SISTEM BERBASIS CONVOLUTIONAL NEURAL NETWORK-LONG SHORT TERM MEMORY UNTUK DETEKSI INJEKSI SQL

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Studi Teknik Komputer

disusun oleh

ALPIUS RANIS RANTETAMPANG

18.83.0327

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

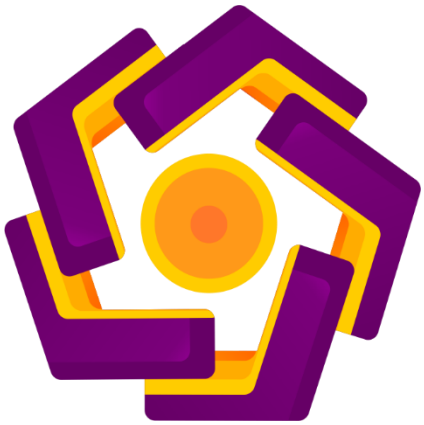
2023

SISTEM BERBASIS CONVOLUTIONAL NEURAL NETWORK-LONG SHORT TERM MEMORY UNTUK DETEKSI INJEKSI SQL

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer



disusun oleh

ALPIUS RANIS RANTETAMPANG

18.83.0327

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2023

HALAMAN PERSETUJUAN

SKRIPSI

SISTEM BERBASIS CONVOLUTIONAL NEURAL NETWORK-LONG SHORT TERM MEMORY UNTUK DETEKSI INJEKSI SQL

yang disusun dan diajukan oleh

Alpius Ranis Rantetampang

18.83.0327

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 04 Agustus 2023

Dosen Pembimbing,

Anggit Ferdita Nugraha, S.T., M.Eng.
NIK. 190302480

HALAMAN PENGESAHAN

SKRIPSI

SISTEM BERBASIS CONVOLUTIONAL NEURAL NETWORK-LONG SHORT TERM MEMORY UNTUK DETEKSI INJEKSI SQL

yang disusun dan diajukan oleh

Alpius Ranis Rantetampang

18.83.0327

Telah dipertahankan di depan Dewan Penguji
pada tanggal 04 Agustus 2023

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Joko Dwi Santoso, M.Kom **NIK. 190302181**	
Jeki Kuswanto, M.Kom **NIK. 190302456**	
Anggit Ferdita Nugraha, S.T., M.Eng **NIK. 190302480**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 04 Agustus 2023

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Alpius Ranis Rantetampang
NIM : 18.83.0327

Menyatakan bahwa Skripsi dengan judul berikut:

Sistem Berbasis Convolutional Neural Network-Long Short Term Memory untuk Deteksi Injeksi SQL

Dosen Pembimbing : Anggit Ferdita Nugraha, S.T., M.Eng.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 04 Agustus 2023

Yang Menyatakan,

Alpius Ranis Rantetampang

HALAMAN PERSEMBAHAN

Dengan penuh rasa syukur, penulis berhasil menyelesaikan skripsi ini, dan kini dengan rendah hati, penulis ingin menyajikannya sebagai persembahan kepada:

1. Dengan doa yang tak pernah berhenti mengalir dari orang tua, kakak, serta adik, penulis berhasil menyelesaikan skripsi tanpa terhalang oleh hambatan apapun.
2. Dosen Pembimbing saya, Anggit Ferdita Nugraha, S.T., M.Eng. yang senantiasa berusaha membimbing dan mengarahkan penelitian saya dengan penuh perhatian, juga tak henti-hentinya mengingatkan agar segera menyelesaikan proses penelitian dan naskah skripsi.
3. Sahabat terdekat senantiasa memberi dorongan dan mengingatkan untuk segera memulai proses menulis naskah ini dengan cara mencicilnya.

KATA PENGANTAR

Dengan rasa syukur dan puji, penulis ingin mengungkapkan keberhasilan menyelesaikan penyusunan skripsi ini atas penyertaan Allah. Skripsi ini berjudul "Sistem Berbasis Convolutional Neural Network - Long Short Term Memory untuk Deteksi Injeksi SQL" dan diajukan sebagai persyaratan kelulusan mata kuliah skripsi di Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.

Proses penyelesaian skripsi ini membutuhkan usaha yang gigih. Segenap ucapan terima kasih saya sampaikan kepada:

1. Prof. Dr. M. Suyanto, M.M., selaku Rektor Universitas Amikom Yogyakarta.
2. Anggit Ferdita Nugraha, S.T., M.Eng., selaku dosen pembimbing yang telah memberikan bimbingan berharga.
3. Para dosen Fakultas Ilmu Komputer yang telah berbagi ilmu yang sangat bermanfaat selama masa studi.

Skripsi ini tak akan terwujud tanpa dukungan dari orang-orang terdekat di sekitar saya yang selalu membantu dan mendukung. Penulis sadar bahwa karya ini tidak sempurna dan masih terdapat kekurangan. Oleh karena itu, penulis mohon maaf atas segala kesalahan yang terjadi.

Terakhir, penulis berharap skripsi ini dapat memberikan manfaat bagi para pembaca dan menjadi referensi yang berguna untuk pengembangan ke arah yang lebih baik.

Yogyakarta, 04 Agustus 2023
Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMBANG DAN SINGKATAN

CANDID	Candidate Evaluation for Discovering Intent Dynamically
BOW	Bag-Of-Words
IVS	Inverted Sentence Vector
OWASP	Open World Appllication Security Project
SQL	Structure Query Language
SQLI	Structure Query Language Injection
AI	Artificial Intelligence
ML	Machine Learning
DL	Deep Learning
LR	Logistic Regression
DTC	Decision Tree Classifier
RF	Random Forest
EB&BT	Ensemble Boosted dan Bagged Trees
TF-IDF	Term Frequency-Inverse Document Frequency
EP-CNN	Elastic Pooling – Convolutional Neural Network
MLP	Multi Layer Preceptron
RNN	Recurrent Neural Network
CNN	Convolutional Neural Network
LSTM	Long Short Term Memory
Bi-LSTM	Bidirectional Long Short-Term Memory
ANFIS	Adaptive Network Fuzzy Inference System
SVM	Support Vector Machines

DAFTAR ISTILAH

String	Tempat untuk menyimpan data teks untuk diolah.
Machine Learning	Sebuah mesin yang dapat belajar secara mandiri.
Deep Learning	Kembangan dari jaringan saraf tiruan untuk data kompleks.
Kueri	Perintah untuk bahasa structure query language
Hybrid	Menggabung dua atau lebih algoritma
Model	Algoritma
Epoch	Satuan untuk deep learning dalam bekerja
Real time	Informasi ditampilkan dengan kecepatan yang sangat cepat.
Source code	Kode program atau rangkaian perintah untuk computer.
Word2vector	Pengubahan kata yang dapat di mengerti computer
Database	Basis data
Backend	Logika pemrograman pada belakang sistem
Php	Bahasa skrip yang disisipkan pada html
Dense	Lapisan pada jaringan saraf tiruan yang setiap neuronnya terhubung dengan setiap neuron pada layer sebelumnya dan setelahnya.
Lightgbm	Gradient Boosting Framework
Feature map	Hasil dari filter yang dilakukan oleh lapisan konvolusi
Confusion matrix	4 tabel yang menunjukan nilai aktual dan nilai prediksi

INTISARI

Ancaman SQL Injection (SQLI) merupakan permasalahan besar dalam bidang keamanan aplikasi web. Mayoritas dari serangan SQL Injection (SQLI) menyebabkan kebocoran data pengguna, yang berakibat pada manipulasi, pembaruan, dan penghapusan data dalam sistem basis data. Untuk mencegah SQL Injection (SQLI), teknik tradisional serta teknik *machine learning* dan *deep learning* telah digunakan, namun teknik ini hanya dapat mengatasi beberapa jenis SQL Injection (SQLI) dan serangan baru yang memiliki representasi fitur yang lemah serta efisiensi algoritma. Tantangan utama terkait serangan SQL Injection (SQLI) adalah kemampuan para peretas untuk menciptakan *kueri* berbahaya baru yang tidak terdeteksi oleh teknik tradisional, serta teknik *machine learning* dan *deep learning* dengan algoritma tunggal memiliki kelemahan dalam representasi fitur dan efisiensi algoritma dalam mendeteksi serangan baru. Namun, masalah ini dapat diatasi secara efektif dengan memanfaatkan representasi fitur kuat dari Convolutional Neural Network (CNN) dan kemampuan Long Short Term Memory (LSTM) dalam memproses urutan kata, *model* dapat mengekstraksi informasi mendalam dari teks, termasuk teks terkait serangan SQL Injection (SQLI), dan mengenali pola urutan yang relevan untuk mendeteksi serangan baru tersebut. Dengan metode *hybrid* yang didukung dengan dataset SQL Injection (SQLI) dari kaggle menggunakan algoritma yaitu Convolutional Neural Network-Long Short Term Memory(CNN-LSTM) digunakan untuk mendeteksi serangan SQL Injection (SQLI) baru dengan tingkat akurasi sebesar 97%. Pada penelitian ini juga menguji *model* atau sistem untuk mendeteksi SQL Injection (SQLI) menggunakan *kueri* injeksi yang belum pernah dilatih pada *model* dengan nilai prediksi *model* sebesar 98% dan menentukan nilai ambang batas dari nilai prediksi untuk mendeteksi *kueri* injeksi yang diberikan pada *model*. Dengan tingkat akurasi sebesar 97% dan nilai prediksi *model* terhadap *kueri* baru sebesar 98%, hasil tersebut akan memberikan perlindungan yang kuat terhadap serangan SQL Injection (SQLI) baru, serta dapat mengurangi resiko potensial terhadap keamanan dan integritas sistem basis data.

Kata kunci: *kueri*, *model*, CNN-LSTM, SQL Injection, deteksi.

ABSTRACT

SQL Injection (SQLI) threats pose a significant issue in the field of web application security. The majority of SQL Injection attacks lead to user data leaks, resulting in manipulation, updates, and deletions of data in the database system. To prevent SQL Injection (SQLI), traditional techniques as well as *machine learning* and *deep learning* approaches have been employed. However, these methods can only address some types of SQL Injection (SQLI) and struggle with newly emerging attacks due to weak feature representations and algorithm efficiency. The main challenge concerning SQL Injection attacks lies in the hackers' ability to create new and undetected malicious queries that escape traditional, *machine learning*, and *deep learning* defenses. Single-algorithm-based *machine learning* and deep learning techniques suffer from weaknesses in feature representation and algorithm efficiency when detecting these novel attacks. Nonetheless, this issue can be effectively addressed by harnessing the powerful feature representation capabilities of Convolutional Neural Networks (CNN) and the sequential word processing abilities of Long Short Term Memory (LSTM). By leveraging these *model*, deep insights can be extracted from text, including text related to SQL Injection attacks, and identifying relevant sequential patterns to detect these new attacks. With a hybrid method supported by a SQL Injection (SQLI) dataset from Kaggle, the Convolutional Neural Network-Long Short Term Memory (CNN-LSTM) algorithm is used to detect new SQL Injection attacks with an accuracy level of 97%. This research also tested the *model* or system's ability to detect SQL Injection (SQLI) using injection queries that were not previously trained on the *model*, achieving a prediction *model* accuracy of 98%. The study determined a threshold value for the prediction score to detect given injection queries on the *model*. With an accuracy rate of 97% and a prediction score of 98% for new queries, these results provide strong protection against new SQL Injection attacks, reducing potential risks to the security and integrity of the database system.

Keyword: *Query*, *model*, CNN-LSTM, SQL Injection, detection.