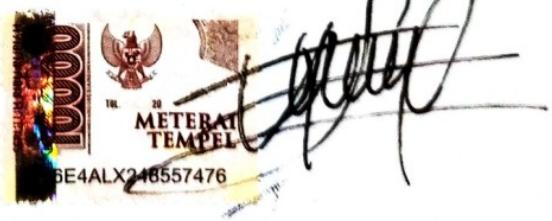
Yang bertanda tangan di bawah ini:

Nama	: M. Friza Dwi Aditya Frinison
NIM	: 09021181924018
Program Studi	: Teknik Informatika
Judul	: Deteksi Serangan *SQL Injection* Menggunakan *Deep Neural Networks*
Hasil Pengecekan Software Turnitin	**: 6%**

Menyatakan bahwa Skripsi ini merupakan hasil karya saya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam Skripsi ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian, pernyataan ini saya buat dengan sebenar-benarnya dan tanpa ada paksaan dari pihak manapun.

Palembang, 30 Juni 2024



M. Friza Dwi Aditya Frinison
NIM. 09021181924018

MOTTO DAN PERSEMBAHAN

قُلْ إِنَّ صَلَاتِى وَنُسُكِى وَمَحْيَاىَ وَمَمَاتِى لِلَّهِ رَبِّ ٱلْعَٰلَمِينَ ١٦٢

“Say, Indeed, my prayer, my rites of sacrifice, my living and my dying are for Allāh, Lord of the worlds.”

“Katakanlah, “Sesungguhnya salatku, ibadahku, hidupku, dan matiku hanyalah untuk Allah, Tuhan semesta alam.”

(**Q.S. Al-An’am: 162**)

“Verily, there is no greater life purpose than to perish while worshipping Allah alone.”

“Sungguh, tidak ada tujuan hidup yang lebih mulia selain mati dalam beribadah kepada Allah semata.”

Kupersembahkan karya tulis ini kepada:

- Allah SWT
- Keluargaku
- Dosen Pembimbing
- Teman-teman seperjuanganku
- Universitas Sriwijaya

ABSTRAK

SQL Injection diklasifikasikan oleh OWASP (*Open Web Application Security Project*) sebagai salah satu serangan yang paling merusak dalam 15 tahun terakhir. Penelitian ini ditunjukan untuk membuat sebuah IDS (*Intrusion Detection System*) yang dapat mendeteksi serangan *SQL Injection* melalui *HTTP POST Request*. Penelitian ini akan menggunakan model komputasi berbasis jaringan syaraf tiruan yang bernama DNN (*Deep Neural Networks)* dengan menggunakan data tabular yang akan dilakukan pra-pemrosesan terlebih dahulu sebelum dapat digunakan untuk membangun model DNN, data ini berisi *statements* beserta labelnya apakah *statement* tersebut merupakan serangan *SQL Injection* atau tidak. Selanjutnya, model akan dikonfigurasi dan dilatih menggunakan parameter-parameter yang berbeda, model dengan performa terbaik selanjutnya akan diintegrasikan dengan *packet capturer* sehingga membentuk sebuah IDS yang selanjutnya akan dilakukan uji coba terhadap serangan yang nyata. Hasil penelitian menunjukkan bahwa model dengan performa terbaik yang dikonfigurasi menggunakan parameter *ngram_range* (1, 2), *min_df* 4, *max_df* 0.8 dan dilatih dengan *epochs* sebanyak 5 menghasilkan *accuration* pada data uji sebesar 96.0% dan *loss* sebesar 20.0%. Selanjutnya, pengujian IDS yang telah terintegrasi dengan model terbaik terhadap serangan nyata menunjukan hasil *confusion matrix* dengan nilai 2935 (*True Negatives*), 841 (*True Positives*), 137 (*False Negatives*), 286 (*False Positives*)

Kata Kunci: *SQL Injection*, *Intrusion Detection System*, *Deep Neural Networks*

Palembang, 28 Juni 2024

Pembimbing I

Mastura Diana Marieska, M.T.
NIP. 198603212018032001

Pembimbing II

Annisa Darmawahyuni, M.Kom.
NIP. 199006302023212044

Mengetahui,
Ketua Jurusan Teknik Informatika

Dr. M. Fachrurrozi, S.Si., M.T.
NIP. 198005222008121002

ABSTRACT

SQL Injection has been classified by OWASP (Open Web Application Security Project) as one of the most damaging attacks in the past 15 years. This research aims to develop an IDS (Intrusion Detection System) capable of detecting SQL Injection attacks through HTTP POST Requests. The study employs a neural network-based computational model known as DNN (Deep Neural Networks), using tabular data that undergoes pre-processing before being utilized to build the DNN model. This data consists of statements labeled to indicate whether they are SQL Injection attacks or not. Subsequently, the model will be configured and trained using different parameters. The best-performing model will be integrated with a packet capturer, forming an IDS that will be tested against real attacks. The research findings indicate that the best-performing model, configured with the parameters ngram_range (1, 2), min_df 4, max_df 0.8, and trained for 5 epochs, achieves an accuracy of 96.0% on test data and a loss of 20.0%. Furthermore, testing the integrated IDS with the best model against real attacks showed a confusion matrix with values of 2935 (True Negatives), 841 (True Positives), 137 (False Negatives), and 286 (False Positives).

Keywords: *SQL Injection*, *Intrusion Detection System*, *Deep Neural Networks*

Palembang, 28 June 2024

Advisor I	Advisor II
Mastura Diana Marieska, M.T.	Annisa Darmawahyuni, M.Kom.
NIP. 198603212018032001	NIP. 199006302023212044

Approved,
Head of Informatics Engineering Department

Dr. M. Fachrurrozi, S.Si., M.T.
NIP. 198005222008121002

KATA PENGANTAR

Penulis mengucapkan puji dan syukur kehadirat Allah SWT, atas rahmat dan karunia-Nya sehingga penulisan Skripsi yang berjudul "**Deteksi Serangan *SQL* Injection Menggunakan Deep Neural Networks**" dapat diselesaikan. Skripsi ini merupakan salah satu syarat untuk menyelesaikan studi Strata-1 di program studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Sriwijaya.

Penulisan Skripsi ini tidak terlepas dari bantuan dan dukungan dari berbagai pihak. Oleh karena itu, penulis ingin menyampaikan terima kasih kepada:

1. Bapak Prof. Dr. Erwin, S.Si., M.Si. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
2. Bapak Dr. M. Fachrurrozi, S.Si., M.T., dan sebelumnya, Ibu Alvi Syahrini Utami, M.Kom. selaku Ketua Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Ibu Mastura Diana Marieska, M.T. selaku Dosen Pembimbing Skripsi pertama dan Ibu Annisa Darmawahyuni, M.Kom. selaku Dosen Pembimbing Skripsi kedua yang telah memberikan arahan dan bimbingan dalam pengerjaan skripsi ini.

4. Orang tua tercinta dan yang paling saya cintai, kakak yang saya kagumi dan banggakan, adik yang saya sayangi dan kasihi, dan seluruh keluarga penulis atas segala dukungan yang telah diberikan.
5. Teman seperjuangan penulis, Abang Muhammad Bagus, dan Ilmi Akbari yang menemani penulis di dalam perjalan ini, sehingga tidak menjadi sendiri, dan tidak menjadi sedih.
6. Teman terbaik penulis saat ini, Sanjaya Wangsadi Putra, M. Rizqi Assabil, Pristi Kartika Suryani, Abdul Khoir, Nursila Alwi Hudori, Alfath Aditya Putra, dll yang telah memberikan banyak dukungan dalam banyak bentuk baik secara langsung maupun tidak langsung.
7. Pak Nadiem Anwar Makarim, selaku menteri pendidikan, kebudayaan, riset, dan teknologi Indonesia saat ini, yang telah membentuk program perkuliahan yang bernama Kampus Merdeka, sehingga mahasiswa-mahasiswa seluruh Indonesia dapat lebih siap dalam menghadapi tantangan dan berinovasi di dunia industri.
8. Bangkit Academy beserta staff dan seluruh jajarannya, teman-teman seperjuangan Bangkit, dan adik-adikku yang saya mentori yang telah berkontribusi banyak terhadap penulis, sehingga penulis bisa berada di titik yang sekarang.
9. Seluruh pihak lainnya yang telah membantu penulis selama ini yang namanya tidak bisa ditulis satu per satu.

Kepada semua pihak yang disebutkan di atas, sekali lagi saya ucapkan terima kasih sebanyak-banyaknya. Penulis harap penelitian yang penulis kerjakan ini tidak hanya dapat menjadi manfaat kepada penulis sendiri, tapi orang-orang di sekitar penulis. Meskipun demikian, apa yang penulis ini tidak luput dari kesalahan maka dari itu, penulis mengharapkan masukkan dan kritik terhadap penelitian ini

Palembang, 23 Juni 2024

Penulis,

M. Friza Dwi Aditya Frinison

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Bab ini merupakan bagian dijelaskannya pokok-pokok pikiran yang menjadi landasan di balik penelitian ini. Adapun maksud dari pokok-pokok pikiran tersebut terdiri dari latar belakang masalah penelitian, perumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, sistematika penulisan, dan diakhiri dengan kesimpulan.

1.2. Latar Belakang Masalah

Teknologi informasi berkembang sangat cepat, *web applications* membawa kemudahan bagi manusia untuk mendapatkan informasi begitu juga dengan isu keamanan yang menyertainya (Chen et al., 2021a). Peretasan website secara ilegal mencapai 30.000 per harinya, dan sebanyak 64% perusahaan di seluruh dunia setidaknya pernah satu kali diserang. Diketahui bahwa pada maret 2021, 20 juta data diakses secara ilegal, dan setidaknya terjadi satu serangan setiap 39 detik (Triloka et al., 2022a). Hampir semua *web applications* memiliki kerentanan terhadap serangan *SQL Injection* yang diklasifikasikan oleh OWASP (*Open Web Application Security Project*) sebagai salah satu serangan yang paling merusak dalam 15 tahun terakhir (Ablahd and Dawwod, 2020)

(Ahmad and Karim, 2021) menjelaskan bahwa *SQL Injection* adalah sebuah metode yang digunakan oleh penyerang untuk mengakses atau mencuri *database* secara ilegal yang dilakukan dengan cara mengirimkan sintaks-sintaks ilegal ke *web applications* untuk nantinya dieksekusi oleh *database*. Secara teori setiap *web applications* yang dibangun dengan *database* memiliki kerentanan untuk diserang *SQL Injection,* karena serangan *SQL Injection* sendiri tidak berbeda dari akses normal user terhadap sistem, serangan dapat dicapai hanya dengan mengirimkan data *form*, *query string,* atau *page requests* di *web application* tersebut (Chen et al., 2021a), berdasarkan permasalahan di atas maka diperlukan sebuah sistem yang dapat melakukan deteksi serangan tersebut. *Intrusion Detection System* (IDS) adalah sistem yang digunakan untuk memonitoring aktivitas-aktivitas pada sebuah jaringan untuk mendeteksi apakah terdapat aktivitas yang illegal, penggunaan yang tidak sah, atau serangan-serangan dan mencegah hal tersebut terjadi (Anantvalee and Wu, 2007). Berdasarkan metode yang digunakan oleh IDS dalam menjalankan tugasnya dibagi menjadi dua: *signature-based detection* dan *anomaly-based detection* (Javaid et al., 2016)

Kebanyakan solusi yang digunakan untuk mitigasi serangan *web applications* dilakukan dengan cara menganalisis secara *static* trafik-trafik yang masuk ke *web applications*, solusi ini masuk ke dalam kategori *signature-based detection*. Strategi ini bekerja dengan cara mencocokkan karakteristik-karakteristik serangan yang sudah dibuat sebelumnya, dan ketika karekteristik

yang dimaksud terjadi, trafik-trafik yang dicurigai tersebut dapat dihentikan oleh *firewal* atau mekanisme-mekanisme pertahanan yang lain. Metode ini mempunyai keunggulan dalam segi kecepatan dan akurasi dalam mendeteksi serangan yang sudah diketahui karakteristiknya, namun kelemahannya terdapat pada keterbatasan dalam mendeteksi serangan baru (Ross, 2018). Sebaliknya kategori *anomaly-based detection* dapat mendeteksi varian-varian serangan baru, tetapi dengan resiko tingginya *false alarm* (Peng et al., 2016).

Deep Neural Network (DNN) memungkinkan model untuk dapat belajar dalam banyak *layers*, struktur ini terdiri dari sebuah *input layer*, sebuah *output layer*, dan banyak *hidden layers*. DNN digunakan untuk memodelkan fungsi *nonlinear* yang kompleks, dengan menambahkan jumlah dari *hidden layers* maka semakin meningkatnya pula level abstraksi sebuah model untuk performa yang lebih tinggi (Ahmad et al., 2021). DNN lebih unggul dalam mengabstraksikan representasi dan dapat mensimulasikan model yang sangat rumit, tak hanya sampai di situ DNN memiliki potensi yang besar untuk dapat secara efektif merepresentasikan data untuk menciptakan solusi yang bermanfaat. DNN menghasilkan output berdasarkan bobot atau *weight* yang terdapat di setiap koneksi dan *activation function* dari *neurons (Thirimanne et al., 2022)*.

Banyak penelitian yang telah dilakukan untuk mengatasi permasalahan ini, dengan berbagai macam teknik kecerdasan buatan untuk mendeteksi serangan *SQL Injection* menggunakan model *Machine Learning* dan *Deep Learning*

(Alghawazi et al., 2022), teknik ini sendiri masuk ke dalam kategori *anomaly-based detection* (Megantara and Ahmad, 2021). Penelitian yang dilakukan oleh (Chen et al., 2021a) menggunakan model *Natural Language Processing* (NLP) dan *Convolutional Neural Network* (CNN) untuk mendeteksi apakah pada sebuah *get request* HTTP (*Hypertext Transfer Protocol*) terdapat *query-query SQL Injection*. Penelitian yang sama juga dilakukan oleh (Triloka et al., 2022a) dengan menggunakan NLP dengan algoritma tradisional seperti *Support Vector Machine* (SVM) dapat menghasilkan akurasi di atas 99%.

Berdasarkan ulasan di atas serangan *SQL Injection* dapat dideteksi dengan cara melakukan pengecekan di bagian *POST Request* HTTP. Penelitian ini akan menggunakan algoritma *Deep Neural Network* untuk mendeteksi *SQL Injection*.

1.3. Rumusan Masalah

Berdasarkan latar belakang dari penelitian yang telah dikemukakan di atas, muncul beberapa permasalahan seperti:

1. Bagaimana cara mendeteksi serangan *SQL Injection* pada *web application* secara *real time*.
2. Bagaimana menggunakan algoritma DNN (*Deep Neural Networks*) untuk mendeteksi serangan *SQL Injection* pada *web application* secara *real time.*

1.4. Tujuan Penelitian

Berdasarkan permasalahan yang telah dikemukakan di atas, tujuan dari penelitian ini adalah:

1. Menghasilkan sebuah perangkat lunak yang dapat mendeteksi serangan *SQL Injection* pada *web application* secara *real time*.
2. Mengimplementasikan fitur dan parameter model DNN (*Deep Neural Networks*) apa saja untuk meningkatkan akurasi model dalam mendeteksi serangan *SQL Injection*.

1.5. Manfaat Penelitian

Berdasarkan ulasan di atas manfaat penelitian ini diantaranya adalah:

1. Perangkat lunak nantinya dapat digunakan untuk mendeteksi terjadinya serangan *SQL Injection* pada sebuah jaringan komputer secara *real-time*, sehingga dapat digunakan oleh *network administrator* dalam memonitor paket-paket yang berlalu lalang.
2. Peneliti lain dapat mengetahui fitur dan parameter model apa saja untuk meningkatkan akurasi model dalam mendeteksi serangan *SQL Injection*.

1.6. Batasan Masalah

Penelitian akan dilakukan dengan batasan-batasan masalah seperti berikut:

1. Serangan yang dideteksi hanya terbatas pada *SQL Injection* dan tidak terbatas pada jenis serangan secara spesifik.
2. Pendeteksian hanya dilakukan pada paket *HTTP* dengan R*equest Method POST*.
3. Menggunakan dataset yang didapatkan dari laman *Kaggle*.
4. Hanya sebatas pendeteksian, tidak melakukan pencegahan serangan *SQL Injection*.
5. Pengujian dilakukan dengan menggunakan laman pencarian buku sederhana dengan menggunakan DBMS (*Database Management System) PostgreSQL*.

1.7. Sistematika Penulisan

Sistematika penulisan proposal skripsi adalah sebagai berikut:

BAB I. PENDAHULUAN

Bab ini diuraikan mengenai latar belakang, perumusan masalah, tujuan, dan manfaat penelitian, batasan masalah/ruang lingkup, dan sistematika penulisan.

BAB II. KAJIAN LITERATUR

Bab ini menjelaskan tentang dasar teori yang digunakan dalam penelitian, hal-hal yang berkaitan dengan teknis seperti penjelasan mengenai serangan *SQL Injection* beserta jenis dan tipenya, algoritma *Deep Neural Network* yang dipakai, desain model, dan sebagainya akan dijelaskan secara detail.

BAB III. METODOLOGI PENELITIAN

Bab ini membahas tentang tahapan-tahapan yang akan dilaksanakan dalam penelitian ini. Segala tahapan pengerjaan akan dijelaskan secara rinci, bab ini juga berisi perancangan manajemen proyek pada pelaksanaan penelitian.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Bab ini membahas tentang desain software yang akan digunakan sebagai alat dalam penelitian, diantaranya diagram *use case*, konfigurasi parameter model, metodologi pengembangan dan desain perangkat lunak.

BAB V. HASIL DAN ANALISIS PENELITIAN

Bab ini mengulas hasil dan evaluasi yang diperoleh dari penelitian dengan menggunakan alat penelitian sesuai dengan rencana pengujian yang telah direncanakan.

BAB VI. KESIMPULAN DAN SARAN

Bab ini menjelaskan kesimpulan dari hasil penelitian yang telah dilakukan dan memberikan saran yang diharapkan dapat diterapkan pada penelitian berikutnya.

1.8. Kesimpulan

Berdasarkan uraian-uraian di atas maka penelitian yang akan dilakukan adalah pembuatan sebuah perangkat lunak yang dapat mendeteksi serangan *SQL*

Injection secara *real time* berdasarkan *payload* pada *POST Request* HTTP menggunakan algoritma *Deep Neural Networks*. Program ini dapat ditaruh pada *web server* sebuah jaringan komputer dan bertindak sebagai mekanisme pertahanan tambahan.

DAFTAR PUSTAKA

Ablahd, A.Z., Dawwod, S.A., 2020. Using Flask for SQLIA Detection and Protection. Tikrit J. Eng. Sci. 27, 1–14. https://doi.org/10.25130/tjes.27.2.01

Acheme, I.D., Vincent, O.R., 2021. Machine-learning models for predicting survivability in COVID-19 patients, in: Data Science for COVID-19. Elsevier, pp. 317–336. https://doi.org/10.1016/B978-0-12-824536-1.00011-3

Ahmad, K., Karim, M., 2021. A Method to Prevent SQL Injection Attack using an Improved Parameterized Stored Procedure. Int. J. Adv. Comput. Sci. Appl. 12. https://doi.org/10.14569/IJACSA.2021.0120636

Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., Ahmad, F., 2021. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Trans. Emerg. Telecommun. Technol. 32. https://doi.org/10.1002/ett.4150

Alghawazi, M., Alghazzawi, D., Alarifi, S., 2022. Detection of SQL Injection Attack Using Machine Learning Techniques: A Systematic Literature Review. J. Cybersecurity Priv. 2, 764–777. https://doi.org/10.3390/jcp2040039

Alias, S.B., Manickam, S., Kadhum, M.M., 2013. A Study on Packet Capture Mechanisms in Real Time Network Traffic, in: 2013 International Conference on Advanced Computer Science Applications and Technologies. Presented at the 2013 International Conference on Advanced Computer Science Applications and Technologies (ACSAT), IEEE, Kuching, Malaysia, pp. 456–460. https://doi.org/10.1109/ACSAT.2013.95

Alkhathami, Alzahrani, 2022. Detection of SQL injection attacks using machine learning in cloud computing platform. J. Theor. Appl. Inf. Technol 100, 5446–5459.

Anantvalee, T., Wu, J., 2007. A Survey on Intrusion Detection in Mobile Ad Hoc Networks, in: Xiao, Y., Shen, X.S., Du, D.-Z. (Eds.), Wireless Network Security, Signals and Communication Technology. Springer US, Boston, MA, pp. 159–180. https://doi.org/10.1007/978-0-387-33112-6_7

Chen, D., Yan, Q., Wu, C., Zhao, J., 2021a. SQL Injection Attack Detection and Prevention Techniques Using Deep Learning. J. Phys. Conf. Ser. 1757, 012055. https://doi.org/10.1088/1742-6596/1757/1/012055

Chen, D., Yan, Q., Wu, C., Zhao, J., 2021b. SQL Injection Attack Detection and Prevention Techniques Using Deep Learning. J. Phys. Conf. Ser. 1757, 012055. https://doi.org/10.1088/1742-6596/1757/1/012055

Dsouza, A., Lanjewar, V., Mahakal, A., Khachane, S., 2022. Real Time Network Intrusion Detection using Machine Learning Technique, in: 2022 IEEE Pune Section International Conference (PuneCon). Presented at the 2022

IEEE Pune Section International Conference (PuneCon), IEEE, Pune, India, pp. 1–5. https://doi.org/10.1109/PuneCon55413.2022.10014863
Farooq, U., 2021. Ensemble Machine Learning Approaches for Detection of SQL Injection Attack. Teh. Glas. 15, 112–120. https://doi.org/10.31803/tg-20210205101347
Fielding, R., Nottingham, M., Reschke, J., 2022. HTTP Semantics (No. RFC9110). RFC Editor. https://doi.org/10.17487/RFC9110
Javaid, A., Niyaz, Q., Sun, W., Alam, M., 2016. A Deep Learning Approach for Network Intrusion Detection System, in: Proceedings of the 9th EAI International Conference on Bio-Inspired Information and Communications Technologies (Formerly BIONETICS). Presented at the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS), ACM, New York City, United States. https://doi.org/10.4108/eai.3-12-2015.2262516
Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J., 2019. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity 2, 20. https://doi.org/10.1186/s42400-019-0038-7
McWhirter, P.R., Kifayat, K., Shi, Q., Askwith, B., 2018. SQL Injection Attack classification through the feature extraction of SQL query strings using a Gap-Weighted String Subsequence Kernel. J. Inf. Secur. Appl. 40, 199–216. https://doi.org/10.1016/j.jisa.2018.04.001
Megantara, A.A., Ahmad, T., 2021. A hybrid machine learning method for increasing the performance of network intrusion detection systems. J. Big Data 8, 142. https://doi.org/10.1186/s40537-021-00531-w
Peng, J., Choo, K.-K.R., Ashman, H., 2016. User profiling in intrusion detection: A review. J. Netw. Comput. Appl. 72, 14–27. https://doi.org/10.1016/j.jnca.2016.06.012
Ross, K., 2018. SQL Injection Detection Using Machine Learning Techniques and Multiple Data Sources (Master of Science). San Jose State University, San Jose, CA, USA. https://doi.org/10.31979/etd.zknb-4z36
Song, J., Chen, Y., 2022. A Study on the Application and the Advancement of Deep Neural Network Algorithm. J. Phys. Conf. Ser. 2146, 012001. https://doi.org/10.1088/1742-6596/2146/1/012001
Thirimanne, S.P., Jayawardana, L., Yasakethu, L., Liyanaarachchi, P., Hewage, C., 2022. Deep Neural Network Based Real-Time Intrusion Detection System. SN Comput. Sci. 3, 145. https://doi.org/10.1007/s42979-022-01031-1
Triloka, J., Hartono, H., Sutedi, S., 2022a. Detection of SQL Injection Attack Using Machine Learning Based On Natural Language Processing. Int. J. Artif. Intell. Res. 6. https://doi.org/10.29099/ijair.v6i2.355
Triloka, J., Hartono, H., Sutedi, S., 2022b. Detection of SQL Injection Attack Using Machine Learning Based On Natural Language Processing. Int. J. Artif. Intell. Res. 6. https://doi.org/10.29099/ijair.v6i2.355
Zhang, W., Li, Y., Li, X., Shao, M., Mi, Y., Zhang, H., Zhi, G., 2022a. Deep Neural Network-Based SQL Injection Detection Method. Secur. Commun. Netw. 2022, 1–9. https://doi.org/10.1155/2022/4836289

Zhang, W., Li, Y., Li, X., Shao, M., Mi, Y., Zhang, H., Zhi, G., 2022b. Deep Neural Network-Based SQL Injection Detection Method. Secur. Commun. Netw. 2022, 1–9. https://doi.org/10.1155/2022/4836289