



## SUPPLEMENTARY EUROPEAN SEARCH REPORT

Application number:  
EP 20 84 37 21

Classification of the application (IPC):  
G06F 21/56, H04L 9/40, G06N 20/00

Technical fields searched (IPC):  
H04L, G06N

DOCUMENTS CONSIDERED TO BE RELEVANT		
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim
A	<p><b>CHRISTIAN WRESSNEGGER ET AL:</b> "A close look on n-grams in intrusion detection" <i>ARTIFICIAL INTELLIGENCE AND SECURITY, ACM, 2 PENN PLAZA, SUITE 701 NEW YORK NY 10121-0701 USA</i>, 04 November 2013 (2013-11-04), DOI: 10.1145/2517312.2517316, ISBN: 978-1-4503-2488-5, pages 67-76, XP058034229</p> <p>* abstract *</p> <p>* Section 1 *</p>	1-16
X	<p><b>WEI-JEN LI ET AL:</b> "Fileprints: identifying file types by n-gram analysis" <i>SYSTEMS, MAN AND CYBERNETICS (SMC) INFORMATION ASSURANCE WORKSHOP, 200 5. PROCEEDINGS FROM THE SIXTH ANNUAL IEEE WEST POINT, NY, USA 15-17 JUNE 2005, PISCATAWAY, NJ, USA, IEEE</i>, 15 June 2005 (2005-06-15), DOI: 10.1109/IAW.2005.1495935, ISBN: 978-0-7803-9290-8, pages 64-71, XP010826316</p> <p>* abstract *</p> <p>* Sections I-III *</p>	1-16
A	<p><b>Oza Adityaram ET AL:</b> "HTTP Attack Detection using N-gram Analysis HTTP Attack Detection using N-gram Analysis" <i>San Jose State University</i>, 01 May 2013 (2013-05-01)</p> <p>URL: <a href="https://scholarworks.sjsu.edu/cgi/viewcontent.cgi?article=1298&amp;context=etd_projects">https://scholarworks.sjsu.edu/cgi/viewcontent.cgi?article=1298&amp;context=etd_projects</a>, DOI: 10.31979/etd.rbtj-p2jh [retrieved on 29 June 2023 (2023-06-29)]</p> <p>XP093059288</p> <p>* Sections 1, 2 and 3 *</p>	1-16
A	<p>WO 2010011411 A1 (UNIV COLUMBIA [US]; SONG YINGBO [US] ET AL.) 28 January 2010 (2010-01-28)</p> <p>* abstract *</p>	1-16

The supplementary search report has been based on the last set of claims valid and available at the start of the search.

Place of search Munich	Date of completion of the search 03 November 2023	Examiner Bertolissi, Edy
---------------------------	--	-----------------------------

### CATEGORY OF CITED DOCUMENTS

X: particularly relevant if taken alone	P: intermediate document
Y: particularly relevant if combined with another document of the same category	T: theory or principle underlying the invention
A: technological background	E: earlier patent document, but published on, or after the filing date
O: non-written disclosure	D: document cited in the application
& : member of the same patent family, corresponding document	L: document cited for other reasons

Disclaimer: this document has been automatically generated using data structured in accordance with WIPO standard ST.36 from the database of search reports of the European Patent Office. For technical reasons, its content and layout may differ from that of the original publication. Only the original published information is legally binding.



## SUPPLEMENTARY EUROPEAN SEARCH REPORT

Application number:  
EP 20 84 37 21

### DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim
X	<p><b>BEEBE NICOLE L ET AL:</b> "Sceadan: Using Concatenated N-Gram Vectors for Improved File and Data Type Classification" <i>IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE, USA</i>, 01 September 2013 (2013-09-01), vol. 8, no. 9, DOI: 10.1109/TIFS.2013.2274728, ISSN: 1556-6013, pages 1519-1530, XP011526429</p> <p>* abstract *</p> <p>* Section 1-3 *</p>	17-24
X	<p><b>CHIH-TA LIN ET AL:</b> "Feature Selection and Extraction for Malware Classification" <i>JOURNAL OF INFORMATION SCIENCE AND ENGINEERING</i>, 01 January 2015 (2015-01-01), vol. 31, pages 965-992, XP055475966</p> <p>* abstract *</p> <p>* Sections 1-3 *</p>	17, 23, 24
X	<p><b>Tahan Gil ET AL:</b> "Mal-ID: Automatic Malware Detection Using Common Segment Analysis and Meta-Features" <i>Journal of Machine Learning Research</i>, 28 February 2012 (2012-02-28)</p> <p>URL: <a href="https://citeseerx.ist.psu.edu/document?repid=rep1&amp;type=pdf&amp;doi=ac447b25cbb796fc159ae8d7895c76240f08449c">https://citeseerx.ist.psu.edu/document?repid=rep1&amp;type=pdf&amp;doi=ac447b25cbb796fc159ae8d7895c76240f08449c</a> [retrieved on 03 November 2023 (2023-11-03)]</p> <p>XP093097882</p> <p>* abstract *</p> <p>* Sections 1-3 *</p>	17, 23, 24
A	<p><b>Mohd Zaki Mas'ud ET AL:</b> "A Comparative Study on Feature Selection Method for N-gram Mobile Malware Detection" <i>International Journal of Network Security</i>, 30 September 2017 (2017-09-30)</p> <p>URL: <a href="http://ijns.jalaxy.com.tw/contents/ijns-v19-n5/ijns-2017-v19-n5-p727-733.pdf">http://ijns.jalaxy.com.tw/contents/ijns-v19-n5/ijns-2017-v19-n5-p727-733.pdf</a>, DOI: 10.6633/IJNS.201709.19(5).10</p> <p>[retrieved on 03 November 2023 (2023-11-03)]</p> <p>XP093097820</p> <p>* abstract *</p> <p>* Sections 1-3 *</p>	17-24

The supplementary search report has been based on the last set of claims valid and available at the start of the search.

Place of search Munich	Date of completion of the search 03 November 2023	Examiner Bertolissi, Edy
---------------------------	--	-----------------------------

### CATEGORY OF CITED DOCUMENTS

X: particularly relevant if taken alone	P: intermediate document
Y: particularly relevant if combined with another document of the same category	T: theory or principle underlying the invention
A: technological background	E: earlier patent document, but published on, or after the filing date
O: non-written disclosure	D: document cited in the application
& : member of the same patent family, corresponding document	L: document cited for other reasons

Disclaimer: this document has been automatically generated using data structured in accordance with WIPO standard ST.36 from the database of search reports of the European Patent Office. For technical reasons, its content and layout may differ from that of the original publication. Only the original published information is legally binding.



## SUPPLEMENTARY EUROPEAN SEARCH REPORT

Application number:  
EP 20 84 37 21

### LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1. claims: 1-16

A system, method and computer program product for preventing propagation of the received file in response to determining that the file is malicious.

2. claims: 17-24

A system, method and computer program product for determining a reduced set of features that includes at least some of the plurality of n grams.

All further search fees have been paid within the fixed time limit. The present (supplementary) European search report has been drawn up for all claims.

The supplementary search report has been based on the last set of claims valid and available at the start of the search.

Place of search Munich	Date of completion of the search 03 November 2023	Examiner Bertolissi, Edy
---------------------------	--	-----------------------------

### CATEGORY OF CITED DOCUMENTS

X: particularly relevant if taken alone	P: intermediate document
Y: particularly relevant if combined with another document of the same category	T: theory or principle underlying the invention
A: technological background	E: earlier patent document, but published on, or after the filing date
O: non-written disclosure	D: document cited in the application
& : member of the same patent family, corresponding document	L: document cited for other reasons

Disclaimer: this document has been automatically generated using data structured in accordance with WIPO standard ST.36 from the database of search reports of the European Patent Office. For technical reasons, its content and layout may differ from that of the original publication. Only the original published information is legally binding.



## ANNEX TO SUPPLEMENTARY EUROPEAN SEARCH REPORT

Application number:  
EP 20 84 37 21

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on 03-11-2023  
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO2010011411	A1	28-01-2010	US	2011167493 A1	07-07-2011
			US	2014373150 A1	18-12-2014
			US	2016366169 A1	15-12-2016
			US	2019182279 A1	13-06-2019
			WO	2010011411 A1	28-01-2010