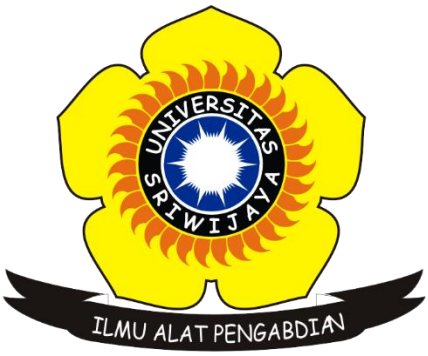
SISTEM PENCEGAHAN SERANGAN *MALWARE BANKING TROJAN* DENGAN METODE *RANDOM FOREST*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer



OLEH :

REZA MAULIDIN

09011181621017

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2020

LEMBAR PENGESAHAN

SISTEM PENCEGAHAN SERANGAN *MALWARE BANKING TROJAN* DENGAN METODE *RANDOM FOREST*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:

REZA MAULIDIN

09011181621017

Indralaya, 2020

Mengetahui,

Pembimbing I Tugas Akhir	Pembimbing II Tugas Akhir
Deris Stiawan, M.T., Ph.D	**Ahmad Heryanto, S.Kom., M.T.**
NIP. 197806172006041002	**NIP. 198701222015041002**

Ketua Jurusan Sistem Komputer

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

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Kamis
Tanggal : 12 November 2020

Tim Penguji:

1. **Ketua : Rahmat Fadli Istanto, M.Sc**
2. **Sekretaris I : Deris Stiawan, M.T., Ph.D**
3. **Sekretaris II : Ahmad Heryanto, S.Kom., M.T.**
4. **Anggota I : Ahmad Zarkasi, M.T**
5. **Anggota II : Aditya Putra Perdana P, M.T**

Mengetahui,
Ketua Jurusan Sistem Komputer

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

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Reza Maulidin
NIM : 09011181621017
Judul : Sistem Pencegahan Serangan *Malware Banking Trojan* dengan Metode *Random Forest.*

Hasil Pengecekan Software *iThenticate/Turnitin*: 12%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/ palgiat 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.

Indralaya, Desember 2020
Yang menyatakan,

Reza Maulidin

HALAMAN PERSEMBAHAN

Skripsi ini saya persembahkan untuk sang pencipta Allah SWT, kedua orang tuaku tercinta, orang-orang terdekat, serta teman-teman yang telah meyakinkan saya dalam menyelesaikan perjuangan ini melalui semangat dan doa yang terus menerus diberikan. Terimakasih atas dukungannya, semoga hal baik tersebut dibalas beribu kebaikan oleh Allah SWT.

"Manusia dilahirkan karena alasan. Maka carilah alasan tersebut dengan berusaha tanpa melupakan doa"

Segenap hati berterima kasih dengan penuh rasa sayang kepada:

- ***Papa (Muslih Arfan) dan Mama (Nelly Novianty) tercinta***
- ***Kakak pertama (Angga Kurniawan), kakak kedua (M Andre Apriansyah) dan adik (Asri Sabrina)***
- ***Keponakan yang lucu (Askanna Havika)***
- ***Teman- teman seperjuangan SK 2016 dan Himasisko***
- ***Keluarga Besar Sistem Komputer Universitas Sriwijaya***
- ***Civitas Akademika Universitas Sriwijaya***

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Puji syukur Penulis panjatkan kehadirat Allah SWT, karena berkat rahmat dan karunia-Nya baik berupa pikiran, ilmu pengetahuan mupun kesehatan dan kekuatan sehingga penulis dapat menyelesaikan penyusunan tugas akhir ini dengan judul *Sistem Pencegahan Serangan Malware Banking Trojan dengan Metode Random Forest.*

Pada penyusunan tugas akhir ini, tidak terlepas dari bantuan, bimbingan, ajaran serta dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur dan terima kasih kepada:

1. Allah Subhanahu Wata'ala yang telah memberikan berkah dan karunia-Nya kepada penulis dalam penyusunan tugas akhir ini.
2. Orangtua tercinta yang selalu memberikan semangat dan do'a serta keluarga besar penulis yang tersayang.
3. Kakak pertama (Angga Kurniawan) yang selalu memberi saran dan nasihat, kakak kedua (M Andre Apriansyah) dan adik (Asri Sabrina) yang selalu memberi semangat dan do'a.
4. Bapak Jaidan Jauhari, S.Pd. M.T selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
6. Deris Stiawan, M.T., Ph.D selaku Pembimbing Tugas Akhir 1.
7. Ahmad Heryanto, S.Kom., M.T. selaku Pembimbing Tugas Akhir 2.
8. Bapak Ahmad Fali Oklilas,M.T. selaku Dosen Pembimbing Akademik.
9. Mbak Winda Kurnia Sari selaku Admin Jurusan Sistem Komputer.
10. Teman yang selalu support, selalu ada, dan selalu membantu selama kuliah dan skripsi (Winda Maida), terima kasih yang sebesar- besarnya.
11. Teman- teman satu kelompok riset yang selalu memberi solusi dan semangat Deri, Aria, Adel, toreq, ardin, hari uda. Sukses untuk kita semua guys!

12. Teman- teman ‘Pemuda Cawa (agil, yusuf, wahid, nedi, teok, dewan)’ dan teman- teman ‘LTS’ yang tidak bisa disebut satu persatu karena rame. Terima kasih telah berbagi canda tawa dikala pusing skripsi.
13. Rekan- rekan BPH HIMASISKO 2017/2018, kakak- kakak alumni BPH HIMASISKO dan teman- teman seperjuagan Organisasi Mahasiswa Fasilkom 2017/2018.
14. Kakak- kakak tingkat yang menjadi panutan, teman-teman seperjuangan Jurusan Sistem Komputer Angkatan 2016 terkhusus kelas A, serta semua pihak yang tidak dapat penulis cantumkan satu persatu.
15. Civitas Akademika Fakultas Ilmu Komputer Universitas Sriwijaya.

Penulis menyadari bahwa masih ada banyak kekurangan dalam laporan tugas akhir ini. Mengingat kurangnya pengetahuan dan pengalaman penulis. Untuk itu segala kritik dan saran, sangatlah penting bagi penulis.

Akhir kata dengan segala keterbatasan, penulis berharap semoga laporan ini menghasilkan sesuatu yang bermanfaat bagi kita semua khususnya bagi mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya secara langsung ataupun tidak langsung sebagai sumbangan pikiran dalam peningkatan mutu pembelajaran.

Wa’alaikumsalam Warahmatullahi Wabarakatuh.

Indralaya, Desember 2020

Penulis

TROJAN MALWARE BANKING ATTACK PREVENTION SYSTEM USING RANDOM RANDOM FOREST METHOD

Reza Maulidin
(09011181621017)

Department of Computer Engineering, Faculty of Computer Science, Sriwijaya University

Email: rezamaulidin0@gmail.com

Abstract

Banking Trojans are one of the most well-known types of malware because they are designed to measure money directly from the bank accounts of mobile or PC users. Tinba is a small malware which is very difficult to detect because of its small size, smaller than other Trojan that is commonly known. The purpose of this paper is to monitor tinba traffic. Before the blocking stage, the initial stage is by checking the traffic with the Snort Engine, the traffic pattern is unique to the traffic. The data sets used were sourced from the Stratosphere IPS. Then the results from the Snort engine obtained attack data which will be processed by machine learning random forest to prove the accuracy of the dataset used. In this study, the accuracy obtained was 99.69%. The next stage is to prevent traffic using the Suricata engine. At this stage a manual simulation is carried out by attacking the victim's device. In the final stage of this research, 27 traffic successfully blocked by the IPS mode Suricata engine.

Keywords: Banking trojan, Malware, Tinba, Snort, Machine learning, Random Forest, Suricata.

SISTEM PENCEGAHAN SERANGAN MALWARE BANKING TROJAN DENGAN METODE RANDOM RANDOM FOREST

Reza Maulidin
(09011181621017)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer,
Universitas Sriwijaya
Email: rezamaulidin0@gmail.com

Abstrak

Banking Trojan adalah salah satu jenis malware yang paling terkenal karena mereka dirancang untuk mencuri uang langsung dari rekening bank para pengguna perangkat mobile maupun PC. Tinba merupakan malware kecil yang sangat sulit dideteksi karena ukurannya yang kecil, lebih kecil dari Trojan lain yang biasa dikenal. Tujuan dari paper ini untuk memblokir traffic tinba. Sebelum ke tahapan bloking, tahapan awal yaitu dengan mendeteksi traffic tinba dengan Snort Engine lalu mengenali pola unik dari traffic tersebut. Dataset yang digunakan bersumber dari Stratosphere IPS. Kemudian hasil dari Snort engine didapat data serangan yang mana akan diolah oleh machine learning random forest untuk membuktikan keakuratan dataset yang digunakan. Pada penelitian ini didapatkan akurasi sebesar 99,69%. Tahapan selanjutnya adalah mencegah/memblokir traffic tinba menggunakan Suricata engine. Pada tahapan ini dilakukan simulasi manual dengan menyerang perangkat korban. Pada tahapan akhir penelitian ini didapatkan 27 traffic tinba yang berhasil di drop/blok oleh Suricata engine mode IPS.

Kata Kunci: Banking trojan, Malware, Tinba, Snort, Machine learning, Random Forest, Suricata.

DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Saat ini, sistem perbankan online adalah cara yang menarik untuk melakukan operasi keuangan seperti *e-commerce*, *e-banking*, dan pembayaran elektronik lainnya tanpa banyak usaha atau perlu kehadiran fisik apa pun [1]. Meningkatnya popularitas layanan perbankan online dan sistem pembayaran ini telah menciptakan motivasi bagi para *hacker* untuk mencuri kredensial dan uang pelanggan.

Banking Trojan adalah salah satu jenis malware yang paling terkenal karena mereka dirancang untuk mencuri uang langsung dari rekening bank para pengguna perangkat *mobile maupun PC.* Jenis serangan ini menarik bagi pelaku kejahatan siber di seluruh dunia, karena keuntungan dapat diperoleh dengan cara yang mudah. *Banking trojan* juga telah menjadi cara melakukan serangan terhadap lembaga-lembaga keuangan selama lebih dari satu dekade, dan mereka telah menjadi salah satu pendorong utama lalu lintas botnet [1]. Terdapat banyak sekali jenis-jenis dari Banking Trojan yaitu *emotet, dridex, zeus, tiny banker trojan, panda, trickbot,* dan masih banyak lagi.

Tiny banker Trojan atau disebut juga dengan tinba, merupakan malware kecil yang sangat sulit dideteksi karena ukurannya yang kecil. Hanya dengan 20kb, lebih kecil dari Trojan lain yang biasa dikenal. Tinba menggunakan metode yang disebut packet sniffing untuk membaca lalu lintas jaringan. Tinba pertama kali menginfeksi sistem saat pengguna mencoba masuk ke salah satu situs web bank yang ditargetkan. Kemudian, korban menerima *fake message* dan formulir web yang meminta korban untuk menuliskan kredensial loginnya [2]. Tiny banker pertama kali ditemukan pada tahun 2012, ketika ditemukan telah menginfeksi ribuan komputer di Turki.

Intrusion Detection System (IDS) dimulai di mana firewall berakhir. Investigasi pemantauan real-time dari data aktivitas jaringan untuk kemungkinan serangan terhadap kerentanan yang sedang berlangsung akan dikenali sebagai *Intrusion Detection System* [3]. *Intrusion Detection System* merupakan suatu proses

memonitor dan mengidentifikasi aktifitas pada suatu host atau network untuk dijadikan informasi apakah host atau network tersebut telah berhasil diserang atau masih sebatas percobaan serangan. Sebuah *Intrusion Detection System* membantu memonitor network kita dari berbagai macam anomali (kejadian yang tidak biasa) yang mungkin itu dapat mengindikasikan suatu ancaman serangan *hacker*, *malware*, ataupun adanya *vulnerability* (celah keamanan) pada sistem kita.

Pada penelitian ini akan membahas tentang bagaimana *tinba banking trojan* yang merupakan jenis dari *malware banking trojan* dapat dicegah pada *network* atau yang dikenal sebagai *instrusion prevention system*. Intrusion Prevention System (IPS) adalah sistem yang dapat secara otomatis mendeteksi aktivitas mencurigakan yang berpotensi jahat dalam jaringan [4]. Intrusion Prevention System (IPS) merupakan solusi keamanan yang lebih advance dari IDS, karena IPS dapat melakukan lebih dari 'sekedar' menganalisis traffic/log dan menghasilkan alert. IPS dapat secara proaktif melakukan 'reaksi' terhadap intrusi yang terdeteksi. Oleh karena itu IPS secara umum diletakkan secara in-line dengan firewall, agar IPS dapat menganalisis secara *real-time* semua traffic yang masuk dan keluar pada *network* untuk mendeteksi *suspicious* atau *malicious activity* dan kemudian secara instan melakukan aksi yang diperlukan untuk mencegah aktivitas (yang merupakan serangan) tersebut berhasil masuk kedalam jaringan atau sistem. Kemudian serangan dari banking trojan ini akan di cegah dengan menggunakan teknologi machine learning.

Istilah *machine learning* pada dasarnya adalah proses komputer untuk belajar dari data (*learn from data*). Tanpa adanya data, komputer tidak akan bisa belajar apa-apa. Semua pengetahuan *machine learning* pasti akan melibatkan data. Data bisa saja sama, akan tetapi algoritma dan pendekatan nya berbeda-beda untuk mendapatkan hasil yang optimal [16]. Pada penelitian penulis pendekatan machine learning yang akan digunakan adalah algoritma *random forest.*

Random Forest adalah klasifikasi *ensemble* dan pendekatan regresi yang tidak tertandingi dalam akurasi antara algoritma penambangan data saat ini [5]. Metode *Random Forest* merupakan salah satu metode dalam *Decision Tree*. *Decision*

Tree atau pohon pengambil keputusan adalah sebuah diagram alir yang berbentuk seperti pohon yang memiliki sebuah *root node* yang digunakan untuk mengumpulkan data, Sebuah *inner node* yang berada pada *root node* yang berisi tentang pertanyaan tentang data dan sebuah *leaf node* yang digunakan untuk memecahkan masalah serta membuat keputusan. *Decision tree* mengklasifikasikan suatu sampel data yang belum diketahui kelasnya kedalam kelas – kelas yang ada. Penggunaan *decision tree* agar dapat menghindari *overfitting* pada sebuah set data saat mencapai akurasi yang maksimum. *Random forest* (RF) [6] adalah pengelompokan *ensemble* yang menghasilkan banyak pohon keputusan, menggunakan subset sampel pelatihan dan variabel pelatihan yang dipilih secara acak.

Berdasarkan penjelasan tersebut, penulis melakukan penelitian mengenai Sistem Pencegahan Malware Banking Trojan dengan pendeketan algoritma *random forest*. Untuk mendeteksi kemudian mencegah serangan *malware banking trojan* ini diharapkan dapat mengurangi kasus serangan *banking trojan* dengan adanya *alert* dan *blocking* di suatu sistem.

1.2 Perumusan Masalah

Berikut adalah rumusan masalah dalam penulisan Proposal Tugas Akhir ini:

1. Bagaimana cara penanganan serangan dari malware *Banking Trojan* menggunakan algoritma *Random Forest*?
2. Bagaimana bentuk dataset yang akan digunakan untuk melakukan penanganan serangan *Tinba Banking Trojan* menggunakan algoritma *Random Forest*?
3. Apa saja *output* yang dihasilkan dari penanganan serangan *Tinba Banking Trojan* menggunakan algoritma *Random Forest*?
4. Apa *software* atau *tools* yang digunakan untuk mengklasifikasikan lalu lintas normal dan abnormal yang disebabkan oleh *Tinba Banking Trojan* menggunakan algoritma *Random Forest?*
5. Mencegah *traffic* paket serangan *Tinba banking Trojan* sebelum sampai ke perangkat korban.

1.3 Tujuan Penelitian

Adapun tujuan tugas akhir ini adalah sebagai berikut:

1. Menentukan *Rules Snort* yang digunakan untuk serangan *Tinba Banking Trojan*.
2. Mendeteksi serangan *tinba banking Trojan* menggunakan snort engine.
3. Mengklarifikasi serangan *Tinba Banking Trojan* menggunakan Algoritma *Machine Learning Random Forest*.
4. Menganalisa keakurasian metode yang digunakan untuk mendeteksi serangan *Tinba Banking Trojan*.
5. Mencegah/memblok paket serangan *Tinba banking Trojan* sebelum sampai ke perangkat korban menggunakan *suricata engine*.

1.4 Manfaat Penelitian

Adapun manfaat tugas akhir ini adalah sebagai berikut:

1. Dapat memblokir jika adanya paket serangan dari *Tinba Banking Trojan*.
2. Memberikan keamanan terhadap mesin server dari attacker khususnya Malware *Banking Trojan*.
3. Memberikan informasi mengenai *performance* metode *Random Forest*.

1.5 Batasan Masalah

Batasan masalah tugas akhir ini yaitu sebagai berikut:

1. Dalam penelitian ini digunakan serangan *Malware Banking Trojan* dengan jenis serangan *Tinba Banking Trojan*.
2. Metode yang digunakan untuk mendeteksi serangan menggunakan *Random Forest*.
3. Pengujian bersifat *offline*.
4. Menggunakan Dataset *Stratosphere*.
5. Membahas cara mendeteksi serangan.
6. Membahas cara mencegah serangan.

1.6 Sistematika Penulisan

Adapun sistematika dalam penulisan tugas akhir ini adalah sebagai berikut:

BAB 1 Pendahuluan

Bab ini berisikan Latar Belakang, Perumusan Masalah, Tujuan Penelitian, Manfaat Penelitian, Batasan Masalah dan Sistematika Penulisan.

BAB 2 Tinjauan Pustaka

Bab ini akan berisi dasar teori *Instrusion Detection System* (IDS), *Intrusion Prevention System* (IPS), *tinba banking trojan, snort, suricata*, algoritma *Random forest* dan yang berhubungan dengan penelitian.

BAB 3 Metodologi

Bab ini menjelaskan secara sistematis, bagaimana proses penelitian dilakukan. Penjelasan pada bab ini meliputi tahapan perancangan sistem dan penerapan metode penelitian.

BAB 4 Hasil dan Analisis

Bab ini memiliki pembahasan mengenai pengekstrakan dataset, Tahap Pemrograman, Perbandingan Hasil Olah dan Dataset, Pengukuran Parameter, Pembahasan, dan Analisis.

BAB 5 Kesimpulan dan Saran

Bab ini berisikan kesimpulan serta menjawab tujuan yang hendak dicapai pada Bab I (Pendahuluan) dan Saran untuk penelitian berikutnya.

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR PUSTAKA

[1] A. Gezer, G. Warner, C. Wilson, and P. Shrestha, "A flow-based approach for Trickbot banking trojan detection," *Comput. Secur.*, vol. 84, pp. 179–192, 2019, doi: 10.1016/j.cose.2019.03.013.

[2] M. Wazid, S. Zeadally, and A. K. Das, "Mobile Banking: Evolution and Threats: Malware Threats and Security Solutions," *IEEE Consum. Electron. Mag.*, vol. 8, no. 2, pp. 56–60, 2019, doi: 10.1109/MCE.2018.2881291.

[3] S. A. Maske, "Advanced Anomaly Intrusion Detection Technique For Host Based System Using System Call Patterns," pp. 2–5.

[4] R. F. Pratama, N. A. Suwastika, and M. A. Nugroho, "Design and implementation adaptive Intrusion Prevention System (IPS) for attack prevention in software-defined network (SDN) architecture," *2018 6th Int. Conf. Inf. Commun. Technol. ICoICT 2018*, vol. 0, no. c, pp. 299–304, 2018, doi: 10.1109/ICoICT.2018.8528735.

[5] M. Belgiu and L. Drăgu, "Random forest in remote sensing: A review of applications and future directions," *ISPRS J. Photogramm. Remote Sens.*, vol. 114, pp. 24–31, 2016, doi: 10.1016/j.isprsjprs.2016.01.011.

[6] L. E. O. Breiman, "Random Forests," pp. 5–32, 2001.

[7] C. Corbett and W. H. Robinson, "Fighting Banking Botnets By Exploiting Inherent Command and Control Vulnerabilities," pp. 93–100, 2014.

[8] D. Kiwia, A. Dehghantanha, K. R. Choo, and J. Slaughter, "computational intelligence," *J. Comput. Sci.*, 2017, doi: 10.1016/j.jocs.2017.10.020.

[9] A. Mohaisen and O. Alrawi, "Unveiling zeus automated classification of malware samples," *WWW 2013 Companion - Proc. 22nd Int. Conf. World Wide Web*, pp. 829–832, 2013, doi: 10.1145/2487788.2488056.

[10] C. Zhang, J. Jiang, and M. Kamel, "Comparison of BPL and RBF Network in," pp. 466–470, 2003.

[11] A. H. Abdullah, "The trends of Intrusion Prevention System network," no. July, 2010, doi: 10.1109/ICETC.2010.5529697.

[12] D. Stiawan and A. H. Abdullah, "Characterizing Network Intrusion Prevention System," vol. 14, no. 1, pp. 11–18, 2011.

[13] E. M. Rudd, A. Rozsa, M. Günther, and T. E. Boult, "A Survey of Stealth Malware Attacks , Mitigation Measures , and Steps Toward Autonomous Open World Solutions," vol. 19, no. 2, pp. 1145–1172, 2017.

[14] B. Khilosiya, K. Makadiya, and A. Professoe, *Malware Analysis and*

Detection Using Memory, vol. 2, no. 2. .

[15] 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).*, 2016, doi: 10.1016/j.ins.2016.01.033.

[16] N. Farnaaz and M. A. Jabbar, "Random Forest Modeling for Network Intrusion Detection System," *Procedia - Procedia Comput. Sci.*, vol. 89, pp. 213–217, 2016, doi: 10.1016/j.procs.2016.06.047.

[16] Bigsmile, Mr (2016). *Mengenal Teknologi Machine Learning (Pembelajaran Mesin)*. Dikutip 7 Februari 2020: https://www.codepolitan.com/mengenal-teknologi-machine-learning-pembelajaran-mesin

[17] pp_pankaj. *Instrusion Detection System (IDS)*. Dikutip 7 Februari 2020: https://www.geeksforgeeks.org/intrusion-detection-system-ids/

[18] pp_pankaj. *Instrusion Prevention System (IPS)*. Dikutip 7 Februari 2020: https://www.geeksforgeeks.org/intrusion-prevention-system-ips/

[19] mastel.id (2016). *Malware berbahaya serang Indonesia*. Dikutip 5 Oktober 2020 https://mastel.id/malware-berbahaya-serang-indonesia/

[20] Khanzode, Girish. (2015). *Machine Learning Algorithms*. Dikutip 2 mei 2020: https://www.slideshare.net/GirishKhanzode/supervised-learning-52218215