Klasifikasi Serangan *Brute Force* Menggunakan Metode *Convolutional Neural Network* (CNN)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat Memperoleh

Gelar Sarjana Komputer

OLEH :

BELLA PUTRI 09011281722059

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2021

HALAMAN PENGESAHAN

KLASIFIKASI SERANGAN *BRUTE FORCE* MENGGUNAKAN METODE *CONVOLUTIONAL NEURAL NETWORK* (CNN)

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

Oleh :

BELLA PUTRI

09011281722059

Indralaya, 2021

Mengetahui,

Pembimbing I

Deris Stiawan, M.T. Ph.D. IPU.
NIP. 197806172006041002

Pembimbing II

Huda Ubaya, M.T.
NIP. 198106162012121003

Ketua Jurusan Sistem Komputer

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Jum'at

Tanggal : 1 Oktober 2021

Tim Penguji :

1. Ketua Sidang	**: Ahmad Fali Oklilas, M.T**	
2. Sekretaris Sidang	**: Iman Saladin B. Azhar, M.MSI**	
3. Penguji Sidang	**: Ahmad Heryanto, M.T**	
4. Pembimbing 1	**: Deris Stiawan, M.T., Ph.D., IPU**	
5. Pembimbing 2	**: Huda Ubaya, S.T., M.T**	

Mengetahui, 4/1/22

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Bella Putri

NIM : 09011281722059

Judul : Klasifikasi Serangan *Brute Force* Menggunakan Metode *Convolutional Neural Network* (CNN)

Hasil Pengecekan Software iThenticate/Turnitin : 7%

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.

Indralaya, November 2021

Bella Putri

NIM. 09011281722059

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Bismillahirrahmanirrahim, Alhamdulilahirabbil'alamin, puji dan syukur penulis selalu panjatkan atas kehadirat Allah Subhanahu Wata'ala yang telah melimpahkan nikmat, taufik, dan hidayah-Nya yang sangat besar dan tidak pernah berhenti kepada penulis sehingga penulis dapat menyelesaikan penulisan Tugas Akhir ini yang berjudul **"Klasifikasi Serangan *Brute Force* Menggunakan Metode *Convolutional Neural Network* (CNN)".** Shalawat serta salam tak lupa kita curahkan kepada junjungan kita Nabi Muhammad Shallallahu'alaihi wa Sallam beserta keluarga,sahabat dan para pengikutnya yang inshaAllah istiqomah hingga akhir zaman. Penulis berharap agar tulisan ini dapat bermanfaat bagi orang banyak dan menjadi bahan bacaan bagiyang tertarik.

Pada kesempatan ini, dengan segala kerendahan hati penulis mengucapkan terima kasih kepada semua pihak atas bantuan, bimbingan, dan saran yang telah diberikan dalam menyelesaikan Tugas Akhir ini, antara lain:

1. Kedua Orang tua saya tercinta yang telah membesarkan saya dengan penuh kasih sayang. Terimakasih untuk segala doa, dukungan dan motivasi yang diberikan selama ini.
2. Kedua kakak saya dan adik perempuan saya yang sangat saya sayangi, yang selalu mendo'akan serta mendukung.
3. Yth, bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Yth, bapak Dr. Ir. H. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Yth, bapak Ir. Bambang Tutuko, M.T., selaku Pembimbing Akademik.
6. Yth, Bapak Deris Stiawan, M.T., Ph.D., IPU., selaku Pembimbing Tugas Akhir I yang telah berkenan meluangkan waktunya guna membimbing, memberikan saran dan motivasi serta bimbingan terbaik untuk penulis dalam menyelesaikan Tugas Akhir ini.
7. Yth, Bapak Huda Ubaya, M.T., selaku Pembimbing Tugas Akhir II yang

telah berkenan meluangkan waktunya guna membimbing, memberikan saran dan motivasi serta bimbingan terbaik untuk penulis dalam menyelesaikan Tugas Akhir ini.

8. Teman-teman seperjuangan di *Network & Infosec Riset Group* yang turut memberikan arahan serta nasihat.
9. Mbak Renny selaku admin terbaik di Jurusan Sistem Komputer yang selalu memberi kemudahan kepada mahasiswa/i dalam mengurus seluruh berkas.
10. Lia, Tamara, dan Fadilla yang telah mewarnai perkuliahan penulis dengan canda dan tawa.
11. Teman-teman seperjuangan dari jurusan Sistem Komputer yang tidak bisa disebutkan satu-persatu. Khususnya seluruh teman-teman dari kelas SK17 A Reguler.
12. Dan semua pihak yang telah membantu.

Penulis menyadari bahwa Tugas Akhir ini masih sangat jauh dari kata sempurna. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan penulis agar penulisan Tugas Akhir ini dapat menjadi lebih baik lagi dan dapat dijadikan sebagai sumber referensi yang bermanfaat bagi semua pihak.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Palembang, 25 November 2021
Penulis,

Bella Putri
NIM. 09011281722059

CLASSIFICATION OF BRUTE FORCE ATTACK USING METHOD CONVOLUTIONAL NEURAL NETWORKS (CNN)

Bella Putri (09011281722059)
Dept. of Computer Engineering, Faculty of Computer Science, Sriwijaya University
Email : bellaputri533@gmail.com

ABSTRACT

Brute Force is a password cracking attack against a computer security system. In launching the attack, the perpetrator uses a trial-and-error method by trying all password combinations in order to pass the authentication process. Actually, brute force is an old and simple attack method, but this type of cybercrime has a fairly high success rate and is considered very effective. That is why this attack is still popular today and is widely used by hackers to carry out their criminal acts. The method used in this research is Convolutional Neural Network (CNN). In this study, classification was carried out for 3 classes of network attacks with a composition of 50% to 80% of training data, on the parameters of learning rate, batch size, and relu activation. Based on the test results, CNN model 1 produces the best performance in classifying with 99.99% accuracy, 100% precision, 100% specificity, and 99.99% fi-score.

Keywords: *Classification, Brute Force, Convolutional Neural Network* (CNN)

Indralaya, 2021

Supervisor I

Deris Stiawan, M.T, Ph.D, IPU.
NIP. 197806172006041002

Supervisor II

Huda Ubaya, S.T, M.T.
NIP. 198106162012121003

Head Of Departement Computer Engineering

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

KLASIFIKASI SERANGAN *BRUTE FORCE* MENGGUNAKAN METODE *CONVOLUTIONAL NEURAL NETWORK* (CNN)

Bella Putri (09011281722059)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : bellaputri533@gmail.com

ABSTRAK

Brute Force adalah serangan peretas kata sandi terhadap sebuah sistem keamanan komputer. Dalam melancarkan serangannya, pelaku menggunakan metode *trial-and-error* dengan mencoba seluruh kombinasi kata sandi agar bisa melewati proses autentikasi. Sebenarnya *brute force* adalah metode serangan lama dan juga terhitung sederhana, namun jenis *cybercrime* ini mempunyai *success rate* yang cukup tinggi dan dinilai sangat efektif. Itulah mengapa serangan ini masih populer sampai saat ini dan banyak digunakan oleh para *hackers* untuk melakukan tindakan kriminalnya. Metode yang digunakan pada penelitian ini adalah *Convolutional Neural Network* (CNN). Pada penelitian ini dilakukan klasifikasi untuk 3 kelas serangan jaringan dengan komposisi 50% sampai 80% data latih, terhadap parameter *learning rate*, *batch size*, dan aktivasi *relu*. Berdasarkan hasil pengujian bahwa model 1 CNN menghasilkan performa paling baik dalam melakukan pengklasifikasian dengan tingkat akurasi sebesar 99.99%, presisi 100%, spesifisitas 100%, dan fi-score 99,99%.

Kata Kunci : Klasifikasi, *Brute Force, Convolutional Neural Network* (CNN)

Indralaya, 2021

Pembimbing I

Deris Stiawan, M.T, Ph.D, IPU.
NIP. 197806172006041002

Pembimbing II

Huda Ubaya, S.T, M.T.
NIP. 198106162012121003

Ketua Jurusan Sistem Komputer

17/1/22

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

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR LAMPIRAN

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Kemajuan manusia dalam menggunakan teknologi telah meningkat sejak dua abad terakhir. *Internet of Things* (IoT) adalah salah satu topik yang paling ramai dan dibahas di bidang penelitian saat ini. Beberapa peneliti juga melihat masa depan dunia dalam teknologi ini. Sejak saat itu penelitian dan pengembangan yang signifikan telah dilakukan pada IoT, namun berbagai kerentanan diamati membuat IoT sebagai teknologi dalam bahaya. Akibatnya, ada begitu banyak serangan terhadap IoT yang telah ditemukan sebelum implementasi komersialnya yang sebenarnya [1]. Salah satu kasus penyalahgunaan yang paling umum yang diantisipasi oleh administrator sistem adalah fakta bahwa sistem akan mengalami serangan [2].

Serangan adalah realisasi ancaman, tindakan yang merugikan bertujuan untuk menemukan dan memanfaatkan kerentanan sistem. Insiden terdiri dari serangan dan respon sistem komputer terhadapnya. Serangan bisa gagal mencapai tujuan yang dimaksudkan karena beberapa alasan, tetapi ada kemungkinan sistem menjadi lebih rentan. Tujuan utama dari setiap klasifikasi adalah untuk menyarankan fitur klasifikasi, yang dengannya objek klasifikasi dijelaskan sepenuhnya [3]. Keamanan jaringan dan layanan menjadi tantangan utama. Seperti, serangan *brute force* dan sebab yang diakibatkannya tersebar luas. *Brute force* adalah salah satu jenis serangan yang paling umum di jaringan komputer [4].

Otentikasi berbasis password tetap menjadi cara yang paling umum untuk memberikan akses karena kemudahannya, meskipun banyak kekurangan yang terdokumentasi dengan baik. Dengan kemajuan teknologi, bahkan kata sandi yang lebih panjang menjadi lebih rentan untuk diretas. Aspek penting lainnya dari keamanan kata sandi adalah seringnya mengubah kata sandi [5]. *Brute force* adalah serangan yang sering digunakan untuk meretas server *ftp*, server web, dan server email [6].

Metode *deep learning* paling populer salah satu nya adalah CNN yakni *Convolutional Neural Network* berdasarkan jaringan neural baru – baru ini memberikan kemajuan yang signifikan untuk banyak praktik aplikasi. [7] CNN memiliki kinerja mesin yang sangat baik khususnya aplikasi yang berhubungan dengan data gambar, seperti kumpulan data klasifikasi gambar terbesar.[8] Ada tiga lapisan utama di CNN yakni lapisan konvolusional, lapisan penyatuan dan lapisan yang terhubung sepenuhnya [9]. Biasanya lapisan konvolusional diselingi dengan lapisan sub-pengambilan sampel untuk mengurangi waktu komputasi dan secara bertahap membangun invariansi spasial dan configural [10].

Dari penjelasan di atas, maka penulis akan membahas tentang klasifikasi serangan yang diberi judul **"Klasifikasi Serangan *Brute Force* dengan metode *Convolutional Neural Network* (CNN)".**

1.2 Perumusan Masalah

1. Bagaimana klasifikasi serangan *Brute Force* dalam metode *Convolutional Neural Network* (CNN) ?

2. Bagaimana hasil yang di dapat saat metode *Convolutional Neural Network* (CNN) digunakan dalam klasifikasi serangan *Brute Force* ?

1.3 Batasan Masalah

1. Penelitian ini hanya klasifikasi pada serangan *Brute Force.*

2. Penelitian ini hanya menghasilkan output berupa evaluasi pada serangan *Brute Force.*

3. Simulasi yang digunakan pada penelitian ini adalah *Python.*

1.4 Tujuan

1. Dapat mengklasifikasikan serangan *Brute Force* dengan metode *Convolutional Neural Network* (CNN).

2. Mengukur dan menganalisa hasil dari akurasi, presisi, *recall* dan *f-1 score* terhadap kinerja pengklasifikasi metode *Convolutional Neural Network* (CNN).

1.5 Manfaat

Berikut manfaat dari hasil penelitian ini diantaranya :

1. Menggunakan algoritma CNN bisa mengklasifikasikan *brute force.*
2. Bisa menjadi referensi untuk tugas akhir berikutnya bisa dengan metode yang sama yaitu CNN untuk tema klasifikasi yang berbeda, atau dengan klasifikasi *brute force* dengan menggunakan metode yang lain selain CNN.

1.6 Metodologi pada Penelitian

Diantara metodologi penelitian yang digunakan dalam tugas akhir ini diantaranya :

1. Penulis menyiapkan data serta informasi dari berbagai sumber yang berkaitan dengan objek yang akan dibahas serta diteliti pada Tugas Akhir yang akan dijalankan.
2. Lalu jika penulis sudah mendapat data / dataset yang sesuai dengan topik Tugas Akhir maka dilakukan pengolahan data untuk memudahkan klasifikasi yang akan dijalankan pada saat pemrograman.
3. Selanjutnya mengklasifikasikan beberapa data dalam sebuah dataset, contohnya ada klasifikasi normal, sedang, dan lainnya, tentu saja menggunakan metode CNN.

4. Berikutnya menganalisa dari hasil yang didapat saat menguji dataset pada klasifikasi *brute force* menggunakan algoritma *Convolutional Neural Network* tersebut.
5. Setelah itu mengumpulkan rangkuman akhir pada penelitian untuk dituliskan pada laporan Tugas Akhir.

1.7 Sistematika pada Penulisan

Untuk memudahkan penulisan saat membuat Tugas Akhir ini maka sistematika pada penulisan juga dibutuhkan, di antara lain :

1. Bab I ini berisikan tentang judul yang dibahas pada Tugas Akhir, serta informasi seperti pada latar belakang yang dibahas oleh penulis sehingga memudahkan penelitian selanjutnya untuk menjadikan referensi tanpa membaca panjang lebar keseluruhan dari tugas akhir tersebut.
2. Bab II lebih spesifik lagi menjelaskan pengertian ataupun yang berhubungan akan objek klasifikasi apa yang dibahas serta metode apa yang digunakan pada tugas akhir ini.
3. Bab III menjelaskan tahapan yang dilakukan pada penelitian ini dalam bentuk kerangka kerja penelitian, serta menjelaskan dataset yang digunakan, persiapan data dan sebagainya.
4. Bab IV tentang hasil serta pembahasan yang didapat saat proses pengklasifikasian dataset dengan metode yang digunakan pada saat penelitian.
5. Bab V berisikan tentang rangkuman yang didapat pada proses pelaksanaan pemrograman serta saran yang bisa digunakan peneliti lain untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, 2017, pp. 32–37.

[2] J. Faust, "Distributed Analysis of SSH Brute Force and Dictionary Based Attacks," 2018.

[3] N. Paulauskas and E. Garsva, "Computer system attack classification," *Elektron. ir elektrotechnika*, vol. 66, no. 2, pp. 84–87, 2006.

[4] M. M. Najafabadi, T. M. Khoshgoftaar, C. Kemp, N. Seliya, and R. Zuech, "Machine learning for detecting brute force attacks at the network level," in *2014 IEEE International Conference on Bioinformatics and Bioengineering*, 2014, pp. 379–385.

[5] M. Wagner, S. Heyse, and C. Guillemet, "Brute-Force Search Strategies for Single-Trace and Few-Traces Template Attacks on the DES Round Keys of a Recent Smart Card.," *IACR Cryptol. ePrint Arch.*, vol. 2017, p. 614, 2017.

[6] S. Vaithyasubramanian, A. Christy, and D. Saravanan, "An analysis of Markov password against brute force attack for effective web applications," *Appl. Math. Sci.*, vol. 8, no. 117, pp. 5823–5830, 2014.

[7] I. Cong, S. Choi, and M. D. Lukin, "Quantum convolutional neural networks," *Nat. Phys.*, vol. 15, no. 12, pp. 1273–1278, 2019.

[8] S. Albawi, T. A. Mohammed, and S. Al-Zawi, "Understanding of a convolutional neural network," *Proc. 2017 Int. Conf. Eng. Technol. ICET 2017*, vol. 2018-Janua, no. April 2018, pp. 1–6, 2018, doi: 10.1109/ICEngTechnol.2017.8308186.

[9] L. Wen, X. Li, L. Gao, and Y. Zhang, "A new convolutional neural network-based data-driven fault diagnosis method," *IEEE Trans. Ind. Electron.*, vol. 65, no. 7, pp. 5990–5998, 2017.

[10] J. Bouvrie, "Notes on convolutional neural networks," 2006.

[11] T. Gautam and A. Jain, "Analysis of brute force attack using TG—Dataset," in *2015 SAI Intelligent Systems Conference (IntelliSys)*, 2015, pp. 984–988.

[12] V. Grover, "An Efficient Brute Force Attack Handling Techniques for Server Virtualization," *SSRN Electron. J.*, pp. 1–4, 2020, doi: 10.2139/ssrn.3564447.

[13] N. Fithria, "Jenis--Jenis Serangan Terhadap Kriptografi," *Tek. Inform. Inst. Teknol. Bandung*, 2007.

[14] J. Wu, "Introduction to convolutional neural networks," *Natl. Key Lab Nov. Softw. Technol. Nanjing Univ. China*, vol. 5, p. 23, 2017.

[15] K. O'Shea and R. Nash, "An introduction to convolutional neural networks," *arXiv Prepr. arXiv1511.08458*, 2015.

[16] B. Warsito, "Kapita Selekta Statistika Neural Network," 2009.

[17] S. Albawi, T. A. Mohammed, and S. Al-Zawi, "Understanding of a convolutional neural network," in *2017 International Conference on Engineering and Technology (ICET)*, 2017, pp. 1–6.

[18] U. R. Acharya *et al.*, "A deep convolutional neural network model to classify heartbeats," *Comput. Biol. Med.*, vol. 89, pp. 389–396, 2017.

[19] A. Khan, A. Sohail, U. Zahoora, and A. S. Qureshi, "A survey of the recent architectures of deep convolutional neural networks," *Artif. Intell. Rev.*, vol. 53, no. 8, pp. 5455–5516, 2020.

[20] E. Prasetyo, "Data mining konsep dan aplikasi menggunakan matlab," *Yogyakarta Andi*, 2012.

[21] H. G. Lewis and M. Brown, "A generalized confusion matrix for assessing area estimates from remotely sensed data," *Int. J. Remote Sens.*, vol. 22, no. 16, pp. 3223–3235, 2001.

[22] M. Story and R. G. Congalton, "Accuracy assessment: a user's perspective," *Photogramm. Eng. Remote Sensing*, vol. 52, no. 3, pp. 397–399, 1986.