

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/340098454>

# Machine Learning and Deep Learning Techniques for Cybersecurity: A Review

**Chapter** in *Advances in Intelligent Systems and Computing* · March 2020

DOI: 10.1007/978-3-030-44289-7\_5

CITATIONS

132

READS

13,140

4 authors:



**Said A. Salloum**

310 PUBLICATIONS 15,064 CITATIONS

SEE PROFILE



**Muhammad Turki Alshurideh**

University of Sharjah and The University of Jordan

578 PUBLICATIONS 20,646 CITATIONS

SEE PROFILE



**Ashraf M Elnagar**

University of Sharjah

155 PUBLICATIONS 2,915 CITATIONS

SEE PROFILE



**Khaled Shaalan**





British University in Dubai

433 PUBLICATIONS 15,082 CITATIONS

SEE PROFILE



# Machine Learning and Deep Learning Techniques for Cybersecurity: A Review

Said A. Salloum<sup>1,2</sup> , Muhammad Alshurideh<sup>3,4</sup> ,  
Ashraf Elnagar<sup>1,5</sup> , and Khaled Shaalan<sup>2</sup> 

<sup>1</sup> Research Institute of Sciences and Engineering,  
University of Sharjah, Sharjah, UAE  
ssalloum@sharjah.ac.ae

<sup>2</sup> Faculty of Engineering and IT, The British University in Dubai, Dubai, UAE

<sup>3</sup> Faculty of Business, University of Jordan, Amman, Jordan

<sup>4</sup> Management Department, University of Sharjah, Sharjah, UAE

<sup>5</sup> Department of Computer Science, University of Sharjah, Sharjah, UAE

**Abstract.** In this review, significant literature surveys on machine learning (ML) and deep learning (DL) techniques for network analysis of intrusion detection are explained. In addition, it presents a short tutorial explanation on every ML/DL method. Data holds a significant position in ML/DL methods; hence this paper highlights the datasets used in machine learning techniques, which are the primary tools for analyzing network traffic and detecting abnormalities. In addition, we elaborate on the issues faced in using ML/DL for cybersecurity and offer recommendations for future studies.

**Keywords:** Cyber security · Machine learning · Deep learning

## 1 Introduction

This paper takes into view the cyber security applications and presents the outcomes of a literature survey of machine learning (ML), deep learning (DL), and data mining (DM) methods. In addition, it explains the (ML/DL)/DM methods and their applications to cyber intrusion detection issues. Besides providing a set of comparison criteria for (ML/DL)/DM methods, the paper analyzes the complexity of different (ML/DL)/DM algorithms. Subsequently, best methods and a set of recommendations are given subject to the attributes of the cyber problem. The set of processes and technologies that are formulated for the prevention of unauthorized access, attack, change, or destruction of networks, computers, data and programs is referred to as the cyber security [1]. The network security systems and computer (host) security systems basically make up the cyber security systems. At least, a single antivirus software, firewall and an intrusion detection system (IDS) must be included in each of these entities [1]. In addition to identification, IDSs do discover and determine the unauthorized use, alteration, duplication and damage of information systems [2]. The internal intrusions (intra-organization attacks) and external intrusions (inter-organization attacks) are known as the security breaches. In sensing security threats, the artificial intelligent and machine learning based methodologies have become an essential part of our lives because of the rise in the ratio of

cyber-attacks [3]. The standards of security play an important role in the provision of the best security applications keeping in view their implementation and security requirements. They are vital for cyber security research from this perspective, such as intrusion detection system. While machine and deep learning algorithms and particular datasets can be corroborated through some research studies, literature doesn't contain much content on the (ML/DL)/DM techniques for cyber security and security-related datasets.

While concentrating on the (ML/DL)/DM methods and their descriptions, the (ML/DL)/DM techniques are focused by this survey paper aiming at cyber security. Besides publication of several reviews [1, 3–7], many papers containing these methods have also been published [8, 9]. Compared to earlier reviews, the publications fulfilling certain criteria will be the major emphasis of our paper. The techniques, such as: “machine learning” or “deep learning” and cybersecurity along with “data mining” were used to perform Google Scholar queries. The highly cited papers containing well-known techniques were among the main concerns. Nevertheless, there was a realization that novel and innovative techniques would possibly be ignored; therefore a few of these articles were also selected. By and large, selection of papers was done with a view to incorporate at least one and preferably a few representative papers about each of the (ML/DL)/DM categories. The remainder of this paper is organized as follows: Sect. 2 offered a summary of some relevant literature. Section 4 overviews different (ML/DL)/DM methods used in cyber security. Section 4 discusses cybersecurity datasets for (ML/DL)/DM and Sect. 5 concludes the paper with a brief summary of the paper's key points and other closing remarks.

## 2 Literature Review

With the assistance of computer software, an exclusive way to solve fundamental scientific and engineering questions is provided by the machine learning applications [10]. During last twenty years, radical advancements have been witnessed in the field of machine learning with an easy access to the beginners [11]. A laboratory “black-box” environment has basically triggered the machine learning, which has then transformed into a practical application and commercial companies are progressively implementing it on a large scale [10, 11]. The software applications computer vision [12, 13], natural language processing [13–15], speech recognition [13–16], robot control [13, 17, 18] and other emerging applications are the innovations of machine learning [10]. For bringing improvements in user experience, to promote special offerings and suggest purchases [10], machine learning is used by major companies such as Amazon, Facebook and Google. Instead of programming the traditional input-process-output, it is far easier for machine learning developers to train a system. They achieve it by developing simulations of anticipated output [11]. Various industries have observed the impact of machine learning in the shape of data-intensive issues, such as, cybersecurity [10]. Some other fields ranging from biology [19–23] to cosmology to social science [24–30] can also take advantages of Machine learning for bringing remarkable transformations [11]. The experimental data can be processed and analyzed by machine learning in new ways [11]. Theoretically, we can better understand the concepts of “big data” by working on machine learning algorithms. Moreover, these technologies can be

employed to improve associated performance metrics in vertical applications. There can be a great variation in the machine learning algorithms with respect to unique functions (e.g., logistic regression, linear Regression, Naive Bayes, decision trees, random forest, support vector machines, deep learning and Gradient Boosting algorithms). Nevertheless, machine learning introduces creative ways to analyze huge amounts of data with an aim to generate evolutionary approach. Moreover, greater optimization can be provided by the successive generations of algorithms [11]. The large volume of data can ideally be processed through machine learning and cybersecurity [11]. The platforms and networks are vulnerable to attack. The effectiveness of these attacks depend on the number of tools to scan and evaluate targets [10]. Machine learning is used by the adversaries to further increase their attacks. Recently, some journals have published few surveys on the security perspective of machine learning and artificial intelligence [4–6, 31, 32]. In addition, [4] emphasized on contemporary literature on Intrusion Detection for computer network security and Machine Learning Techniques used in Internet-of-Things. Subsequently, for network analysis of intrusion detection, [6] explained key literature surveys on machine learning (ML) and deep learning (DL) methods with an explanatory description of each ML/DL method.

During training and testing or inferring of machine learning from a data driven view, a comprehensive literature review regarding defensive techniques and security threats was presented by [5]. In addition, [31] briefed on security issues regarding artificial intelligence, especially the reinforcement and supervised learning algorithms. In contrast, updates on security issues and defensive methods in the life cycle of a machine learning-based system from training to inference were reviewed by [32].

### **3 Classification of Machine Learning Algorithms to Cybersecurity**

#### **3.1 Classical Machine Learning Techniques**

Development of models receiving input data besides utilizing statistical analysis to forecast an output value within an suitable range is the key objective of ML [3]. The ML is one of the rapidly growing areas with comprehensive applications in the domain of computer science [3]. The supervised, unsupervised and Reinforcement Learning are among the classifications of ML algorithms. The well-known procedures used in the machine learning algorithms are none other than the supervised algorithms. Furthermore, regression and classification are the further sub-divisions of supervised algorithms. A number of machine learning algorithms are used in literature [33, 34]. The Logistic Regression [35], Decision Tree [36], Naive Bayes [35, 37, 38], SVM [35, 37, 39, 40], K-Means [38], KNN [37, 40] and Random Forest [41] are among the commonly used machine-learning algorithms.

### 3.2 Deep Learning Techniques

A new branch of machine learning, i.e., the deep learning has currently gained widespread recognition and the same has been used for intrusion detection. Moreover, traditional methods are outshined by the deep learning as per the findings of the studies [8]. For flow-based anomaly detection, a deep learning approach subject to a deep neural network has been utilized by the authors in [42]. According to the experimental outcomes, anomaly detection in software defined networks can also be performed through deep learning. In [43], using self-taught learning (STL) on the benchmark NSL-KDD dataset, a deep learning based approach is proposed in a network intrusion detection system. The technique is found to be more efficient in terms of its performance as compared to those discussed in previous studies. Nonetheless, the feature reduction ability of the deep learning is emphasized by this category of references. It implements classification through the traditional supervision model and deep learning methods are primarily used for pre-training. Applying the deep learning method to directly perform classification is an unusual task, and literature is devoid of the studies illustrating the performance in multiclass classification. The RNNs are believed to be the reduced-size neural networks according to [31]. In this article, three-layer RNN architecture was suggested for misuse-based IDs with 41 features as inputs and four intrusion categories as outputs. The ability of deep learning for modeling high-dimensional features is not exhibited by the reduced RNNs and the nodes of layers are partially connected. The performance of the model in the binary classification is not explored by the authors.

[8] learned to model an intrusion detection system on the basis of deep learning and a deep learning approach was recommended for intrusion detection using recurrent neural networks (RNN-IDS). Furthermore, the performance of the model in binary classification and multiclass classification was also investigated. It was discovered that the performance of the proposed model is affected by different learning rate and the number of neurons. For modeling a classification model with high accuracy, the RNN-IDS are found very suitable according to the experimental outcomes. In both multiclass and binary classification, it depicts high performance than the traditional machine learning classification methods. The RNN-IDS model offers a new research technique for intrusion detection and the accuracy of the intrusion detection is also enhanced.

## 4 Cybersecurity Datasets

Currently, data is prepared by various research groups both for their own analysis and for provision to community repositories [3]. Using machine learning and artificial intelligent research, the present security-related datasets are explained by this section.

### 4.1 KDD Cup 1999 Dataset

The data obtained from MIT Lincoln Labs entails BSM list files and tcpdump in addition to KDD Cup 1999 [3]. The data captured in DARPA'98 IDS evaluation program contributed to this particular dataset [11]. For assessment of intrusion detection systems,

this dataset is also considered as benchmark data. One of the renowned data sets to assess performance of anomaly detection methods is none other than the KDD'99 [3]. Presently, KDD dataset is being used by various researchers [38, 44–46]

## 4.2 ISOT (Information Security and Object Technology) Dataset

The openly available botnets and normal datasets comprising of 1,675,424 total traffic flow collectively formulate the ISOT dataset. As far as malicious traffic in ISOT is concerned, the same was acquired from French chapter of honeynet project encompassing Storm and Waledac botnets [3, 35, 47, 48].

## 4.3 HTTP CSIC 2010 Dataset

Thousands of web requests automatically generated and developed at Information Security Institute of CSIC (Spanish Research National Council) are collectively known as HTTP CSIC 2010 dataset [3]. The web attack protection systems can be tested through this dataset. Nearly 6,000 normal requests and above 25,000 anomalous requests formulate this data. Moreover, HTTP requests are labeled as anomalous or normal [3]. The web detection in [49–51] is successfully accomplished through this dataset.

## 4.4 CTU-13 (Czech Technical University) Dataset

The mixture of seizures of 13 different malwares in a nonfictional network environment is referred to as the CTU-13 (Czech Technical University) dataset. This dataset aims to acquire real mixed botnet traffic. Foregoing in view, normal traffic is generated by verified normal hosts, while botnet traffic is generated by Infected hosts [3]. This dataset is a carefully labeled dataset capturing the procedures carried out in a controlled environment, which is one of the benefits of using it [39, 40, 48, 52].

## 4.5 UNSW-NB15 Dataset

In the Cyber Range Lab of the Australian Centre for Cyber Security (ACCS), the IXIA Perfect Storm tool has reportedly generated the UNSW-NB15 Dataset [3]. Nearly one hour of anonymized traffic traces from a DDoS attack in 2007 are included in this dataset [47, 49, 53]. This dataset entails nine types of major attacks, including Fuzzers, Backdoors, Analysis, Exploits, DoS, Reconnaissance, Generic, Worms and Shellcode [3].

# 5 Conclusion and Future Work

One of the key issues for national and international security is the safety of computer systems from cyber-attacks. With numerous machine learning techniques, a survey on security concerns has been presented in this article. Several datasets have been employed to conduct various researches. In addition, a significant role in protection of computer systems is performed by machine learning and artificial intelligence.

The literature review of ML/DL and DM methods used for cyber is explained by this paper. The example papers explaining various ML/DL and DM techniques in the cyber domain were carefully found and widespread classes of various datasets have been defined along with their advantages and disadvantages. We aim to generate new dataset in the future, which will be open to all.

## References

1. Buczak, A.L., Guven, E.: A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Commun. Surv. Tutor.* **18**(2), 1153–1176 (2015)
2. Mukkamala, S., Sung, A., Abraham, A.: Cyber security challenges: designing efficient intrusion detection systems and antivirus tools. In: Vemuri, V.R. (ed.) *Enhancing Computer Security with Smart Technology 2006*, pp. 125–163 (2005)
3. Yavanoglu, O., Aydos, M.: A review on cyber security datasets for machine learning algorithms. In: *2017 IEEE International Conference on Big Data (Big Data)*, pp. 2186–2193 (2017)
4. da Costa, K.A.P., Papa, J.P., Lisboa, C.O., Munoz, R., de Albuquerque, V.H.C.: Internet of Things: a survey on machine learning-based intrusion detection approaches. *Comput. Netw.* **151**, 147–157 (2019)
5. Liu, Q., Li, P., Zhao, W., Cai, W., Yu, S., Leung, V.C.M.: A survey on security threats and defensive techniques of machine learning: a data driven view. *IEEE Access* **6**, 12103–12117 (2018)
6. Xin, Y., et al.: Machine learning and deep learning methods for cybersecurity. *IEEE Access* **6**, 35365–35381 (2018)
7. Dua, S., Du, X.: *Data Mining and Machine Learning in Cybersecurity*. Auerbach Publications (2016)
8. Yin, C., Zhu, Y., Fei, J., He, X.: A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access* **5**, 21954–21961 (2017)
9. Xiao, L., Wan, X., Lu, X., Zhang, Y., Wu, D.: IoT security techniques based on machine learning (2018). *arXiv Prepr.* [arXiv:1801.06275](https://arxiv.org/abs/1801.06275)
10. Jordan, M.I., Mitchell, T.M.: Machine learning: Trends, perspectives, and prospects. *Science (80-.)* **349**(6245), 255–260 (2015)
11. Fraley, J.B., Cannady, J.: The promise of machine learning in cybersecurity. *SoutheastCon* **2017**, 1–6 (2017)
12. Alazab, M., Tang, M.: *Deep Learning Applications for Cyber Security*. Springer, Heidelberg (2019)
13. Li, J.: Cyber security meets artificial intelligence: a survey. *Front. Inf. Technol. Electron. Eng.* **19**(12), 1462–1474 (2018)
14. Jones, C.L., Bridges, R.A., Huffer, K.M.T., Goodall, J.R.: Towards a relation extraction framework for cyber-security concepts. In: *Proceedings of the 10th Annual Cyber and Information Security Research Conference*, p. 11 (2015)
15. McNeil, N., Bridges, R.A., Iannacone, M.D., Czejdo, B., Perez, N., Goodall, J.R.: Pace: pattern accurate computationally efficient bootstrapping for timely discovery of cyber-security concepts. In: *2013 12th International Conference on Machine Learning and Applications*, vol. 2, pp. 60–65 (2013)
16. Zhang, Q., Man, D., Yang, W.: Using HMM for intent recognition in cyber security situation awareness. In: *2009 Second International Symposium on Knowledge Acquisition and Modeling*, vol. 2, pp. 166–169 (2009)

17. Bonaci, T., Herron, J., Yusuf, T., Yan, J., Kohno, T., Chizeck, H.J.: To make a robot secure: an experimental analysis of cyber security threats against teleoperated surgical robots (2015). arXiv Prepr. [arXiv:1504.04339](https://arxiv.org/abs/1504.04339)
18. Hacıoglu, U., Sevgilioglu, G.: The evolving role of automated systems and its cyber-security issue for global business operations in Industry 4.0. *Int. J. Bus. Ecosyst. Strategy* **1**(1), 1–11 (2019)
19. Alhashmi, S.F.S., Salloum, S.A., Abdallah, S.: Critical success factors for implementing artificial intelligence (AI) projects in Dubai government United Arab Emirates (UAE) health sector: applying the extended technology acceptance model (TAM). In: *International Conference on Advanced Intelligent Systems and Informatics*, pp. 393–405 (2019)
20. Darwish, A., Ezzat, D., Hassanien, A.E.: An optimized model based on convolutional neural networks and orthogonal learning particle swarm optimization algorithm for plant diseases diagnosis. *Swarm Evol. Comput.* **52**, 100616 (2020)
21. Abdelghafar, S., Darwish, A., Hassanien, A.E.: Intelligent health monitoring systems for space missions based on data mining techniques. In: *Machine Learning and Data Mining in Aerospace Technology*, pp. 65–78. Springer (2020)
22. Elsayad, D., Ali, A., Shedeed, H.A., Tolba, M.F.: PAGeneRN: parallel architecture for gene regulatory network. In: *Data Analytics in Medicine: Concepts, Methodologies, Tools, and Applications*, pp. 1052–1075. IGI Global (2020)
23. Pacheco, A.G.C., Ali, A.-R., Trappenberg, T.: Skin cancer detection based on deep learning and entropy to detect outlier samples (2019). arXiv Prepr. [arXiv:1909.04525](https://arxiv.org/abs/1909.04525)
24. Salloum, S.A., Al-Emran, M., Monem, A., Shaalan, K.: A survey of text mining in social media: facebook and twitter perspectives. *Adv. Sci. Technol. Eng. Syst. J.* **2**(1), 127–133 (2017)
25. Alomari, K.M., AlHamad, A.Q., Salloum, S.: Prediction of the digital game rating systems based on the ESRB. *Opción* **35**(19), 1368–1393 (2019)
26. Salloum, S.A., Al-Emran, M., Shaalan, K.: Mining social media text: extracting knowledge from facebook. *Int. J. Comput. Digit. Syst.* **6**(2), 73–81 (2017)
27. Salloum, S.A., Al-Emran, M., Abdallah, S., Shaalan, K.: Analyzing the Arab Gulf newspapers using text mining techniques. In: *International Conference on Advanced Intelligent Systems and Informatics*, pp. 396–405 (2017)
28. Salloum, S.A., Al-Emran, M., Shaalan, K.: Mining text in news channels: a case study from facebook. *Int. J. Inf. Technol. Lang. Stud.* **1**(1), 1–9 (2017)
29. Salloum, S.A., AlHamad, A.Q., Al-Emran, M., Shaalan, K.: A survey of Arabic text mining, vol. 740 (2018)
30. Salloum, S.A., Mhamdi, C., Al-Emran, M., Shaalan, K.: Analysis and classification of Arabic newspapers' facebook pages using text mining techniques. *Int. J. Inf. Technol. Lang. Stud.* **1**(2), 8–17 (2017)
31. Amodei, D., Olah, C., Steinhardt, J., Christiano, P., Schulman, J., Mané, D.: Concrete problems in AI safety (2016). arXiv Prepr. [arXiv:1606.06565](https://arxiv.org/abs/1606.06565)
32. Papernot, N., McDaniel, P., Sinha, A., Wellman, M.: Towards the science of security and privacy in machine learning (2016). arXiv Prepr. [arXiv:1611.03814](https://arxiv.org/abs/1611.03814)
33. Feily, M., Shahrestani, A., Ramadass, S.: A survey of botnet and botnet detection. In: *2009 Third International Conference on Emerging Security Information, Systems and Technologies*, pp. 268–273 (2009)
34. Ben Salem, M., Hershkop, S., Stolfo, S.J.: A survey of insider attack detection research. In: *Insider Attack and Cyber Security*, pp. 69–90. Springer (2008)
35. Bhamare, D., Salman, T., Samaka, M., Erbad, A., Jain, R.: Feasibility of supervised machine learning for cloud security. In: *2016 International Conference on Information Science and Security (ICISS)*, pp. 1–5 (2016)



36. Gallagher, B., Eliassi-Rad, T.: Classification of http attacks: a study on the ECML/PKDD 2007 discovery challenge. Lawrence Livermore National Lab. (LLNL), Livermore, CA (United States) (2009)
37. Haddadi, F., Le Cong, D., Porter, L., Zincir-Heywood, A.N.: On the effectiveness of different botnet detection approaches. In: International Conference on Information Security Practice and Experience, pp. 121–135 (2015)
38. Xie, M., Hu, J., Slay, J.: Evaluating host-based anomaly detection systems: application of the one-class SVM algorithm to ADFA-LD. In: 2014 11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), pp. 978–982 (2014)
39. Kato, K., Klyuev, V.: An intelligent DDoS attack detection system using packet analysis and support vector machine. In: IJICR, pp. 478–485 (2014)
40. Yusof, A.R., Udzir, N.I., Selamat, A.: An evaluation on KNN-SVM algorithm for detection and prediction of DDoS attack. In: International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems, pp. 95–102 (2016)
41. Hasan, M.A.M., Nasser, M., Ahmad, S., Molla, K.I.: Feature selection for intrusion detection using random forest. *J. Inf. Secur.* **7**(03), 129 (2016)
42. Javaid, A., Niyaz, Q., Sun, W., Alam, M.: A deep learning approach for network intrusion detection system. In: Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS), pp. 21–26 (2016)
43. Tang, T.A., Mhamdi, L., McLernon, D., Zaidi, S.A.R., Ghogho, M.: Deep learning approach for network intrusion detection in software defined networking. In: 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), pp. 258–263 (2016)
44. Chowdhury, S., et al.: Botnet detection using graph-based feature clustering. *J. Big Data* **4**(1), 14 (2017)
45. Neethu, B.: Adaptive intrusion detection using machine learning. *Int. J. Comput. Sci. Netw. Secur.* **13**(3), 118 (2013)
46. Kozik, R., Choraś, M., Renk, R., Hołubowicz, W.: A proposal of algorithm for web applications cyber attack detection. In: IFIP International Conference on Computer Information Systems and Industrial Management, pp. 680–687 (2015)
47. Lippmann, R., Haines, J.W., Fried, D.J., Korba, J., Das, K.: The 1999 DARPA off-line intrusion detection evaluation. *Comput. Netw.* **34**(4), 579–595 (2000)
48. Saad, S., et al.: Detecting P2P botnets through network behavior analysis and machine learning. In: 2011 Ninth Annual International Conference on Privacy, Security and Trust, pp. 174–180 (2011)
49. Torrano-Gimenez, C., Perez-Villegas, A., Alvarez, G.: A self-learning anomaly-based web application firewall. In: Computational Intelligence in Security for Information Systems, pp. 85–92. Springer (2009)
50. Torrano-Gimenez, C., Pérez-Villegas, A., Álvarez, G., Fernández-Medina, E., Malek, M., Hernando, J.: An anomaly-based web application firewall. In: SECRIPT, pp. 23–28 (2009)
51. Nguyen, H.T., Torrano-Gimenez, C., Alvarez, G., Petrović, S., Franke, K.: Application of the generic feature selection measure in detection of web attacks. In: Computational Intelligence in Security for Information Systems, pp. 25–32. Springer (2011)
52. Hoque, N., Bhattacharyya, D.K., Kalita, J.K.: A novel measure for low-rate and high-rate DDoS attack detection using multivariate data analysis. In: 2016 8th International Conference on Communication Systems and Networks (COMSNETS), pp. 1–2 (2016)
53. Torrano-Giménez, C., Perez-Villegas, A., Alvarez Marañón, G.: An anomaly-based approach for intrusion detection in web traffic (2010)