Klasifikasi *Malware Banking* Pada Android Menggunakan Algoritma *Random Forest*

OLEH:

AHMAD AJI GUNTUR SAPUTRA

09011181621004

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2021

Klasifikasi *Malware Banking* Pada Android Menggunakan Algoritma *Random Forest*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer (S1)

OLEH:

AHMAD AJI GUNTUR SAPUTRA

09011181621004

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2021

LEMBAR PENGESAHAN

KLASIFIKASI *MALWARE BANKING* PADA ANDROID MENGGUNAKAN ALGORITMA *RANDOM FOREST*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

AHMAD AJI GUNTUR SAPUTRA

09011181621004

Indralaya, Mei 2021

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

Mengetahui,
Ketua Jurusan Sistem Komputer

Dr.Ir.Sukemi, MT
NIP. 196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Kamis

Tanggal : 01 April 2021

Tim Penguji:

1. **Ketua** : **Sarmayanta Sembiring, S.SI., M.T.** (.....)
2. **Sekretaris Sidang** : **Rendyansyah, S.Kom., M.T.** (.....)
3. **Penguji Sidang** : **Huda Ubaya, S.T., M.T.** (.....)

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, MT

NIP. 196612032006041001

HALAMAN PERSEMBAHAN

Kutipan:

"Desire Becomes Surrender and Surrender Becomes Power"

(Joker – Suicide Squad)

"Fortis Fortuna Adiuvat"

(John Wick – John Wick)

"Aut Libertatem Aut Mortem Mihi Da"

(Patrick Henry – American Revolutionary War On March 23, 1775)

Tugas Akhir ini kupesembahkan untuk:

- ***ALLAH SWT***
- ***Nabi Muhammad SAW***
- ***Kedua orang tua yang senantiasa mendoakan, memberi semangat, dan dukungan baik secara moral maupun material.***
- ***Saudaraku dan Keluarga besar yang telah mendoakan dan membantu urusan selama proses perkuliahan.***
- ***Kekasihku yang senantiasa menyemangati dan membantu segala urusan selama proses perkuliahan.***
- ***Rekan – rekan seperjuangan di jurusan Sistem Komputer 2016.***
- ***Jurusan Sistem Komputer.***
- ***Almamater Universitas Sriwijaya.***

KATA PENGANTAR

Segala puji bagi Allah SWT yang telah memberikan rahmat dan karuniaNya kepada penulis, sehingga penulis dapat menyelesaikan penyusunan tugas akhir dengan judul "Klasifikasi *Malware Banking* Pada Android Menggunakan Algoritma *Random Forest (RF)*". Shalawat dan salam senantiasa tercurah kepada Rasulullah SAW yang mengantarkan manusia dari zaman kegelapan ke zaman yang terang benderang ini. Penyusunan tugas akhir ini dimaksudkan untuk memenuhi sebagian syarat-syarat guna mencapai gelar Sarjana Sistem Komputer di Universitas Sriwijaya.

Dalam tugas akhir ini penulis menjelaskan mengenai teknik Klasifikasi *Malware Banking* Pada Android Menggunakan Algoritma *Random Forest (RF)*. Penulis berharap tulisan ini dapat bermanfaat bagi orang banyak, dan menjadi tambahan bahan bacaan bagi yang tertarik meneliti tentang keamanan jaringan komputer.

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

1. Tuhan Yang Maha Esa, yang telah memberikan rahmat dan karunia-Nya sehingga pelaksanaan kerja praktek dan penulisan laporan kerja praktek ini dapat berjalan dengan lancar.
2. Kedua orang tua beserta keluarga yang selalu mendoakan serta memberikan motivasi, dukungan, dan semangat.
3. Bapak Jaidan Jauhari, S.Pd. M.T selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya
4. Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Kompuer Fakutas Ilmu Komputer Universitas Sriwijaya
5. Bapak Deris Stiawan, Ph. D selaku Pembimbing Tugas Akhir Penulis.
6. Bapak Ahmad Heryanto, S.kom.,M.T selaku Pembimbing Tugas Akhir.
7. Bapak Rossi Passarella, S.T.,M.Eng selaku Pembimbing Akademik.
8. Mbak Nurul Afifah, S.Kom, M.Kom yang telah membantu saya dalam menyelesaikan Tugas Akhir.

9. Kekasihku Yulia Respita, S.Pd. yang telah menemani selama proses perkuliahan baik disaat susah maupun senang.
10. Seluruh teman-teman Jurusan Sistem Komputer khusunya kelas A angkatan 2016 yang tidak dapat saya sebutkan satu persatu.
11. Dan semua pihak yang telah membantu dalam pembuatan laporan tugas akhir ini

Penulis menyadari bahwa laporan ini masih jauh dari kesempurnaan, oleh karena itu penulis sangat mengharapkan kritik dan saran yang bersifat membangun agar lebih baik lagi dikemudian hari.

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.

Indralaya, Mei 2021

AHMAD AJI GUNTUR SAPUTRA
09011181621004

KLASIFIKASI *MALWARE BANKING* PADA ANDROID MENGGUNAKAN ALGORITMA *RANDOM FOREST*

Ahmad Aji Guntur Saputra (09011181621004)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : ahmadajiguntursaputra@gmail.com

ABSTRAK

Smartphone android sangat marak digunakan untuk transaksi perbankan. Dengan demikian hal tersebut dapat beresiko terjadinya serangan *malware*. Klasifikasi *malware* merupakan sebuah metode yang berfungsi untuk mengenali dan membedakan jenis data yang digolongkan sebagai *malware* atau normal. *Banking Malware* adalah malware khusus yang dirancang untuk mendapatkan akses ke akun perbankan online pengguna dengan meniru aplikasi perbankan atau antarmuka web perbankan asli. Penelitian ini bertujuan untuk mendapatkan tingkat akurasi terbaik pada klasifikasi *Banking Malware* menggunakan algoritma *random forest* dengan dataset yang berasal dari *Universitas of New Brunswick* yaitu CICMALDROID2020. Fitur ekstraksi yang digunakkan adalah tools *CICFlowMeters* untuk memproses dataset dari file PCAP menjadi file CSV. Pada Penelitian ini juga menggunakan fitur seleksi *boruta* yang berfungsi untuk memilih fitur terbaik pada dataset. Hasil klasifikasi menggunakan algoritma *random forest* dievaluasi menggunakan *confusion matrix*. Akurasi tertinggi yang didapat pada penelitian ini sebesar 92.5%, dengan nilai presisi sebesar 93.28% dan recall sebesar 93.73%.

Kata Kunci : Klasifikasi , *Banking Malware* , *CICFlowMeters*, *Boruta*, *Random Forest*

CLASSIFICATION OF MALWARE BANKING ON ANDROID USING RANDOM FOREST ALGORITHM

Ahmad Aji Guntur Saputra (09011181621004)

Department of Computer Engineering, Faculty of Computer Science

Sriwijaya University

Email : ahmadajiguntursaputra@gmail.com

ABSTRACT

Android smartphones is widely used for banking transactions. Thus, it can be at risk of malware attacks. Malware classification is a method that serves to identify and distinguish types of data classified as malware or normal. Banking Malware is malware designed to gain access to user's online banking accounts by impersonating a real banking application or web banking interface. This study aims to obtain the best level of accuracy in the classification of Banking Malware using the random forest algorithm with a dataset originating from the University of New Brunswick, namely CICMALDROID2020. The extraction feature used is the CICFlowMeters tool to process a dataset from a PCAP file into a CSV file. This research also use feature selection boruta which functions to select the best features in the dataset. The classification results using the random forest algorithm are evaluated using a confusion matrix. The highest accuracy obtained in this study was 92.5%, with a precision value of 93.28% and a recall of 93.73%.

Keywords : *Classification*, *Banking Malware*, *CICFlowMeters*, *Boruta*, *Random Forest*

BAB I
PENDAHULUAN

1.1 Latar Belakang

Banking Malware adalah malware khusus yang dirancang untuk mendapatkan akses ke akun perbankan online pengguna dengan meniru aplikasi perbankan atau antarmuka web perbankan asli. Sebagian besar malware Mobile Banking berbasis Trojan, yang dirancang untuk menginfiltrasi perangkat, untuk mencuri detail sensitif, seperti login bank dan kata sandi, dan untuk mengirim informasi yang dicuri ke server perintah dan kontrol [1]. Malware perbankan, telah menjadi populer dan semakin banyak mekanisme umum untuk memonetisasi pengembangan malware. Sejak pengembangan kit malware Zeus pada tahun 2007, file frekuensi dan kompleksitas malware perbankan telah meningkat [2]. Malware saat ini semakin sulit untuk dideteksi perangkat lunak anti-virus tradisional karena terlalu banyak variasi konten biner. Langkah logisnya adalah bergerak menuju dinamika deteksi, tempat kami dapat memutuskan apakah sampel dari sumber berbahaya perilakunya, bukan bentuk dan isinya yang mudah disamarkan. Masalahnya adalah untuk mengamati tindakan berbahaya, sampel harus dijalankan dan berpotensi menyebabkan kerugian yang tidak dapat diperbaiki bagi pengguna [3].

Random Forest merupakan tata cara pembelajaran essemble buat klasifikasi serta regresi yang beroperasi dengan membangun banyak tumbuhan keputusan serta menciptakan kelas yang ialah modus kelas (klasifikasi) ataupun prediksi rata-rata (regresi) dari tiap- tiap tumbuhan. Pada proses klasifikasi dicoba bersumber pada majority vote (suara paling banyak) buat mengambil keputusan serta akurasi yang optimal [4]. Saat sebelum melaksanakan proses klasifikasi, dicoba proses ekstraksi terhadap dataset buat menciptakan kode-kode malicious yang setelah itu digunakan buat proses klasifikasi malware. Proses ekstraksi tersebut memakai feature extraction. Salah satu fitur ekstrasi ialah *CICFlowmeter*, *CICFlowmeter* merupakan tool yang untuk mengekstraksi

fitur-fitur yang dibutuhkan dalam melakukan proses klasifikasi ML dari file berformat *packet capture* (PCAP) menjadi *comma-separated values* (CSV) [5].

Pada penelitian [6], membahas tentang *android malware* dengan dataset yang diolah adalah dataset CICAndroid2017 yang mana dataset tersebut adalah dataset versi lawas dari dataset CICMALDROID2020, Fitur ekstraksi yang digunakan untuk mengekstrak datasetnya adalah *CICFlowmeter*. Lalu pada penelitian tersebut juga didapat hasil klasifikasi menggunakan *Random Forest* dengan hasil akurasi hanya 86.65% pada hasil percobaan pertama dan 79.91% pada hasil percobaan kedua.

Pada penelitian [7], membahas tentang evaluasi performa fitur seleksi untuk meningkatkan akurasi dari metode *Random Forest* dan didapatkan hasil bahwa fitur seleksi terbaik untuk meningkatkan tingkat akurasi dari metode *Random Forest* adalah *feature selection Boruta*.

Pada penelitian [8], membahas mengenai *trickbot banking* dengan menggunakan algoritma *Random Forest*. Data yang digunakan berupa pcap yang terlebih dahulu diekstrasi sebelumnya. Hasil yang didapat dari penelitian ini mencapai akurasi klasifikasi 99,9534% dengan tingkat positif sejati malware 91,7%. Pada penelitian [9], juga dijelaskan bahwa penelitian tersebut membahas tentang klasifikasi android malware dengan menggunakan metode Decision tree, Random forest, Gradient boosting, dan Ext. randomized serta mendapatkan hasil bahwa Random forest merupakan metode terbaik dengan tingkat akurasi sebesar 97.24%, dengan demikian bisa disimpulkan bahwa Algoritma *Random Forest* memiliki tingkat akurasi yang bagus untuk mengolah dataset tipe android malware.

Pada penelitian [1], didapatkan hasil bahwa semakin banyak jumlah dataset yang digunakan maka akan semakin besar akurasi yang akan didapatkan namun pada penelitian tersebut tidak dibahas apakah semakin banyak fitur pada dataset yang digunakan akan mempengaruhi tingkat akurasi klasifikasi.

Dari beberapa ulasan diatas, penulis akan membahas mengenai pengklasifikasian terhadap data *banking malware* yang merupakan salah satu jenis serangan *malware* pada *android* dengan menggunakan Algoritma *Random Forest.*

Pada dataset terdapat fitur data normal dan malware yang telah digabungkan dan akan di seleksi menggunakan *Boruta* untuk mendapatkan tingkat akurasi yang tinggi dan membuktikan apakah semakin banyak fitur yang digunakan akan memperbesar akurasi atau tidak.

1.2 Batasan dan Perumusan Masalah

Adapun ruang lingkup dan perumusan masalah dalam penulisan Proposal Tugas Akhir ini adalah sebagai berikut:

1.2.1 Batasan Masalah

Berikut merupakan batasan masalah dalam penulisan Proposal Tugas Akhir ini:

1. Dataset yang digunakan pada penelitian ini merupakan dataset yang berasal dari *University of New Brunswick* dengan nama dataset CICMALDROID2020.
2. *Feature selection* yang digunakan adalah *Boruta*.
3. Metode yang digunakan untuk Mengklasifikasikan serangan yang disebabkan oleh *Banking Malware* adalah *Random Forest (RF).*
4. Analisa *Banking Malware* dilakukan secara *statis*.
5. Dalam penelitian ini tidak membahas mengenai bagaimana cara mencegah *Banking Malware*.

1.2.2 Perumusan Masalah

Berikut adalah rumusan masalah dalam penulisan Proposal Tugas Akhir ini:

1. Bagaimana proses dalam ekstraksi dataset yang kemudian digunakan dalam proses klasifikasi malware?
2. Bagaimana cara menerapkan algoritma *feature selection Boruta* pada proses klasifikasi *malware banking*?
3. Bagaimana algoritma *Random Forest* dapat melakukan klasifikasi malware sehingga ditemukan tingkat akurasi terbaik?
4. Bagaimana cara menvalidasi hasil dari klasifikasi *malware banking* menggunakan algoritma *Random Forest*?

1.3 Tujuan

Tujuan dari penulisan Proposal Tugas Akhir ini adalah sebagai berikut :

1. Melakukan ekstraksi *Dataset CICMALDROID2020* dengan menggunakan feature ekstraksi *CICFlowmeter*.
2. Menerapkan algoritma *feature selection Boruta* untuk meningkatkan hasil klasifikasi.
3. Melakukan klasifikasi malware menggunakan algoritma *Random Forest.*
4. Melakukan validasi terhadap hasil klasifikasi *malware banking* menggunakan algoritma *Random Forest*.

1.4 Manfaat

Adapun manfaat dari penulisan Proposal Tugas Akhir ini adalah sebagai berikut :

1. Dapat mengekstrak paket data serangan *banking malware* dan paket data normal pada *Dataset CICMALDROID2020* menggunakan *feature extraction CICFlowmeter*.
2. Dapat menerapkan algoritma *feature selection Boruta* untuk meningkatkan hasil klasifikasi.
3. Dapat mempelajari proses dalam klasifikasi dan mengetahui tingkat akurasi dari Algoritma *Random Forest* untuk mengklasifikasikan *banking malware.*
4. Dapat mempelajari hasil validasi terhadap hasil klasifikasi *banking malware* menggunakan algoritma *Random Forest.*

1.5 Metodologi Penelitian

Metodologi yang digunakan dalam penyusunan tugas akhir ini hendak melewati tahapan sebagai berikut :

1. Studi Pustaka/*literature*

   Pada tahapan awal dicoba sesudah permasalahan yang hendak dibahas sudah cocok serta relevan buat dijadikan selaku acuan riset, dengan

metode mambaca postingan ataupun makalah riset yang berhubungan langsung dengan tugas akhir.

2. Perancangan Sistem

   Tahapan kedua, yaitu tahap bagaimana menyusun metode dan menerapkannya pada sistem tugas akhir. Selain itu, apa yang digunakan dalam penelitian seperti perangkat keras dan perangkat lunak, kemudian bagaimana cara mengkonfigurasi metode pada tugas akhir atau menulis kode untuk penerapan metode tersebut.

3. Pengujian

   Tahapan ketiga merupakan tahap pengujian metode penelitian dan penelitian sebelumnya guna mendapatkan data hasil pengujian yang sesuai / searah dengan algoritma yang digunakan.

4. Analisa

   Tahap keempat adalah proses menganalisis data hasil pengujian dengan menerapkan metode tertentu, sehingga diperoleh hasil yang obyektif dimana data tersebut diperoleh dari proses pengujian.

5. Kesimpulan dan Saran

   Tahap kelima dilakukan melalui kesimpulan yang diambil dari analisis dan penelitian pustaka serta saran bagi calon penulis (jika digunakan sebagai bahan referensi). Dan menarik kesimpulan dari hasil penelitian.

1.6 Sistematika Penulisan

Sistematika penulisan dalam pengerjaan Proposal Tugas Akhir ini yaitu sebagai berikut:

BAB I. PENDAHULUAN

Pada Bab ini memiliki isi penjelasan secara sistematis tentang landasan topik penelitian meliputi Latar Belakang, Tujuan, Manfaat, Ruang Lingkup masalah, Perumusan masalah, Batasan masalah, kemudian Metodologi Penelitian, dan terakhir mengenai Sistematika Penulisan.

BAB II. TINJAUAN PUSTAKA

Pada Bab II akan berisi dasar teori terkait mengenai *Malware*, *Taksonomi malware, Malware analysis* , *Banking Malware*, *Feature Extraction CICFlowmeter*, *Feature Selection Boruta* dan algoritma *Random Forest (RF).*

BAB III. METODOLOGI PENELITIAN

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

BAB IV. HASIL DAN ANALISA SEMENTARA

Pada Bab IV membahas hasil pengujian serta analisa pengklasifikasian dari serangan *Malware Banking.*

BAB V. KESIMPULAN DAN SARAN

Pada bab V berisi kesimpulan dari bab-bab yang sudah dicantumkan mengenai hasil dari implementasi algoritma *Random Forest (RF)* untuk mengklasifikasi serangan *Malware Banking*. Pada bab ini juga akan berisi saran yang diharapkan dapat digunakan sebagai rujukan untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] S. Mahdavifar, A. F. Abdul Kadir, R. Fatemi, D. Alhadidi, and A. A. Ghorbani, "Dynamic Android Malware Category Classification using Semi-Supervised Deep Learning," *Proc. - IEEE 18th Int. Conf. Dependable, Auton. Secur. Comput. IEEE 18th Int. Conf. Pervasive Intell. Comput. IEEE 6th Int. Conf. Cloud Big Data Comput. IEEE 5th Cybe*, pp. 515–522, 2020.

[2] P. Black and J. Opacki, "Anti-analysis trends in banking malware," *2016 11th Int. Conf. Malicious Unwanted Software, MALWARE 2016*, pp. 129–135, 2017.

[3] G. Cab, "Malware Classification Based on Dynamic Behavior."

[4] L. Breiman, "No Title," pp. 1–33, 2001.

[5] I. Ramadhan, P. Sukarno, and M. A. Nugroho, "Analisis Perbandingan Algoritma K-Nearest Neighbor dan Decision Tree Dalam Mendeteksi Distributed Denial of Service," vol. 6, no. 2, pp. 8548–8558, 2019.

[6] M. K. A. Abuthawabeh and K. W. Mahmoud, "Android malware detection and categorization based on conversation-level network traffic features," *Proc. - 2019 Int. Arab Conf. Inf. Technol. ACIT 2019*, pp. 42–47, 2019.

[7] S. S. Kumar and T. Shaikh, "Empirical Evaluation of the Performance of Feature Selection Approaches on Random Forest," *2017 Int. Conf. Comput. Appl. ICCA 2017*, pp. 227–231, 2017.

[8] 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.

[9] M. S. Rana, S. S. M. M. Rahman, and A. H. Sung, *Evaluation of tree based machine learning classifiers for android malware detection*, vol. 11056 LNAI, no. January. Springer International Publishing, 2018.

[10] A. Qamar, A. Karim, and V. Chang, "Mobile malware attacks : Review , taxonomy & future directions," *Futur. Gener. Comput. Syst.*, vol. 97, pp. 887–909, 2019.

[11] R. Adenansi and L. A. Novarina, "Malware dynamic," *J. Educ. Inf. Commun. Technol.*, vol. 1, no. 1, pp. 37–43, 2017.

[12] M. Ijaz, M. H. Durad, and M. Ismail, "Static and Dynamic Malware Analysis Using Machine Learning," no. January, 2019.

[13] D. Uppal, V. Mehra, and V. Verma, "Basic survey on Malware Analysis, Tools and Techniques," *Int. J. Comput. Sci. Appl.*, vol. 4, no. 1, pp. 103–112, 2014.

[14] E. Gandotra, D. Bansal, and S. Sofat, "Malware Analysis and Classification : A Survey," no. April, pp. 56–64, 2014.

[15] P. Black, I. Gondal, and R. Layton, "A Survey of Similarities in Banking Malware Behaviours," *Comput. Secur.*, 2017.

[16] G. Iadarola, F. Martinelli, F. Mercaldo, and A. Santone, "Formal Methods for Android Banking Malware Analysis and Detection," *2019 Sixth Int. Conf. Internet Things Syst. Manag. Secur.*, pp. 331–336, 2019.

[17] H. Ham, "Analysis of Android Malware Detection Performance using Machine Learning Classifiers," pp. 490–495, 2013.

[18] Y. Shyong, T. Jeng, and Y. Chen, "Combining Static Permissions and Dynamic Packet Analysis to Improve Android Malware Detection," pp. 75–81, 2020.

[19] A. Roihan, P. A. Sunarya, and A. S. Rafika, "Pemanfaatan Machine Learning dalam Berbagai Bidang: Review paper," *IJCIT (Indonesian J. Comput. Inf. Technol.*, vol. 5, no. 1, pp. 75–82, 2020.

[20] V. ENGEN, "Machine Learning For Network Based Intrusion Detection," 2010.

[21] M. B. Kursa and W. R. Rudnicki, "The All Relevant Feature Selection using Random Forest," no. June 2011, 2011.

[22] M. A. Manhar, I. Soesanti, and N. A. Setiawan, "Improving Feature Selection on Heart Disease Dataset with Boruta Approach," vol. 1, no. 1, pp. 41–48, 2020.

[23] 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.

[24] Mohan Patro and M. Ranjan Patra, "A Novel Approach to Compute Confusion Matrix for Classification of n-Class Attributes with Feature

Selection," *Trans. Mach. Learn. Artif. Intell.*, 2015.