SYSTEMATIC LITERATURE REVIEW DAN ANALISIS BIBLIOMETRIK TERHADAP *SOFTWARE TAMPERING*: TREN DAN UPAYA PENCEGAHAN

Oleh:

FADILA AMANDA

NIM: 21206052003

PROGRAM STUDI INFORMATIKA

PROGRAM MAGISTER FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA YOGYAKARTA

2023

PROGRAM STUDI INFORMATIKA

PROGRAM MAGISTER FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA YOGYAKARTA

2023

FADILA AMANDA

NIM: 21206052003

SYSTEMATIC LITERATURE REVIEW DAN ANALISIS BIBLIOMETRIK TERHADAP *SOFTWARE TAMPERING*: TREN DAN UPAYA PENCEGAHAN

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-2342/Un.02/DST/PP.00.9/08/2023

Tugas Akhir dengan judul : Systematic literature review dan analisis bibliometrik terhadap software tampering: tren dan upaya pencegahan

yang dipersiapkan dan disusun oleh:

Nama : FADILA AMANDA, S.Kom
Nomor Induk Mahasiswa : 21206052003
Telah diujikan pada : Rabu, 23 Agustus 2023
Nilai ujian Tugas Akhir : A

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Ir. Maria Ulfah Siregar, S.Kom., MIT., Ph.D.
SIGNED

Valid ID: 64e71657744bc

Penguji I

Dr. Agung Fatwanto, S.Si., M.Kom.
SIGNED

Valid ID: 64e5faacddd06

Penguji II

Dr. Ir. Bambang Sugiantoro, S.Si., M.T., IPM., ASEAN Eng.
SIGNED

Valid ID: 64e5f8e103aad

Yogyakarta, 23 Agustus 2023
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED

Valid ID: 64e846f1ce324

PERNYATAAN KEASLIAN

Yang bertandatangan di bawah ini:

Nama	: Fadila Amanda
NIM	: 21206052003
Jenjang	: Magister
Program Studi	: Informatika

Menyatakan bahwa naskah tesis ini dengan judul "*Systematic Literature Review* dan Analisis Bibliometrik Terhadap *Software Tampering*: Tren dan Upaya Perlindungan" tidak terdapat pada karya yang pernah diajukan untuk memperoleh gelar Magister di suatu Perguruan Tinggi, serta naskah tesis saya secara keseluruhan merupakan hasil penelitian/karya saya sendiri, kecuali pada bagian-bagian yang dirujuk sumbernya.

Yogyakarta, 16 Agustus 2023

Saya yang menyatakan,

Fadila Amanda

NIM: 21206052003

PERNYATAAN BEBAS PLAGIASI

Yang bertandatangan di bawah ini:

Nama	: Fadila Amanda
NIM	: 21206052003
Jenjang	: Magister
Program Studi	: Informatika

Menyatakan bahwa dalam naskah tesis saya secara keseluruhan bebas dari plagiasi. Demikian surat ini saya buat dengan sesungguhnya dan penuh kesadaran, jika dikemudian hari terbukti adanya plagiasi, maka saya siap ditindak sesuai ketentuan hukum yang berlaku.

Yogyakarta, 16 Agustus 2023

Saya yang menyatakan,

Fadila Amanda

NIM: 21206052003

vi

KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
MAGISTER INFORMATIKA
Jl. Marsda Adisucipto Yogyakarta. Telp (0274) 515856 Yogyakarta 55281

SURAT PERSETUJUAN TUGAS AKHIR

Hal : Persetujuan Tugas Akhir

Kepada:
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga
Yogyakarta

Assalammu'alaikum Wr.Wb.

Setelah melakukan bimbingan, arahan, dan koreksi terhadap penulisan tesis yang berjudul: "*SYSTEMATIC LITERATURE REVIEW* DAN ANALISIS BIBLIOMETRIK TERHADAP *SOFTWARE TAMPERING* : TREN DAN UPAYA PENCEGAHAN" yang ditulis oleh :

Nama : Fadila Amanda
NIM : 21206052003
Jenjang : Magister
Program Studi : Informatika

Sudah dapat diajukan kepada Program Studi Magister Informatika Fakultas Sains dan Teknologi UIN sunan Kalijaga sebagai salah satu syarat untuk memperoleh gelar Magister Informatika.
Dengan ini saya mengharap agar tugas tersebut di atas agar dapat segera dimunaqosyahkan.
Atas perhatiannya saya ucapkan terimakasih.

Wasaalammu'alaikum Wr.Wb.

Yogyakarta, 16 Agustus 2023
Pembimbing

Ir. Maria Ulfah Siregar, M.Kom., MIT., Ph.D.
NIP. 19780106 200212 2 001

ABSTRAK

Penelitian ini bertujuan untuk menganalisis tren perkembangan penelitian mengenai *software tampering*, serta mengidentifikasi upaya yang dilakukan peneliti terdahulu dalam mencegah terjadinya *software tampering* dengan menggunakan metode *systematic literature review* (SLR) dan analisis bibliometrik. Berdasarkan hasil seleksi data literatur menggunakan metode PRISMA, diperoleh 112 data literatur yang kemudian dilakukan analisis bibliometrik menggunakan *co-authorship analysis* dan *co-occurrence analysis* dengan menggunakan perangkat lunak VOSviewer untuk menyajikan hasil visualisasi, untuk melakukan SLR diperoleh 56 literatur yang dapat dilakukan analisis isi dalam menjawab pertanyaan penelitian yang telah dilakukan sebelumnya. Hasil penelitian menunjukkan tren perkembangan penelitian dari hasil *co-authorship analysis* diperoleh 13 penulis yang saling berhubungan dimana penulis yang memiliki jaringan terbanyak yaitu Mariano Ceccato, sedangkan pada hasil *co-occurrence analysis* diperoleh 56 kata kunci yang terbagi menjadi lima *cluster*, kata kunci "*blockchain*" merupakan kata kunci yang masih jarang digunakan dapat dijadikan peluang bagi peneliti di masa yang akan datang. Tren penelitian mengenai *software tampering* dengan publikasi terbanyak yaitu pada tahun 2019 dengan total 8 penelitian, kemudian dipimpin oleh United States sebagai negara dengan jumlah publikasi terbanyak. Selanjutnya berdasarkan SLR yang dilakukan dalam menganalisis isi dari data literatur, diperoleh 40 metode sebagai upaya dalam mencegah terjadinya *software tampering* dimana metode *obfuscation code* merupakan metode terbanyak yang digunakan oleh para peneliti terdahulu.

Kata kunci: *software tampering*, *systematic literature review*, analisis bibliometrik, PRISMA, VOSviewer

ABSTRACT

This study aims to analyze the development trend of research on software tampering, as well as identify efforts made by previous researchers in preventing software tampering by using systematic literature review (SLR) method and bibliometric analysis. Based on the results of the selection of literature data using the PRISMA method, 112 literature data were obtained which were then subjected to bibliometric analysis using co-authorship analysis and co-occurrence analysis using VOSviewer software to present visualization results, to conduct SLR obtained 56 literature that could be carried out content analysis in answering research questions that had been done previously. The results showed the trend of research development from the results of co-authorship analysis obtained 13 authors who are interconnected where the author who has the most network is Mariano Ceccato (2015), while the results of co-occurrence analysis obtained 56 keywords which are divided into five clusters, the keyword "blockchain" is a keyword that is still rarely used can be used as an opportunity for researchers in the future. The trend of research on software tampering with the most publications is in 2019 with a total of 8 studies, then led by the United States as the country with the highest number of publications. Furthermore, based on SLR conducted in analyzing the content of literature data, 40 methods were obtained as an effort to prevent software tampering where the obfuscation code method was the most common method used by previous researchers.

Keyword: *software tampering, systematic literature review, bibliometric analysis, PRISMA, VOSviewer*

MOTTO

Kejarlah surga sebelum neraka mengejarmu

PERSEMBAHAN

Tesis ini penulis persembahkan untuk:

- Kedua orang tua saya Masri Jalil dan Isnalimar yang senantiasa memberikan doa maupun dukungan kepada penulis dalam menyelesaikan Pendidikan selama ini.
- Kakak perempuan saya Nora Isma Dewi, Novita Gustina Dewi, Lisa Wahyuni, dan Ayu Febriani Fitri, serta satu-satunya kakak laki-laki saya Muhammad Fadli, yang telah memberikan dukungan dan semangat selama ini.
- Untuk Almamater Universitas Islam Negeri Sunan Kalijaga Yogyakarta serta teman-teman Program Studi Magister Informatika angkatan 2021 Genap.

KATA PENGANTAR

Dengan menyebut nama Allah yang Maha Pengasih dan Maha Penyayang, kami panjatkan puji syukur atas rahmat dan karunia-Nya sehingga penulis mampu menyelesaikan penyusunan Tugas Akhir yang berjudul "*Systematic Literature Review* dan Analisis Bibliometrik terhadap *Software Tampering*". Penyusunan Tugas Akhir ini merupakan salah satu syarat untuk menyelesaikan Pendidikan Program Studi Magister Informatika UIN Sunan Kalijaga Yogyakarta.

Atas tersusunnya Tugas Akhir ini, penulis mengucapkan terimakasih sebesar-besarnya kepada:

1. Allah Subahanahu Wa Ta'ala yang telah memberikan rahmat dan karunia-Nya
2. Kedua orang tua saya, yang selalu memberikan dukungan baik berupa semangat maupun doa
3. Bapak Prof. Dr. Phil. Al Makin, S. Ag., M.A., selaku Rektor UIN Sunan Kalijaga Yogyakarta
4. Bapak Dr. Dra. Hj. Khurul Wardati, M.Si., selaku Dekan Fakultas Sains dan Teknologu UIN Sunan Kalijaga Yogyakarta
5. Bapak Dr. Ir. Bambang Sugiantoro, S.Si., M.T., selaku Ketua Program Studi Magister Informatika UIN Sunan Kalijaga Yogyakarta

6. Ibu Ir. Maria Ulfah Siregar, S. Kom., MIT., Ph.D., selaku Pembimbing tesis yang telah membimbing dan mengarahkan dalam penyusunan tesis
7. Kakak-kakak, Abang, beserta Ipar, yang dalam memberikan dukungan dan doa
8. Sahabat terbaik saya Meisa Santri Liyana, Samyra Nabila Yasmin, Mega Aulia, dan Ana Sari Pulsande, serta teman seperjuangan saya Tachiyya Nailal Khusna yang telah memberikan dukungan serta semangat kepada saya.

Penulis menyadari bahwa penelitian ini masih memiliki banyak kekurangan karena keterbatasan kemampuan yang dimiliki oleh penulis. Harapan penulis semoga penelitian ini dapat bermanfaat bagi pembaca, serta menjadi acuan bagi adik tingkat dalam hal memperoleh informasi dan ilmu pengetahuan.

Yogyakarta, 16 Agustus 2023

Penulis,

Fadila Amanda

NIM: 21206052003

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

A. Latar Belakang

Pada perkembangan era digital yang semakin maju, perangkat lunak (*software*) memiliki peran penting dalam hampir semua aspek kehidupan kita, baik itu dalam dunia bisnis, pemerintahan, maupun dalam kehidupan sehari-hari. Namun semakin berkembangnya teknologi serta ketergantungan kita terhadap perangkat lunak, maka semakin besar pula terjadinya berbagai ancaman keamanan. Salah satu ancaman keamanan yang terjadi terhadap perangkat lunak yaitu *software tampering*.

Software tampering merupakan suatu tindakan yang dilakukan untuk memanipulasi atau memodifikasi perangkat lunak komputer yang dilakukan oleh pihak yang tidak bertanggung jawab dengan tujuan memperoleh keuntungan yang ilegal (Al-wosabi, A., & Shukur, Z., 2015; Bryant, E. D., dkk, 2004). Contoh umum dari *software tampering* antara lain memodifikasi program dengan tujuan untuk menghilangkan batas lisensi, mengubah hasil perhitungan dalam program akuntansi, mengubah tampilan program agar terlihat lebih menarik akan tetapi dilakukan dengan cara menyisipka kode berbahaya, menyisipkan kode berbahaya ke dalam program dengan tujuan merusak sistem atau mencuri data, serta masih

banyak lagi. Beberapa dampak yang ditimbulkan dari *software tampering* yakni kerugian finansial, pelanggaran privasi, kerentanan terhadap serangan *cyber*, dan potensi bahaya bagi pengguna.

Upaya untuk mencegah ancaman-ancaman yang ditimbulkan, beberapa negara menetapkan undang-undang dan peraturan yang khusus mengatur *software tampering*, dimana undang-undang tersebut dirancang untuk memberikan kerangka hukum yang jelas guna melindungi pengguna perangkat lunak dari tindakan yang tidak sah. Salah satu undang-undang di Indonesia yaitu UU ITE 2016 nomor 26 mengenai perlindungan data pribadi, dimana jika terjadi penyalahgunaan informasi data pribadi yang menyebabkan kerugian maka dapat dipidana penjara paling lama 12 (dua belas) tahun dan/atau membayar denda paling banyak Rp. 12.000.000.000,- (dua belas miliar rupiah) (www.kominfo.go.id).

Sebuah survey terhadap lebih dari 300 profesional teknologi mengungkapkan keprihatinan mendalam mengenai ancaman *software tampering* dan serangan rantai pasokan perangkat lunak. Terdapat 37% vendor perangkat lunak yang menyatakan bahwa mereka memiliki cara untuk mendeteksi *software tampering* di seluruh rantai pasokan mereka. Kurangnya deteksi *tampering* yang komprehesif, kemudian perangkat lunak yang rentan, menciptakan vector serangan

baru dan terus meningkat, hal ini berarti bahwa *software tampering* merupakan ancaman signifikan yang ahrus diatasi melalui penelitian (ReversimgLabs, 2022).

Dalam menghadapi ancaman *software tampering* yang semakin kompleks dan merusak, maka peneliti ingin melakukan analisis bibliometrik untuk mengkaji penelitian terdahulu terkait *software tampering* dengan tujuan menganalisis tren perkembangan penelitian mengenai *software tampering* serta memperoleh informasi mengenai upaya untuk mencegah maupun melindungi ancaman terhadap perangkat lunak, dalam melakukan kajian literatur peneliti menerapkan metode *systematic literature review*. Dengan adanya penelitian ini diharapkan dapat memberikan kontribusi penting baik dalam memperoleh informasi maupun memahami kajian dari penelitian sebelumnya mengenai *software tampering*, serta menjadi landasan untuk pengembangan penilitian di masa depan dalam mengembangkan kebijakan yang lebih efektif dalam mengatasi ancaman *software tampering*.

B. Rumusan Masalah

Berdasarkan dari latar belakang yang telah diuraikan, maka dapat dibuat suatu rumusan masalah yaitu:

1. Bagaimana tren perkembangan penelitian mengenai *software tampering*?

2. Apa upaya yang dilakukan untuk mencegah terjadinya kejahatan terhadap perangkat lunak (*software tampering*)?

C. Batasan Masalah

Batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Literatur yang digunakan pada rentang waktu 2000-2023
2. Sumber data yang digunakan yaitu jurnal berasal dari *google scholar* dan *scopus*
3. Metode penelusuran menggunakan kata kunci "*software tampering*"
4. Fokus penelitian menguji artikel jurnal yang berbahasa Inggris
5. Data literatur yang akan diteliti adalah literatur dalam bentuk artikel dan *conference paper*
6. Analisis bibliometrik menggunakan *co-authorship analysis* dan *co-occurrence analysis*

D. Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Menganalisis tren perkembangan penelitian mengenai *software tampering*
2. Mengetahui informasi mengenai upaya yang dilakukan untuk mencegah *software tampering*

BAB V
PENUTUP

A. Kesimpulan

Hasil dari pencarian yang dilakukan dari dua database yaitu *scopus* dan *google scholar* dengan kata kunci "*software tampering*" diperoleh 1.194 data literatur yang kemudian dilakukan seleksi data yang sesuai dengan kriteria inklusi dan ekslusi yang telah ditentukan sebelumnya serta dengan menerapkan metode PRISMA, sehingga diperoleh 112 data literatur yang akan dilakukan analisis bibliometrik (*co-authorship analysis* dan *co-occurrence analysis*) dengan menggunakan perangkat lunak VOSviewer guna memberikan visualisasi pada hasil analisis. Untuk melakukan *systematic literature review* (SLR) peneliti menentukan data literatur yang digunakan harus dapat diakses keseluruhan isi agar bisa digunakan dalam penelitian lebih lanjut (*quality assessment*), sehingga dari jumlah 112 data literatur diperoleh 56 data literatur yang dapat diakses keseluruhan isi jurnal dimana data tersebut digunakan untuk menjawab pertanyaan yang telah ditentukan sebelumnya (*research question*).

Berdasarkan penelitian yang telah dilakukan, hasil *co-authorship analysis* diperoleh 13 penulis yang saling berhubungan dimana penulis yang memiliki jaringan terbanyak yaitu Mariano Ceccato (2015), sedangkan pada hasil

co-occurrence analysis diperoleh 56 kata kunci yang terbagi menjadi lima *cluster*, kata kunci "*blockchain*" merupakan kata kunci yang masih jarang digunakan dapat dijadikan peluang bagi peneliti di masa yang akan datang. Tren penelitian mengenai *software tampering* dengan publikasi terbanyak yaitu pada tahun 2019 dengan total 8 penelitian, kemudian dipimpin oleh United States sebagai negara dengan jumlah publikasi terbanyak. Selanjutnya berdasarkan SLR yang dilakukan dalam menganalisis isi dari data literatur, diperoleh 40 metode sebagai upaya dalam mencegah terjadinya *software tampering* dimana metode *obfuscation code* merupakan metode terbanyak yang digunakan oleh para peneliti terdahulu.

Peneliti berhasil menganalisis tren perkembangan penelitian mengenai *software tampering* serta memperoleh informasi mengenai upaya yang dilakukan untuk mencegah *software tampering*, dengan menggunakan metode SLR dan analisis bibliometrik. Alasan peneliti mengangkat topik mengenai *software tampering* dikarenakan ancaman *software tampering* yang semakin kompleks dan merusak, serta belum banyak ditemukan penelitian yang membahas mengenai *software tampering*. Seperti yang diketahui bahwa penelitian yang sama sebelumnya dilakukan oleh Abdullah Al-Wosabi dan Zarina Shukur (2015) mengenai deteksi *software tampering* pada sistem tertanam (*embedded system*) dengan menggunakan metode *systematic literature review* (SLR),

penelitian ini merangkum berbagai solusi yang diperoleh dari studi-studi terpilih dalam mengatasi terjadinya *software tampering* pada sistem tertanam dengan memfokuskan tiga pendekatan utama yaitu pendekatan perangkat lunak, pendekatan perangkat keras, dan pendekatan gabungan (*hybrid approach*). Hal ini menunjukkan bahwa penelitian yang dilakukan peneliti saat ini memberikan hasil yang lebih baik dari penelitian sebelumnya, ditandai dengan peneliti tidak hanya menerapkan metode SLR namun juga melakukan analisis bibliometrik serta berfokus pada solusi dalam mencegah berbagai jenis serangan *software tampering* (bukan hanya berfokus pada sistem tertanam).

Berdasarkan hasil dari keseluruhan penelitian, ditemukan beberapa topik yang dapat dijadikan dasar untuk menentukan arah penelitian di masa mendatang:

a. SLR dan analisis bibliometrik yang membahas mengenai *software tampering* belum banyak ditemukan
b. Tren penelitian berdasarkan hubungan antar penulis menunjukkan hubungan yang terbentuk masih terbatas dimana belum banyak penulis yang terlibat dalam kerja sama penelitian sehingga memberikan peluang bagi para peneliti untuk melakukan perluasan penelitian.
c. Penelitian mengenai *software tampering* dominan dilakukan negara di luar Indonesia, hal ini dikarenakan

belum ditemukan penelitian yang berasal dari negara Indonesia

d. Tren penelitian di masa mendatang terkait *software tampering* meliputi pencegahan *software tampering*, deteksi dan pencegahan *forgery*, keamanan jaringan dan sistem, analisis data dan forensic *digital*, serta teknologi enkripsi dan *watermarking* dimana bertujuan untuk meningkatkan keamanan dan mencegah terjadinya kejahatan pada perangkat lunak di masa yang akan datang
e. Metode-metode yang masih ditemukan hanya pada 1 jurnal menunjukkan metode tersebut masih jarang diteliti dan digunakan, sehingga dapat dijadikan sebagai acuan bagi para peneliti dimasa mendatang baik itu dalam menciptakan metode baru maupun mengembangkan metode yang sudah ada menjadi lebih baik dari sebelumnya.

B. Saran

Sama halnya dengan para peneliti lainnya, penelitian ini memiliki keterbatasan sehingga diharapkan kepada para peneliti yang akan datang agar dapat menyempurnakan penelitian ini dengan:

a. Menambahkan kata kunci yang lebih banyak sehingga hasil literatur yang diperoleh memiliki pembahasan yang lebih luas

b. Menambahkan sumber database lain seperti *web of science*, *taylor & francis* agar memperoleh data literatur yang lebih banyak dengan topik yang meluas
c. Menambahkan analisis bibliometrik lain seperti *citation analysis*, *bibliographic coupling analysis*, *co-citation analysis*, dan analisis lainnya

DAFTAR PUSTAKA

Abrath, B., B. Coppens, J. Van Den Broeck, B. Wyseur, A. Cabutto, P. Falcarin, dan B.D. Sutter. "Code Renewability for Native Software Protection." *ACM Transactions on Privacy and Security* 23, no. 4 (2020). https://doi.org/10.1145/3404891.

Aghaei Chadegani, A., Salehi, H., Md Yunus, M. M., Farhadi, H., Fooladi, M., Farhadi, M., & Ale Ebrahim, N. (2013). A comparison between two main academic literature collections: Web of science and scopus databases. *Asian Social Science*, *9*(5), 18–26. https://doi.org/10.5539/ass.v9n5p18

Aljawarneh, Shadi, Faisal Alkhateeb, dan Eslam Al Maghayreh. "A Semantic Data Validation Service for Web Applications." *Journal of Theoretical and Applied Electronic Commerce Research* 5, no. 1 (April 2010). https://doi.org/10.4067/S0718-18762010000100005.

Al-Wosabi, A.A.A., dan Z. Shukur. "A Secure Protocol for Remote-Code Integrity Attestation of Embedded Systems: The CSP Approach." *IEEE Access* 7 (2019): 170238–69. https://doi.org/10.1109/ACCESS.2019.2955160.

Al-Wosabi, AAA, Z Shukur, dan ... "Framework for software tampering detection in embedded systems." ... *Conference on Electrical …*, no. Query date: 2023-06-09 23:17:46 (2015). https://ieeexplore.ieee.org/abstract/document/7352507/.

Al-wosabi, A. A. L. I. A., & Shukur, Z. (2015). *SOFTWARE TAMPERING DETECTION IN EMBEDDED – A SYSTEMATIC LITERATURE REVIEW*. *76*(2), 211–221.

Anna Budiani, S. (2022). GREEN HUMAN RESOURCE MANAGEMENT: A SYSTEMATIC LITERATURE REVIEW (SLR) AND BIBLIOMETRIC ANALYSIS. *JURNAL SYNTAX FUSION*, *2*(11).

Baleanu, D., A.S. Al-Shamayleh, dan R.W. Ibrahim. "Image Splicing Detection Using Generalized Whittaker Function Descriptor." *Computers, Materials and Continua* 75, no. 2 (2023): 3465–77. https://doi.org/10.32604/cmc.2023.037162.

Bardin, Sebastien, Robin David, dan Jean-Yves Marion. "Backward-Bounded DSE: Targeting Infeasibility Questions on Obfuscated Codes." Dalam *2017 IEEE Symposium on Security and Privacy (SP)*, 633–51. San Jose, CA, USA: IEEE, 2017. https://doi.org/10.1109/SP.2017.36.

Basile, C., D. Canavese, L. Regano, P. Falcarin, dan B.D. Sutter. "A meta-model for software protections and reverse engineering attacks." *Journal of Systems and Software* 150 (2019): 3–21. https://doi.org/10.1016/j.jss.2018.12.025.

Bryant, E. D., Atallah, M. J., Stytz, M. R., Atallah, M. J., Bryant, E. D., & Stytz, M. R. (2004). *A Survey of Anti-Tamper Technologies*.

Buzydlowski, J. W. (2015). Co-occurrence analysis as a framework for data mining. Journal of Technology Research, 6, 1–19.

Cappaert, Jan, Bart Preneel, Bertrand Anckaert, Matias Madou, dan Koen De Bosschere. "Towards Tamper Resistant Code Encryption: Practice and Experience." Dalam *Information Security Practice and Experience*, disunting oleh Liqun Chen, Yi Mu, dan Willy Susilo, 4991:86–100. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008. https://doi.org/10.1007/978-3-540-79104-1_7.

Carvalho, T.J.D., C. Riess, E. Angelopoulou, H. Pedrini, dan A.D.R. Rocha. "Exposing digital image forgeries by illumination color classification." *IEEE Transactions on Information Forensics and Security* 8, no. 7 (2013): 1182–94. https://doi.org/10.1109/TIFS.2013.2265677.

Ceccato, Mariano, Massimiliano Di Penta, Paolo Falcarin, Filippo Ricca, Marco Torchiano, dan Paolo Tonella. "A Family of Experiments to Assess the Effectiveness and Efficiency of Source Code Obfuscation Techniques." *Empirical Software Engineering*, 23 Februari 2013. https://doi.org/10.1007/s10664-013-9248-x.

Collberg, C, GR Myles, dan A Huntwork. "Sandmark-a tool for software protection research." *IEEE security &privacy*, no. Query date: 2023-06-09 23:17:46 (2003). https://ieeexplore.ieee.org/abstract/document/1219058/.

Collberg, CS, dan C Thomborson. "Watermarking, tamper-proofing, and obfuscation-tools for software protection." *IEEE Transactions on software ...*, no. Query date: 2023-06-09 23:17:46 (2002). https://ieeexplore.ieee.org/abstract/document/1027797/.

Cristin, R., dan V. Cyril Raj. "Exposing image manipulation with curved surface reflection." *Indian Journal of Science and Technology* 9, no. 38 (2016). https://doi.org/10.17485/ijst/2016/v9i38/99998.

De, A., M. Nasim Imtiaz Khan, K. Nagarajan, dan S. Ghosh. "HarTBleed: Using Hardware Trojans for Data

Leakage Exploits.” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 28, no. 4 (2020): 968–79. https://doi.org/10.1109/TVLSI.2019.2961358.

Dedić, N, M Jakubowski, dan R Venkatesan. “A graph game model for software tamper protection.” *... IH 2007, Saint Malo, France, June ...*, no. Query date: 2023-06-09 23:17:46 (2007). https://doi.org/10.1007/978-3-540-77370-2_6.

El-Latif, E.I.A., A. Taha, dan H.H. Zayed. “A Passive Approach for Detecting Image Splicing using Deep Learning and Haar Wavelet Transform.” *International Journal of Computer Network and Information Security* 11, no. 5 (2019): 28–35. https://doi.org/10.5815/ijcnis.2019.05.04.

Ellison, Robert J., dan Carol Woody. “Supply-Chain Risk Management: Incorporating Security into Software Development.” Dalam *2010 43rd Hawaii International Conference on System Sciences*, 1–10. Honolulu, Hawaii, USA: IEEE, 2010. https://doi.org/10.1109/HICSS.2010.355.

Fatmala, F. D. A., & Sopiah. (2023). a Systematic Literature Review and Bibliometric Analysis of Transactional Leadership. *Jurnal Penelitian Administrasi Publik*,

3(01). https://aksiologi.org/index.php/praja/article/view/624

Fawzi, L.M., S.Y. Ameen, S.M. Alqaraawi, dan S.A. Dawwd. "Embedded real-time video surveillance system based on multi-sensor and visual tracking." *Applied Mathematics and Information Sciences* 12, no. 2 (2018): 345–59. https://doi.org/10.18576/amis/120209.

Fiskiran, AM, dan RB Lee. "Runtime execution monitoring (REM) to detect and prevent malicious code execution." *... Conference on Computer Design: VLSI in ...*, no. Query date: 2023-06-09 23:17:46 (2004). https://ieeexplore.ieee.org/abstract/document/1347961/.

Horne, B, L Matheson, C Sheehan, dan ... "Dynamic self-checking techniques for improved tamper resistance." *Security and Privacy in ...*, no. Query date: 2023-06-09 23:17:46 (2002). https://doi.org/10.1007/3-540-47870-1_9.

Islam, Md Nazmul, Vinay C Patii, dan Sandip Kundu. "On IC Traceability via Blockchain." Dalam *2018 International Symposium on VLSI Design, Automation and Test (VLSI-DAT)*, 1–4. Hsinchu: IEEE, 2018. https://doi.org/10.1109/VLSI-DAT.2018.8373269.

Iwendi, Celestine, Zunera Jalil, Abdul Rehman Javed, Thippa Reddy G., Rajesh Kaluri, Gautam Srivastava, dan Ohyun Jo. "KeySplitWatermark: Zero Watermarking Algorithm for Software Protection Against Cyber-Attacks." *IEEE Access* 8 (2020): 72650–60. https://doi.org/10.1109/ACCESS.2020.2988160.

Jakubowski, Mariusz H., Chit Wei (Nick) Saw, dan Ramarathnam Venkatesan. "Tamper-Tolerant Software: Modeling and Implementation." Dalam *Advances in Information and Computer Security*, disunting oleh Tsuyoshi Takagi dan Masahiro Mambo, 5824:125–39. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. https://doi.org/10.1007/978-3-642-04846-3_9.

Jin, X.-L., M. Zhang, Z. Zhou, dan X. Yu. "Application of blockchain platform to manage and secure personal genomic data: A case study of lifecode.AI in China." *Journal of Medical Internet Research* 21, no. 9 (2019). https://doi.org/10.2196/13587.

Jun Yang, Youtao Zhang, dan Lan Gao. "Fast Secure Processor for Inhibiting Software Piracy and Tampering." Dalam *22nd Digital Avionics Systems Conference. Proceedings (Cat. No.03CH37449)*, 351–60. San Diego, CA, USA: IEEE Comput. Soc, 2003. https://doi.org/10.1109/MICRO.2003.1253209.

Junod, Pascal, Julien Rinaldini, Johan Wehrli, dan Julie Michielin. “Obfuscator-LLVM -- Software Protection for the Masses.” Dalam *2015 IEEE/ACM 1st International Workshop on Software Protection*, 3–9. Florence, Italy: IEEE, 2015. https://doi.org/10.1109/SPRO.2015.10.

Kakar, P, N Sudha, dan W Ser. “Exposing digital image forgeries by detecting discrepancies in motion blur.” *IEEE Transactions on Multimedia*, no. Query date: 2023-06-09 23:17:46 (2011). https://ieeexplore.ieee.org/abstract/document/5721842/.

Karam, Robert, Tamzidul Hoque, Sandip Ray, Mark Tehranipoor, dan Swarup Bhunia. “MUTARCH: Architectural Diversity for FPGA Device and IP Security.” Dalam *2017 22nd Asia and South Pacific Design Automation Conference (ASP-DAC)*, 611–16. Chiba, Japan: IEEE, 2017. https://doi.org/10.1109/ASPDAC.2017.7858391.

Karnik, Neeran M., dan Anand R. Tripathi. “Security in the Ajanta Mobile Agent System.” *Software: Practice and Experience* 31, no. 4 (10 April 2001): 301–29. https://doi.org/10.1002/spe.364.

Knopf, J. W. (2006). Doing a Literature Review. Political Science and Politics, 39(1), 127– 132.

Lie, D., J. Mitchell, C.A. Thekkath, dan M. Horowitz. "Specifying and Verifying Hardware for Tamper-Resistant Software." Dalam *Proceedings 19th International Conference on Data Engineering (Cat. No.03CH37405)*, 166–77. Berkeley, CA, USA: IEEE Comput. Soc, 2003. https://doi.org/10.1109/SECPRI.2003.1199335.

Manu, VT, dan BM Mehtre. "Blind technique using blocking artifacts and entropy of histograms for image tampering detection." *Second International Workshop on ...*, no. Query date: 2023-06-09 23:17:46 (2017). https://doi.org/10.1117/12.2280306.short.

Marrington, Andrew, Ibrahim Baggili, George Mohay, dan Andrew Clark. "CAT Detect (Computer Activity Timeline Detection): A Tool for Detecting Inconsistency in Computer Activity Timelines." *Digital Investigation* 8 (Agustus 2011): S52–61. https://doi.org/10.1016/j.diin.2011.05.007.

Mary, DJP, dan CS Joyce. "Digital Image Protection against Tampering and Self Recovery with High Image Quality using Efficient Watermarking Algorithm." *... of Science and Innovative Engineering & ...*, no. Query date: 2023-06-09 23:17:46 (2016). https://www.researchgate.net/profile/Pricilla-Mary-D-J/publication/321097578_Digital_Image_Protection_a

gainst_Tampering_and_Self_Recovery_with_High_Image_Quality_using_Efficient_Watermarking_Algorithm/links/5a0d454f4585153829b1a97d/Digital-Image-Protection-against-Tampering-and-Self-Recovery-with-High-Image-Quality-using-Efficient-Watermarking-Algorithm.pdf.

Milenković, M, A Milenković, dan E Jovanov. "Using instruction block signatures to counter code injection attacks." *ACM SIGARCH Computer ...*, no. Query date: 2023-06-09 23:17:46 (2005). https://doi.org/10.1145/1055626.1055641.

Moher, D. (2018). Reporting Guidelines: Doing Better for Readers. *BMC Med*, *16*(1), 233. Diambil dari 10.1186/s12916-018-1226-0 pmid:30545364

Morel, C. M., Serruya, S. J., Penna, G. O., & Guimarães, R. (2009). Co-authorship Network Analysis: A Powerful Tool for Strategic Planning of Research, Development and Capacity Building Programs on Neglected Diseases. PLoS Neglected Tropical Diseases, 3(8), e501. https://doi.org/10.1371/journal.pntd.0000501

Nazmul Islam, M.D., dan S. Kundu. "Enabling IC traceability via blockchain pegged to embedded PUF." *ACM Transactions on Design Automation of Electronic Systems* 24, no. 3 (2019). https://doi.org/10.1145/3315669.

Ollivier, Mathilde, Sébastien Bardin, Richard Bonichon, dan Jean-Yves Marion. "How to Kill Symbolic Deobfuscation for Free (or: Unleashing the Potential of Path-Oriented Protections)." Dalam *Proceedings of the 35th Annual Computer Security Applications Conference*, 177–89. San Juan Puerto Rico USA: ACM, 2019. https://doi.org/10.1145/3359789.3359812.

Pati, D., & Lorusso, L. N. (2018). How to write a systematic review of the literature. HERD: Health Environments Research & Design Journal, 11(1), 15–30. https://doi.org/10.1177/1937586717747384

Perry, A. & Hammond, N. (2002). Systematic Review: The Experience of a PhD Student. Psychology Learning and Teaching, 2(1), 32–35.

Poilpré, MC, P Perrot, dan H Talbot. "Image tampering detection using Bayer interpolation and JPEG compression." *1st International conference on Forensic ...*, no. Query date: 2023-06-09 23:17:46 (2013). https://core.ac.uk/download/pdf/48344583.pdf.

Prilatama, A., & Sopiah. (2022). Keselamatan Kerja : Systematic Literature Review (Slr) Dan Analisa Bibliometrik. *Transekonomika: Akuntansi, Bisnis Dan*

Keuangan, *3*(1), 12–22. https://doi.org/10.55047/transekonomika.v3i1.330

Putra, G. Y., Andrianingsih, A., & Aldisa, R. T. (2022). *Perancangan User Experience Aplikasi Lapor Vaksin Kelurahan Menggunakan Metode UCD (User Centered Design). 6*, 428–439.

Rafika, A. S., Putri, H. Y., & Widiarti, F. D. (2017). Analisis Mesin Pencarian Google Scholar Sebagai Sumber Baru Untuk Kutipan. *Journal CERITA*, *3*(2), 193–205. https://doi.org/10.33050/cerita.v3i2.657

Rahmatulloh, A., & Gunawan, R. (2020). Web Scraping with HTML DOM Method for Data Collection of Scientific Articles from Google Scholar. *Indonesian Journal of Information Systems*, *2*(2), 95–104. https://doi.org/10.24002/ijis.v2i2.3029

Salwan, Jonathan, Sebastien Bardin, dan Marie-Laure Potet. "Symbolic Deobfuscation: From Virtualized Code Back to the Original." Dalam *15th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2018*, Vol. Volume 10885 LNCS. Springer Verlag, 2018.

Sebastian, D.J., U. Agrawal, A. Tamimi, dan A. Hahn. "DER-TEE: Secure Distributed Energy Resource Operations Through Trusted Execution Environments." *IEEE*

Internet of Things Journal 6, no. 4 (2019): 6476–86. https://doi.org/10.1109/JIOT.2019.2909768.

Shaikh, M, dan D Patil. "IMAGE FORGERY/TAMPERING DETECTION USING DEEP LEARNING AND CLOUD." *irjmets.com*, no. Query date: 2023-06-09 23:17:46 (2022). https://www.irjmets.com/uploadedfiles/paper/issue_6_june_2022/26554/final/fin_irjmets1655807910.pdf.

Sharifi, A. (2021). Urban sustainability assessment: An overview and bibliometric analysis. *Ecological Indicators*, *121*, 107102. https://doi.org/10.1016/j.ecolind.2020.107102

Shashidhar, T.M., dan K.B. Ramesh. "Novel framework for optimized digital forensic for mitigating complex image attacks." *International Journal of Electrical and Computer Engineering* 10, no. 5 (2020): 5198–5207. https://doi.org/10.11591/IJECE.V10I5.PP5198-5207.

Sidiq, M. (2019). *Panduan Analisis Bibliometrik Sederhana*. *June*. https://doi.org/10.13140/RG.2.2.15688.37125

Siswanto. (2010). Systematic Review Sebagai Metode Penelitian Untuk Mensintasis Hasil-Hasil Penelitian (Sebuah Pengantar) (Systematic Review as a Research Method to Synthesize Research Results (An

Introduction)). *Buletin Penelitian Sistem Kesehatan*, *13*(4), 326–333.

Sun, K, G Cao, Q Zhao, dan J Zhang. "Differential Abnormality-Based Tampering Detection in Digital Document Images." *2019 IEEE/ACIS 18th …*, no. Query date: 2023-06-09 23:17:46 (2019). https://ieeexplore.ieee.org/abstract/document/8940190/.

Sun, Y., dan G. Huang. "A control flow obfuscation scheme based on garbage code." *Journal of Theoretical and Applied Information Technology* 46, no. 1 (2012): 284–88.

Swaminathan, A, M Wu, dan KJR Liu. "Image tampering identification using blind deconvolution." *... International Conference on …*, no. Query date: 2023-06-09 23:17:46 (2006). https://ieeexplore.ieee.org/abstract/document/4107028/.

Tang, Z., M. Li, G. Ye, S. Cao, M. Chen, X. Gong, D. Fang, dan Z. Wang. "VMGuards: A novel virtual machine based code protection system with VM security as the first class design concern." *Applied Sciences (Switzerland)* 8, no. 5 (2018). https://doi.org/10.3390/app8050771.

Torres-Arias, S, AK Ammula, R Curtmola, dan ... "On Omitting Commits and Committing Omissions: Preventing Git Metadata Tampering That (Re) introduces Software Vulnerabilities." *USENIX Security ...*, no. Query date: 2023-06-09 23:17:46 (2016). https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_torres-arias.pdf.

Viticchié, Alessio, Cataldo Basile, Andrea Avancini, Mariano Ceccato, Bert Abrath, dan Bart Coppens. "Reactive Attestation: Automatic Detection and Reaction to Software Tampering Attacks." Dalam *Proceedings of the 2016 ACM Workshop on Software PROtection*, 73–84. Vienna Austria: ACM, 2016. https://doi.org/10.1145/2995306.2995315.

Viticchié, Alessio, Leonardo Regano, Marco Torchiano, Cataldo Basile, Mariano Ceccato, Paolo Tonella, dan Roberto Tiella. "Assessment of Source Code Obfuscation Techniques." Dalam *2016 IEEE 16th International Working Conference on Source Code Analysis and Manipulation (SCAM)*, 11–20, 2016. https://doi.org/10.1109/SCAM.2016.17.

Wang, W, dan H Farid. "Exposing digital forgeries in video by detecting double MPEG compression." *Proceedings of the 8th workshop on Multimedia and ...*, no. Query

date: 2023-06-09 23:17:46 (2006). https://doi.org/10.1145/1161366.1161375.

———. "Exposing digital forgeries in video by detecting double quantization." *Proceedings of the 11th ACM workshop on ...*, no. Query date: 2023-06-09 23:17:46 (2009). https://doi.org/10.1145/1597817.1597826.

———. "Exposing digital forgeries in video by detecting duplication." *Proceedings of the 9th workshop on Multimedia & ...*, no. Query date: 2023-06-09 23:17:46 (2007). https://doi.org/10.1145/1288869.1288876.

Wu, Y, W Abd-Almageed, dan ... "Busternet: Detecting copy-move image forgery with source/target localization." *Proceedings of the ...*, no. Query date: 2023-06-09 23:17:46 (2018). http://openaccess.thecvf.com/content_ECCV_2018/html/Rex_Yue_Wu_BusterNet_Detecting_Copy-Move_ECCV_2018_paper.html.

Xiao, Shucai, Jung-Min "Jerry" Park, dan Yanzhu Ye. "Tamper Resistance for Software Defined Radio Software." Dalam *2009 33rd Annual IEEE International Computer Software and Applications Conference*, 383–91. Seattle, Washington, USA: IEEE, 2009. https://doi.org/10.1109/COMPSAC.2009.58.

Xiao, Y., & Watson, M. (2019). Guidance on Conducting a Systematic Literature Review. Journal of Planning Education and Research, 39, 93-112.

Xu, H, Y Zhou, dan MR Lyu. "N-version obfuscation: Impeding software tampering replication with program diversity." *arXiv preprint arXiv:1506.03032*, no. Query date: 2023-06-09 23:17:46 (2015). https://arxiv.org/abs/1506.03032.

Yang, J, Y Zhang, dan L Gao. "Fast secure processor for inhibiting software piracy and tampering." *Proceedings. 36th Annual IEEE/ACM ...*, no. Query date: 2023-06-09 23:17:46 (2003). https://ieeexplore.ieee.org/abstract/document/1253209/.

Yang, T, J Wu, dan Z Fang. "Image Tampering Detection for Splicing based on Rich Feature and Convolution Neural Network." *Proceedings of the 2020 4th High Performance ...*, no. Query date: 2023-06-09 23:17:46 (2020). https://doi.org/10.1145/3409501.3409530.

https://www.kominfo.go.id/content/detail/12865/siaran-pers-no-85hmkominfo042018-tentang-jamin-perlindungan-data-pribadi-kominfo-beri-sanksi-terhadap-penyalahgunaan-oleh-pihak-ketiga/0/siaran_pers

https://www.reversinglabs.com/blog/survey-finds-software-supply-chain-security-top-of-mind-for-dev-teams