Cyber Intrusion Detection Using Machine Learning Classification Techniques

Chapter *in* Communications in Computer and Information Science · July 2020

DOI: 10.1007/978-981-15-6648-6_10

6 authors, including:

Hamed Alqahtani
Macquarie University
35 PUBLICATIONS **1,390** CITATIONS
SEE PROFILE

Iqbal H. Sarker
Edith Cowan University
235 PUBLICATIONS **11,245** CITATIONS
SEE PROFILE

Asra Kalim
Jazan University
12 PUBLICATIONS **230** CITATIONS
SEE PROFILE

Syed Mohammod Minhaz Hossain
Premier University
32 PUBLICATIONS **370** CITATIONS
SEE PROFILE

Cyber Intrusion Detection Using Machine Learning Classification Techniques

Hamed Alqahtani[1,7], Iqbal H. Sarker[2(✉)], Asra Kalim[3], Syed Md. Minhaz Hossain[2,4], Sheikh Ikhlaq[5], and Sohrab Hossain[2,6(✉)]

[1] King Khalid University, Abha, Saudi Arabia
[2] Chittagong University of Engineering and Technology, Chittagong, Bangladesh
iqbal@cuet.ac.bd
[3] Jazan University, Jizan, Saudi Arabia
[4] Premier University, Chittagong, Bangladesh
[5] Accenture Solutions Private Limited, Mumbai, India
[6] East Delta University, Chittagong, Bangladesh
sohrab.h@eastdelta.edu.bd
[7] Macquarie University, Sydney 2109, Australia

Abstract. As the alarming growth of connectivity of computers and the significant number of computer-related applications increase in recent years, the challenge of fulfilling cyber-security is increasing consistently. It also needs a proper protection system for numerous *cyberattacks*. Thus, detecting inconsistency and attacks in a computer network and developing *intrusion detection system* (IDS) that performs a potential role for cyber-security. Artificial intelligence, particularly *machine learning techniques*, has been used to develop a useful data-driven intrusion detection system. In this paper, we employ various popular machine learning classification algorithms, namely Bayesian Network, Naive Bayes classifier, Decision Tree, Random Decision Forest, Random Tree, Decision Table, and Artificial Neural Network, to detect intrusions due to provide intelligent services in the domain of cyber-security. Finally, we test the effectiveness of various experiments on cyber-security datasets having several categories of cyber-attacks and evaluate the effectiveness of the performance metrics, precision, recall, f1-score, and accuracy.

Keywords: Cybersecurity · Cyber-attacks · Intrusions · Intrusion detection system · Machine learning · Classification · Cyber-attack prediction · Artificial intelligence · Cybersecurity analytics

1 Introduction

In recent days, cyber-security and protection against numerous *cyber-attacks* are becoming a burning question. The main reason behind that is the tremendous growth of computer networks and the vast number of relevant applications used by individuals or groups for either personal or commercial use, specially after the acceptance of Internet-of-Things (IoT). The cyber-attacks cause severe damage and severe financial losses in

N. Chaubey et al. (Eds.): COMS2 2020, CCIS 1235, pp. 121–131, 2020.
https://doi.org/10.1007/978-981-15-6648-6_10

large-scale networks [25]. The existing solutions like hardware and software firewalls, user's authentication, and data encryption method are not sufficient to meet the challenge of upcoming demand, and unfortunately, not able to protect the computer network's several cyber-threats. These conventional security structures are not sufficient as safeguard due to the faster rigorous evolution of intrusion systems [13, 26, 27]. Firewall only controls every accesses from network to network, which means prevent access between networks. But it does not provide any signal in case of an internal attack. So, it is obvious to develop accurate defense techniques such as *machine learning-based intrusion detection system (IDS)* for the system's security.

In general, an intrusion detection system (IDS) is a system or software that detects infectious activities and violations of policy in a network or system. An IDS identifies the inconsistencies and abnormal behavior on a network during the functioning of daily activities in a network or system used to detect risks or attacks related to network security, like denial-of-service (DoS). An intrusion detection system also helps to locate, decide, and control unauthorized system behavior such as unauthorized access, or modification and destruction [12, 31]. There are different types of intrusion detection systems based on the user perspective. For instance, they are host-based and network-based IDS [25].

These are in the scope of single computers to large networks some extend. In a host-based intrusion detection system (HIDS), it lies on an individual system and keeps track of operating system files for inconsistency and abnormalities in the activity. In contrast, the network intrusion detection system (NIDS) investigates and scans connections in the network for unwanted traffic. On the other hand, there are two approaches based on detection, one is signature-based, and another one is anomaly-based detection [25, 18]. Signature-based IDS explores the byte patterns in the path of the network. One can treat it as malicious instruction sequences used by malware. It arises from antivirus software referred to the groups or patterns as signatures detected in it. Signature-based IDS cannot detect attacks, for which there is no pattern available before. An anomaly-based IDS, it examines the behavior of the network and finds patterns, automatically creates a data-driven model for profiling the expected behavior, and thus detects deviations in the case of any anomalies [18]. The merit of this anomaly-based IDS is to trace current, latest, and unseen inconsistencies or cyber-attacks like denial-of-services.

For developing computational methods to identify various cyber-attacks, it needs to analyze different incident patterns, and eventually predict the threats utilizing cyber-security data. It is known as a data-driven intelligent intrusion detection system [25]. To build a data-driven intrusion detection model, the knowledge of artificial intelligence, particularly *machine learning* techniques, is essential. However, the prediction of cyber-attacks using machine learning algorithms is problematic due to the several identifications of multiple classifiers results in different contexts depending on data characteristics [23]. For this reason, we analyze several machine learning algorithms on intrusion detection systems for utilizing cyber-security data. For this purpose, we employ various popular machine learning classification techniques, such as Bayesian Network (BN), Naive Bayes (NB), Random Forest (RF), Decision Tree (DT), Random Tree (RT), Decision Table (DTb), and Artificial Neural Network (ANN), for providing intelligent services in the domain of cyber-security, particularly for intrusion detection. Finally, the effectiveness is tested by conducting numerous experiments on

cyber-security datasets consisting of several categories of cyberattacks, and evaluates the effectiveness by measuring the performance metrics precision, recall, f1-score, and accuracy for these machine learning-based IDS models.

The remaining part of the paper arranges as follows. Section 2 depicts background and related works. Data-driven intrusion detection modeling is incorporated in Sect. 3. Section 4 presents experimental analysis and results followed by the conclusion in Sect. 5.

2 Background and Related Work

In this section, we first define cyber-security, represents the systems or software of protection of data, program, connections among computers from several unwanted attacks such as unauthorized attacks, modification, fabrication [2]. As conventional security systems are not enough for detecting network security [13, 26, 27], we focus on developing an *intrusion detection system (IDS)* to explore and detect the system's security.

Intrusion defines as an unauthorized activity that causes damage to an information system [10]. That means any attack that could pose a possible threat to information confidentiality, integrity, or availability is considered an intrusion. Presently firewalls, access control, and cryptography are the main defensive mechanisms deployed against intrusions used for detecting internal attacks [5]. However, intrusion detection systems are used for detecting internal as well as external attacks. Despite detecting known attacks on signature-based IDS discussed above, in this work, we aim to focus on an anomaly-based intrusion detection model [10].

An anomaly is a state of deviation from familiarized behavior. Profiles are the general or wanted behaviors extracted from tracking activities of users, network connections, and hosts during a fixed time [11]. Anomaly-based intrusion detection model is also called the behavior-based model and represented as a dynamic approach [11]. The fundamental merit of an anomaly-based intrusion detection model is to detect zero-day attacks because it is not reliable to acknowledge the unwanted users' activity in the signature database [3]. Further, another technique exists, and it is a hybrid detection [28] technique or protocol analysis [11] detection techniques. The hybrid technique has the advantage of a high detection rate in the misuse detection and high potentiality of inconsistency detectors in recognizing the latest attacks. It expands the rate of detection of previously known intrusions and to decrease the false-positive rate of undefined attacks [31]. This work focuses on an intrusion detection model constructed in machine learning techniques utilizing cyber-security data.

Machine learning uses to make decision using computers [8, 29]. It is a part of artificial intelligence and further related to computational statistics. Classification refers to supervised learning that predicts the cyber-attack class labels of samples from training security data [8, 23]. Thus, we analyze various popular classification techniques that include Bayesian approach [17, 22], Tree-based model [14, 20, 24, 18], Artificial Neural Network based model [23] that are used frequently in predictive analytics [8, 16, 29, 30], to develop a fruitful data-driven IDS predictive model for providing intelligent services of cyber security.

In this paper, we employ various popular machine learning classification techniques, such as Bayesian Network (BN), Naive Bayes (NB), Random Forest (RF), Decision Tree

(DT), Random Tree (RT), Decision Table (DTb), and Artificial Neural Network (ANN) for classifying cyber-attacks and make a comparative analysis with experiments.

3 Data-Driven IDS Modeling

This section presents our data-driven IDS model of numerous machine learning techniques. It incorporates several steps: dataset exploration, data processing, and machine learning-based security modeling. It has been discussed these steps chronologically, as below.

3.1 Dataset Exploration and Preprocessing

Datasets represent a collection of information records that consist of several attributes or features and related facts related to the cyber-security model [25]. So, it is essential to realize the nature of cyber-security data containing various types of cyber-attacks and relevant features. The reason is that raw security data collected from relevant cyber sources could be used to analyze the various patterns of security incidents or malicious behavior, to build a data-driven security model to achieve our goal. In this work, KDD'99 cup data has been used [1] to develop predictive models for differentiating the relationship between intrusions or several attacks. This dataset contains 4898431 instances with 41 attributes. In Table 1, we have shown the features of KDD'99 cup datasets [1]. In this dataset, attacks are classified into four main groups:

- DoS: Denial of service (DoS) is a kind of attack in which a legitimate user does not have access to the system and network resources. Online banking services, email may be affected. DoS attacks comprise of the SYN flood attack and the Smurf attack.
- R2L: Remote to Local (R2L) is an attack where an attacker tries to gain access to the victim machine without having an account in it.
- U2R: User to Root (U2R) is an attack where an attacker tries to gain privileges having local access in the victim machine.
- PROBE: In Probe, the attacker targets the host and tries to get information about the host.

We first prepare the dataset, including these attack categories and available attributes for developing machine learning-based IDS models. There are four types of features used in this dataset; they are Basic features, Content Features, Time-based Traffic Features, and Host-based Traffic Features. Feature-based attributes are extracted from TCP/IP connections. Traffic features are computed by window interval. It divides into two groups; one is 'same host features' and another one is 'same service features.' They are both called time-based features. Sometimes, in the case of probing, there is a slower scan than 2 s. To solve this problem, 'same host features' and 'same service features' are recomputed by the connection window. Then it is called connection based features. DoS and probing may have several connections to a host/s during a period. In Table 2, we have summarized these categories of attacks. In contrast to that, Root to Local (R2L) and User to Root (U2R) attacks generally require a single connection. Content-based features

have been used to detect these attacks. Then process these features according to the requirements and design the target machine learning-based IDS model. This data-driven pattern-based decision analysis plays a useful role in providing data-driven intelligent cyber-security services.

3.2 Machine Learning Classification Based Modeling

Classification is a supervised learning technique and popularly used to model cyber intrusions based on multi-category of attacks. In supervised learning, data is always labeled previously. In the training phase, the classifier learns the labels so that in the test phase, it can predict correctly for unseen data. In our analysis, we implement the popular machine learning techniques used for various purposes. Several techniques summarize as below:

- *Bayesian Network and Naive Bayes:* A Bayesian Network, breaks up a probability distribution based on the conditional independencies, while Bayesian inference is used to infer a marginal distribution given some observed evidence [29]. Bayesian Network is used to detect, diagnose, and reasoning. Naive Bayes is a kind of Bayesian network and is a commonly used machine learning algorithm. [9]. It is a basic probabilistic based technique that calculates the probability to classify or predict the cyber-attack class in a given dataset. This method assumes each feature's value as independent and considers the correlation or relationship between the features [8]. Naive Bayes includes two probabilities; one is the conditional probability, and another one is class probability. Class probability is determined by dividing the frequency of each class instance by total instances. Conditional probability is the ratio of the occurrence of each attribute for a given class, and the occurrence of samples for that class. Naive Bayes is faster than other classifiers.
- *Decision Tree and Decision Table:* Decision tree is one of the most popular classification and prediction algorithms in machine learning [14, 23]. ID3 proposed by J. R. Quinlan [14] is a common top-down approach for building decision trees. Based on this, the C4.5 algorithm [15], and later BehavDT approach [20], IntruDTree model [18] have been constructed to generate the decision trees. Decision Tree is a tree-like structure, in which an internal node represents attributes, and branches represent the outcome, and leaf represents a class label. These algorithms generate decision rules to predict the outcome for unseen test cases. These algorithms provide high accuracy and better interpretation. The Decision Tree can work with both continuous and discrete data. A Decision Table illustrates the complex decision rules representing a tabular form consists of rows and columns [8, 29].
- *Random Forest and Random Tree:* Random Forest is a classifier comprising of decision trees operated as an ensemble learning [7]. Breiman et al. propose it. The reason is that it combines both the different set of data called bootstrap aggregation [6] and also numerous features selection [4], to predict the outcome. Similarly, Random Trees are essentially the combination of single model trees with Random Forest ideas, where each node contains k randomly chosen attributes in tree [29]. So, it increases the accuracy of Random Forest than that of a single tree.

Table 1. An example of features of KDD'99 cup dataset.

No.	Features	Types	No.	Features	Types
1	duration	Continuous	22	is_guest_login	Symbolic
2	protocal_type	Symbolic	23	count	Continuous
3	service	Symbolic	24	srv_count	Continuous
4	flag	Symbolic	25	serror_rate	Continuous
5	stc_bytes	Continuous	*26*	srv_serror_rate	Continuous
6	dst_bytes	Continuous	*27*	rerror_rate	Continuous
7	Land	Symbolic	28	srv_rerror_rate	Continuous
8	wrong_fragment	Continuous	*29*	same_srv_rate	Continuous
9	urgent	Continuous	30	diff_srv_rate	Continuous
10	hot	Continuous	31	drv_diff_host_rate	Continuous
11	num_failed_logins	Continuous	32	dst_host_count	Continuous
12	logged_in	Symbolic	33	dst_host_srv_count	Continuous
13	num_compromised	Continuous	34	dst_host_same_srv_rate	Continuous
14	root_shell	Continuous	35	dst_host_diff_srv_rate	Continuous
15	su_attempted	Continuous	36	dst_host_same_src_port_rate	Continuous
16	num_root	Continuous	37	dct_host_srv_diff_host_rate	Continuous
17	num_file_creations	Continuous	38	dst_host_serror_rate	Continuous
18	num_shells	Continuous	39	dst_host_srv_serror_rate	Continuous
19	num_access_files	Continuous	40	dst_host_rerror_rate	Continuous
20	num_outbound_cmds	Continuous	41	dst_bost_srv_rerror_rate	Continuous
21	is_host_login	Symbolic			

– *Artificial Neural Network:* In addition to the above classical machine learning techniques, we also take into account a neural network learning model. The most commonly used form of neural network architecture is the Multilayer Perceptron that has an input layer consisting of several inputs, one or more hidden layers that typically use sigmoid activation functions and one output layer to predict the attack. This approach uses backpropagation to build the network [8, 29].

We discuss our machine learning-based intrusion detection model that carries out on four main components:

– *Attack Class Label:* All the diverse threats have been counted as different distinct class labels to put them into model intrusion detection systems. For instance, different types of attacks such as DoS, U2R, R2L, PROBE shown in Table 2 are represented as distinct classes; Class 1, Class 2, Class 3, and Class 4 respectively.

Table 2. Various types of attacks in KDD'99 cup dataset.

Categories of attack	Attack name	Number of instances
DOS	SMURF	2807886
	NEPTUNE	1072017
	Back	2203
	POD	264
	Teardrop	979
U2R	Buffer Overflow	30
	Load Module	9
	PERL	3
	Rootkit	10
R2L	FTP Write	8
	Guess Password	53
	IMAP	12
	MultiHop	7
	PHF	4
	SPY	2
	Warez client	1020
	Warez Master	20
PROBE	IPSWEEP	12481
	NMAP	2316
	PORTSWEEP	10413
	SATAN	15892
normal		972781

– *Security Features or Attributes:* These are used independently to predict the above cyber threats. These are also known as features such as protocol type, service, duration, and error-rate. shown in Table 1, on which the cyberattacks class levels are dependent.
– *Training and Testing Dataset:* The dataset is categorized into two; one is a training dataset, and another one is the test dataset. The training data set is used to train the IDS model, and the testing dataset is used to evaluate the generalization of that IDS model. We use a large amount of the cybersecurity data mentioned above for developing the IDS model and the rest for testing purposes.

4 Experimental Evaluation

This section defines the performance metrics in terms of intrusion detection and discusses the outcome by conducting experiments on cybersecurity datasets with different

categories of attacks. If TP denotes true positives, FP denotes false positives, TN denotes true negative, and FN denotes false negatives, then the formal definition of below metrics are [30]:

$$Precision = \frac{TP}{TP + FP} \tag{1}$$

$$Recall = \frac{TP}{TP + FN} \tag{2}$$

$$Fscore = 2 * \frac{Precision * Recall}{Precision + Recall} \tag{3}$$

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{4}$$

4.1 Experimental Results and Discussion

In the section, we show the effectiveness of machine learning classification techniques for detecting intrusions. For this, we analyze various popular classification techniques that include the Bayesian approach, tree-based model, Artificial Neural Network in our IDS model. Notably, we have compared the effectiveness of several popular classification techniques, such as Bayesian Network (BN), Naive Bayes (NB), Random Forest (RF), Decision Tree (DT), Random Tree (RT), Decision Table (DTb), and Artificial Neural Network (ANN), to evaluate the intrusion detection model. To test the IDS model, we use the 10-fold cross-validation on the dataset. 10-fold cross-validation evaluates models by breaking the data into ten different sets of samples. From them, nine partitioned sets are trained, and the remaining one is tested. It continues ten times and then takes the average accuracy. To compare the potentiality of models, precision, recall, f1-score, and accuracy, are calculated as defined above.

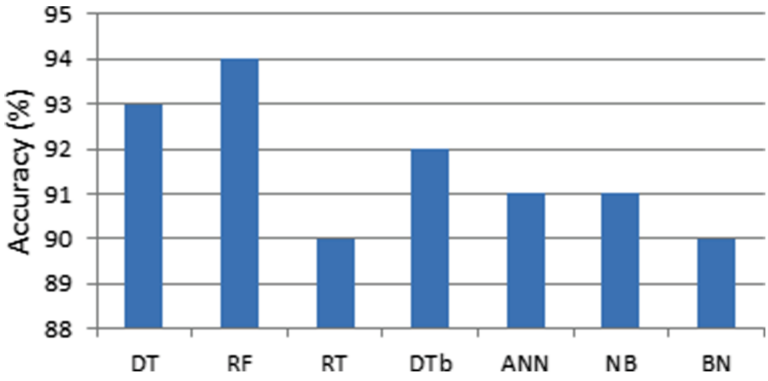

Fig. 1. Performance comparison results with respect to accuracy for numerous machine learning based IDS model.

To evaluate the performances of each classifier based IDS model, Fig. 1 and Fig. 2 show the comparison of accuracy, precision, recall, and f1-score, respectively. For evaluation, we use the same set of train and testing data in each classification based IDS model.

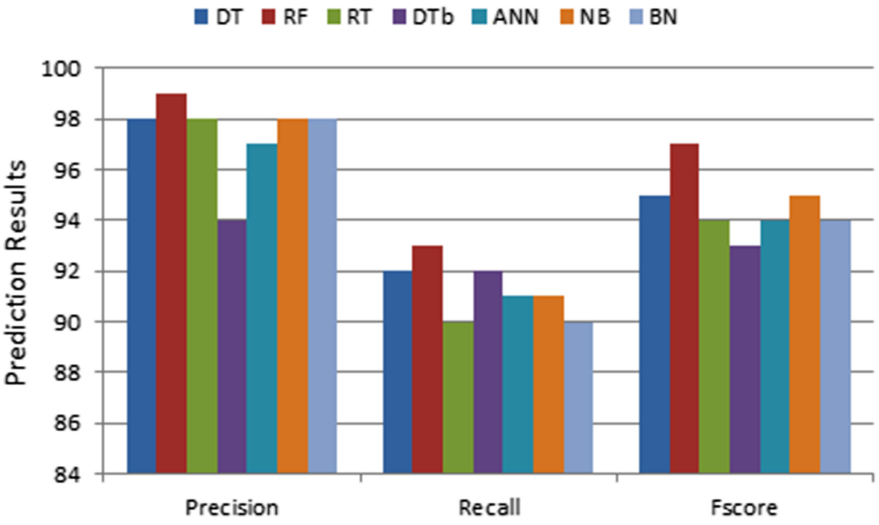

Fig. 2. Performance comparison results with respect to precision, recall, f1-score for numerous machine learning classification based IDS model.

From Fig. 1 and Fig. 2, we find that Random Forest classifier based IDS model consistently performs better than other classifiers for detecting intrusions. In particular, the Random Decision Forest gives the best results concerning the accuracy, precision, recall, f1-score. The reason behind it is that the Random Forest classifier at first originates several decision trees and thus deduces a set of rules in the forest. Every tree in a Random Forest Model behaves as a different machine learning classification technique, and thus it generates more logic rules by taking into account the majority voting of these trees while producing the outcome. For this reason, the Random Forest Model performs better in precision, recall, f1-score, and accuracy. Overall, the machine learning classifier based IDS model discussed above is fully data-oriented that reflects the behavioral patterns of various cyber-attacks. Although we consider data-driven prediction according to the patterns available in a given dataset using machine learning techniques, a recency-based model [19] could be more effective in developing a data-driven intrusion detection system. Moreover, incorporating contextual information and their analysis [21, 16] could play an important role to build smart intrusion detection system.

5 Conclusion and Future Work

The potentiality and fruitfulness of a machine learning-based intrusion detection modeling is a great concern for IT personals, e-commerce, and application developers for

security purposes. Generally, a cyber-security data set consists of different categories of cyber attacks with relevant features. Hence, some classifiers may not perform well in terms of accuracy and their actual prediction rate based on diverse categories of attacks and a variety of features. In this paper, we have discussed the effectiveness of the data-driven intrusion detection model by taking into account popular classification techniques in machine learning. We have evaluated various performance metrics like precision, recall, f1-score, and overall accuracy. In the future, we extend the cyber-security datasets and have a plan to design a data-driven intrusion detection system for providing automated security services for the cyber-security community.

References

1. Kdd cup 99. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. Accessed 20 Oct 2019
2. Aftergood, S.: Cybersecurity: the cold war online. Nature **547**(7661), 30 (2017)
3. Ammar, A., Michael, H., Jemal, A., Moutaz, A.: Using feature selection for intrusion detection system. In: 2012 International Symposium on Communications and Information Technologies (ISCIT), pp. 296–301. IEEE (2012)
4. Amit, Y., Geman, D.: Shape quantization and recognition with randomized trees. Neural Comput. **9**(7), 1545–1588 (1997)
5. Shahid, A., et al.: From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions. Algorithms, **10**(2), 39 (2017)
6. Breiman, L.: Bagging predictors. Mach. Learn. **24**(2), 123–140 (1996)
7. Breiman, L.: Random forests. Mach. Learn. **45**(1), 5–32 (2001)
8. Han, J., Pei, J., Kamber, M.: Data Mining: Concepts and Techniques. Elsevier, Amsterdam (2011)
9. John, G.H., Langley, P.: Estimating continuous distributions in bayesian classifiers. In: Proceedings of the Eleventh Conference on Uncertainty in Artificial Intelligence, pp. 338–345. Morgan Kaufmann Publishers Inc. (1995)
10. Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J.: Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity **2**(1), 20 (2019)
11. Liao, H.-J., Lin, C.-H.R., Lin, Y.-C., Tung, K.-Y.: Intrusion detection system: a comprehensive review. J. Netw. Comput. Appl. **36**(1), 16–24 (2013)
12. Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A., Payne, B.D.: Evaluating computer intrusion detection systems: a survey of common practices. ACM Comput. Surv. (CSUR) **48**(1), 1–41 (2015)
13. Mohammadi, S., Mirvaziri, H., Ghazizadeh-Ahsaee, M., Karimipour, H.: Cyber intrusion detection by combined feature selection algorithm. J. Inf. Secur. Appl. **44**, 80–88 (2019)
14. Quinlan, J.R.: Induction of decision trees. Mach. Learn. **1**(1), 81–106 (1986)
15. Quinlan, J.R.: C4.5: programs for machine learning. Machine Learning (1993)
16. Sarker, I.H.: Context-aware rule learning from smartphone data: survey, challenges and future directions. J. Big Data **6**(1), 1–25 (2019). https://doi.org/10.1186/s40537-019-0258-4
17. Sarker, I.H.: A machine learning based robust prediction model for real-life mobile phone data. Internet of Things **5**, 180–193 (2019)
18. Sarker, I.H., Abushark, Y.B., Alsolami, F., Khan, A.I.: Intrudtree: a machine learning-based cyber security intrusion detection model. Symmetry **12**, 754 (2020)
19. Sarker, I.H., Colman, A., Han, J.: Recencyminer: mining recency-based personalized behavior from contextual smartphone data. J. Big Data **6**(1), 49 (2019)

20. Sarker, I.H., Colman, A., Han, J., Khan, A.I., Abushark, Y.B., Salah, K.: Behavdt: a behavioral decision tree learning to build user-centric context-aware predictive model. Mobile Netw. Appl. **1**, 1–11 (2019)
21. Sarker, I.H., Colman, A., Kabir, M.A., Han, J.: Individualized time-series segmentation for mining mobile phone user behavior. The Comput. J., **61**(3), 349–368 (2018). Oxford University, UK
22. Sarker, I.H., Kabir, M.A., Colman, A., Han, J.: An improved naive bayes classifier-based noise detection technique for classifying user phone call behavior (2017)
23. Sarker, I.H., Kayes, A., Watters, P.: Effectiveness analysis of machine learning classification models for predicting personalized context-aware smartphone usage. Journal of Big Data (2019)
24. Sarker, I.H., Salim, F.D.: Mining user behavioral rules from smartphone data through association analysis. In: Phung, D., Tseng, V.S., Webb, G.I., Ho, B., Ganji, M., Rashidi, L. (eds.) PAKDD 2018. LNCS (LNAI), vol. 10937, pp. 450–461. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-93034-3_36
25. Sarker, I.H., et al.: Cybersecurity data science: an overview from machine learning perspective (2020)
26. Tapiador, J.E., Orfila, A., Ribagorda, A., Ramos, B.: Keyrecovery attacks on kids, a keyed anomaly detection system. IEEE Trans. Dependable Sec. Comput. **12**(3), 312–325 (2013)
27. Tavallaee, M., Stakhanova, N., Ghorbani, A.A.: Toward credible evaluation of anomaly-based intrusion-detection methods. IEEE Trans. Syst. Man Cybern. Part C (Applications and Reviews), **40**(5), 516–524 (2010)
28. Viegas, E., Santin, A.O., Franca, A., Jasinski, R., Pedroni, V.A., Oliveira, L.S.: Towards an energy-efficient anomaly-based intrusion detection engine for embedded systems. IEEE Trans. Comput. **66**(1), 163–177 (2016)
29. Witten, I.H., Frank, E.: Data Mining: Practical Machine Learning Tools and Techniques. Morgan Kaufmann, Burlington (2005)
30. Witten, I.H., Frank, E., Trigg, L.E., Hall, M.A., Holmes, G., Cunningham, S.J.: Weka: practical machine learning tools and techniques with java implementations (1999)
31. Xin, Y., et al.: Machine learning and deep learning methods for cybersecurity. IEEE Access **6**, 35365–35381 (2018)