KLASIFIKASI SERANGAN *SQL INJECTION* PADA *INTRUSION DETECTION SYSTEM* MENGGUNAKAN METODE *LONG SHORT TERM MEMORY STACKED*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

TRI PUTRI RAHMADANI
09011281823063

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2022

HALAMAN PENGESAHAN

KLASIFIKASI SERANGAN *SQL INJECTION* PADA *INTRUSION DETECTION SYSTEM* MENGGUNAKAN METODE *LONG SHORT TERM MEMORY STACKED*

TUGAS AKHIR

Program Studi Sistem Komputer

Jenjang S1

Oleh :

TRI PUTRI RAHMADANI
09011281823063

Palembang, Desember 2022

Mengetahui,

Ketua Jurusan Sistem Komputer	Pembimbing Tugas Akhir
Dr. Ir. H. Sukemi, M.T.	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 196612032006041001	**NIP. 198701222015041002**

AUTHENTICATION PAGE

CLASSIFICATION OF SQL INJECTION ATTACKS ON INTRUSION DETECTION SYSTEM USING THE LONG SHORT TERM MEMORY STACKED METHOD

FINAL TASK

Submitted to Complete One of the

Conditions Obtaining Strata 1 Degree

By

TRI PUTRI RAHMADANI

09011281823063

Palembang, December 2022

Acknowledge,

Head of Computer System Department	**Final Project Advisor**
Dr. Ir. H. Sukemi, M.T.	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 196612032006041001	**NIP. 198701222015041002**

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Jum'at

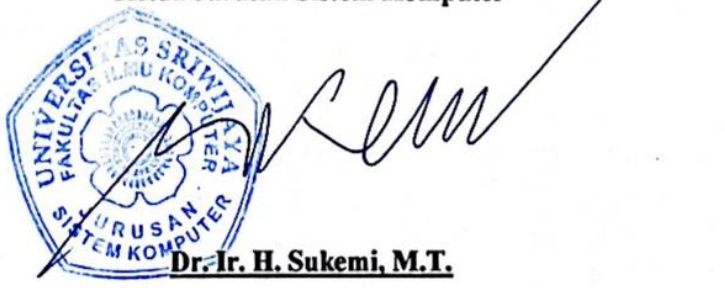
Tanggal : 23 Desember 2022

Tim Penguji :

1. **Ketua : Sarmayanta Sembiring, S.SI, M.T**
2. **Sekretaris : Nurul Afifah S.Kom, M.Kom.**
3. **Penguji : Ahmad Fali Oklilas S.T, M.T.**
4. **Pembimbing : Ahmad Heryanto S.Kom, M.T.**

Mengetahui,

Ketua Jurusan Sistem Komputer



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

NIP. 196612032006041000

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Tri Putri Rahmadani

NIM : 09011281823063

Judul : Klasifikasi Serangan *Sql Injection* Pada *Intrusion Detection System* Menggunakan Metode *Long Short Term Memory Stacked*

Hasil Pengecekan Software iThenticate/Turnitin : 6%

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

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.

Palembang, Desember 2022

Tri Putri Rahmadani

NIM.09011281823063

KATA PENGANTAR

Puji syukur kepada Allah SWT atas rahmat-Nya sehingga penulis diberi kesempatan untuk menyelesaikan Tugas Akhir yang berjudul "**Klasifikasi Serangan *Sql Injection* Pada *Intrusion Detection System* Menggunakan *Metode Long Short Term Memory Stacked***". Pada kesempatan ini, penulis menyampaikan rasa terima kasih kepada semua pihak yang telah membantu dan mendukung sehingga dapat memberikan dorongan kepada penulis dalam penyelesaian Tugas Akhir ini.

Oleh karena itu, penulis mengucapkan rasa terima kasih kepada:

- Allah SWT, yang telah memberikan rahmat dan karunia-Nya sehingga saya dapat menyelesaikan penulisan tugas akhir ini dengan baik.

- Kedua orang tua dan keluarga saya yang tidak berhenti memberikan do'a restu dan dukungan selama menempuh perkuliahan.

- Yang terhormat, Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.

- Yang terhormat, Bapak Dr. Ir. H. Sukemi, M.T., selaku ketua jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

- Yang terhormat, Bapak Ahmad Heryanto, S.Kom., M.T., selaku pembimbing akademik dan pembimbing tugas akhir yang selalu meluangkan waktu untuk memberikan bimbingan, arahan dan dukungan dalam menyelesaikan tugas akhir.

- Mbak Reni selaku admin jurusan Sistem Komputer yang telah membantu mengurus segala keperluan dan berkas selama perkuliahan.

- Kepada Hanna Pertiwi, Caturning Anjarwati, Rani Octaviani, Prazna Paramitha Avi, Berby Febriana Audrey, Jumhadi, Dimas, Taufik, Yusdiansya dan seluruh teman-teman satu angkatan Sistem Komputer 2018, serta kepada Dwi Ajeng Widuri, Siti Inda Pratiwi, Dyah Ayu Pangestika, Tiara Vingki Lestari, Izmiyati, Diah Tunjung Sari dan Puji Lestari yang telah memberikan bantuan dan dukungan kepada penulis sehingga penulis bisa menyelesaikan tugas akhir ini dengan baik.

- Terkhusus kepada Yadi yang selalu memberikan dukungan dan semangat kepada penulis dalam penyelesaian tugas akhir ini.

- Semua pihak yang telah membantu.

Penulis menyadari bahwa dalam penulisan Tugas Akhir ini masih banyak terdapat kekurangan, oleh karena itu seluruh saran dan kritik sangatlah berguna untuk menjadi bahan evaluasi bagi penulis.

Indralaya, Desember 2022

Penulis

Tri Putri Rahmadani

NIM.09011281823063

CLASSIFICATION OF SQL INJECTION ATTACKS ON INTRUSION DETECTION SYSTEM USING THE LONG SHORT TERM MEMORY STACKED METHOD

TRI PUTRI RAHMADANI
Computer Engineering Department, Computer Science Faculty, Sriwijaya University

Email : tprahmadani@gmail.com

ABSTRACT

SQL Injection is an attack technique by entering malicious SQL commands (queries) and can manipulate command logic to gain access to databases and other sensitive information. The main aim of this attack is to exploit the victim's database to reveal personal information about web applications such as passwords, usernames, secret keys and so on. There are two objectives in this study, among others, to build a Stacked LSTM method model for the ability to classify Sql Injection attacks on the CIC-IDS 2018 dataset. Second, produce a model with performance that is as expected. Therefore, to overcome the previous problem, the deep learning method was used. The Deep Learning method used is the Stacked LSTM method which is a branch of LSTM. In this study the Principal Component Analysis (PCA) technique was used to reduce dimensions and training time efficiency, the Synthetic Minority Over-sampling Technique (SMOTE) technique was also applied to balance the dataset to be processed, then Hyperparameter Tuning is applied to see the best parameters that will be applied to the research model. Research validation was carried out 5 times in the study. The best validation results from the overall results were 90% training data and 10% testing data where in this study the results obtained were 98.76% accuracy, 99.94% recall, 97.59% specificity, 97.64% precision, and F1 -Score 98.78%.

Keywords *: Sql Injection, Stacked LSTM, PCA, SMOTE, CIC-IDS-2018 Datasets*

Acknowledge,

Head of Computer System Department	**Final Project Advisor**
Dr. Ir. H. Sukemi, M.T.	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 196612032006041001	**NIP. 198701222015041002**

KLASIFIKASI SERANGAN *SQL INJECTION* PADA *INTRUSION DETECTION SYSTEM* MENGGUNAKAN METODE *LONG SHORT TERM MEMORY STACKED*

TRI PUTRI RAHMADANI
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : tprahmadani@gmail.com

ABSTRACT

SQL Injection atau Injeksi SQL adalah teknik penyerangan dengan memasukkan perintah (query) SQL yang berbahaya dan dapat memanipulasi logika perintah untuk mendapatkan akses pada database dan informasi sensitif lainnya. Tujuan utama dari serangan ini adalah untuk mengeksploitasi database korban untuk memperlihatkan informasi pribadi mengenai aplikasi web seperti kata sandi, nama pengguna, kunci rahasia, dan sebagainya. Terdapat dua tujuan dalam Penelitian ini antara lain untuk Membangun model metode Stacked LSTM untuk kemampuan klasifikasi serangan Sql Injection pada dataset CIC-IDS 2018. Kedua Menghasilkan model dengan kinerja yang sesuai dengan yang diharapkan. Oleh karena itu untuk mengatasi masalah sebelumnya digunakan metode deep learning. Adapun metode Deep Learning yang dipakai adalah memakai metode Stacked LSTM yang merupakan cabang dari LSTM Dalam penelitian ini menggunakan teknik Principal Component Analysis (PCA) untuk mereduksi dimensi dan juga efisiensi waktu pelatihan, diterapkan juga teknik Synthetic Minority Over-sampling Technique (SMOTE) untuk menyeimbangkan dataset yang akan diolah, lalu diterapkan Tuning Hyperparameter untuk melihat parameter terbaik yang akan diterapkan pada model penelitian. Validasi penelitian dilakukan sebanyak 5 kali dalam penelitian. Hasil validasi terbaik dari keseluruhan hasil yaitu pada 90% data training dan 10% data testing dimana pada penelitian ini didapatkan hasil poin akurasi 98,76%, recall 99,94%, spesifitas 97,59%, presisi 97,64%, dan F1-Score 98,78%.

***Kata Kunci** : Sql Injection, Stacked LSTM, PCA, SMOTE, CIC-IDS-2018 Datasets*

Mengetahui,

Ketua Jurusan Sistem Komputer	**Pembimbing Tugas Akhir**
Dr. Jr. H. Sukemi, M.T.	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 196612032006041001	**NIP. 198701222015041002**

DAFTAR ISI

Halaman

HALAMAN PENGESAHAN ..... **i**
AUTHENTICATION PAGE ..... **ii**
HALAMAN PERSETUJUAN ..... **iii**
HALAMAN PERNYATAAN ..... **iv**
KATA PENGANTAR ..... **v**
ABSTRACT ..... **vii**
ABSTRAK ..... **viii**
DAFTAR ISI ..... **ix**
DAFTAR GAMBAR ..... **xii**
DAFTAR TABEL ..... **xiv**
BAB I PENDAHULUAN **1**
1.1. Latar Belakang 1
1.2. Perumusan Masalah 2
1.3. Batasan Masalah 3
1.4. Tujuan 3
1.5. Sistematika Penulisan 3
BAB II TINJAUAN PUSTAKA **5**
2.1. Penelitian Terdahulu 5
2.2. Penelitian Terkait 12
2.3. SQL Injection 14
2.4. Intrusion Detection System (IDS) 16
2.5. *Synthetic Minority Over-sampling Technique* (SMOTE) 19
2.6. Deep Learning 21
2.7. Long Short-Term Memory 21
2.8. *Stacked* LSTM 23
2.9. Confusion Matrix 24

BAB III METODOLOGI PENELITIAN 27

3.1. Pendahuluan 27

3.2. Kerangka Kerja 27

3.3. Pre-Processing Data 29

3.3.1. Persiapan Dataset 29

3.3.2. Filtering dan SMOTE Data 35

3.3.3. Pembagian Data Uji dan Latih 36

3.4. Procesing Data 36

3.4.1. Seleksi Fitur dengan PCA 36

3.4.2. Rancangan Model *Stacked* LSTM 37

3.4.3. Validasi Performa Model 39

3.4.4. Tuning Hyperparameter 39

3.5. Skenario Penelitian 39

BAB IV HASIL DAN ANALISIS 42

4.1 Pendahuluan 42

4.2 Hasil Ekstraksi Dataset 42

4.3 Seleksi Fitur PCA 44

4.4 Hyperparameter *LSTM Stacked* 44

4.5 Tuning Hyperparameter *LSTM Stacked* 45

4.5.1 Hyperparameter Utama 47

4.6 Hasil Klasifikasi 48

4.7 Validasi Hasil Klasfikasi 49

4.8 Validasi Hasil Rasio 50:50 49

4.9 Validasi Hasil Rasio 60:40 51

4.10 Validasi Hasil Rasio 70:30 54

4.11 Validasi Hasil Rasio 80:20 57

4.12 Validasi Hasil Rasio 90:10 60

4.13 Analisis Validasi BACC dan MCC 63

BAB V KESIMPULAN 64

5.1 Kesimpulan 64

5.2 Saran 64

DAFTAR PUSTAKA 65

DAFTAR GAMBAR

Halaman

Gambar 2.1 Timeline Penelitian Terkait 14

Gambar 2.2 Komponen Kerja IDS [40] 16

Gambar 2.3 Cara Kerja *Anomaly Based* IDS[41] 18

Gambar 2.4 Cara Kerja *Signatured Based* IDS[41] 19

Gambar 2.5 *Flowchart* SMOTE[43] 20

Gambar 2.6 (a) Arsitektur Long Short-term Memory, (b) Stacked LSTM [45]..... 22

Gambar 2.7 Perbandingan Arsitektur LSTM dan *Stacked* LSTM[49] 23

Gambar 3.1 Metodologi Penelitian 28

Gambar 3.2 *Pre-Processing* Data 29

Gambar 3.3 Perbandingan Jumlah Data *SQL Injection* dan Normal 35

Gambar 3.4 Arsitektur Model *Stacked* LSTM 37

Gambar 3.5 Rancangan *Stacked* LSTM 38

Gambar 3.6 Skenario Penelitian 40

Gambar 4.1 Data .pcap 42

Gambar 4.2 Hasil Ekstraksi Data 43

Gambar 4.3 Proses Ekstraksi Data 43

Gambar 4.4 Data PCA 44

Gambar 4.5 Analisis Hasil Klasifikasi 48

Gambar 4.6 Grafik loss rasio data 50:50 49

Gambar 4.7 Grafik Akurasi rasio data 50:50 50

Gambar 4.8 ROC Curve rasio data 50:50 51

Gambar 4.9 Grafik loss rasio data 60:40 52

Gambar 4.10 Grafik Akurasi rasio data 60:40 52

Gambar 4.11 ROC Curve rasio data 60:40 54

Gambar 4.12 Grafik loss rasio data 70:30 55

Gambar 4.13 Grafik Akurasi rasio data 70:30 55

Gambar 4.14 ROC Curve rasio data 70:30 56

Gambar 4.15 Grafik loss rasio data 80:20 57

Gambar 4.16 Grafik Akurasi rasio data 80:20 58

Gambar 4.17 ROC Curve rasio data 80:20 59

Gambar 4.18 Grafik loss rasio data 90:10 60
Gambar 4.19 Grafik Akurasi rasio data 90:10 60
Gambar 4.20 ROC Curve rasio data 90:10 62
Gambar 4.21 Analisis BACC dan MCC 63

DAFTAR TABEL

Halaman

Tabel 2.1 Penelitian Terdahulu 5
Tabel 2.2 Penelitian Terkait 13
Tabel 2.3 Perbandingan Formula LSTM dan *Stacked* LSTM[51] 24
Tabel 2.4 *Confussion Matrix* Dua Kelas[42] 25
Tabel 3.1 Daftar Bentuk Penyerangan dan Durasi Penyerangan 30
Tabel 3.2 Fitur *Dataset* CSE-CIC-2018 yang Diekstraksi dengan *CICFlowMeter-V3* 31
Tabel 3.3 Persebaran Banyak Skenario Serangan 35
Tabel 3.4 Jumlah Pembagian Data Latih dan Data Uji 36
Tabel 3.5 Matriks Konfusi Hasil Klasifikasi dengan Model yang Dirancang 39
Tabel 3.6 Skenario Penelitian 41
Tabel 4.1 Unit node tuning hyperparameter 45
Tabel 4.2 Drop out tuning hyperparameter 46
Tabel 4.3 Learning Rate tuning hyperparameter 46
Tabel 4.4 Batch size tuning hyperparameter 47
Tabel 4.5 Hyperparameter utama 47
Tabel 4.6 Confusion matrix rasio data 50:50 50
Tabel 4.7 Hasil performa klasifikasi rasio data 50:50 51
Tabel 4.8 Confusion matrix rasio data 60:40 53
Tabel 4.9 Hasil performa klasifikasi rasio data 60:40 53
Tabel 4.10 Confusion matrix rasio data 70:30 56
Tabel 4.11 Hasil performa klasifikasi rasio data 70:30 56
Tabel 4.12 Confusion matrix rasio data 80:20 58
Tabel 4.13 Hasil performa klasifikasi rasio data 80:20 59
Tabel 4.14 Confusion matrix rasio data 90:10 61
Tabel 4.15 Hasil performa klasifikasi rasio data 90:10 61
Tabel 4.16 Hasil Validasi BACC dan MCC 62

DAFTAR LAMPIRAN

Lampiran 1. Form Perbaikan

Lampiran 2. Cek Plagiat

BAB I
PENDAHULUAN

1.1 Latar Belakang

Sekarang ini, teknologi internet telah menjadi salah satu kebutuhan primer dalam kehidupan modern. Perkembangan teknologi informasi yang pesat menjadi suatu faktor pendukung kemajuan internet sekarang ini. Kemudahan akses yang diberikan oleh teknologi ini memberikan kemudahan bagi manusia untuk mengakses berbagai macam jenis informasi secara *real-time*. Sehingga hal inilah yang mendukung internet menjadi media yang paling banyak digunakan saat ini [1], [2].

Sekarang ini, banyak sekali aktivitas yang bisa diakses dalam aplikasi web. Selain mengakses informasi, pengguna juga dapat melakukan pertukaran informasi dalam aplikasi web. Oleh sebab itu, dalam eksekusinya aplikasi web membutuhkan suatu media untuk menampung berbagai informasi yang terdapat dalam aplikasi web tersebut dimana media ini yang kemudian disebut dengan d*atabase*[1], [3].

Aplikasi web dengan database yang menyimpan berbagai informasi penting merupakan salah satu target dari SQL *Injection*. Penyerangan ini dilakukan dengan tujuan agar penyerang dapat mengakses informasi penting dengan menyuntikkan *Querry* SQL sehingga informasi ini kemudian dapat menghilang [1]. Hingga saat ini SQL *Injection* masih menjadi suatu ancaman besar bagi keamanan aplikasi web. Oleh sebab itu, penelitian dalam mengidentifikasi dan klassifikasi penyerangan ini harus dilakukan [4]–[6].

Sekarang ini penelitian mengenai SQL *Injection* telah mulai mengarah kepada metode *machine learning*, terutama *deep learning* [7]. Telah banyak metode *machine learning* klasik yang digunakan dalam deteksi dan klasifikasi SQL *Injection* seperti *Naïve Bayes*, SVM, *Multilayer Percepton, Random Forest*, dan *Decision Tree* akan tetapi metode ini masih belum maksimal dalam performanya [1], [4]–[8]. Pada [9]–[11], tampak bahwa dengan metode machine learning permasalahan seperti pemilihan fitur masukkan yang tepat masih terbatas karena pemilihan berdasarkan set kombinasi fitur masih dipilih secara manual

oleh manusia. Selain itu, beberapa penelitian dengan metode machine learning mempu menghasilkan hasil klasifikasi yang baik akan tetapi membutuhkan penigkatan performa saat implementasi model dalam lingkungan *real-life* seperti yang diungkapkan pada [5], [12]. Berdasarkan beberapa limitasi tersebut maka salah satu metode yang dapat menjadi salah satu solusi adalah dengan menggunakan *deep learning* [9].

Beberapa penelitian sebelumnya telah mulai menggunakan metode *deep learning* dalam deteksi dan klasifikasi serangan SQL *Injection*. Beberapa arsitektur yang pernah digunakan sebelumnya adalah CNN [8] dan LSTM [7]. Berdasarkan kedua penelitian tersebut dapat disimpulkan bahwa performa klasifikasi SQL *Injection* menunjukkan performa yang jauh lebih baik dari pada metode dengan *machine learning*. Meskipun *deep learning* telah menunjukkan hasil yang baik dalam melakukan klasifikasi serangan, metode ini masih membutuhkan peningkatan performa agar dapat menjadi sistem yang *robust*.

Pada penelitian ini, peeliti akan membangun model dengan arsitektur LSTM *Stacked* sebagai metode klasifikasi serangan SQL *Injection* pada IDS. Penelitian ini akan berfokus pada pemilihan fitur masukkan dan kombinasi parameter model. Evaluasi performa model akan dilakukan dengan menggunakan *cross-validation* dimana dataset akan dibagi menjadi beberapa partisi guna menemukan partisi dengan performa terbaik. Model akan dievaluasi dengan perhitungan *confussion matrix* seperti presisi, recall, akurasi, dan F *Score*.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang dijelaskan, maka perumusan masalah yang akan dibahas adalah sebagai berikut :

1. Bagaimana membangun model *Stacked Long Short Term Memory* untuk melakukan klasifikasi serangan SQL *Injection* pada *dataset* CSE-CIC-IDS 2018?
2. Bagaimana arsitektur dan parameter model agar model dapat memperoleh performa terbaik?

1.3 Batasan Masalah

Berikut batasan masalah pada Tugas Akhir ini, yaitu :

1. Penelitian ini menggunakan *dataset* CSE-CIC-IDS-2018 dari Universitas of New Brunswick (UNB).
2. Penelitian ini merupakan simulasi program dengan menggunakan Bahasa pemrograman *Python*.
3. Simulasi program ini merupakan klasifikasi biner.

1.4 Tujuan

Tujuan yang akan dicapai dari penelitian ini adalah sebagai berikut :

1. Membangun model *Long Short Term Memory Stacked* untuk melakukan klasifikasi serangan SQL *Injection* dengan menggunakan *dataset CSE-CIC-IDS 2018* Universitas of New Brunswick (UNB).
2. Menghasilkan model dengan kinerja yang sesuai dengan yang diharapkan.

1.5 Sistematika Penulisan

Sistematika yang akan digunakan dalam penulisan tugas akhir adalah sebagai berikut :

BAB I PENDAHULUAN

Bab pertama akan memaparkan sistematis mengenai latar belakang, tujuan penelitian, rumusan masalah, serta bentuk sistematika penelitian.

BAB II TINJAUAN PUSTAKA

Bab kedua akan menjelaskan teori-teori dasar yang akan menjadi landasan dari penelitian ini. Dasar teori yang akan dibahas pada bab ini adalah literatur mengenai *SQL Injection, Intrusion Detection System, Long Short Term Memory Stacked* dan performa validasi.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan proses dan rangkaian kegiatan dalam penelitian. Penelitian akan dimulai dari persiapan data,

BAB IV HASIL DAN ANALISIS

Bab ini akan memaparkan hasil pengujian yang diperoleh dan menjelaskan Analisa terhadap hasil penelitian yang telah dilakukan.

BAB V KESIMPULAN

Bab ini akan menampung simpulan yang dapat disimpulkan dari hasil keseluruhan penelitian dan analisa terhadap penelitian yang telah dilakukan.

DAFTAR PUSTAKA

[1] E. Prasetyo, P. Sukarno, and E. M. Jadied, "Klasifikasi SQL Injection Menggunakan Algoritma Naïve Bayes," vol. 8, no. 5, pp. 10605–10620, 2021.

[2] A. S. Irawan, E. S. Pramukantoro, and A. Kusyanti, "Pengembangan Intrusion Detection System Terhadap SQL Injection Menggunakan Metode Learning Vector Quantization," *J. Pengemb. Teknol. Inf. dan Ilmu Komput. Univ. Brawijaya*, vol. 2, no. 6, pp. 2295–2301, 2018.

[3] N. M. Dahlan M., Latubessy A., "Analisa Keamanan Web Server Terhadap Serangan Possibility Sql Injection," *Pros. SNATIF*, vol. 0, no. 0, pp. 251–258, 2015.

[4] K. Zhang, "A machine learning based approach to identify SQL injection vulnerabilities," *Proc. - 2019 34th IEEE/ACM Int. Conf. Autom. Softw. Eng. ASE 2019*, pp. 1286–1288, Nov. 2019, doi: 10.1109/ASE.2019.00164.

[5] M. Hasan, Z. Balbahaith, and M. Tarique, "Detection of SQL Injection Attacks: A Machine Learning Approach," *2019 Int. Conf. Electr. Comput. Technol. Appl. ICECTA 2019*, Nov. 2019, doi: 10.1109/ICECTA48151.2019.8959617.

[6] A. Rai, M. M. I. Miraz, D. Das, H. Kaur, and Swati, "SQL Injection: Classification and Prevention," *Proc. 2021 2nd Int. Conf. Intell. Eng. Manag. ICIEM 2021*, pp. 367–372, 2021, doi: 10.1109/ICIEM51511.2021.9445347.

[7] Q. Li, F. Wang, J. Wang, and W. Li, "LSTM-Based SQL Injection Detection Method for Intelligent Transportation System," *IEEE Trans. Veh. Technol.*, vol. 68, no. 5, pp. 4182–4191, 2019, doi: 10.1109/TVT.2019.2893675.

[8] A. Luo, W. Huang, and W. Fan, "A CNN-based Approach to the Detection of SQL Injection Attacks," *Proc. - 18th IEEE/ACIS Int. Conf. Comput. Inf. Sci. ICIS 2019*, pp. 320–324, Jun. 2019, doi: 10.1109/ICIS46139.2019.8940196.

[9] D. Chen, Q. Yan, C. Wu, and J. Zhao, "SQL Injection Attack Detection and Prevention Techniques Using Deep Learning," *J. Phys. Conf. Ser.*, vol.

1757, no. 1, 2021, doi: 10.1088/1742-6596/1757/1/012055.

[10] S. Scholarworks and S. Mishra, “SQL Injection Detection Using Machine Learning,” *Master’s Proj.*, May 2019, doi: https://doi.org/10.31979/etd.j5dj-ngvb.

[11] A. Joshi and V. Geetha, “SQL Injection detection using machine learning,” *2014 Int. Conf. Control. Instrumentation, Commun. Comput. Technol. ICCICCT 2014*, pp. 1111–1115, Dec. 2014, doi: 10.1109/ICCICCT.2014.6993127.

[12] L. Erdődi, Å. Å. Sommervoll, and F. M. Zennaro, “Simulating SQL injection vulnerability exploitation using Q-learning reinforcement learning agents,” *J. Inf. Secur. Appl.*, vol. 61, no. July, p. 102903, 2021, doi: 10.1016/j.jisa.2021.102903.

[13] F. Ertam, I. F. Kilinçer, and O. Yaman, “Intrusion detection in computer networks via machine learning algorithms,” *IDAP 2017 - Int. Artif. Intell. Data Process. Symp.*, 2017, doi: 10.1109/IDAP.2017.8090165.

[14] C. Khammassi and S. Krichen, “A GA-LR wrapper approach for feature selection in network intrusion detection,” *Comput. Secur.*, vol. 70, pp. 255–277, 2017, doi: 10.1016/j.cose.2017.06.005.

[15] A. Verma and V. Ranga, “Statistical analysis of CIDDS-001 dataset for Network Intrusion Detection Systems using Distance-based Machine Learning,” *Procedia Comput. Sci.*, vol. 125, pp. 709–716, 2018, doi: 10.1016/j.procs.2017.12.091.

[16] V. Hajisalem and S. Babaie, “A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection,” *Comput. Networks*, vol. 136, pp. 37–50, 2018, doi: 10.1016/j.comnet.2018.02.028.

[17] M. Injadat, F. Salo, A. B. Nassif, A. Essex, and A. Shami, “Bayesian Optimization with Machine Learning Algorithms Towards Anomaly Detection,” *2018 IEEE Glob. Commun. Conf. GLOBECOM 2018 - Proc.*, pp. 1–6, 2018, doi: 10.1109/GLOCOM.2018.8647714.

[18] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward generating a new intrusion detection dataset and intrusion traffic characterization,” *ICISSP 2018 - Proc. 4th Int. Conf. Inf. Syst. Secur. Priv.*, vol. 2018-Janua,

no. Cic, pp. 108–116, 2018, doi: 10.5220/0006639801080116.

[19] J. David and C. Thomas, “Efficient DDoS flood attack detection using dynamic thresholding on flow-based network traffic,” *Comput. Secur.*, vol. 82, pp. 284–295, 2019, doi: 10.1016/j.cose.2019.01.002.

[20] M. Awad and A. Alabdallah, “Addressing imbalanced classes problem of intrusion detection system using weighted Extreme Learning Machine,” *Int. J. Comput. Networks Commun.*, vol. 11, no. 5, pp. 39–58, 2019, doi: 10.5121/ijcnc.2019.11503.

[21] F. Gottwalt, E. Chang, and T. Dillon, “CorrCorr: A feature selection method for multivariate correlation network anomaly detection techniques,” *Comput. Secur.*, vol. 83, pp. 234–245, 2019, doi: 10.1016/j.cose.2019.02.008.

[22] N. Moustafa, J. Slay, and G. Creech, “Novel Geometric Area Analysis Technique for Anomaly Detection Using Trapezoidal Area Estimation on Large-Scale Networks,” *IEEE Trans. Big Data*, vol. 5, no. 4, pp. 481–494, 2017, doi: 10.1109/tbdata.2017.2715166.

[23] V. Kanimozhi and T. P. Jacob, “Artificial Intelligence based Network Intrusion Detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing,” *ICT Express*, vol. 5, no. 3, pp. 211–214, 2019, doi: 10.1016/j.icte.2019.03.003.

[24] V. Kanimozhi and D. T. P. Jacob, “Calibration of Various Optimized Machine Learning Classifiers in Network Intrusion Detection System on the Realistic Cyber Dataset Cse-Cic-Ids2018 Using Cloud Computing,” *Int. J. Eng. Appl. Sci. Technol.*, vol. 04, no. 06, pp. 209–213, 2019, doi: 10.33564/ijeast.2019.v04i06.036.

[25] W. Tao, W. Zhang, C. Hu, and C. Hu, “A Network Intrusion Detection Model Based on Convolutional Neural Network,” *Adv. Intell. Syst. Comput.*, vol. 895, no. 4, pp. 771–783, 2020, doi: 10.1007/978-3-030-16946-6_63.

[26] I. F. Kilincer, F. Ertam, and A. Sengur, “Machine learning methods for cyber security intrusion detection: Datasets and comparative study,” *Comput. Networks*, vol. 188, no. December 2020, p. 107840, 2021, doi:

10.1016/j.comnet.2021.107840.

[27] A. Rashid, M. J. Siddique, and S. M. Ahmed, “Machine and Deep Learning Based Comparative Analysis Using Hybrid Approaches for Intrusion Detection System,” *3rd Int. Conf. Adv. Comput. Sci. ICACS 2020*, pp. 1–9, 2020, doi: 10.1109/ICACS47775.2020.9055946.

[28] M. M. Hassan, A. Gumaei, A. Alsanad, M. Alrubaian, and G. Fortino, “A hybrid deep learning model for efficient intrusion detection in big data environment,” *Inf. Sci. (Ny).*, vol. 513, pp. 386–396, 2020, doi: 10.1016/j.ins.2019.10.069.

[29] I. Bouteraa, M. Derdour, and A. Ahmim, “Intrusion Detection using Data Mining: A contemporary comparative study,” *Proc. - PAIS 2018 Int. Conf. Pattern Anal. Intell. Syst.*, pp. 1–8, 2018, doi: 10.1109/PAIS.2018.8598494.

[30] S. M. Kasongo and Y. Sun, “A deep learning method with wrapper based feature extraction for wireless intrusion detection system,” *Comput. Secur.*, vol. 92, 2020, doi: 10.1016/j.cose.2020.101752.

[31] J. Zhang, Y. Ling, X. Fu, X. Yang, G. Xiong, and R. Zhang, “Model of the intrusion detection system based on the integration of spatial-temporal features,” *Comput. Secur.*, vol. 89, p. 101681, 2020, doi: 10.1016/j.cose.2019.101681.

[32] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, “Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study,” *J. Inf. Secur. Appl.*, vol. 50, p. 102419, 2020, doi: 10.1016/j.jisa.2019.102419.

[33] S. Lika, R. Dwi, P. Halim, and I. Verdian, “ANALISA SERANGAN SQL INJEKSI MENGGUNAKAN SQLMAP,” *POSITIF J. Sist. dan Teknol. Inf.*, vol. 4, no. 2, pp. 88–94, Nov. 2018, doi: 10.31961/POSITIF.V4I2.610.

[34] J. J. Malik, *Best Tools Hacking & Recovery Password*. Penerbit Andi.

[35] R. Watrianthos *et al.*, *Forensik Digital*. Yayasan Kita Menulis, 2021.

[36] K. Kemalis and T. Tzouramanis, “SQL-IDS: A specification-based approach for SQL-injection detection,” *Proc. ACM Symp. Appl. Comput.*, pp. 2153–2158, 2008, doi: 10.1145/1363686.1364201.

[37] “Layanan | SQL Injection | CSIRT Kementerian PPN/Bappenas.” .

[38] “NEWS : Awas Serangan SQL Injection Paling Sering Terjadi.” .

[39] “Daftar Statistik Keamanan Siber Definitif Tahun 2019.” .

[40] J. Gondohanindijo, “Sistem Untuk Mendeteksi Adanya Penyusup (IDS : Intrusion Detection System),” *Semarang*, vol. 2, pp. 46–54, 2011.

[41] S. Alviana and I. D. Sumitra, “ANALISIS PENGUKURAN PENGGUNAAN SUMBER DAYA KOMPUTER PADA INTRUSION DETECTION SYSTEM DALAM MEMINIMALKAN SERANGAN JARINGAN,” *Komputa J. Ilm. Komput. dan Inform.*, vol. 7, no. 1, pp. 27–34, Mar. 2018, doi: 10.34010/KOMPUTA.V7I1.2533.

[42] M. Dahlan, A. Latubessy, M. Nurkamid, and L. Hidayah Anggraini, “Pengujian Dan Analisa Keamanan Website Terhadap Serangan SQL Injection (Studi Kasus : Website UMK),” *J. Sains dan Teknol.*, vol. 7, pp. 13–19, 2014.

[43] A. Bustillo, D. Pimenov, M. Mia, and W. Kapłonek, “Machine-learning for automatic prediction of flatness deviation considering the wear of the face mill teeth,” *J. Intell. Manuf.*, pp. 1–18, Mar. 2021, doi: 10.1007/s10845-020-01645-3.

[44] E. Sutoyo and M. A. Fadlurrahman, “Penerapan SMOTE untuk Mengatasi Imbalance Class dalam Klasifikasi Television Advertisement Performance Rating Menggunakan Artificial Neural Network,” *J. Edukasi dan Penelit. Inform.*, vol. 6, no. 3, p. 379, 2020, doi: 10.26418/jp.v6i3.42896.

[45] I. Cholissodin, A. A. Soebroto, U. Hasanah, and Y. I. Febiola, “AI, Machine Learning & Deep Learning.” Fakultas Ilmu Komputer, Universitas Brawijaya, Malang, 2020.

[46] H. Liu and B. Lang, “Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey,” 2019, doi: 10.3390/app9204396.

[47] Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,” *Nature*, vol. 521, no. 7553, pp. 436–444, 2015, doi: 10.1038/nature14539.

[48] S. Atef and A. B. Eltawil, “Assessment of stacked unidirectional and bidirectional long short-term memory networks for electricity load forecasting,” *Electr. Power Syst. Res.*, vol. 187, p. 106489, Oct. 2020, doi: 10.1016/J.EPSR.2020.106489.

[49] A. Sahar and D. Han, “An LSTM-based indoor positioning method using Wi-Fi signals,” *ACM Int. Conf. Proceeding Ser.*, no. January, 2018, doi: 10.1145/3271553.3271566.

[50] L. Sun, Y. Wang, J. He, H. Li, D. Peng, and Y. Wang, “A stacked LSTM for atrial fibrillation prediction based on multivariate ECGs,” *Heal. Inf. Sci. Syst.*, vol. 8, no. 1, p. 19, 2020, doi: 10.1007/s13755-020-00103-x.

[51] Z. Karevan, “Spatio-temporal Stacked LSTM for Temperature Prediction in Weather Forecasting.”

[52] A. N. Jahromi, S. Hashemi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo, “An Enhanced Stacked LSTM Method with No Random Initialization for Malware Threat Hunting in Safety and Time-Critical Systems,” *IEEE Trans. Emerg. Top. Comput. Intell.*, vol. 4, no. 5, pp. 630–640, 2020, doi: 10.1109/TETCI.2019.2910243.