Information & Security

Published since 1998

P. Panagiotou, N. Mengidis, et al.
vol. 50, no. 1 (2021): 37-48
https://doi.org/10.11610/isij.5016

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Host-based Intrusion Detection Using Signature-based and AI-driven Anomaly Detection Methods

Panos Panagiotou (✉), ***Notis Mengidis***, ***Theodora Tsikrika***, ***Stefanos Vrochidis***, ***Ioannis Kompatsiaris***

Centre for Research and Technology-Hellas (CERTH), Thessaloniki, Greece
https://www.certh.gr/

ABSTRACT:

Cyberattacks are becoming more sophisticated, posing even greater challenges to traditional intrusion detections methods. Failure to prevent the intrusions could jeopardise security services' credibility, including data confidentiality, integrity, and availability. Anomaly-based Intrusion Detection Systems and Signature-based Intrusion Detection Systems are two types of systems that have been proposed in the literature to detect security threats. In the current work, a taxonomy of current IDSs is presented, a review of recent works is performed, and we discuss some of the most common datasets used for evaluation. Finally, the survey concludes with a discussion of future IDS research directions and broader observations.

ARTICLE INFO:

RECEIVED: 21 JUNE 2021
REVISED: 26 AUG 2021
ONLINE: 11 SEP 2021

KEYWORDS:

intrusion detection, anomaly detection, artificial intelligence, AI, computer security, cybersecurity

1. Introduction

In the context of information systems, an intrusion can be defined as any attempt to gain unauthorised access and potentially cause damage to any given system. This means that any attack that may pose a threat to the confidentiality, integrity, or availability of information meets the definition of an intrusion.

Corresponding Author: E-mail: panagiotou@iti.gr

Intrusion detection is a mechanism that acts as the first line of defence and whose goal, as the name implies, is to detect harmful activity occurring on a computer or a network. A variety of intrusion detection systems (IDSs) have been designed and developed due to the importance of intrusion detection to the research communities and the industrial ones since IDSs are a great asset in the proactive approach towards achieving the much-desired digital resilience. Developing new intrusion detection methods, techniques, and tools present a great research interest, especially if we consider the fact that the variety of IDSs have grown in both number and complexity.[1]

Because the capabilities of an IDS are primarily dependent on the data that is available to it, the location of the IDS is an important architectural decision. This is also the main difference between network-based intrusion detection systems (NIDS) versus host-based intrusion detection systems (HIDS). Both approaches are presented, albeit the latter are the ones that we mainly focus on in this study.

In more detail, in Section 2, we present the most common types and detection methods used by IDSs, the types of data used and the available datasets, as well as the challenges faced. In Section 3, we present the recent advances in the field, which are mainly related to the adoption of Neural Networks and Deep Learning solutions and, to a lesser extent, feature engineering. In the same section, we also propose some future research directions based on the current state of the literature and the challenges that need to be addressed. In Section 4, we examine existing surveys related to IDSs, and in Section 5, we present our conclusions.

2. Intrusion Detection Systems

2.1 Types of IDS

It is common practice for an IDS to be classified according to the information source that it utilises as well as its location within the network infrastructure.[2]

2.1.1 NIDS

In general, NIDS are standalone devices that exist on the same network with the system being monitored, and in their typical deployment, monitor many separate systems on a common network. As a result, the NIDS is frequently completely transparent to the systems it is monitoring, allowing for excellent isolation and making NIDSs significantly less susceptible to interference from an attacker. However, because these systems are agnostic to the internal state of the systems being monitored, detection can be a more challenging task. Furthermore, encrypted network traffic is becoming the norm, which may pose a problem for NIDS.[3] However, we should point out that “break-and-inspect” capabilities are becoming increasingly common in practice, allowing encryption of all traffic while providing visibility to network appliances.[4] Figure 1 illustrates a typical NIDS architecture where two sensors are deployed and are sending their captured data to a centralised NIDS Management system.

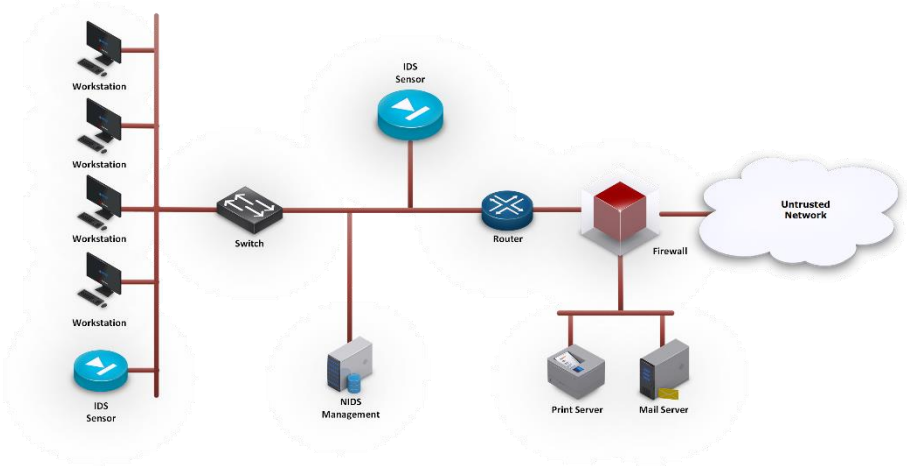

Figure 1: A typical network topology of a NIDS.

2.1.2 HIDS

On the other hand, HIDSs are software components that are installed on the monitored system and usually are responsible for the monitoring of a single system, providing them with a great overall overview of the system state but poor isolation from the system itself, which means that a malicious actor with access to the system can disable or tamper the HIDS as a result of the poor isolation. Additionally, host-based data is frequently context-rich, allowing for a more in-depth understanding of processes and activities.[4] However, this collection and management of potentially large and sensitive datasets from these hosts come at the cost of additional complexity and overhead.

Figure 2 illustrates a typical HIDS architecture where each workstation has an agent collecting system information and sending it to a centralised HIDS Management system.

2.2 Types of Detection

During the detection stage, two approaches can be used: signature and anomaly. The signature-based approach involves searching the received events for well-known attack patterns, whereas the anomaly-based approach seeks to detect new and unknown attacks by modelling the activities that are considered normal within a system and identifying potential attacks from behaviours that deviate from the known normal behaviour patterns.[5]

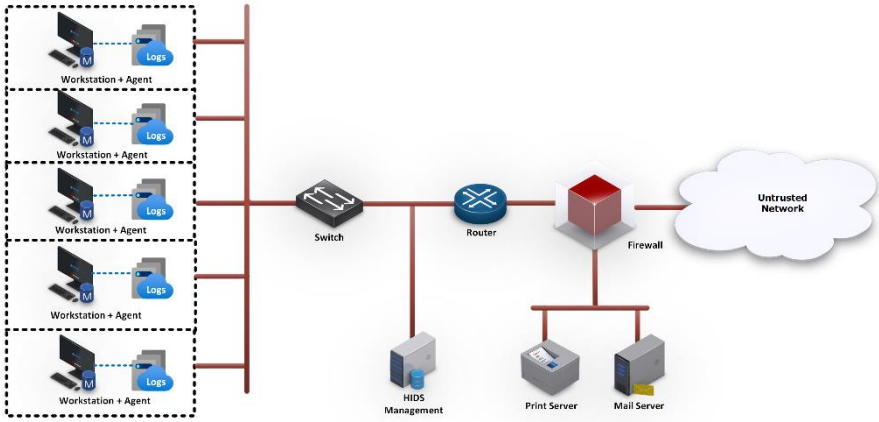

Figure 2: A typical network topology of a HIDS.

2.2.1 Signature-based

Signature intrusion detection systems (SIDS) use pattern matching techniques to detect a known attack; these are also referred to as Knowledge-based Detection or Misuse Detection.[6] Matching methods are used in SIDS to locate a previous intrusion triggering an alarm signal whenever an intrusion signature matches one from a previous intrusion existing in the signature database. The most well-known SIDS currently available are Snort,[7,8] Suricata,[9] NetSTAT,[10] and Bro.[11]

For previously known intrusions, SIDS typically provides excellent detection accuracy and are still more popular;[12] however, they have difficulty detecting zero-day attacks because no matching signature exists until the signature of the new attack is extracted and stored. Traditional SIDS approaches examine network packets and attempt to match them against a signature database. However, these techniques are incapable of detecting attacks that are either intentionally fragmented across multiple packets. Due to the sophistication of modern malware, extracting signature information across multiple packets may be necessary. This necessitates the IDS recalling the contents of previous packets. In terms of creating a SIDS signature, there have been a variety of methods where signatures are created as state machines or semantic conditions.[13,14] Because no prior signature exists for any such attack, zero-day attacks have rendered traditional SIDS progressively less effective. Polymorphic malware variants and an increase in targeted attacks may further undermine the efficiency of this traditional paradigm.[15]

2.2.2 Anomaly-based

The anomaly-based approach, on the other hand, aims to detect new (unknown) attacks by modelling the activities that are considered normal within a system and identifying potential attacks from behaviours that deviate from the known normal behaviour pattern.[16]

Statistical analysis and machine learning methods have been used for this purpose. The goal of machine learning in this context is to classify an event (e.g., normal or attack/intrusion). The first events captured from the environment are stored in a database during the process. A set of features is extracted and stored in a dataset from each event in the database. The dataset is then used by a machine learning algorithm to infer a pattern and create a model that represents such behaviour.

There are various types of data sources that have been considered in order to perform host-based intrusion detection. System log files contain information related with warnings, errors and system failures. System audit data are produced by the applications and contain more granular information than system logs, which is related to user sessions (such as command line actions, login times, privilege escalations, etc.). Both of the above types of data are costly to collect.[4] For this reason, system call data, which do not require any pre-processing, are currently a more popular source of information. A system call trace is a sequence of all the system calls produced by a process or application in a specific time interval. Finally, Windows registry and file systems have also been used as sources of information, although more seldom.

The application of anomaly-based methods relies upon the existence of data of one of the above types. Nowadays, there are some available datasets, which also make the comparison of different methods easier. The ADFA Linux Dataset (ADFA-LD12) presented by Creech and Hu [17] has been used in order to evaluate machine learning and deep learning methods in many research papers and is a system call dataset that has been collected in a Linux environment. Furthermore, two Windows-based datasets, ADFA-WD and ADFA-WD:SAA were presented by Haider et al.,[18] both consisting of audit data selections. More recently, the same research group presented a synthetic dataset named NGIDS-DS (Next-Generation IDS Dataset),[19] which consists of both network traffic and host system logs data, reflecting the critical cyber infrastructures of different enterprises. In addition, the AWSCTD dataset [20] contains system call data created in a Windows host (including system calls arguments and return values). In some cases, datasets that are mainly intended to be used for NIDS, such as NSL-KDD, have also been used for the development and evaluation of HIDS systems.[21]

A challenge for the anomaly-based detection approaches is that they typically yield high false-alarm rates (FAR), which means that a relatively high number of normal sequences of data are characterised as anomalous. This evaluation metric is most commonly referred to as False-Positive Rate (FPR).

3. Recent Developments and Future Directions

3.1 Recent Developments

As the data used in the anomaly-based methods are of a sequential nature, and most of the approaches attempt to capture this sequential information, Hidden Markov models have been frequently used in the past. One can refer, for example, to Hoang, Hu and Bertok.[22] However, such approaches have been proven insufficient, as they fail to capture long-term dependencies among system calls.

Recent research in anomaly-based HIDS algorithms has focused on the application of Neural Networks (NNs) and Deep Learning (DL) algorithms with the purpose of system call language-modelling in order to predict if a sequence of system calls is normal or anomalous. Such language models determine a probability distribution for the next system call given the sequence of previous system calls, and then the probability of a sequence occurring is estimated using these distributions.

Kim et al. [23] use LSTM units [24] (following an embedding layer) in order to better capture long-range dependencies between system calls. The output is the normalised probability values of the possible calls that will follow in the sequence. Given a new sequence of system calls, if it is one with an average negative log-likelihood above a threshold, it is classified as abnormal, while if it has an average negative log-likelihood below this threshold, it is classified as normal. In the aforementioned paper, the authors also attempt to tackle the problem of high false-alarm rates by using an ensemble method of multiple thresholding classifiers, using the rectified linear units (ReLU) method.[25] They compare three LSTM solutions (with varying numbers of layers and cells) with a k-nearest neighbour (kNN) and a k-means clustering (kMC) classifier, and the results show the superiority of their method.

Chawla et al.[26] deploy multiple 1-dimensional (1D) convolutional networks (CNNs) as a pre-processing step before an RNN layer made up of Gated Recurrent Units (GRUs),[27] following the architecture proposed by Wang, Jiang, and Luo.[28] They compared variations of this architecture (using six, seven and eight 1D CNNs and a varying number of GRU units) with RNN architectures (with LSTM and GRU implementations). The proposed CNN/GRU architecture is significantly faster than the LSTM solution. In addition, the addition of CNN layers before the GRU layer yielded better accuracy. Specifically, a solution with CNN and 600 GRU units yielded 100 % True Detection Rate and 60 % False Alarm Rate, which they claim to be better than a False Alarm Rate between 50 % and 60 % achieved by Kim et al.[23]

GRUs are also used by Lv et al.[29] for their system call prediction model. Their model is an RNN implementation of the encoder-decoder framework.[30] They experiment with a varying number of hidden layers (one, two and three) and learning rates. They use the BLEU score, the TF-IDF model and the cosine values between the semantic encoding vectors of the predicted sequences and the true ones (called the target sequences) to evaluate the quality of the predictions. The results show that the architecture with the single hidden layer did not

perform well, in contrast to the other solutions. An evaluation of the predicted sequences on the task of anomaly detection with sequence classification is also performed, using classification algorithms such as CNNs, RNNs, SVM and Random Forest. The effectiveness of using the predicted sequences on this task is demonstrated.

The applicability of some more complex, dual-flow Deep Learning models, such as long short-term memory fully convolutional network (LSTM-FCN) [31] and GRU-FCN [32] is investigated by Ceponis and Goranin.[33] Compared to more simple models, which are more efficient in training and testing times, they are not producing better results. A relatively simple CNN solution with a static value of kernels parameter performed the best among the models considered, while a CNN-GRU model had the best False Positive Rate.

The application of NN and DL algorithms is not the only area of research interest since other recent works focus on feature engineering. Besharati, Naderan and Namjoo perform feature selection before the application of an ML-based classifier, whereby a host-based IDS is designed to be deployed in hypervisors in a cloud environment.[21] Specifically, the most important features for each class (the normal and each of the different attack types) are determined with logistic regression and only those features are used to distinguish the corresponding class from the rest. Liu et al. present a novel feature extraction method that aims to produce a platform-independent feature set.[34] Their method relies on the transformation of system calls into frequency sequences of n-grams and the extraction of statistical features of those frequency sequences.

In Table 1, we present the aforementioned works with the datasets that were used in order to evaluate the methods, as well as the evaluation metrics.

3.2 Future Directions

The aforementioned inherent deficiency of anomaly-based methods with regard to the FPR evaluation metric indicates the importance of the inclusion of this metric in the evaluation process of those methods. In addition, this metric can also be used in the optimisation process of the proposed intrusion systems. For example, Besharati, Naderan and Namjoo use TPR and FPR diagrams to determine the optimal number of features for each class.[21]

As far as the NN and DL approaches are concerned, we can assume that the advances that are currently made in the NNs and DL field will be further adopted in the domain of host-based IDS, resulting in more successful solutions. Still, the combination of such approaches with feature engineering, or even with signature-based techniques, is an even more intriguing prospect.

Last but not least, the application of HIDS in domains such as cloud computing and the IoT imposes requirements for more efficient approaches [35] that will need to be addressed. For example, in the aforementioned paper, audit logs of only the failed processes are analysed for the cases of users other than the root.

Table 1. Summary of the recent solutions, with the datasets and metrics used for their evaluation.

Publication	Dataset	Metrics
Kim et al., 2016 [23]	ADFA-LD	ROC curve
Chawla et al., 2018 [26]	ADFA-LD	AUC, True Detection Rate, FPR
Lv et al., 2018 [29]	ADFA-LD	ROC curve
Ceponis and Goranin, 2020 [33]	AWSCTD	accuracy, confusion matrix, precision, recall, F-score, FPR, False Negative Rate, classification error
Besharati, Naderan and Namjoo, 2019 [21]	NSL-KDD	accuracy, precision, recall, FPR, error rate, F-score
Liu et al., 2020 [34]	ADFA-LD, ADFA-WD, NGIDS-DS	AUC

4. Related Work

In the literature, there are some surveys about host-based IDSs. Bridges et al. put emphasis on the data sources and the types of data that are leveraged by the various intrusion detection methods.[4] Ming Liu et al. [36] survey previous work that relies on system calls data. Challenges such as the high FPR values and some possible directions for their mitigation are discussed, while an analysis of the available datasets is also presented. In another related work, Jose et al. [37] present a taxonomy of anomaly-based methods, but most presented methods presented are not recent enough.

In this work, we present some recent advances in the methods that are applied to the task of intrusion detection, specifically the application of NNs and DL approaches.

5. Conclusions

In this work, we presented a taxonomy of host-based IDS solutions. We have also presented the available datasets that are used for the implementation and evaluation of the data-driven approaches in the literature. We focused on the more recent approaches, the majority of which are based on NN and DL techniques, expecting that the application of such approaches in the domain will be continued in the future. Finally, we have provided some future research directions.

Acknowledgements

This work was supported by the ECHO project which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no 830943.

References

[1] Aleksandar Milenkoski, Marco Vieira, Samuel Kounev, Alberto Avritzer, and Bryan D. Payne, "Evaluating Computer Intrusion Detection Systems: A Survey of Common Practices," *ACM Computing Surveys (CSUR)* 48, no. 1 (2015.): 1-41, https://doi.org/10.1145/2808691.

[2] Preeti Mishra, Emmanuel S. Pilli, Vijay Varadharajan, and Udaya Tupakula, "Intrusion Detection Techniques in Cloud Environment: A Survey," *Journal of Network and Computer Applications* 77 (2017): 18-47, https://doi.org/10.1016/j.jnca.2016.10.015.

[3] Tiina Kovanen, Gil David, and Timo Hämäläinen, "Survey: Intrusion Detection Systems in Encrypted Traffic," in *Internet of Things, Smart Spaces, and Next Generation Networks and Systems* (Springer, 2016), 281-293.

[4] Robert A. Bridges, Tarrah R. Glass-Vanderlan, Michael D. Iannacone, Maria S. Vincent, and Qian Chen, "A Survey of Intrusion Detection Systems Leveraging Host Data," *ACM Computing Surveys (CSUR)* 52, no. 6 (2019): 1-35, https://doi.org/10.1145/3344382.

[5] Robin Sommer and Vern Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," *2010 IEEE symposium on security and privacy,* Oakland, CA, USA, 2010, https://doi.org/10.1109/sp.2010.25.

[6] Ansam Khraisat, Iqbal Gondal, Peter Vamplew, and Joarder Kamruzzaman, "Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges," *Cybersecurity* 2, no. 1 (2019): 1-22, https://doi.org/10.1186/s42400-019-0038-7.

[7] Vinod Kumar and Om Prakash Sangwan, "Signature Based Intrusion Detection System Using SNORT," *International Journal of Computer Applications & Information Technology* 1 no. 3 (2012): 35-41.

[8] Martin Roesch, "Snort: Lightweight Intrusion Detection for Networks," *LISA'99: Proceedings of the 13th USENIX Conference on System administration*, November 1999, pp. 229–238.

[9] Adeeb Alhomoud, Rashid Munir, Jules Pagna Disso, Irfan Awan, and Abdullah Al-Dhelaan, "Performance Evaluation Study of Intrusion Detection Systems," *Procedia Computer Science* 5 (2011): 173-180, https://doi.org/10.1016/j.procs.2011.07.024.

[10] Giovanni Vigna and Richard A. Kemmerer, "NetSTAT: A Network-based Intrusion Detection System," *Journal of Computer Security* 7, no. 1 (1999): 37-71.

[11] Vern Paxson, "Bro: A System for Detecting Network Intruders in Real-time," *Computer networks* 31, no. 23-24 (1999): 2435-2463.

[12] Monther Aldwairi, Ansam M. Abu-Dalo, and Moath Jarrah, "Pattern Matching for Signature-based IDS Using MapReduce Framework and Myers Algorithm," *EURASIP Journal on Information Security* 2017, no. 9 (2017), https://doi.org/10.1186/s13635-017-0062-7.

[13] Po-Ching Lin, Ying-Dar Lin, and Yuan-Cheng Lai, "A Hybrid Algorithm of Backward Hashing and Automaton Tracking for Virus Scanning," *IEEE Transactions on Computers* 60, no. 4 (2010): 594-601, https://doi.org/10.1109/TC.2010.95.

[14] Chad R. Meiners, Jignesh Patel, Eric Norige, Eric Torng, and Alex X. Liu, "Fast Regular Expression Matching Using Small TCAMs for Network Intrusion Detection and Prevention Systems," *Proceedings of the 19th USENIX conference on Security*, Washington, D.C., 2010.

[15] Eduardo K. Viegas, Altair O. Santin, and Luiz S. Oliveira, "Toward a Reliable Anomaly-based Intrusion Detection in Real-world Environments," *Computer Networks* 127 (2017): 200-216, https://doi.org/10.1016/j.comnet.2017.08.013.

[16] Marzia Zaman and Chung-Horng Lung, "Evaluation of Machine Learning Techniques for Network Intrusion Detection," *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*, Taipei, Taiwan, 2018, https://doi.org/10.1109/noms.2018.8406212.

[17] Gideon Creech and Jiankun Hu, "Generation of a New IDS Test Dataset: Time to Retire the KDD Collection," in *2013 IEEE Wireless Communications and Networking Conference (WCNC)*, Shanghai, China, 2013, pp, 4487-4492, https://doi.org/10.1109/wcnc.2013.6555301.

[18] Waqas Haider, Gideon Creech, Yi Xie, and Jiankun Hu, "Windows Based Data Sets for Evaluation of Robustness of Host Based Intrusion Detection Systems (IDS) to Zero-day and Stealth Attacks," *Future Internet* 8, no. 3 (2016): 29, https://doi.org/10.3390/fi8030029.

[19] Waqas Haider, Jiankun Hu, Jill Slay, Benjamin P. Turnbull, and Yi Xie, "Generating Realistic Intrusion Detection System Dataset Based on Fuzzy Qualitative Modelling," *Journal of Network and Computer Applications* 87 (2017): 185-192, https://doi.org/10.1016/j.jnca.2017.03.018.

[20] Dainius Ceponis and Nikolaj Goranin, "Towards a Robust Method of Dataset Generation of Malicious Activity on a Windows-Based Operating System for Anomaly-Based HIDS Training," In *Doctoral Consortium/Forum@ DB&IS*, 2018, pp. 23-32, https://doi.org/10.22364/bjmc.2018.6.3.01.

[21] Elham Besharati, Marjan Naderan, and Ehsan Namjoo, "LR-HIDS: Logistic Regression Host-based Intrusion Detection System for Cloud Environments," *Journal of Ambient Intelligence and Humanized Computing* 10, no. 9 (2019): 3669-3692. https://doi.org/10.1007/s12652-018-1093-8.

[22] Xuan Dau Hoang, Jiankun Hu, and Peter Bertok, "A program-based Anomaly Intrusion Detection Scheme Using Multiple Detection Engines and Fuzzy Inference," *Journal of Network and Computer Applications* 32, no. 6 (2009): 1219-1228, https://doi.org/10.1016/j.jnca.2009.05.004.

[23] Gyuwan Kim, Hayoon Yi, Jangho Lee, Yunheung Paek, and Sungroh Yoon, "LSTM-based System-call Language Modeling and Robust Ensemble Method for Designing Host-Based Intrusion Detection Systems," *arXiv preprint arXiv:1611.01726* (2016).

[24] Sepp Hochreiter and Jürgen Schmidhuber, "Long Short-term Memory," *Neural computation* 9, no. 8 (1997): 1735-1780.

[25] Andrew L. Maas, Awni Y. Hannun, and Andrew Y. Ng, "Rectifier Nonlinearities Improve Neural Network Acoustic Models," *Proceedings of ICML Workshop on Deep Learning for Audio, Speech and Language*, Atlanta, Georgia, USA, 2013, vol. 30, no. 1, p. 3.

[26] Ashima Chawla, Brian Lee, Sheila Fallon, and Paul Jacob, "Host Based Intrusion Detection System with Combined CNN/RNN Model," in *Joint European Conference on Machine Learning and Knowledge Discovery in Databases* (Cham: Springer, 2018), 149-158, https://doi.org/10.1007/978-3-030-13453-2_12.

[27] Yoshua Bengio, Réjean Ducharme, Pascal Vincent, and Christian Janvin, "A Neural Probabilistic Language Model," *The Journal of Machine Learning Research* 3 (2003): 1137-1155.

[28] Xingyou Wang, Weijie Jiang, and Zhiyong Luo, "Combination of Convolutional and Recurrent Neural Network for Sentiment Analysis of Short Texts," *Proceedings of COLING 2016, the 26th international conference on computational linguistics: Technical papers*, 2016, pp. 2428-2437.

[29] Shaohua Lv, Jian Wang, Yinqi Yang, and Jiqiang Liu, "Intrusion Prediction with System-call Sequence-to-Sequence Model," *IEEE Access* 6 (2018): 71413-71421, https://doi.org/10.1109/access.2018.2881561.

[30] Dzmitry Bahdanau, Kyunghyun Cho, and Yoshua Bengio, "Neural Machine Translation by Jointly Learning to Align and Translate," *arXiv preprint arXiv:1409.0473* (2014).

[31] Fazle Karim, Somshubra Majumdar, Houshang Darabi, and Shun Chen, "LSTM Fully Convolutional Networks for Time Series Classification," *IEEE access* 6 (2017): 1662-1669, https://doi.org/10.1109/access.2019.2916828.

[32] Nelly Elsayed, Anthony S. Maida, and Magdy Bayoumi, "Deep Gated Recurrent and Convolutional Network Hybrid Model for Univariate Time Series Classification," *arXiv preprint arXiv:1812.07683* (2018), https://doi.org/10.14569/ijacsa.2019.0100582.

[33] Dainius Čeponis and Nikolaj Goranin, "Investigation of Dual-flow Deep Learning Models LSTM-FCN and GRU-FCN Efficiency against Single-flow CNN Models for the Host-based Intrusion and Malware Detection Task on Univariate Times Series Data," *Applied Sciences* 10, no. 7 (2020): 2373, https://doi.org/10.3390/app10072373.

[34] Zhen Liu, Nathalie Japkowicz, Ruoyu Wang, Yongming Cai, Deyu Tang, and Xianfa Cai, "A Statistical Pattern Based Feature Extraction Method on System Call Traces for Anomaly Detection," *Information and Software Technology* 126 (2020): 106348, https://doi.org/10.1016/j.infsof.2020.106348.

[35] Prachi Deshpande, Subhash Chander Sharma, Sateesh K. Peddoju, and S. Junaid, "HIDS: A Host Based Intrusion Detection System for Cloud Computing Environment," *International Journal of System Assurance Engineering and Management* 9, no. 3 (2018): 567-576, https://doi.org/10.1007/s13198-014-0277-7.

[36] Ming Liu, Zhi Xue, Xianghua Xu, Changmin Zhong, and Jinjun Chen, "Host-based Intrusion Detection System with System Calls: Review and Future Trends," *ACM Computing Surveys (CSUR)* 51, no. 5 (2018): 1-36, https://doi.org/10.1145/3214304.

[37] Shijoe Jose, D. Malathi, Bharath Reddy, and Dorathi Jayaseeli, "A Survey on Anomaly Based Host Intrusion Detection System," *Journal of Physics: Conference Series*, 1000, no. 1 (2018): 012049, https://doi.org/10.1088/1742-6596/1000/1/012049.

About the Authors

Panos Panagiotou received his Computer and Telecommunications Engineering degree from the University of Western Macedonia and his MSc in Informatics from the Aristotle University of Thessaloniki. He works as a research assistant at CERTH-ITI and more specifically in the Multimodal Data Fusion and Analytics Group since January 2019. His research interests include machine learning, artificial intelligence, and their application in domains such as cyber security.

Notis Mengidis received his Computer Science degree from the Aristotle University of Thessaloniki and his MSc in Telecommunications and Cybersecurity, from International Hellenic University. Since January 2019, he is a research assistant at CERTH-ITI and a member of the Multimodal Data Fusion and Analytics Group. His research interests include botnets, penetration testing, malware analysis and blockchain technologies.

Dr. Theodora Tsikrika is Postdoctoral Research Fellow with CERTH-ITI and a member of the Multimodal Data Fusion and Analytics Group. Her research interests are in the areas of Data Mining and Information Retrieval, focusing on AI for (cyber)security applications, and include Web and social media mining, multimodal analytics, and evaluation. She has participated in more than 20 research projects and is the co-author of more than 60 journal and conference publications.

Dr. Stefanos Vrochidis is a Senior Researcher (Grade C') with CERTH-ITI and the Head of the Multimodal Data Fusion and Analytics Group. His research interests include multimodal fusion, computer vision, AI for e-Health, environmental, Media/Arts, industrial and security applications. Dr. Vrochidis has participated in more than 50 research projects. He is also the co-author of 3 books, 39 refereed journal, 175 conferences and 15 book chapter articles.

Dr. Ioannis (Yiannis) Kompatsiaris is a Research Director at CERTH-ITI. His research interests include AI/Machine Learning for multimedia, Semantics, Social Media Analytics, Multimodal and Sensors Data Analysis, Human Computer Interfaces, e-Health, Arts and Cultural, Media/Journalism, Environmental and Security applications. He is the co-author of 178 papers in journals, 63 book chapters, 8 patents and 560 papers in conferences.