DETEKSI SERANGAN BRUTE FORCE MENGGUNAKAN METODE BIDIRECTIONAL RECURRENT NEURAL NETWORKS

TUGAS AKHIR

OLEH :

M.Alfat Hayatur Rizon
09011381823120

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2022

LEMBAR PENGESAHAN

DETEKSI SERANGAN BRUTE FORCE MENGGUNAKAN METODE BIDIRECTIONAL RECURRENT NEURAL NETWORKS

TUGAS AKHIR

Sebagai syarat untuk memenuhi persyaratan gelar sarjana

Program Studi Sistem Komputer
Jenjang S1

Oleh

M.Alfat Hayatur Rizon
09011381823120

Palembang , Desember 2022

Mengetahui,

Pembimbing I Tugas Akhir	Pembimbing II Tugas Akhir
Ahmad Heryanto, S. Kom, M.T	**Adi Hermansyah, S. Kom, M.T**
NIP. 198701222015041002	**NIK. 161303300489001**

Ketua Jurusan Sistem Komputer

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Selasa
Tanggal : 20 Desember 2022

Tim Penguji :

1. **Ketua** : Kemahyanto Exaudi, M.T.
2. **Penguji** : Aditya Putra Perdana P, M.T.
3. **Sekretaris** : Abdurahman, S.Kom., M.Han
4. **Pembimbing I** : Ahmad Heryanto, M.T.
5. **Pembimbing II** : Adi Hermansyah, M.T.

Mengetahui,
Ketua Jurusan Sistem Komputer

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

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : M. Alfat Hayatur Rizon

NIM : 09011381823120

Judul : DETEKSI SERANGAN BRUTE FORCE MENGGUNAKAN METODE BIDIRECTIONAL RECURRENT NEURAL NETWORKS

Hasil Pengecekan Software iThenticate/Turnitin : 17%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan / plagiat dari penelitian orang lain. Apabila ditemukan unsur penjiplakan / plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Palembang, Desember 2022

Penulis,

M. Alfat Hayatur Rizon

NIM. 09011381823120

`

HALAMAN PERSEMBAHAN

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيم

Skripsi ini penulis dedikasikan kepada kedua orang tua tercinta, Ayahanda dan Ibunda, ketulusanya dari hati atas doa yang tak pernah putus, semangat yang tak ternilai. Serta Untuk Orang-Orang Terdekatku Yang Tersayang, Dan Untuk Almamater Ku Kebanggaanku Program Studi Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

Dengan mengucap syukur Alhamdulillah atas rahmat Allah Subhanahu wa Ta'alamyang telah membrikan izin serta ridhonya sehingga penulis mampu memenuhi harapan keluarga besar, rekan seperjuagan, serta civitas akademik agar segera menyelesaikan masa studi untuk mendapatkan gelar sarjana komputer.

"*Don't do anything half-heartedly*"

"Lakukan apapun jangan dengan setengah hati"

Desember 2022

KATA PENGANTAR

Assalamualaikum Warahmatullahi Wabarakatuh

Segala puji dan syukur atas kehadirat Tuhan Yang Maha Esa, yang atas segala berkat,kasih sayang,serta karunia-Nya penulis dapat menyelesaikan penulisan proposal tugas akhir ini yang berjudul "DETEKSI SERANGAN BRUTE FORCE MENGGUNAKAN METODE BIDIRECTIONAL RECURRENT NEURAL NETWORKS ".

Pada penyusunan laporan ini, penulis banyak mendapatkan ide dan saran serta bantuan dari berbagai pihak baik secara langsung maupun tidak langsung. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Tuhan Yang Maha Esa dan terimakasih kepada yangterhormat:

*1.*Kedua orang tua, saudara, dan Keluarga Besar yang selalu mendoakan dan memberikan motivasi dan *support.*

2.Bapak Jaidan Jauhari selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.

3.Bapak Dr.Ir.Sukemi,M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer.

3. Bapak Huda Ubaya,M.T. Selaku Dosen Pembimbing Akademik

5. Bapak Ahmad Heryanto, S. Kom, M.T. selaku Dosen Pembimbing I Tugas Akhir.

6. Bapak Adi Hermansyah, S. Kom, M.T. selaku Dosen Pembimbing II Tugas Akhir.

7.Mba Sari selaku Administrasi Jurusan Sistem Komputer yang telah membantu melancarkan proses administrasi terkait Tugas Akhir

8.Seluruh staff dan pegawai jurusan sistem komputer beserta teman seperjuagan yang telah membersamai jalan juang.

9.Dan semua pihak yang telah membantu..

Penulis menyadari bahwa laporan ini masih sangat jauh dari kata sempurna. Untuk itu kritik dan saran yang membangun sangatlah diharapkan penulis agar dapat segera diperbaiki sehingga laporan ini dapat dijadikan sebagai masukkan ide dan pemikiran yang bermanfaat bagi semua pihak dan menjadi tambahan bahan bacaan bagi yang tertarik dalam penelitian networking khususnya pada serangan *BRUTE FORCE*.

Wassalamualaikum Warahmatullahi Wabarakatuh

Palembang, Desember 2022

Penulis,

M.Alfat Hayatur Rizon

NIM. 09011381823120

DETEKSI SERANGAN BRUTE FORCE MENGGUNAKAN METODE BIDIRECTIONAL RECURRENT NEURAL NETWORKS

M. ALFAT HAYATUR RIZON (09011381823120)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : andrialfat92@gmail.com

ABSTRAK

Brute Froce Attack adalah serangan yang mengincar bagian informasi pribadi seperti *username*, kata sandi, frasa sandi dan informasi lainnya. *Brute force attack* mengirimkan kombinasi secara terus - menerus berupa angka, huruf atau simbol yang berbeda, hingga mendapatkan kombinasi yang tepat sehingga dapat mengakses data yang di lindungin *Brute force attack* mencoba memecahkan informasi krendesial yang berharga bagi penyerang . Algoritma-algoritma yang sering digunakan pada sistem tersebut adalah *CNN , Naïve Bayes, SVM , KNN , Decision Tree, Logistic Regression, Random Forest, K-Means, Gradient Bossting, Dimensionality Reduction* , Berdasarkan algoritma cnn dan pendeteksi serangan brutefoce, mengatakan bahwa kelemahan dari metode cnn adalah dalam paper tersebut, menyajikan kerangka kerja baru yang mengintegrasikan cnn lokal dan cnn global yang keduanya didasarkan pada Hasil penelitian menunjukkan bahwa model berbasis CNN lebih unggul dari metode pembelajaran mesin tradisional dengan akurasi 94,3%, tingkat presisi 92,5%, tingkat recall 97,8% dan F1-score 91,8% dalam hal kemampuan mendeteksi *SSH-Brute Froce*. serangan paksa. Setelah analisis komparatif dari berbagai model pengklasifikasi, ditemukan bahwa pengklasifikasi *Naive Bayes* sangat cocok untuk klasifikasi gambar dari fitur-fiturnya, banyak penelitian terkait – mengatakan bahwa algoritma RNN dapat mengatasi permasalahan bahwasannya metode *bi-directional rnn* dapat menyelesaikan lebih cepat dengan cara perulagan sehingga memunculkan hasil yang terbaik pada data yang diteliti.

Kata Kunci : *Brute force attack, Bi-directional recurrent neural network*

Mengetahui,

Pembimbing I Tugas Akhir	**Pembimbing II Tugas Akhir**
Ahmad Heryanto, S. Kom, M.T	**Adi Hermansyah, S. Kom, M.T**
NIP. 198701222015041002	**NIK. 161303300489001**

Ketua Jurusan Sistem Komputer

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

BRUTE FORCE ATTACK DETECTION USING THE BIDIRECTIONAL RECURRENT NEURAL NETWORKS METHOD

M. ALFAT HAYATUR RIZON (09011381823120)

Department of Computer Systems, Faculty of Computer Science, Universitas Sriwijaya

Email : [redacted]

ABSTRACT

Brute Force Attack is an attack that targets private information such as usernames, passwords, passphrases and other information. Brute force attack sends combinations continuously in the form of different numbers, letters or symbols, until it gets the right combination so that it can access the protected data. Brute force attack tries to break credential information that is valuable for attackers. The algorithms that are often used in these systems are CNN , Naïve Bayes , SVM , KNN , Decision Tree, Logistic Regression, Random Forest, K-Means, Gradient Boosting, Dimensionality Reduction , Based on the CNN algorithm and bruteforce attack detection, said that the weakness of the cnn method is in the paper, presenting a new framework that integrates local cnn and global cnn both of which are based on the results of the study showing that the CNN-based model is superior to traditional machine learning methods with an accuracy of 94.3%, a precision rate of 92.5%, 97.8% recall rate and 91.8% F1-score in terms of the ability to detect SSH-Brute Froce. forced attack. After a comparative analysis of various classifier models, it was found that the Naive Bayes classifier is very suitable for image classification from its features, many related studies say that the RNN algorithm can overcome the problem that the bi-directional rnn method can solve faster by iteratively so that results emerge the best in the data studied.

Keyword : *Brute force attack, Bi-directional recurrent neural network*

Mengetahui,

Supervisor	**Co-Supervisor**
Ahmad Heryanto, S. Kom, M.T	**Adi Hermansyah, S. Kom, M.T**
NIP. 198701222015041002	**NIK. 161303300489001**

Head Of Computer System Departement

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

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
PENDAHULUAN

1.1 Latar Belakang

"Brute Froce Attack" adalah serangan yang mengincar bagian informasi pribadi seperti username, kata sandi, frasa sandi dan informasi lainnya. *Brute force attack* mengirimkan kombinasi secara terus - menerus berupa angka, huruf atau simbol yang berbeda, hingga mendapatkan kombinasi yang tepat sehingga dapat mengakses data yang di lindungin [1].

Brute force attack mencoba memecahkan informasi krendesial yang berharga bagi penyerang[2]**.** Berdasarkan penelitian[3]–[6] isu terpenting dalam proses deteksi *brute force attack* adalah akurasi dan prediksi, Metode-metode dalam mendeteksi serangan *brute force* telah banyak dikembangkan oleh peneliti [3]–[6], adapun metode tersebut dapat dikelompokkan menjadi dua kategori utama, yaitu *statistic* dan *machine learning* algoritma[7]. Pada penelitian tersebut, umumnya melakukan pengoptimalan proses deteksi serangan dengan mengurangi waktu eksekusi atau mengurangi biaya eksekusi[8].

Pada penelitian[4], [5], [9], [10] untuk meningkatkan waktu dan mengurangi biaya eksekusi proses pendeteksi serangan, penelitian tersebut menggunakan algoritma *machine learning/deep learning* (*Convolutional neural network*[4]). Algoritma-algoritma yang sering digunakan pada sistem tersebut adalah CNN (*Convolution Neural Network*), *Naïve Bayes*, SVM (*Support Vector Machine*), KNN (*K-Nearest Neighbors*), *Decision Tree, Logistic Regression, Random Forest, K-Means, Gradient Bossting, Dimensionality Reduction*[4], [11]–[14].

Berdasarkan penelitian dari[4], [5], [15], [16] mengenai algoritma cnn (*Convolution Neural Network*) dan pendeteksi serangan brutefoce, mengatakan bahwa kelemahan dari metode cnn (*Convolution Neural Network*) adalah dalam *paper* tersebut, menyajikan kerangka kerja baru

yang mengintegrasikan cnn lokal dan cnn *global* yang keduanya didasarkan pada ResNet-20 untuk identifikasi skrip. Adapun hasil dari penelitian tersebut adalah Hasil penelitian menunjukkan bahwa model berbasis CNN lebih unggul dari metode pembelajaran mesin tradisional dengan akurasi 94,3%, tingkat presisi 92,5%, tingkat *recall* 97,8% dan *F1-score* 91,8% dalam hal kemampuan mendeteksi SSH-Brute Froce. serangan paksa.

Berdasarkan penelitian dari [4], [17]–[19] tentang *Naïve Bayes* Pada pendeteksi serangan *brute force*, mengatakan bahwa kelemahan dari metode algoritma cnn adalah arsitektur jaringan saraf yang menggunakan pembagian bobot ekstensif untuk mengurangi derajat kebebasan model yang beroperasi pada fitur yang berkorelasi spasial. topologi dasar cnn terdiri dari tumpukan lapisan yang terdiri dari lapisan convolutional, lapisan pooling, dan lapisan yang terhubung penuh banyak model cnn memiliki struktur standar yang terdiri dari lapisan convolutional bergantian dan lapisan pooling lapisan terakhir adalah sejumlah kecil lapisan yang terhubung penuh dengan pengklasifikasi softmax atau sigmoid, setiap lapisan mengestimasi fitur non-linier yang diteruskan ke lapisan berikutnya dan lapisan terakhir dalam jaringan deep learning melakukan klasifikasi. Fungsi aktivasi pada setiap lapisan tersembunyi adalah fungsi aktivasi ReLU, dan untuk normalisasi dan regularisasi batch, tingkat putus sekolah sebesar 0,2 digunakan pada setiap lapisan tersembunyi untuk menghindari overfitting dan mempercepat pelatihan model.

Berdasarkan penelitian dari [4], [20]–[22], mengatakan bahwa kelemahan dari metode algoritma cnn (*Convolution Neural Network*) dan *Naïve Bayes* adalah untuk algoritma cnn (*Convolution Neural Network*) yang dimana mempertimbangkan strategi fusi fitur multilayer yang dalam, dan dengan demikian menggabungkan fitur dari lapisan hierarkis yang berbeda untuk mengekstrak informasi spektral-spasial berkorelasi kuat di antara mereka, sedangkan algoritma *Naïve Bayes* data gabungan, yang berisi fitur statistik dan fitur geometris, diberikan ke berbagai model pengklasifikasi pembelajaran mesin dan kinerjanya dianalisis. Setelah

analisis komparatif dari berbagai model pengklasifikasi, ditemukan bahwa pengklasifikasi Naive Bayes sangat cocok untuk klasifikasi gambar dari fitur-fiturnya. Pada pengujian didapatkan bahwa model classifier Naïve Bayes yang dihasilkan mampu mengklasifikasikan tingkat deformasi secara akurat sebagai deformasi aman dan deformasi berlebihan.

Untuk mengatasi kelemahan dari metode CNN (Convolution Neural Network), Naïve Bayes, SVM (Support Vector Machine), KNN (K-Nearest Neighbors), Decision Tree, Logistic Regression, Random Forest, K-Means, Gradient Bossting, Dimensionality Reduction[4], [11]–[14], banyak penelitian terkait[23]–[26] mengatakan bahwa algoritma RNN dapat mengatasi permasalahan bahwasannya metode bi-directional rnn dapat menyelesaikan lebih cepat dengan cara perulagan sehingga memunculkan hasil yang terbaik pada data yang diteliti.

"*Recurrent neural network* (*RNN*)" merupakan jenis arsitektur jaringan saraf tiruan yang pemerosesannya di panggil berulang untuk memproses masukan yang biasanya adalah data sekuensial, penelitian berfokus pada peramalan dengan kata lain metode tersebut bertujuan untuk di gunakan pada tingkat pelanggan[27].

Analisis perdiktif yang digunakan telah menjadi sarana penting untuk memastikan normal dan teratur produksi karena merugikan bagi perkembangan yang pesat untuk mengandalkan pemeliharan[28], metode untuk meramalkan harus di pilih dengan cermat agar sesuai dengan kondisi spesifik[27].

Jenis *RNN* dapat menyimpan memori ke arah tertentu dari urutan secara berurutan berkolerasi di bagian jadi menggunakan GRU dua arah untuk memodelkan data *logging*[29], model *Bi-directional RNN* juga sebagai model jaringan saraf sekuensial sering di gunakan sebagai kode informasi interaksi histori untuk menangkap pengguna[30], *Bi-directional RNN* merupakan sebuah *feed forward neural network* yang telah di perluas *Bi-directional RNN* lebih untuk memodelkan urutan dari pada jaringan saraf umpan maju karena memiliki siklus koneksi[31].

Oleh karena itu, berdasarkan latar belakang yang telah disebutkan pada pembahasan diatas, maka penelitian tugas akhir membahas tentang "**Deteksi Serangan *Brute Force* Menggunakan Metode *Bi-Directional Recurrent Neural Network***".

1.2 Tujuan

Tujuan dari penulisan tugas akhir ini, yaitu :

1. Mendeteksi serangan *brute force pada cloud* dengan menggunakan metode *bi-directional (RNN).*
2. Menampilkan tingkat akurasi, persisi, *recall* dan *F1-Score* serangan *brute force* dengan menggunakan metode *bi-directional (RNN).*
3. Mencari hasil terbaik dengan menggunakan metode *feature selection.*

1.3. Manfaat

Manfaat dari penulisan tugas akhir ini, yaitu :

1. Penelitian ini diharapakan dapat melakukan pembuktian serangan *brute force* yang terjadi kepada *cloud*.
2. Dapat mendeteksi serangan *brute force* dengan menggunakan metode *bi-directional (RNN).*
3. Dapat memberikan informasi mengenai metode *bi-directional RNN* dan pengaplikasiannya dalam deteksi serangan *brute force*

1.4. Batasan Masalah

Perumusan Masalah

Bedasarkan latar belakang yang telah dijabarkan, jenis *bi-directional RNN* dapat menyimpan memori ke arah tertentu dari urutan secara berurutan berkolerasi di bagian jadi menggunakan GRU dua arah

untuk memodelkan data *logging*,model *bi-directional RNN* sebagai model jaringan saraf sekuensial sering di gunakan sebagai kodekan informasi interaksi histori untuk menangkap pengguna, *bi-directional RNN* adalah sebuah *feedforward neural network* yang telah di perluas *bi-directional RNN* lebih untuk memodelkan urutan dari pada jaringan saraf umpan maju karena memiliki siklus koneksi.

Batasan Masalah

Berikut batasan masalah dari tugas akhir ini, yaitu :

1. Penelitian menganalisa serangan *brute froce* pada *cloud public* menggunakan metode *bi-directional(RNN).*
2. Penelitian menggunakan dataset dari CICIDS 2017.
3. Algoritma yang digunakan pada penelitian yang di lakukan adalah algoritma *bi-directional(RNN).*
4. Parameter yang diteliti adalah hasil akurasi serangan brute force dengan menggunakan *bi-directional(RNN).*

1.5 Metodelogi Penelitian

Pada tugas akhir ini menggunakan metodelogi sebagai berikut :

Metodologi yang digunakan dalam penulisan tugas akhir, akan melewati beberapa tahapan sebagai berikut:

1. Tahap pertama (Perumusan Masalah)

Tahap ini ialah tahap yang menentukan permasalahan yang ada pada *cloud computing* yang telah dibahas pada penelitian sebelumnya yaitu keamanan pada *cloud computing* untuk mengidentifikasi serangan yang terjadi dan membuktikan serangan tersebut.

2. Tahap kedua (Studi Pustaka / *Literature Review*)

Tahap ini ialah tahap mencari referensi atau *literature* ilmiah yang berhubungan dengan judul tugas akhir untuk menunjang penelitian yang dilakukan.

3. Tahap ketiga (Perancangan)

Tahap ini ialah tahap perancangan sistem yang akan dibuat sesuai dengan rumusan masalah penelitian.Dalam tahap ini melakukan instalasi *operation system* membangun jaringan *cloud* dan konfigurasi *cloud* tersebut.

4. Tahap keempat (Pengujian)

Tahap ini ialah tahap pengujian dari sistem yang telah dirancang. Ditahap ini akan diuji serangan *brute force* menggunakan *brup suite* kepada *cloud* yang telah dibangun.

5. Tahap kelima (Analisis)

Tahap ini ialah tahap analisa dari hasil pengujian. Disini akan dianalisa bagaimana serangan tersebut dilakukan dan oleh siapa serta dibuktikan dengan bukti yang jelas dan kronologis.

6. Kesimpulan dan Saran

Pada tahap ini ditarik kesimpulan dari hasil analisa penelitian dan dibuat saran sebagai referensi apabila penelitian ini dilanjutkan.

1.6 Sistematika Penulisan

Penyusunan laporan tugas akhir ini terdiri dari beberapa bab agar pembahasan lebih sistematik dan spesifik dengan rincian sebagai berikut:

BAB I. LATAR BELAKANG

Pada bab I berisikan penjelasan secara sistematis mengenai topik penelitian yang diambil meliputi latar belakang, tujuan, manfaat, rumusan masalah, batasan masalah, metodologi penulisan dan sistematika penulisan.

BAB II. TINJAUAN PUSTAKA

Pada bab II berisikan mengenai dasar teori dari penelitian terkait mengenai *Brute Force Attack, Cloud Computing, Network Forensic, Bi-Directional RNN (Recurrent neural network)* yang berkaitan dengan penelitian. Bab ini akan menjadi tinjauan atau landasan dalam menganalisis batasan masalah yang telah dikemukakan pada bab sebelumnya.

BAB III. METODOLOGI

Bab III berisikan tentang penjelasan secara bertahap mengenai proses penelitian yang dilakukan. Penjelasan tersebut meliputi tahapan perancangan sistem dan penerapan metode penelitian.

BAB IV. PENGUJIAN DAN ANALISIS

Bab ini menjelaskan mengenai hasil dari pengujian yang telah dilakukan selama penelitian tugas akhir. Hasil dari pengujian tersebut akan dianalisi dari serangan *Brute Force* yang dilakukan pada *Cloud*.

BAB V. KESIMPULAN DAN SARAN

Bab V berisi kesimpulan akhir dari pembahasan penelitian yang telah dilakukan. Pada bab ini juga terdapat saran yang diperlukan untuk pengembangan penelitian selanjutnya dari pengujian dan analisis tugas akhir.

DAFTAR PUSTAKA

[1] S. Zhang, X. Xie, and Y. Xu, "A Brute-Force Black-Box Method to Attack Machine Learning-Based Systems in Cybersecurity," *IEEE Access*, vol. 8, pp. 128250–128263, 2020, doi: 10.1109/ACCESS.2020.3008433.

[2] D. Xi *et al.*, "Exploiting bi-directional global transition patterns and personal preferences for missing POI category identification," *Neural Networks*, vol. 132, pp. 75–83, 2020, doi: 10.1016/j.neunet.2020.08.015.

[3] Z. Tian, H. Qiao, J. Tian, H. Zhu, and X. Li, "An Automated Brute Force Method Based on Webpage Static Analysis," in *Proceedings - 10th International Conference on Measuring Technology and Mechatronics Automation, ICMTMA 2018*, Apr. 2018, vol. 2018-January, pp. 100–103. doi: 10.1109/ICMTMA.2018.00031.

[4] S. K. Wanjau, G. M. Wambugu, and G. N. Kamau, "SSH-Brute Force Attack Detection Model based on Deep Learning," *Int. J. Comput. Appl. Technol. Res.*, vol. 10, no. 01, pp. 42–50, 2021, doi: 10.7753/ijcatr1001.1008.

[5] B. Abibullaev, I. Dolzhikova, and A. Zollanvari, "A Brute-Force CNN Model Selection for Accurate Classification of Sensorimotor Rhythms in BCIs," *IEEE Access*, vol. 8, pp. 101014–101023, 2020, doi: 10.1109/ACCESS.2020.2997681.

[6] D. Stiawan, S. Sandra, E. Alzahrani, and R. Budiarto, "Comparative analysis of K-Means method and Naïve Bayes method for brute force attack visualization," *2017 2nd Int. Conf. Anti-Cyber Crimes, ICACC 2017*, pp. 177–182, 2017, doi: 10.1109/Anti-Cybercrime.2017.7905286.

[7] J. Ma, Z. Li, J. C. P. Cheng, Y. Ding, C. Lin, and Z. Xu, "Air quality prediction at new stations using spatially transferred bi-directional long short-term memory network," *Sci. Total Environ.*, vol. 705, p. 135771, 2020, doi: 10.1016/j.scitotenv.2019.135771.

[8] G. Cheng, S. Ying, and B. Wang, "Tuning configuration of apache spark on public clouds by combining multi-objective optimization and performance prediction model," *J. Syst. Softw.*, vol. 180, p. 111028, 2021, doi: 10.1016/j.jss.2021.111028.

[9] S. Khan, S. Anjum, U. A. Gulzari, T. Umer, and B. S. Kim, "Bandwidth-Constrained Multi-Objective Segmented Brute-Force Algorithm for Efficient Mapping of Embedded Applications on NoC Architecture," *IEEE Access*, vol. 6, no. c, pp. 11242–11254, 2017, doi: 10.1109/ACCESS.2017.2778340.

[10] M. Nadeem, A. Arshad, S. Riaz, S. S. Band, and A. Mosavi, "Intercept the cloud network from brute force and ddos attacks via intrusion detection and prevention system," *IEEE Access*, vol. 9, pp. 152300–152309, 2021, doi: 10.1109/ACCESS.2021.3126535.

[11] K. Shinde, V. Itier, J. Mennesson, and D. Vasiukov, "Dimensionality reduction through convolutional autoencoders for fracture patterns prediction," *Appl. Math. Model.*, vol. 114, pp. 94–113, 2023, doi: 10.1016/j.apm.2022.09.034.

[12] R. Nasiboglu and E. Nasibov, "WABL method as a universal defuzzifier in the fuzzy gradient boosting regression model," *Expert Syst. Appl.*, vol. 212, no. September 2022, p. 118771, 2023, doi: 10.1016/j.eswa.2022.118771.

[13] C. L. Wang, Y. K. Chan, S. W. Chu, and S. S. Yu, "r-Reference points based k-means algorithm," *Inf. Sci. (Ny).*, vol. 610, pp. 204–214, 2022, doi: 10.1016/j.ins.2022.07.166.

[14] W. Gao and Z. H. Zhou, "Towards convergence rate analysis of random forests for classification," *Adv. Neural Inf. Process. Syst.*, vol. 2020-Decem, p. 103788, 2020, doi: 10.1016/j.artint.2022.103788.

[15] D. Kollias and S. Zafeiriou, "Exploiting Multi-CNN Features in CNN-RNN Based Dimensional Emotion Recognition on the OMG in-the-Wild Dataset," *IEEE Trans. Affect. Comput.*, vol. 12, no. 3, pp. 595–606, 2021, doi: 10.1109/TAFFC.2020.3014171.

[16] H. Guo, J. Liu, J. Yang, Z. Xiao, and Z. Wu, "Deep Collaborative Attention Network for

Hyperspectral Image Classification by Combining 2-D CNN and 3-D CNN," *IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens.*, vol. 13, pp. 4789–4802, 2020, doi: 10.1109/JSTARS.2020.3016739.
[17] S. Meister, M. Wermes, J. Stüve, and R. M. Groves, "Cross-evaluation of a parallel operating SVM – CNN classifier for reliable internal decision-making processes in composite inspection," *J. Manuf. Syst.*, vol. 60, no. July, pp. 620–639, 2021, doi: 10.1016/j.jmsy.2021.07.022.
[18] S. Hosseini and B. M. H. Zade, "New hybrid method for attack detection using combination of evolutionary algorithms, SVM, and ANN," *Comput. Networks*, vol. 173, no. February 2019, p. 107168, 2020, doi: 10.1016/j.comnet.2020.107168.
[19] G. A. MM, J. N. K. S, U. M. R, and M. R. TF, "An efficient SVM based DEHO classifier to detect DDoS attack in cloud computing environment," *Comput. Networks*, vol. 215, no. July, p. 109138, 2022, doi: 10.1016/j.comnet.2022.109138.
[20] P. Ramesh Kumar and A. Vijaya, "Naïve Bayes machine learning model for image classification to assess the level of deformation of thin components," *Mater. Today Proc.*, no. xxxx, 2022, doi: 10.1016/j.matpr.2022.08.489.
[21] L. Li *et al.*, "Naive Bayes classifier based on memristor nonlinear conductance," *Microelectronics J.*, vol. 129, no. September, 2022, doi: 10.1016/j.mejo.2022.105574.
[22] D. H. Vu, T. S. Vu, and T. D. Luong, "An efficient and practical approach for privacy-preserving Naive Bayes classification," *J. Inf. Secur. Appl.*, vol. 68, no. June, p. 103215, 2022, doi: 10.1016/j.jisa.2022.103215.
[23] B. Roy and H. Cheung, "A Deep Learning Approach for Intrusion Detection in Internet of Things using Bi-Directional Long Short-Term Memory Recurrent Neural Network," *2018 28th Int. Telecommun. Networks Appl. Conf. ITNAC 2018*, pp. 1–6, 2019, doi: 10.1109/ATNAC.2018.8615294.
[24] S. Li, Z. Yan, X. Wu, A. Li, and B. Zhou, "A Method of Emotional Analysis of Movie Based on Convolution Neural Network and Bi-directional LSTM RNN," *Proc. - 2017 IEEE 2nd Int. Conf. Data Sci. Cyberspace, DSC 2017*, pp. 156–161, 2017, doi: 10.1109/DSC.2017.15.
[25] S. Abujar, A. K. M. Masum, S. M. M. H. Chowdhury, M. Hasan, and S. A. Hossain, "Bengali Text generation Using Bi-directional RNN," *2019 10th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2019*, pp. 1–5, 2019, doi: 10.1109/ICCCNT45670.2019.8944784.
[26] B. Jia *et al.*, "Bidirectional RNN-Based Few-Shot Training for Detecting Multi-stage Attack," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 12612 LNCS, pp. 37–52, 2021, doi: 10.1007/978-3-030-71852-7_3.
[27] H. Su, E. Zio, J. Zhang, M. Xu, X. Li, and Z. Zhang, "A hybrid hourly natural gas demand forecasting method based on the integration of wavelet transform and enhanced Deep-RNN model," *Energy*, vol. 178, pp. 585–597, 2019, doi: 10.1016/j.energy.2019.04.167.
[28] Y. Chang, J. Chen, H. Lv, and S. Liu, "Heterogeneous bi-directional recurrent neural network combining fusion health indicator for predictive analytics of rotating machinery," *ISA Trans.*, no. xxxx, 2021, doi: 10.1016/j.isatra.2021.04.024.
[29] Z. Liu, J. Cao, J. You, S. Chen, Y. Lu, and P. Zhou, "A lithological sequence classification method with well log via SVM-assisted bi-directional GRU-CRF neural network," *J. Pet. Sci. Eng.*, vol. 205, no. 42030812, p. 108913, 2021, doi: 10.1016/j.petrol.2021.108913.
[30] S. Zhang, H. Liu, J. He, S. Han, and X. Du, "A deep bi-directional prediction model for live streaming recommendation," *Inf. Process. Manag.*, vol. 58, no. 2, p. 102453, 2021, doi: 10.1016/j.ipm.2020.102453.
[31] P. TS and P. Shrinivasacharya, "Evaluating neural networks using Bi-Directional LSTM for network IDS (intrusion detection systems) in cyber security," *Glob. Transitions Proc.*, vol. 2, no. 2, pp. 448–454, 2021, doi: 10.1016/j.gltp.2021.08.017.
[32] S. Salamatian, W. Huleihel, A. Beirami, A. Cohen, and M. Medard, "Centralized vs Decentralized Targeted Brute-Force Attacks: Guessing with Side-Information," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, no. c, pp. 3749–3759, 2020, doi: 10.1109/TIFS.2020.2998949.

[33] L. Lu, Y. Yi, F. Huang, K. Wang, and Q. Wang, “Integrating local CNN and global CNN for script identification in natural scene images,” *IEEE Access*, vol. 7, pp. 52669–52679, 2019, doi: 10.1109/ACCESS.2019.2911964.
[34] E. M. Hassib, A. I. El-Desouky, L. M. Labib, and E. S. M. El-kenawy, “WOA + BRNN: An imbalanced big data classification framework using Whale optimization and deep neural network,” *Soft Comput.*, vol. 24, no. 8, pp. 5573–5592, 2020, doi: 10.1007/s00500-019-03901-y.
[35] Z. Tian, H. Qiao, J. Tian, H. Zhu, and X. Li, “An Automated Brute Force Method Based on Webpage Static Analysis,” *Proc. - 10th Int. Conf. Meas. Technol. Mechatronics Autom. ICMTMA 2018*, vol. 2018-Janua, pp. 100–103, 2018, doi: 10.1109/ICMTMA.2018.00031.
[36] A. Nursetyo, D. R. Ignatius Moses Setiadi, E. H. Rachmawanto, and C. A. Sari, “Website and Network Security Techniques against Brute Force Attacks using Honeypot,” *Proc. 2019 4th Int. Conf. Informatics Comput. ICIC 2019*, 2019, doi: 10.1109/ICIC47613.2019.8985686.
[37] V. Chiriaco, A. Franzen, R. Thayil, and X. Zhang, “Finding partial hash collisions by brute force parallel programming,” *2017 IEEE Long Isl. Syst. Appl. Technol. Conf. LISAT 2017*, pp. 5–6, 2017, doi: 10.1109/LISAT.2017.8001964.
[38] K. Lee, “Comments on ‘Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption,’” *IEEE Trans. Cloud Comput.*, vol. 8, no. 4, pp. 1299–1300, 2020, doi: 10.1109/TCC.2020.2973623.
[39] H. Viswanathan, E. K. Lee, I. Rodero, and D. Pompili, “Uncertainty-Aware Autonomic Resource Provisioning for Mobile Cloud Computing,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 8, pp. 2363–2372, 2015, doi: 10.1109/TPDS.2014.2345057.
[40] I. Sadooghi *et al.*, “Understanding the Performance and Potential of Cloud Computing for Scientific Applications,” *IEEE Trans. Cloud Comput.*, vol. 5, no. 2, pp. 358–371, 2017, doi: 10.1109/TCC.2015.2404821.
[41] L. Wu, S. K. Garg, S. Versteeg, and R. Buyya, “SLA-based resource provisioning for hosted software-as-a-service applications in cloud computing environments,” *IEEE Trans. Serv. Comput.*, vol. 7, no. 3, pp. 465–485, 2014, doi: 10.1109/TSC.2013.49.
[42] S. Chaisiri, B. S. Lee, and D. Niyato, “Optimization of resource provisioning cost in cloud computing,” *IEEE Trans. Serv. Comput.*, vol. 5, no. 2, pp. 164–177, 2012, doi: 10.1109/TSC.2011.7.
[43] R. N. Calheiros, E. Masoumi, R. Ranjan, and R. Buyya, “Workload prediction using ARIMA model and its impact on cloud applications’ QoS,” *IEEE Trans. Cloud Comput.*, vol. 3, no. 4, pp. 449–458, 2015, doi: 10.1109/TCC.2014.2350475.
[44] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization,” no. Cic, pp. 108–116, 2018, doi: 10.5220/0006639801080116.