SISTEM KLASIFIKASI ANDROID RANSOMWARE BERBASIS *DEEP NEURAL NETWORK* (DNN)

OLEH:

NURUL AFIFAH

09042611822001

PROGRAM STUDI MAGISTER ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
TAHUN 2019

SISTEM KLASIFIKASI ANDROID RANSOMWARE BERBASIS *DEEP NEURAL NETWORK* (DNN)

TESIS

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Magister

OLEH:

NURUL AFIFAH

09042611822001

PROGRAM STUDI MAGISTER ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
TAHUN 2019

LEMBAR PENGESAHAN

SISTEM KLASIFIKASI ANDROID RANSOMWARE BERBASIS *DEEP NEURAL NETWORK* (DNN)

TESIS

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Magister

OLEH :
NURUL AFIFAH
09042611822001

Palembang, November 2019

Pembimbing 1,

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

Pembimbing 2,

Prof.Dr.Ir.Siti Nurmaini, M.T.
NIP.196908021994012001

Mengetahui,
Ketua Program Studi Magister Ilmu Komputer

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

HALAMAN PERSETUJUAN

Pada hari Jumat tanggal 15 November 2019 telah dilaksanakan ujian sidang tesis oleh Magister Ilmu Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Nurul Afifah

NIM : 09042611822001

Judul : Sistem Klasifikasi Android Ransomware Berbasis Deep Neural Network (DNN)

1. Pembimbing I

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

2. Pembimbing II

   Prof. Dr. Ir. Siti Nurmaini, M.T. .....
   NIP. 196908021994012001

3. Penguji I

   Dian Palupi Rini, M.Kom., Ph.D. .....
   NIP. 197802232006042002

4. Penguji II

   Dr. Yusuf Hartono, M.Sc. .....
   NIP. 196411161990031002

Mengetahui,
Ketua Program Studi Magister Ilmu Komputer

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

LEMBAR PERNYATAAN

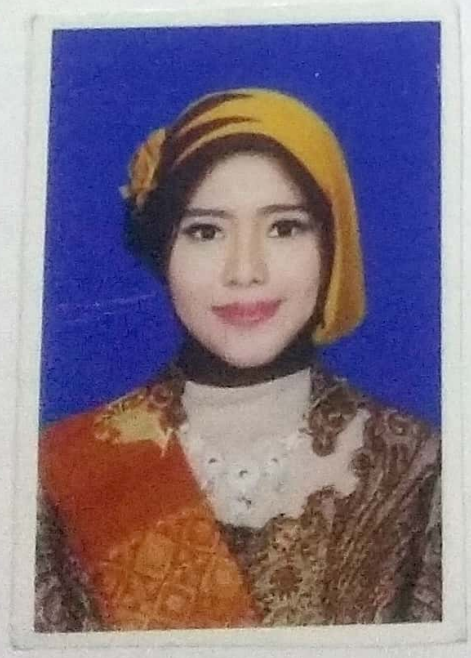
Yang bertanda tangan di bawah ini :

Nama	: Nurul Afifah
NIM	: 09042611822001
Program Studi	: Magister Ilmu Komputer
Judul Tesis	: Sistem Klasifikasi Android Ransomware Berbasis Deep Neural Network (DNN)

Hasil Pengecekan Software iThenticate/Turnitin : **3 %**

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

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.



Palembang, November 2019

METERAI TEMPEL

53D93AHF054860155

6000

ENAM RIBU RUPIAH

(Nurul Afifah)

NIM. 09042611822001

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Allah SWT atas rahmat-nya sehingga penulis dapat menyelesaikan tesis yang berjudul "Sistem Klasifikasi Android Ransomware Berbasis Deep Neural Network (DNN)" di susun untuk memenuhi sebagian persyaratan kelulusan untuk memperoleh gelar Magister Komputer pada Program Studi Magister Ilmu Komputer Universitas Sriwijaya.

Pada kesempatan ini penulis menyadari keterbatasan dan kelemahan yang ada dalam menyelesaikan tesis ini sehingga penulis ingin menyampaikan ucapan terima kasih kepada pihak-pihak yang telah memberikan dukungan, bimbingan dan motivasi kepada penulis untuk menyelesaikan tesis ini, kepada :

1. Bapak Jaidan Jauhari, S.Pd, M.T selaku dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
2. Bapak Dr. Ir. Sukemi, M.T., sebagai Ketua Program Studi Magister Teknik Informatika Universitas Sriwijaya.
3. Bapak Deris Stiawan, M.T., Ph.D dan Prof. Dr. Ir. Siti Nurmaini, M.T selaku pembimbing yang telah meluangkan waktu, bantuan serta saran dan kritiknya dalam penyusunan tesis ini.
4. Terkusus kepada almarhum bapak selaku support system terbesar dalam menyelesaikan s2.
5. Suami tercinta yang selalu mendukung dan terus menyuport dalam penyelesaian s2.
6. Tim COE ajran, ridho yang sudah membantu emak dalam menyelesaikan tesis
7. Seluruh teman-teman Magister Ilmu Komputer yang telah membantu dan memberikan semangat pada masa-masa perkuliahan.

Akhir kata, penulis menyadari bahwa tesis ini masih banyak kekurangan baik dari isi maupun susunan. Semoga tesis ini dapat bermanfaat untuk kita semua.

Palembang, November 2019

Penulis

LEMBAR PERSEMBAHAN

لَا يُكَلِّفُ اللَّهُ نَفْسًا إِلَّا وُسْعَهَا

"Allah tidak membebani seseorang melainkan sesuai dengan kesanggupannya"
(QS. Al-Baqarah: 286)

Kupersembahkan untuk

Almarhum Bapak

Mama

Suamiku dan Anak-Anakku

ANDROID RANSOMWARE CLASSIFICATION SYSTEM BASED ON DEEP NEURAL NETWORK (DNN)

ABSTRACT

Currently there are tons of applications available on the Google Play Store. But some of these applications have been infiltrated by malware files. On Android, each program is contained in apk file, which contains all program code, resources, assets, certificates, and manifest files. Users can download applications from any website and copy the apk file to the device, which further increases the popularity of Android. In open the network still provides many possibilities for the attacker. For example, spread via email and phishing sites. This is the root of the problem if the application that has been infiltrated by the malware file has been installed on the Android user's device, then automatically the file on the Android device can be blocked by malware. The type of malware that is very dangerous and growing rapidly is the type of ransomware. Given their rapid growth, there is an urgent need to develop an effective countermeasure solution by classifying the ransomware using the DNN algorithm and optimizing it by initializing the weights of Xavier and He. The results were significant, with a score of 99.96% for training and testing accuracy, 99.95% for precision, 99.99% for sensitivity, 99.07% for specificity and 99.97% for F1-score. The greater the value obtained from the test results, the better the performance in the testing system.

Keywords: *Ransomware, DNN, Xavier, He, Android*

SISTEM KLASIFIKASI ANDROID RANSOMWARE BERBASIS *DEEP NEURAL NETWORK* (DNN)

ABSTRAK

Saat ini banyak sekali aplikasi yang tersedia di *google play store*, namun tidak menutup kemungkinan beberapa aplikasi tersebut telah disusupi file *malware*. Pada *android*, setiap program terdapat dalam file apk, yang berisi semua kode program, sumber daya, aset, sertifikat, dan file *manifest*. Pengguna dapat mengunduh aplikasi dari situs web apa pun dan menyalin file apk ke perangkat, yang semakin meningkatkan popularitas *android*. Keterbukaan jaringan masih menyediakan banyak kemungkinan bagi penyerang. Misalnya menyebar melalui email dan situs *phishing.* Inilah yang menjadi akar permasalahan jika aplikasi yang telah disusupi file *malware* tersebut sudah diinstal dalam perangkat *android user*, maka otomatis file pada perangkat *android* tersebut bisa di blokir oleh *malware*. Tipe malware yang sangat berbahaya dan berkembang pesat yaitu tipe *ransomware*. Mengingat pertumbuhan mereka yang cepat, ada kebutuhan mendesak untuk mengembangkan solusi penanggulangan yang efektif yaitu dengan mengklasifikasi ransomware menggunakan algoritma DNN dan mengoptimasi dengan inisialisasi bobot Xavier dan He. Hasilnya signifikan yaitu dengan menghasilkan nilai 99.96% untuk akurasi training dan testing, 99.95% untuk presisi, 99.99% untuk sensitivitas, 99.07% untuk spesifisitas dan 99.97% untuk F1-score. Semakin besar nilai yang didapat dari hasil pengujian, semakin bagus performa dalam sistem pengujian.

Kata Kunci: *Ransomware, DNN, Xavier, He, Android*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

DNN	= Deep Neural Network
TP	= True Positif
TN	= True Negatif
FP	= False Positif
FN	= False Negatif
GN	= Girvan Newman
DT	= Decision Tree
SVM	= Support Vector Machine
CNN	= Convolutional Neural Network
DBN	= Deep Belief Network
BACC	= Balanced Accuracy
MCC	= Matthew's Correlation Coefficient

DAFTAR LAMPIRAN

BAB I. PENDAHULUAN

Pendahuluan bab ini menjelaskan tentang latar belakang penelitian yang berjudul: "Sistem Klasifikasi *Android Ransomware* Berbasis *Deep Neural Network*". Permasalahan *malware ransomware* dipilih menjadi topik dikarenakan jenis serangan ini yang paling berbahaya jika sudah menyerang perangkat dan mengakibatkan perangkat tersebut tidak bisa dibuka dan *hacker* meminta tebusan jika ingin membuka akses file tersebut Chen dkk. (2018). Pengimplementasian *Deep Learning* sebagai algoritma klasifikasi agar fitur dipelajari secara otomatis. *Deep Neural Network* (DNN) adalah algoritma yang digunakan dalam penelitian ini dikarenakan karakter data yang bersifat vektor tabular.

1.1 Latar Belakang

Malware merupakan file berbahaya yang dapat menyusup ke sistem operasi sehingga dapat merusak sistem dan juga dapat mencuri file penting pada sistem. Pada publikasi Idika dan Mathur (2007) *malware* mencakup virus komputer, *trojan horse*, *ransomware* dan perangkat lunak lainnya yang berniat jahat dan tidak diinginkan. Seiring berkembangnya teknologi pun memiscu dikembangkannya *malware* baru, sehingga semakin banyak pihak yang dirugikan karena adanya *malware* ini. Bahkan saat ini, *malware* telah menjangkit hampir seluruh jenis sistem operasi salah satunya sistem operasi *android*. Sistem *android* memiliki kelebihan dibanding sistem operasi lain yakni bersifat *open access*, Akan tetapi, salah satu keunggulan sistem *android* menjadi salah satu kelemahannya. Bersifat *open access*, dimana *user* dapat menciptakan dan mengembangkan aplikasi sendiri sehingga dapat digunakan pada bermacam perangkat seluler. Hal ini malah menimbulkan kemudahan pada pihak yang tidak bertanggung jawab untuk membangun dan mengembangkan *malware* menjadi aplikasi yang dapat masuk ke system Arp dkk. (2014).

Saat ini banyak sekali aplikasi yang tersedia di *google play store*, namun tidak menutup kemungkinan beberapa aplikasi tersebut telah disusupi file *malware*. Pada *android*, setiap program terdapat dalam file apk, yang berisi semua kode program, sumber daya, aset, sertifikat, dan file *manifest*.

Pengguna dapat mengunduh aplikasi dari situs web apa pun dan menyalin file apk ke perangkat, yang semakin meningkatkan popularitas *android*. Sayangnya, popularitas seperti itu juga menarik perhatian peneliti *malware*. Bahkan jika pasar resmi dan pihak ketiga menyebarkan skema keamanan untuk mencegah penyebaran *malware*, keterbukaan jaringan masih menyediakan banyak kemungkinan bagi penyerang. Misalnya menyebar melalui email dan situs *phishing* Arp dkk. (2014). Inilah yang menjadi akar permasalahan jika aplikasi yang telah disusupi file *malware* tersebut sudah diinstal dalam perangkat *android user*, maka otomatis file pada perangkat *android* tersebut bisa di blokir oleh *malware*. Didalam publikasi Chen dkk. (2018) ditemukan *malware* yang dapat memblokir data pada perangkat *android* yaitu *malware* tipe *ransomware*.

Tingkat infeksi paling banyak oleh *ransomware android* adalah di Eropa Timur dan Rusia hingga 59%, diikuti oleh Inggris dan AS (25%), dan kemudian Cina (16%). Mengingat pertumbuhan mereka yang cepat, ada kebutuhan mendesak untuk mengembangkan solusi penanggulangan yang efektif Chen dkk. (2018)

Algoritma konvensional telah diusulkan untuk mengklasifikasi *malware* yaitu Algoritma *Girvan-Newman* (GN). Algoritma tersebut melatih klasifikasi biner. Metode *machine learning* seperti yang dilakukan oleh Lashkari dkk. (2018) menyatakan bahwa dengan menggunakan metode *Decision Tree* (DT) dapat menghasilkan *Precision* 85% dan *Recall* 88% dalam mengklasifikasi jenis *malware*. Penelitian Dan Lo dkk. (2016) menghasilkan akurasi 99,60%. Penelitian Yerima dan Sezer (2019) menghasilkan tingkat sensitivitas sebesar 95,80% dalam mengklasifikasi *malware*. Metode *machine learning* seperti yang dilakukan oleh Lashkari dkk. (2018), Dan Lo dkk. (2016), Yerima dan Sezer (2019) menggunakan metode SVM, *Decision tree* dan *Random forest*. Metode *machine learning* tersebut masih mempelajari fitur secara manual (ekstraksi fitur) sehingga muncul paradigma *deep learning*. Contoh penerapan teknik *deep learning* dalam permasalahan *malware* antara lain *Deep Neural Network* (DNN), *Convolutional Neural Network*

(CNN) dan *Deep Belief Network* (DBN). Metode yang diusulkan dalam penyelesaian tesis ini adalah DNN. Hal ini dikarenakan karakteristik dari dataset *malware* tersebut yang bersifat matriks vector tabulasi dan *cross section* sangat cocok jika diimplementasikan menggunakan metode DNN (Zhou, 2018). DNN mampu menghasilkan kinerja yang lebih baik dan lebih unggul dalam hal klasifikasi dengan cara mempelajari fitur secara otomatis. Teknik dalam pembelajaran fitur otomatis yaitu *autoencoder* tercantum dalam penelitian Naway dan Li (2019) dan Le dkk. (2018). *Autoencoder* merupakan model pembelajaran fitur otomatis dalam DNN yang mampu melakukan *dimensionality reduction* terhadap data tanpa mengurangi informasi yang ada dalam dataset tersebut Kunang dkk. (2019). Namun implementasi DNN pada kasus klasifikasi *malware* pada penelitian Cui dkk. (2018) memiliki kelemahan yaitu pada saat *training* data terjadi ketidakstabilan nilai *gradien*. Ketidakstabilan nilai *gradien* dapat mempengaruhi tingkat *konvergen* dan waktu dalam *training* data. Itu dapat ditanggulangi dengan menerapkan teknik inisialisasi bobot dari penelitian Kwon dkk. (2019) dan He dkk. (2015). Penelitian ini dianggap sangat berguna agar dapat mengklasifikasi *android ransomware* dengan hasil klasifikasi yang lebih *konvergen* antara data *training* dan *testing*.

1.2 Perumusan Masalah

DNN merupakan algoritma yang memiliki performa sangat baik untuk klasifikasi malware pada penelitian Afifah dkk. (2019) karena dapat menyelesaikan permasalahan klasifikasi *malware.* DNN menginisialisasi bobot secara acak dalam proses klasifikasi. Apabila nilai bobot awal terlalu kecil maka *input* ke setiap lapisan *hidden layer* dan *output* akan sangat kecil yang dapat menyebabkan terjadinya *vanishing gradient*. Jika bobot awal terlalu besar maka terjadi *exploding gradient* seperti pada pada penelitian Karbab dkk. (2018) yang memicu nilai *loss* menjadi naik turun pada proses pelatihan data sehingga menjadi tidak konvergen berdasarkan penelitian Kwon dkk. (2019). Berdasarkan latar belakang diatas, terdapat beberapa masalah yang dirumuskan dalam penelitian ini yaitu:

1. Bagaimana cara mengatasi ketidakstabilan nilai *gradien* dalam proses klasifikasi DNN?
2. Bagaimana cara menerapkan inisialisasi bobot *Xavier* dan *He*?

3. Bagaimana pengaruh inisialisasi bobot terhadap nilai akurasi, sensitivitas, spesifisitas, presisi dan *F1 score* terhadap kinerja dari sistem klasifikasi *android ransomware* menggunakan DNN?

1.3 Batasan Masalah

Terdapat beberapa batasan masalah yang dirancang dalam tesis ini yaitu:

1. Data yang digunakan merupakan dataset dari *Drebin Project* Arp dkk. (2014).
2. Analisis *malware ransomware* dan *benign* menggunakan *static analysis* Arp dkk. (2014) Naway dan Li (2018)
3. Proses *dimentionality reduction* yang digunakan adalah *Autoencoder*
4. Inisialisasi bobot menggunakan Persamaan *Xavier* dan *He*.

1.4 Tujuan

Tujuan dalam penelitian tesis ini adalah sebagai berikut :

1. Mengetahui teknik inisialisasi bobot terbaik yang dapat menyelesaikan permasalahan ketidakstabilan *gradien*
2. Menerapkan teknik inisialisasi bobot *Xavier* dan *He* sehingga didapat grafik yang konvergen dari nilai akurasi dan *loss* dari proses *training* data
3. Mengukur akurasi, sensitivitas, spesifisitas, presisi dan *F1 score* terhadap kinerja pengklasifikasi DNN

1.5 Manfaat

Hasil dari penelitian ini dapat menjadi landasan dalam pengembangan sistem klasifikasi *android ransomware* secara lebih lanjut. Selain itu manfaat dari penelitian ini secara praktis yaitu sebagai berikut:

1. Inisialisasi bobot menggunakan persamaan *Xavier* dan *He* berhasil membuat hasil dari proses *training* data menjadi konvergen
2. Hasil dari penelitian ini dapat menjadi referensi untuk meningkatkan nilai performa akurasi, sensitivitas, spesifisitas, presisi dan *F1 score* dalam sistem klasifikasi yang menerapkan metode DNN

1.6 Metodologi Penulisan

Agar memperoleh gambaran jelas mengenai penelitian ini, maka dibuatlah suatu sistematika penulisan yang berisi gambaran dalam tiap bab penelitian ini, yaitu:

1. **BAB I** **Pendahuluan**

   Bab ini menjelaskan tentang latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat dari topik yang dipilih berupa sistem klasifikasi data file normal dan serangan *malware ransomware* menggunakan metode DNN.

2. **BAB II** **Tinjauan Pustaka**

   Bab ini menjelaskan mengenai *literature review* yang berhubungan dengan masalah *malware* dengan metode DNN yang mengacu pada beberapa penelitian publikasi.

3. **BAB III** **Metodologi Penelitian**

   Bab ini menjelaskan pembahasan secara bertahap dan rinci langkah yang digunakan untuk mengumpulkan dan menganalisa jenis file normal dan jenis file *malware*. Metodologi ini menjelaskan pendekatan algoritma DNN serta model yang digunakan sehingga tujuan dari penulisan tercapai.

4. **BAB IV** **Analisa dan Pembahasan**

   Bab ini berisi hasil pengujian yang dilakukan, data yang diuji akan dianalisa menggunakan berbagai macam teknik serta validasi hasil.

5. **BAB V** **Kesimpulan**

   Bab ini menjelaskan kesimpulan dari hasil yang diperoleh, serta merupakan jawaban yang diperoleh dari tujuan yang ingin dicapai.

DAFTAR PUSTAKA

Afifah, N., Stiawan, D., & Nurmaini, S. (2019). The Implementation of Deep Neural Networks Algorithm for Malware Classification. *Computer Engineering Applications Journal8*(3), 189–202.

Arp, D., Spreitzenbarth, M., Malte, H., Gascon, H., & Rieck, K. (2013). DREBIN: Effective and Explainable Detection of Android Malware in Your Pocket Daniel. *Choice Reviews Online*, *45*(02), 45-0765-45–0765. https://doi.org/10.5860/choice.45-0765

Brodersen, K. H., Soon Ong, C., Stephan, K. E., & Buhmann, J. M. (2010). *The balanced accuracy and its posterior distribution*. https://doi.org/10.1109/ICPR.2010.764

Chen, J., Wang, C., Zhao, Z., Chen, K., Du, R., & Ahn, G. J. (2018). Uncovering the Face of Android Ransomware: Characterization and Real-Time Detection. *IEEE Transactions on Information Forensics and Security*, *13*(5), 1286–1300. https://doi.org/10.1109/TIFS.2017.2787905

Cui, Z., Xue, F., Cai, X., Cao, Y., Wang, G., Chen, J., & Member, S. (2018). *Detection of Malicious Code Variants Based on Deep Learning*. https://doi.org/10.1109/TII.2018.2822680

Dan Lo, C. T., Ordóñez, P., & Cepeda, C. (2016). Feature selection and improving classification performance for malware detection. *Proceedings - 2016 IEEE International Conferences on Big Data and Cloud Computing, BDCloud 2016, Social Computing and Networking, SocialCom 2016 and Sustainable Computing and Communications, SustainCom 2016*, 560–566. https://doi.org/10.1109/BDCloud-SocialCom-SustainCom.2016.87

He, K., Zhang, X., Ren, S., & Sun, J. (2015). Delving deep into rectifiers: Surpassing human-level performance on imagenet classification. *Proceedings of the IEEE International Conference on Computer Vision*, *2015 Inter*, 1026–1034. https://doi.org/10.1109/ICCV.2015.123

Idika, N., & Mathur, A. P. (2007). *A Survey of Malware Detection Techniques*. *initialization weight malware*. (n.d.).

Kelimeler, A. (n.d.). *Zararlı Mobil Uygulamaların Derin Yapay Sinir A ˘ gı ile Tespit Edilmesi Mobile Malware Detection Using Deep Neural Network*.

Kunang, Y. N., Nurmaini, S., Stiawan, D., Zarkasi, A., & Jasmir, F. (2019). Automatic Features Extraction Using Autoencoder in Intrusion Detection System. *Proceedings of 2018 International Conference on Electrical Engineering and Computer Science, ICECOS 2018*, (June 2019), 219–224. https://doi.org/10.1109/ICECOS.2018.8605181

Lashkari, A. H., Kadir, A. F. A., Taheri, L., & Ghorbani, A. A. (2018). Toward Developing a Systematic Approach to Generate Benchmark Android Malware Datasets and Classification. *Proceedings - International Carnahan Conference on Security Technology*, *2018-Octob*(Cic), 1–7. https://doi.org/10.1109/CCST.2018.8585560

Le, Q., Boydell, O., Namee, B. Mac, & Scanlon, M. (2018). Deep learning at the shallow end: Malware classification for non-domain experts. *Digital Investigation*, *26*, S118–S126. https://doi.org/10.1016/j.diin.2018.04.024

Lecun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, *521*(7553), 436–444. https://doi.org/10.1038/nature14539

Luque, A., Carrasco, A., Martín, A., & De Las Heras, A. (2019). The impact of class imbalance in classification performance metrics based on the binary confusion matrix. *Pattern Recognition*, *91*, 216–231. https://doi.org/10.1016/j.patcog.2019.02.023

MacLennan, B. J. (2016). Field computation: A framework for quantum-inspired computing. In *Quantum Inspired Computational Intelligence: Research and Applications*. https://doi.org/10.1016/B978-0-12-804409-4.00003-6

Naway, A., & Li, Y. (2018). International Journal of Computer Science and Mobile Computing A Review on The Use of Deep Learning in Android Malware Detection. In *International Journal of Computer Science and Mobile Computing* (Vol. 7).

Naway, A., & Li, Y. (2019). *Android Malware Detection Using Autoencoder*. 1–9. Retrieved from http://arxiv.org/abs/1901.07315

Nix, R., & Zhang, J. (n.d.). *Classification of Android Apps and Malware Using Deep Neural Networks*.

Nurmaini, S., Umi P, R., Naufal, M., & Gani, A. (2018). Cardiac Arrhythmias Classification Using Deep Neural Networks and Principle Component Analysis Algorithm. In *Int. J. Advance Soft Compu. Appl* (Vol. 10).

Nwankpa, C., Ijomah, W., Gachagan, A., & Marshall, S. (2018). *Activation Functions: Comparison of trends in Practice and Research for Deep Learning*. 1–20. Retrieved from http://arxiv.org/abs/1811.03378

Xavier Glorot, Y. B. (1993). Initializing weights to a hidden layer of a multilayer neural network by linear programming. *Proceedings of the International Joint Conference on Neural Networks*, *2*, 1701–1704.

Yerima, S. Y., & Sezer, S. (2019). DroidFusion: A Novel Multilevel Classifier Fusion Approach for Android Malware Detection. *IEEE Transactions on Cybernetics*, *49*(2), 453–466. https://doi.org/10.1109/TCYB.2017.2777960Y

Zhou, B. (2018). Deep Learning and the Cross-Section of Stock Returns: Neural Networks Combining Price and Fundamental Information. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3179281