SISTEM KLASIFIKASI SERANGAN SQL *INJECTION* & XSS PADA RAMA *REPOSITORY* DENGAN METODE *LONG SHORT-TERM MEMORY* (LSTM)

TUGAS AKHIR
Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

LISA MELINDA

09011381722088

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2021

LEMBAR PENGESAHAN

SISTEM KLASIFIKASI SERANGAN SQL *INJECTION* & XSS PADA RAMA *REPOSITORY* DENGAN METODE *LONG-SHORT TERM MEMORY* (LSTM)

TUGAS AKHIR

Program Studi Sistem Komputer
Jenjang S1

Oleh:

LISA MELINDA

09011381722088

Indralaya, 29/7 2021

Mengetahui,

Pembimbing I Tugas Akhir	Pembimbing II Tugas Akhir
Deris Stiawan, M.T., Ph.D.	**Ali Bardadi, S.SI., M.Kom.**
NIP. 197806172006041002	**NIP. 198806292019031007**

Ketua Jurusan Sistem Komputer

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Kamis

Tanggal : 15 Juli 2021

Tim Penguji :

1.	**Ketua Sidang**	**: Sarmayanta Sembiring, M.T**	
2.	**Sekretaris Sidang**	**: Iman Saladin B. Azhar, M.MSI**	
3.	**Penguji Sidang**	**: Ahmad Heryanto, M.T**	
4.	**Pembimbing I**	**: Deris Stiawan, M.T., Ph.D., IPU**	
5.	**Pembimbing II**	**:Ali Bardadi, S.SI., M.Kom.**	

Mengetahui,

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama	: Lisa Melinda
Nim	: 09011381722088
Program Studi	: Sistem Komputer
Judul Penelitian	: Klasifikasi Serangan SQL Injection & XSS Pada RAMA Repository Dengan Metode Long Short-Term Memory (LSTM)

Hasil Pengecekkan Software iTehnticate/ Turnitin : 8%

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

Demikin surat pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

ralaya, 2021

METERAI TEMPEL

a Melinda

NIM. 09011381722088

HALAMAN PERSEMBAHAN

"Aku persembahkan hasil karya ini untuk kedua orang tuaku. Dukungan serta doa-doa yang senantiasa mengiringi hingga aku bisa sampai di tahap ini"

-Keluarga Besarku-

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji dan syukur atas kehadirat Allah Subhanahu Wata'ala yang telah melimpahkan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan judul **"Sistem Klasifikasi Serangan SQL *Injection* & XSS Pada RAMA *Repository* Dengan Metode *Long Short-Term Memory* (LSTM)"**. Shalawat dan salam tak lupa penulis curahkan kepada Nabi Muhammad SAW beserta keluarga, sahabat dan para pengikut-Nya.

Selesainya penyusunan Tugas Akhir ini tidak terlepas dari peran serta semua pihak. Oleh karena itu, pada kesempatan ini penulis menyampaikan ucapan terima kasih kepada :

1. Allah Subhanahu Wata'ala yang telah memberikan berkah kesempatan dan kesehatan kepada penulis dalam menyusun Tugas Akhir ini.
2. Orangtua tercinta, Bapak Merin dan Ibu Bunaiyah yang telah memberikan dukungan moral serta dukungan finansial kepada penulis.
3. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya
4. Bapak Dr.Ir. H. Sukemi, M.T. selaku Pembimbing Akademik.
5. Bapak Deris Stiawan,M.T.,Ph.D selaku Pembimbing Tugas Akhir I.
6. Bapak Ali Bardadi S.SI.,M.Kom selaku Pembimbing Tugas Akhir II
7. Mba Nurul Afifah, M.Kom yang telah memberikan arahan untuk penulis menyelesaikan tugas akhir.

8. Mba Renny selaku Admin Jurusan Sistem Komputer yang telah membantu penulis dalam hal-hal administrasi.
9. Meutia, Selly, Leni, Aulia, Bella, Mita, Helti, dan Ira dari squad sohib.
10. Afidin dan Jannes yang membantu penulis saat kebingungan.
11. Tia, Amartya, Febi, Agung, Nuzula teman seperjuangan riset comnet 2017.
12. Mini sebagai peliharaan yang mengalihkan stress.
13. Lisa Melinda
14. Teman-teman Sistem Komputer 2017.
15. Seluruh pihak yang tidak dapat penulis sebutkan satu persatu, yang telah memberikan semangat serta do'a.
16. Almamater.

Penulis menyadari dalam penyusunan Tugas Akhir ini masih terdapat banyak kekurangan, karenanya penulis mengharapkan kritik dan saran untuk perbaikan. Semoga laporan Tugas Akhir ini dapat bermanfaat bagi siapa saja yang membacanya.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Indralaya, 2021

Penulis

Sistem Klasifikasi Serangan SQL *Injection* & XSS pada RAMA *Repository* dengan Metode *Long Short-Term Memory* (LSTM)

Lisa Melinda (09011381722088)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer,
Universitas Sriwijaya
Email : lisamelinda77@gmail.com

Abstrak

Serangan SQL *Injection* dan XSS adalah salah satu contoh serangan kerentanan yang ada di aplikasi web. Serangan SQL *Injection* adalah salah satu dari lima teratas dalam semua risiko keamanan aplikasi web. Serangan SQL *Injection* dilakukan dengan memasukkan perintah sql ke dalam bentuk web, nama domain, atau permintaan halaman, dan akhirnya menipu server untuk menjalankan perintah SQL yang berbahaya, menyebabkan kerusakan besar pada situs web dan pengguna.

XSS adalah singkatan dari *Cross-Site Scripting* terjadi ketika kode web berbahaya dikirim atau dijalankan, biasanya dalam bentuk skrip, dari browser di komputer korban. Dengan eksekusi ini penyerang dapat mengambil informasi pribadi atau mencuri data pengguna.

Serangan SQL *injection* dan *Cross Site Scripting* pada dataset RAMA *Repository* dapat dikenali dengan beberapa parameter ciri dari *request url* dan *type attack.* Dari penelitian ini, metode LSTM memiliki hasil yang baik dalam mengklasifikasi serangan SQL *Injection* & XSS.

Kata Kunci : SQL *Injection, Cross Site Scripting, RAMA Repository, LSTM.*

Classification System of SQL Injection & XSS Attack on RAMA Repository Using Long Short-Term Memory (LSTM)

Lisa Melinda (09011381722088)

Departement of Computer Engineering, Faculty of Computer Science,
University of Sriwijaya
Email : lisamelinda77@gmail.com

Abstract

SQL Injection and XSS attacks are one example of vulnerability attacks that exist in web applications. SQL Injection attacks are one of the top five in all web application security risks. SQL Injection attacks are carried out by inserting sql commands into web forms, domain names, or page queries, and ultimately tricking the server into running malicious SQL commands, causing major damage to websites and users.

XSS stands for Cross-Site Scripting occurs when malicious web code is sent or executed, typically in the form of scripts, from a browser on the victim's computer. With this execution an attacker can retrieve personal information or steal user data.

SQL injection and Cross Site Scripting attacks on rama repository datasets can be recognized by several parameter characteristics of request url and attack type. From this study, LSTM method has good results in classifying SQL Injection &XSS attacks.

Keyword : *SQL Injection, Cross Site Scripting, RAMA Repository, LSTM***.**

DAFTAR ISI

Halaman

HALAMAN JUDUL ..... **i**
HALAMAN PENGESAHAN ..... **ii**
HALAMAN PERSETUJUAN ..... **iii**
HALAMAN PERNYATAAN ..... **iv**
HALAMAN PERSEMBAHAN ..... **v**
KATA PENGANTAR ..... **vi**
ABSTRAK ..... **viii**
ABSTRACT ..... **ix**
DAFTAR ISI ..... **vii**
DAFTAR GAMBAR ..... **viii**
DAFTAR TABEL ..... **xiv**

BAB I PENDAHULUAN **1**
1.1 Latar Belakang 1
1.2 Perumusan Masalah 2
1.3 Batasan Masalah 2
1.4 Tujuan 3
1.5 Manfaat 3
1.6 Metode Penelitian 3
1.7 Sistematika Penulisan 4
BAB II TINJAUAN PUSTAKA **6**
2.1 Pendahuluan 6
2.2 SQL *Injection* 7
2.3 *Cross-site scripting* (XSS) 8
2.4 Dataset RAMA *Repository* 8
2.5 *Principal Component Analysis* 8
2.6 SMOTE 9
2.7 *Long Short-Term Memory* (LSTM) 9

2.8 *Confusion Matrix* 10
BAB III METODOLOGI PENELITIAN 13
3.1 Pendahuluan 13
3.2 Kerangka Kerja Penelitian 13
3.3 Kerangka Kerja Metodologi Penelitian 14
3.4 Kebutuhan Perangkat 15
3.5 Persiapan Dataset 15
3.6 Konversi Dataset 15
3.7 Seleksi Fitur 16
3.8 Klasifikasi Dengan Algoritma LSTM 17
3.9 Validasi Hasil 18
BAB IV HASIL DAN ANALISA 19
4.1 Pendahuluan 19
4.2 *Exploratory Data Analysis* 19
4.3 Seleksi Fitur PCA 23
4.4 Hasil Klasifikasi 24
4.4.1 Validasi Hasil Rasio Data 50% latih 50% uji 24
4.4.2 Validasi Hasil Rasio Data 60% latih 40% uji 27
4.4.3 Validasi Hasil Rasio Data 70% latih 30% uji 30
4.4.4 Validasi Hasil Rasio Data 80% latih 20% uji 33
4.4.5 Validasi Hasil Rasio Data 90% latih 10% uji 35
4.5 Hasil Validasi BCC dan MCC 40
4.6 Analisis Perbandingan Fitur Seleksi 42
4.7 Analisis Akurasi dan Loss Data 43
4.8 Analisis Validasi BCC dan MCC 45
BAB V KESIMPULAN 46
5.1 Kesimpulan 46
5.2 Saran 46

DAFTAR PUSTAKA 47

DAFTAR GAMBAR

Halaman

Gambar 2.1 Unit LSTM..... 9

Gambar 2.2 *Confusion Matrix*..... 11

Gambar 3.1 Kerangka Kerja Penelitian..... 13

Gambar 3.2 Kerangka Kerja Metodologi Penelitian 14

Gambar 3.3 Flowchart Seleksi Fitur..... 16

Gambar 3.4 Flowchart Klasifikasi LSTM 17

Gambar 3.5 Arsitektur LSTM 18

Gambar 4.1 QUERY UNION 19

Gambar 4.2 TAUTOLOGY..... 20

Gambar 4.3 Count 20

Gambar 4.4 Script Alert 20

Gambar 4.5 JAVASCRIPT..... 20

Gambar 4.6 alert(XSS)..... 21

Gambar 4.7 Data SQL pada localhost PHPMyAdmin 21

Gambar 4.8 Konversi dataset csv 22

Gambar 4.9 Hasil Konversi data..... 22

Gambar 4.10 Grafik dataset berdasarkan Label 23

Gambar 4.11 Grafik dataset setelah menggunakan SMOTE..... 23

Gambar 4.12 Data PCA..... 24

Gambar 4.13 Hasil *Loss* rasio data 50% latih 50% uji 24

Gambar 4.14 Hasil Akurasi rasio data 50% latih 50% uji..... 25

Gambar 4.15 Kurva Presisi & Sensitivitas rasio 50% latih 50% uji 26

Gambar 4.16 Hasil *Loss* rasio data 60% latih 40% uji 27

Gambar 4.17 Hasil Akurasi rasio data 60% latih 40% uji..... 27

Gambar 4.18 Kurva Presisi & Sensitivitas rasio 60% latih 40% uji 29

Gambar 4.19 Hasil *Loss* rasio data 70% latih 30% uji 30

Gambar 4.20 Hasil Akurasi rasio data 70% latih 30% uji..... 30

Gambar 4.21 Kurva Presisi & Sensitivitas rasio 70% latih 30% uji 31

Gambar 4.22 Hasil *Loss* rasio data 80% latih 20% uji 33

Gambar 4.23 Hasil Akurasi rasio data 80% latih 20% uji..... 33

Gambar 4.24 Kurva Presisi & Sensitivitas rasio 80% latih 20% uji 35

Gambar 4.25 Hasil *Loss* rasio data 90% latih 10% uji 38

Gambar 4.26 Hasil Akurasi rasio data 90% latih 10% uji..... 38

Gambar 4.27 Kurva Presisi & Sensitivitas rasio 90% latih 10% uji 40

Gambar 4.28 Analisis Tanpa PCA & SMOTE..... 42

Gambar 4.29 Analisis Menggunakan PCA & SMOTE..... 42

Gambar 4.30 Analisis plot akurasi dan *loss* 43

Gambar 4.31 Analisis hasil klasifikasi 44

Gambar 4.32 Analisis BCC & MCC 45

DAFTAR TABEL

Halaman

Tabel 2.1 Penelitian Terkait Mengenai SQL dan XSS 6

Tabel 2.2 Perbedaan dengan penelitian terdahulu 7

Tabel 3.1 Spesifikasi Perangkat Keras 15

Tabel 3.2 Spesifikasi Perangkat Lunak 15

Tabel 3.3 Atribut *Feature Extraction* 16

Tabel 3.4 *Hyper Parameter* pada LSTM..... 18

Tabel 4.1 Hasil *Confusion Matrix* rasio data 50% latih 50% uji..... 25

Tabel 4.2 Hasil perhitungan rasio data 50% latih 50% uji 26

Tabel 4.3 Hasil *Confusion Matrix* rasio data 60% latih 40% uji..... 28

Tabel 4.4 Hasil perhitungan rasio data 60% latih 40% uji 28

Tabel 4.5 Hasil *Confusion Matrix* rasio data 70% latih 30% uji..... 31

Tabel 4.6 Hasil perhitungan rasio data 70% latih 30% uji 31

Tabel 4.7 Hasil *Confusion Matrix* rasio data 80% latih 20% uji..... 34

Tabel 4.8 Hasil perhitungan rasio data 80% latih 20% uji 34

Tabel 4.9 Hasil *Confusion Matrix* rasio data 90% latih 10% uji..... 39

Tabel 4.10 Hasil perhitungan rasio data 90% latih 10% uji 39

Tabel 4.11 Hasil Validasi BCC dan MCC..... 41

Tabel 4.12 Perbandingan Fitur Seleksi..... 42

BAB I
PENDAHULUAN

1.1 Latar Belakang

Serangan SQL *Injection* dan XSS adalah salah satu contoh serangan kerentanan yang ada di aplikasi web [1][2]. Serangan SQL *Injection* adalah salah satu dari lima teratas dalam semua risiko keamanan aplikasi web, itulah sebabnya orang sangat prihatin tentang serangan injeksi SQL[3]. Teknik serangan SQL *Injection* menjadi semakin kompleks, dimana penyerang menggunakan SQL *Injection* untuk mendapatkan akses dan melakukan modifikasi data yang tidak sah. [4][5]. Serangan SQL *Injection* dilakukan dengan memasukkan perintah SQL ke dalam bentuk web, nama domain, atau permintaan halaman, dan akhirnya menipu server untuk menjalankan perintah SQL yang berbahaya, menyebabkan kerusakan besar pada situs web dan pengguna[6].

XSS adalah singkatan dari *Cross-Site Scripting*, adalah kerentanan umum dalam aplikasi web, terjadi ketika kode web berbahaya dikirim atau dijalankan, biasanya dalam bentuk skrip, dari browser di komputer korban. Dengan eksekusi ini penyerang dapat mengambil informasi pribadi atau mencuri data pengguna[1]. Memungkinkan penyerang untuk memasukkan kode berbahaya ke dalam halaman web, dan korban melihat halaman atau mengklik link akan memicu *malicious scripts*. XSS beberapa kali telah terdaftar di OWASP (*Open Web Application Security Project*) sebagai TOP 10 risiko keamanan aplikasi web[7].

RAMA *Repository* adalah *website* nasional kumpulan laporan hasil penelitian seperti tugas akhir, proyek mahasiswa, skripsi, tesis, disertasi, ataupun jurnal maupun buku, dan laporan penelitian dosen yang diintegrasikan dari *repository* yang disebut RAMA *Repository*, dari Perguruan Tinggi dan Lembaga Penelitian di Indonesia[8].

Synthetic Minority Oversampling Technique (SMOTE) adalah salah satu metode *oversampling* yang paling umum digunakan untuk mengatasi masalah ketidakseimbangan[9]. Ini bertujuan untuk menyeimbangkan distribusi kelas secara acak dengan mereplikasinya. Penelitian ini mengusulkan penggunaan algoritme berbasis sampel, yang pada gilirannya berfungsi untuk meningkatkan algoritme SMOTE untuk menyesuaikan distribusi kelas yang tidak seimbang[10].

Pada penelitian [11] membahas tentang deteksi dan pencegahan SQL *Injection* dengan klasifikasi penerapan *machine learning* menggunakan metode SVM yang menghasilkan akurasi sebesar 98%. Pada penelitian tersebut disarankan penelitian selanjutnya menggunakan metode *machine learning* yang lain menggunakan data *multi-class* karena metode sebelumnya menggunakan data biner untuk melakukan penelitian.

Pada penelitian [12] membahas cara mendeteksi SQL *Injection* dengan menggunakan metode MLP dan LSTM, kedua metode ini mencapai hasil akurasi hingga 99% dan 97%, hasil akurasi MLP lebih besar dibandingkan dengan LSTM. Pendeteksian model LSTM, kemampuan pengenalan *keyword* dan karakter tertentu kurang baik. Sehingga karakter khusus, simbol, dan perbedaan ukuran numerik tidak jelas, yang juga menyebabkan kaburnya batas antara huruf dan karakter dalam proses deteksi LSTM.

Pada penelitian [3] membahas cara mendeteksi SQL *Injection* menggunakan metode LSTM dan komparasi dengan metode lain seperti metode MLP dan KNN. Dimana tingkat peforma metode MLP mencapai hasil akurasi sebesar 87% dan metode KNN mencapai hasil akurasi sebesar 89%. Sedangkan, untuk metode LSTM menghasilkan tingkat akurasi paling tinggi sebesar 91%, ini merupakan hasil paling tinggi setelah melihat hasil komparasi dengan metode lain.

Dari beberapa rujukan di atas, metode yang diajukan untuk klasifikasi serangan SQL *Injection* dan XSS pada RAMA *Repository* menggunakan algortima SMOTE untuk melakukan penyeimbangan kelas dan algoritma *Long-Short Term Memory* (LSTM).

1.2 Perumusan Masalah

1. Bagaimana memilih atribut yang baik untuk meminimalisir proses komputasi?
2. Bagaimana cara mengklasifikasi serangan SQL *Injection* dan XSS pada RAMA *Repository*?

1.3 Batasan Masalah

1. Data yang digunakan dalam penelitian merupakan data dari *website* RAMA *Repository*

2. Metode yang digunakan pada penelitian ini menggunakan metode *Long Short-Term Memory* (LSTM).
3. Data yang diujikan berupa paket data normal dan paket data serangan SQL *Injection* & XSS.
4. Seleksi fitur yang digunakan pada penelitian ini menggunakan algoritma PCA.
5. Tidak membahas bagaimana cara pencegahan serangan tersebut.

1.4 Tujuan

1. Menerapkan seleksi fitur PCA pada dataset RAMA *Repository*.
2. Menerapkan metode *Long Short-Term Memory* (LSTM) untuk mengklasifikasi serangan SQL *Injection* dan XSS pada RAMA *Repository*.

1.5 Manfaat

Adapun manfaat dari penilitain proposal Tugas Akhir ini adalah:

1. Dapat mempercepat proses komputasi dari klasifikasi SQL *Injection* & XSS
2. Dapat mempelajari proses klasifikasi SQL *Injection* & XSS dari RAMA *Repository*

1.6 Metode Penelitian

Metode penelitian yang digunakan memeliki beberapa tahapan, antara lain sebagai berikut:

1. Metode Studi Pustaka dan Literatur

   Metode ini melakukan studi dengan mempelajari dari referensi yang berkaitan dengan serangan SQL *Injection* & XSS dengan algoritma LSTM melalui berbagai sumber seperti buku, jurnal ilmiah, dan artikel terkait.

2. Metode Konsultasi

Pada langkah ini, melakukan konsultasi terhadap orang-orang memiliki pengetahuan lebih terhadap serangan atau metode yang diteliti untuk penyusunan Proposal Tugas Akhir.

3. Metode Pengumpulan Data

Pada metode ini dilakukan pengambilan data yang berkaitan dengan serangan SQL *Injection* & XSS dari RAMA *Repository* dan sistem klasifikasi.

4. Metode Pengujian

Pada metode selanjutnya, melakukan perancangan sistem terhadap serangan SQL *Injection* & XSS pada RAMA *Repository*. Pada metode ini dilakukan percobaan terhadap sistem klasifikasi yang dibuat, apakah sistem tersebut menghasilkan akurasi yang bagus atau buruk.

5. Metode Analisa dan Kesimpulan

Pada tahap ini menganalisis hasil dari sistem klasifikasi, selanjutnya dianalisis kekurangan sehingga dapat menjadi penelitian di masa yang akan datang.

1.7 Sistematika Penulisan

Sistematika penulisan dibuat untuk memperjelas dan mempertegas setiap bab yang akan dibuat pada penelitian ini. Adapun sistematika penulisan yang akan digunakan dalam penyusnan tugas akhir ini adalah sebagai berikut:

BAB I. PENDAHULUAN

Pada bab pertama terdapat latar belakang, tujuan, manfaat, rumusan dan batasan masalah, metodologi penelitian serta sistematika penulisan.

BAB II. TINJAUAN PUSTAKA

Pada Bab kedua berisi dasar teori mengenai SQL *Injection*, XSS, algoritma LSTM serta tinjauan pustaka lain yang memiliki kaitan dengan penelitian kali ini.

BAB III. METODOLOGI

Pada bab ketiga akan membahas perancangan sistem klasifikasi serangan SQL *Injection* & XSS serta implementasi metode yang dipakai.

BAB IV. HASIL DAN ANALISIS

Pada bab keempat membahas tentang alur penelitian, dan hasil analisis dari sistem klasifikasi akurasi menggunakan metode *Long Short-Term Memory* (LSTM)

BAB V. KESIMPULAN DAN SARAN

Pada bab terakhir berisi kesimpulan yang dapat diambil dari setiap bab yang telah dibuat, dan juga memberikan saran untuk penelitian diselanjutnya.

DAFTAR PUSTAKA

[1] G. E. Rodríguez, J. G. Torres, P. Flores, and D. E. Benavides, "Cross-site scripting (XSS) attacks and mitigation: A survey," *Comput. Networks*, vol. 166, p. 106960, 2020, doi: 10.1016/j.comnet.2019.106960.

[2] K. Vijayalakshmi and A. A. Leema, "Extenuating web vulnerability with a detection and protection mechanism for a secure web access," *2017 4th Int. Conf. Signal Process. Commun. Networking, ICSCN 2017*, pp. 16–19, 2017, doi: 10.1109/ICSCN.2017.8085652.

[3] 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.

[4] M. S. Aliero, K. N. Qureshi, M. F. Pasha, I. Ghani, and R. A. Yauri, *Systematic Review Analysis on SQLIA Detection and Prevention Approaches*, vol. 112, no. 4. Springer US, 2020.

[5] L. Zhang, D. Zhang, C. Wang, J. Zhao, and Z. Zhang, "ART4SQLi: The ART of SQL Injection Vulnerability Discovery," *IEEE Trans. Reliab.*, vol. 68, no. 4, pp. 1470–1489, 2019, doi: 10.1109/TR.2019.2910285.

[6] X. Xie, C. Ren, Y. Fu, J. Xu, and J. Guo, "SQL Injection Detection for Web Applications Based on Elastic-Pooling CNN," *IEEE Access*, vol. 7, pp. 151475–151481, 2019, doi: 10.1109/ACCESS.2019.2947527.

[7] Y. Zhou and P. Wang, "An ensemble learning approach for XSS attack detection with domain knowledge and threat intelligence," *Comput. Secur.*, vol. 82, pp. 261–269, 2019, doi: 10.1016/j.cose.2018.12.016.

[8] RISTEKDIKTI, "RAMA REPOSITORY," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2013.

[9] J. Mathew, S. Member, C. K. Pang, and S. Member, "Classification of Imbalanced Data by Oversampling in Kernel Space of Support Vector Machines," pp. 1–12, 2017.

[10] S. Guo, Y. Liu, R. Chen, X. Sun, and X. Wang, "Improved SMOTE Algorithm to Deal with Imbalanced Activity Classes in Smart Homes," *Neural Process. Lett.*, 2018, doi: 10.1007/s11063-018-9940-3.

[11] S. O. Uwagbole, W. J. Buchanan, and L. Fan, "Applied Machine Learning Predictive Analytics to SQL Injection Attack Detection and Prevention," 2017.

[12] P. Tang, W. Qiu, Z. Huang, H. Lian, and G. Liu, "Detection of SQL injection based on artificial neural network," *Knowledge-Based Syst.*, vol. 190, p. 105528, 2020, doi: 10.1016/j.knosys.2020.105528.

[13] S. G. Selvaganapathy, M. Nivaashini, and H. P. Natarajan, "Deep belief network based detection and categorization of malicious URLs," *Inf. Secur.*

J., vol. 27, no. 3, pp. 145–161, 2018, doi: 10.1080/19393555.2018.1456577.

[14] P. Tang, W. Qiu, Z. Huang, H. Lian, and G. Liu, *SQL injection behavior mining based deep learning*, vol. 11323 LNAI. Springer International Publishing, 2018.

[15] S. Akaishi and R. Uda, "Classification of XSS Attacks by Machine Learning with Frequency of Appearance and Co-occurrence," *2019 53rd Annu. Conf. Inf. Sci. Syst. CISS 2019*, pp. 1–6, 2019, doi: 10.1109/CISS.2019.8693047.

[16] S. Kascheev and T. Olenchikova, "The Detecting Cross-Site Scripting (XSS) Using Machine Learning Methods," *Proc. - 2020 Glob. Smart Ind. Conf. GloSIC 2020*, pp. 265–270, 2020, doi: 10.1109/GloSIC50886.2020.9267866.

[17] S. Abaimov and G. Bianchi, "CODDLE: Code-Injection Detection with Deep Learning," *IEEE Access*, vol. 7, pp. 128617–128627, 2019, doi: 10.1109/ACCESS.2019.2939870.

[18] A. Ghafarian, "A hybrid method for detection and prevention of SQL injection attacks," *Proc. Comput. Conf. 2017*, vol. 2018-Janua, no. July, pp. 833–838, 2018, doi: 10.1109/SAI.2017.8252192.

[19] S. Gupta and B. B. Gupta, "Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art," *Int. J. Syst. Assur. Eng. Manag.*, vol. 8, pp. 512–530, 2017, doi: 10.1007/s13198-015-0376-0.

[20] M. Mateen, J. Wen, Nasrullah, S. Song, and Z. Huang, "Fundus image classification using VGG-19 architecture with PCA and SVD," *Symmetry (Basel).*, vol. 11, no. 1, 2019, doi: 10.3390/sym11010001.

[21] X. Kang, S. Member, X. Xiang, S. Li, and S. Member, "PCA-Based Edge-Preserving Features for Hyperspectral Image Classification," pp. 1–12, 2017.

[22] Y. Yan, R. Liu, Z. Ding, X. Du, J. I. E. Chen, and Y. Zhang, "A Parameter-Free Cleaning Method for SMOTE in Imbalanced Classification," *IEEE Access*, vol. 7, pp. 23537–23548, 2019, doi: 10.1109/ACCESS.2019.2899467.

[23] R. Pruengkarn, K. W. Wong, and C. C. Fung, "Imbalanced Data Classification using Complementary Fuzzy Support Vector Machine Techniques and SMOTE," pp. 978–983, 2017.

[24] L. Ma and S. Fan, "CURE-SMOTE algorithm and hybrid algorithm for feature selection and parameter optimization based on random forests," *BMC Bioinformatics*, vol. 18, no. 1, pp. 1–18, 2017, doi: 10.1186/s12859-017-1578-z.

[25] A. Sherstinsky, "Fundamentals of Recurrent Neural Network (RNN) and Long Short-Term Memory (LSTM) network," *Phys. D Nonlinear Phenom.*,

vol. 404, p. 132306, 2020, doi: 10.1016/j.physd.2019.132306.

[26] Ö. Yildirim, “A novel wavelet sequences based on deep bidirectional LSTM network model for ECG signal classification,” *Comput. Biol. Med.*, vol. 96, no. January, pp. 189–202, 2018, doi: 10.1016/j.compbiomed.2018.03.016.

[27] X. Deng, Q. Liu, Y. Deng, and S. Mahadevan, “An improved method to construct basic probability assignment based on the confusion matrix for classification problem,” *Inf. Sci. (Ny).*, vol. 340–341, pp. 250–261, 2016, doi: 10.1016/j.ins.2016.01.033.