Attribute Ratio. Attribute Ratio (AR) method is a filter technique for feature selection. It is calculated by features frequency or average (Avg). Before calculating AR, we need to calculate the class ratio (CR). CR defines the ratio of each class for attribute i. CR is calculated through two methods according to the type of attributes [148, 149]. The AR feature selection formula is as follows :

$$AR(i) = MAX(CR(y)) \tag{4}$$

Here, CR represents the class ratio. For numeric attributes, the CR is calculated as follows :

$$CR(y) = \frac{Avg(C(y))}{AVG(total)} \tag{5}$$

For binary attributes, the CR is calculated as follows :

$$CR(y) = \frac{Frequency(1)}{Frequency(0)} \tag{6}$$

Genetic Algorithm. The Genetic algorithm (GA) is a heuristic algorithm inspired from the natural selection, where fitter creatures survive and their genes are simulated. The GA starts with a random population of individuals and improves the population using three operators: selection, crossover, and mutation. The best solution in the last population is returned as the best global optimum approximation for a given problem. This algorithm evaluates each individual fitness in the population using a fitness function. It associates probabilities to individuals and select them with a selection mechanism for creating the next generation proportional to their fitness values. The selection operator is able to choose the best solution since the probability is proportional to the fitness. There are many selection techniques used to choose the best solution such as the fuzzy selection, the fitness uniform selection [150], the proportional selection [147], the linear rank selection [147], and the steady-state reproduction [151]. The GA algorithm uses the crossover and mutation operators that simulate the biological process for introducing diversity to the population. With the crossover operator two solutions selected randomly are combined to produce two new solutions. There are different techniques for this operator notably the single point and double point techniques [152]. The mutation operator prevents solutions from becoming similar and increases avoiding local solutions probability. There are many techniques in the literature for the mutation operator such as the power mutation, Uniform [153], Gussian [154], shrink [155], supervised mutation [156], uniqueness mutation [157], and varying probability mutation [158–160].

Binary Particle Swarm Optimization. Binary Particle Swarm Optimization (BPSO) is a wrapper method. The PSO technique is a population-based algorithm, where each individual in a population corresponds to a particle. Each particle represents a candidate solution to the problem at hand. Particles change their positions by flying around in a multidimensional search space until a relatively unchanged position has been found, or until computational limitations are exceeded. Each particle has its fitness evaluated by a fitness function. A particle fitness value is called a personal best *pbest* solution achieved so far. The particle, which has the best solution among all *pbest*, is called the global best particle *gbest* [161, 162]. A particle velocity and position update can be described as follows :

$$\begin{aligned} v_i^d(t+1) = v_i^d(t) + c_1 r_1 * (pbest_i^d(t) - x_i^d(t)) \\ + c_2 r_2 * (gbest^d(t) - x_i^d(t)) \end{aligned} \tag{7}$$

$$x_i^d(t+1) = x_i^d(t) + v_i^d(t+1) \tag{8}$$

Here, d is the particle dimension, t is the iteration, $r1$ and $r2$ are random number in the interval $(0, 1)$, and $c1$ and $c2$ are positive acceleration constants.

An improved Binary Particle Swarm Optimization:. An Improved Binary Particle Swarm Optimization technique (IBPSO) is a solution proposed to improve the BPSO technique. This IBPSO technique aims to prevent particles from getting trapped in a local optimum by introducing a boolean algebra operation. In fact, it assumes that the particles have fallen into the local optimum when the *gbest* values are unchanged after three generations. The particles have to be induced to leave the local optimum using the 'and logical operation' *'and' pbest* of all particles [163, 164].

IBPSO+IG. The Improved Binary Particle Swarm Optimization and Information Gain technique (IBPSO+IG) is a hybrid solution to enhance the IBPSO technique. This hybrid solution combines filter and wrapper feature selection methods. First, IG is used to calculate the importance of each feature with respect to the class. Then, to effectively remove usefulness features, the traditional BPSO and the improved BPSO wrapper methods are used to select the features again [163].

6.2. Supervised ML Approaches

The supervised approaches are predictive models developed based on a labeled training dataset that contains normal and anomalous data instances. New data instances are compared with the model to determine which class they belong to. There are several supervised machine learning algorithms such as linear classifier, K-Nearest Neighbor (KNN), Decision Tree, and Artificial Neural Network [165, 166].

Linear classifier.

Logistic regression The logistic regression is a predictive analysis. This technique is used to conduct the analysis when the dependent variable is binary. It is a statistical way of modeling a binomial outcome. The outcome can be 0 or 1, which performs a binary classification of positive class from negative one. It uses a sigmoid curve to output a probability value and, thus, performs a classification [167]. Its hypothesis function is as follows :

$$h(x) = S(w_0 + w_0 x_1 + ...w_n x_n) \tag{9}$$

$$S_Z = \frac{1}{1+e^-z} \tag{10}$$

$S(w)$ is the sigmoid curve with as output an estimated classification likelihood.

Support Vector Machines The Support Vector Machines (SVM) technique divides the space into planes and finds a separating hyperplanes between them to classify data. Then, a new unseen data point is classified based on which side of the hyperplane it falls. The SVM technique is suitable for medium-sized datasets of features with similar meaning. The advantages of SVM technique are its scalability and its capabilities to perform real-time intrusion detection and update the training patterns dynamically [168–170]

Naive Bayes It is a probabilistic machine learning model. This classifier is based on the Bayes theorem. It learns parameters by considering that the value of each feature is independent of the other features given the class variable. Then, it collects simple per-class statistics from each feature. This classification technique is faster in training compared to the other linear classifiers and it is good for very large datasets and high-dimensional data. However, it often provides the worst generalization and accuracy performances of the linear classifier techniques [171, 172].

K-Nearest Neighbor. It builds the model by storing the training dataset. To make a prediction for a new unseen data point, it finds the closest data points in the training dataset, which is considered as the nearest neighbors. This technique is generally used with small datasets [173, 174].

Decision Tree. Learning a decision tree means learning the sequence questions that gets us to the answer most quickly. These questions are called tests. A decision tree is a flowchart-like structure in which each internal node represents a test on an attribute. Each branch represents the test outcome, and each leaf node (i.e., terminal node) represents a class label. The paths from root (i.e., the entire sample) to leaf (i.e., terminal node) represent the classification rules. This technique is simple to interpret. However, it requires high computation, it is often relatively inaccurate, and unstable (i.e., a small change in the data can lead to a large change in the structure of the optimal decision tree) [175].

Artificial Neural Network. This technique is a brain-inspired system, which mimic the way humans learn. The neural networks consists of the artificial neuron called perceptron. Neural networks have input and output layers, as well as hidden layers consisting of units that transform the input into results the output layer can use. This technique can be viewed as linear models generalizations that perform multiple stages of processing to come to a decision [176].

6.3. Unsupervised ML Approaches

Unsupervised approaches associated no explicit labels with the training dataset. It aims to learn about data by modeling the structure and the distribution of the data. There are several unsupervised machine learning algorithms such as K-means clustering, Hidden Markov Model, and Fuzzy Logic [177].

K-means Clustering. The k-means clustering method was leveraged in WSN for intrusion detection to enhance security in IoT systems [178, 179]. This method aims to generate k clusters from a given dataset by iteratively allocating each data point according to the existing features to one of the k clusters. As a result, each cluster will hold samples with similar features. Indeed, the k centroids, which define the clusters centers, are estimated. Then, each data point is assigned to its nearest cluster centroid using the square Euclidean distance. After that, the cluster centroids are recalculated by computing all the samples mean assigned to that cluster. These steps are iterated until no sample that can modify the clusters exists. It is clear that this method depends on specifying the parameter k, which defines the clusters number, before executing the algorithm [180].

Hidden Markov Model. The Hidden Markov Model (HMM) method is a probabilistic model with mathematical structure. It is designed by a state sequence that has the Markovian property and an observation sequence where each symbol is emitted by the current state. In this method, the set of states are connected by transition probabilities and the states are from a first order Markov chain. Many extensions have been proposed in the literature in order to boost this method, such as the Higher-Order HMMs (HOHMM) and the Student's t-Mixture Model (SMM). The HMM is able to capture the dependencies between the consecutive sequences and it is considered as a readable probabilistic graph model. However, it has an important computational complexity and many of its parameters are freely estimated [181, 182].

Fuzzy Logic. This method is able to deal with uncertainty; therefore, it has been widely used for network threats detection. It is a useful method when decision should be made based on non-numerical and imprecise information. The Fuzzy logic systems rely in their decisions on inputs in the form of linguistic variables derived from membership functions. Membership functions are formulas used to define the fuzzy set to which a value belongs and the membership degree in that set. Fuzzification operations in this method map mathematical input values into fuzzy membership functions. However, the defuzzification operations map a fuzzy output membership function into a continuous variable that can be used for decision purposes. This method has been used in correlation with IDS. However, the fuzzy logic is not enough to detect all attack types. It should be combined with other classifiers to perform well [183, 184].

6.4. Semi-Supervised ML Approaches

With semi-supervised approaches, the training data instances contain only labels for normal class. Data instances are not labeled for the anomalous class. Semi-supervised approaches allocate great interest in machine learning because it can exploit available unlabeled data to improve supervised learning tasks when the labeled data are expensive or scarce. The most common semi-supervised algorithms are the Expectation–Maximization [185] with generative mixture models [186], and the transductive SVM algorithm [187–189].

7. Related Surveys

This section introduced the related works that survey and overview the intrusion detection techniques using machine learning algorithms in the IoT network by highlighting their main contributions. There are many surveys that discuss the intrusion detection, privacy and security issues for IoT. Despite the various research works dealing with intrusion detection systems, it is still infancy for IoT applications. As far as we know, there are scarce investigations focused on overviewing intrusion detection using machine learning mechanisms for IoT network. We focused on intrusion detection for IoT network using machine learning algorithms in this paper. In order to compare our survey to the existing IoT network overviews and surveys, table 3 sets side by side our survey work and other recent works that study security issues and intrusion detection in the IoT network.

8. Conclusion

IoT is a technology trend that enables new protocols, applications and services. It is able to connect a large number of physical objects to the Internet, and produces extensive data traffic in the network. However, the IoT traffic could be leveraged to conceive malicious activities. Indeed, IoT systems have some security flaws and vulnerabilities, the commonest of which is that when attackers may misuse this emerging technology to threaten users' privacy. Therefore, security issues cannot be neglected and IoT security solutions should be developed. This paper elaborated taxonomy of the IoT security challenges and attacks, and highlighted the open issues in IoT security. It surveyed and provided taxonomy of various intrusion detection methods that are possible to mitigate different attacks. The intrusion detection techniques are classified into three types based on the detection mechanism: signature-based IDS, anomaly-based IDS, and specification-based IDS. Signature based IDS can detect all known attacks based on their signatures. However, with anomaly-based IDS, the IDS builds a normal activity profile, which represents the normal behaviors that are accepted in the network system. Then, it becomes able to trigger alert in anomaly detection, which mismatch the normal behavior. The specification-based IDS technique exploits the benefits of both signature and anomaly-based detection techniques. It attempts, then, to detect known as well as unknown attacks. Machine learning is a field in the artificial intelligence (AI), which has been already applied in multiple disciplines and can bring a potential benefit to the IoT security systems. Accordingly, this paper presented a comprehensive study of different machine leaning methods used for intrusion detection in the IoT network context. These methods could be classified into three categories based on the availability of labeled data traffic: supervised, unsupervised, and semi-supervised methods.

References

[1] Statista Research Department (2016), Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025, Available at https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. Online; accessed 19 March 2020.

[2] Malik, A. and Om, H. (2017) Cloud computing and internet of things integration: Architecture, applications, issues, and challenges. *Sustainable Cloud and Energy Services* : 1–24.

[3] Kaur, K., Garg, S., Aujla, G.S., Kumar, N., Rodrigues, J.J. and Guizani, M. (2018) Edge computing in the industrial internet of things environment: Software-defined-networks-based edge-cloud interplay. *IEEE communications magazine* **56**: 44–51.

[4] Stergiou, C., Psannis, K.E., Kim, B.G., and Gupta, B. (2018) Secure integration of iot and cloud computing. *Future Generation Computer Systems* **78**: 964–975.

Table 3. Recent surveys on IoT security.

	Authors and Publication Date	Studied Points
Surveys and overviews on Intrusion Detection	N. A. Azeez and al. Date 2020 [190]	- It provides an update overview of the intrusion detection systems. - It discusses the use of the IDS to detect and identify vulnerabilities. - It studies the prevention mechanisms applied to avoid intrusion.
	A. Ahmim and al. Date 2020 [191]	- It studies some supervised machine learning schema for IDS. - It surveys intrusion detection systems and their mechanisms. - It reviews common public data sets used in experiments.
	K. A.P. da Costa and al. Date 2019 [192]	- It overviews research progress in security-related issues in IoT environments. - It discusses methods based on machine learning and evolutionary computation.
	D. Kumar and al. Date 2019 [193]	- It presents comprehensive investigation of security for IoT systems. - It proposes a taxonomy for the IoT ecosystem. - It provides state-of-the-art attacks on IoT systems and their defenses.
	C. Patel and al. Date 2019 [194]	- It discusses security challenges for IoT. - It examines cyber threats, attacks and security solutions for IoT.
	N. Chaabouni and al. Date 2019 [195]	- It identifies and classifies IoT threats. - It studies and compare intrusion detection systems based on machine learning techniques.
	A.Mudassar and al. Date 2019 [196]	- It discusses the generic architecture of IoT and protocols. - It surveys IoT security challenges and issues.
	S. Deep and al. Date 2019 [197]	- It examines security and privacy issues at each layer of the IoT system. - It overviews the existing security solutions for IoT.
	L.Deng and al. Date 2018 [198]	- It overviews the IoT network security issues. - It discusses some intrusion detection technologies and compares between them.
	E. Benkhelifa and al. Date 2018 [199]	- It discusses protocols and technologies of the IoT system. - It studies Intrusion Detection Systems (IDS) architecture. - It identifies security issues in IoT architectures and examines some proposed solutions.
	N. Zhang and al. Date 2017 [200]	- It provides a large-scale empirical analysis of 83M IoT devices in 16M real-world homes. - It analyzed the security profile of different IoT devices and networks. - It describes the current landscape of IoT devices and their security posture.
	Z.A.Khan and al. Date 2017 [114]	- It examines the trust based intrusion detection mechanism for IoT used to allow nodes building trust relation with their adjacent nodes, which guide the messages routing through the network. - It proposes a design and evaluation for intrusion detection system mechanisms for IoT that uses a trust management technique to detect intruder nodes.
	B.B.Zarpelão and al. Date 2017 [201]	- It surveys the IDS research work for IoT. - It proposes a classification of intrusion detection systems based on their placement strategy, detection technique and security threat.
Our contribution	H.Mliki and al. Date 2020	- This paper studies network technologies and services at each layer in the basic IoT model. - Elaborates a taxonomy of the IoT security challenges and attacks. - Surveys the existing intrusion detection mechanisms for the IoT network and elaborates a taxonomy to classify these mechanisms. - Develops a comprehensive study of different machine learning methods used for intrusion detection in the IoT network context.

[5] Fu, J.S., Liu, Y., Chao, H.C., Bhargava, B.K. and Zhang, Z.J. (2018) Secure data storage and searching for industrial iot by integrating fog computing and cloud computing. *IEEE Transactions on Industrial Informatics* **14**: 4519–4528.

[6] Kaur, K. (2018) A survey on internet of things–architecture, applications, and future trends. *First International Conference on Secure Cyber Computing and Communication (ICSCCC), Jalandhar, India* : 581–583.

[7] Ammar, M., Russello, G. and Crispo, B. (2018) Internet of things: A survey on the security of iot frameworks. *Journal of Information Security and Applications* **38**: 8–27.

[8] Cui, L., Yang, S., Chen, F., Ming, Z., Lu, N. and Qin, J. (2018) A survey on application of machine learning for internet of things. *International Journal of Machine Learning and Cybernetics* **9**: 1399–1417.

[9] Aswale, P., Shukla, A., Bharati, P., Bharambe, S. and Palve, S. (2018) An overview of internet of things: Architecture, protocols and challenges. *Information and Communication Technology for Intelligent Systems. Smart Innovation, Systems and Technologies* **106**: 299–308.

[10] Muccini, H. and Moghaddam, M.T. (2018) Iot architectural styles. *Software Architecture. ECSA 2018. Lecture Notes in Computer Science* **11048**: 68–85.

[11] Verma, H. and Chahal, K. (2017) A review on security problems and measures of internet of things. In *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)*: 71–76.

[12] chaari Fourati, L., Fourati, M. and Benmnaouer, A. (2018) Security challenges against cognitive iot development. In *2018 14th International Wireless Communications Mobile Computing Conference (IWCMC)*: 1069–1073.

[13] for Information technology, I.S. (2006) *Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)*. Tech. rep., Telecommunications and information exchange between systems—Local and metropolitan area networks— Specific requirements.

[14] Yen, L.H. and Tsai, W.T. (2010) The room shortage problem of tree-based zigbee/ieee 802.15.4 wireless networks. *Computer Communications* **33**: 454–462.

[15] Haddara, M. and AnnaStaaby (2018) Rfid applications and adoptions in healthcare: A review on patient safety. *Procedia Computer Science* **138**: 80–88.

[16] Li, C.T., Lee, C.C., Weng, C.Y. and Chen, C.M. (2018) Towards secure authenticating of cache in the reader for rfid-based iot systems. *Peer-to-Peer Networking and Applications* **11**: 198–208.

[17] Park, S.S. (2018) An iot application service using mobile rfid technology. *International Conference on Electronics, Information, and Communication (ICEIC), Honolulu, HI, USA* : 1–4.

[18] ren Lin, J., Talty, T. and Tonguz, O.K. (2015) On the potential of bluetooth low energy technology for vehicular applications. *IEEE Communications Magazine* **53**(1): 267–275.

[19] Raza, S., Misra, P., He, Z. and Voigt, T. (2017) Building the internet of things with bluetooth smart. *Ad Hoc Networks* **57**: 19–31.

[20] Collotta, M., Pau, G., Talty, T. and Tonguz, O.K. (2018) Bluetooth 5: A concrete step forward toward the iot. *IEEE Communications Magazine* **56**(7): 125–131.

[21] Fürst, J., Chen, K., Kim, H.S. and Bonnet, P. (2018) Evaluating bluetooth low energy for iot. In *2018 IEEE Workshop on Benchmarking Cyber-Physical Networks and Systems (CPSBench)*: 1–6.

[22] Hasan, K., Biswas, K., Ahmed, K., S.Nafi, N. and Islam, M.S. (2019) A comprehensive review of wireless body area network. *Journal of Network and Computer Applications* **143**: 178–198.

[23] Nabila, A. and Mohamed, E.B. (2019) A qos based comparative analysis of the ieee standards 802.15.4 802.15.6 in wban-based healthcare monitoring systems. In *2019 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)*: 1–5.

[24] minh Linh An, P. and Kim, T. (2018) A study of the z-wave protocol: Implementing your own smart home gateway. In *2018 3rd International Conference on Computer and Communication Systems (ICCCS)*: 411–415.

[25] Naidu, G.A. and Kumar, J. (2019) Wireless protocols: Wi-fi son, bluetooth, zigbee, z-wave, and wi-fi. In K, S.H.S.R.K.G.R.G.S. [ed.] *Innovations in Electronics and Communication Engineering* (Springer, Singapore), **65**, chap. Lecture Notes in Networks and Systems, 229–239.

[26] Lavric, A. and Petrariu, A.I. (2018) Lorawan communication protocol: The new era of iot. In *2018 International Conference on Development and Application Systems (DAS)*: 74–77.

[27] Haxhibeqiri, J., Poorter, E.D., Moerman, I. and Hoebeke, J. (2018) A survey of lorawan for iot: From technology to application. *Sensors* **18**: 1–38.

[28] Jalaian, B., Gregory, T., Suri, N., Russell, S., Sadler, L. and Lee, M. (2018) Evaluating lorawan-based iot devices for the tactical military environment. In *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*: 124–128.

[29] Mekki, K., Bajic, E., Chaxel, F. and Meyer, F. (2018) Overview of cellular lpwan technologies for iot deployment: Sigfox, lorawan, and nb-iot. In *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*: 197–202.

[30] Ayoub, W., Samhat, A.E., Nouvel, F., Mroue, M. and Prévotet, J.C. (2019) Internet of mobile things: Overview of lorawan, dash7, and nb-iot in lpwans standards and supported mobility. *IEEE Communications Surveys Tutorials* **21**(2): 1561–1581.

[31] Lavric, A., Petrariu, A.I. and Popa, V. (2019) Sigfox communication protocol: The new era of iot? In *2019 International Conference on Sensing and Instrumentation in IoT Era (ISSI)*: 1–4.

[32] Mekki, K., Bajic, E., Chaxel, F. and Meyer, F. (2018) Overview of cellular lpwan technologies for iot deployment: Sigfox, lorawan, and nb-iot. In *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*: 197–202.

[33] Khalifeh, A., Aldahdouh, K.A., Darabkh, K.A. and Al-Sit, W. (2019) A survey of 5g emerging wireless technologies featuring lorawan, sigfox, nb-iot and lte-m. In *2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET)*: 561–566.

[34] Osman, N.I. and Abbas, E.B. (2018) Simulation and modelling of lora and sigfox low power wide area network technologies. In *2018 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)*: 1–5.

[35] Chere, M., Ngqondi, T. and Bembe, M. (2019) Wireless low power area networks in the internet of things: A glimpse on 6lowpan. In *2019 International Conference on Electronics, Information, and Communication (ICEIC)*: 1–10.

[36] Nikshepa and Pai, V. (2018) 6LowPan—performance analysis on low power networks. In S., S. and I., B.R.C.J.K. [eds.] *International Conference on Computer Networks and Communication Technologies* (Springer, Singapore), **15**, chap. Lecture Notes on Data Engineering and Communications Technologies, 145–156.

[37] Al-Kashoash, H.A.A., Kharrufa, H., Al-Nidawi, Y. and Kemp, A.H. (2019) Congestion control in wireless sensor and 6lowpan networks: toward the internet of things. *Wireless Networks* **25**: 493–4522.

[38] Witwit, A.J.H. and Idrees, A.K. (2018) A comprehensive review for rpl routing protocol in low power and lossy networks. In mamory S., A. and A., A.J.H. [eds.] *New Trends in Information and Communications Technology Applications* (Springer, Cham), **938**, chap. Communications in Computer and Information Science, 50–66.

[39] Ghaleb, B., Al-Dubai, A.Y., Ekonomou, E., Alsarhan, A., Nasser, Y., Mackenzie, L.M. and Boukerche, A. (2019) A survey of limitations and enhancements of the ipv6 routing protocol for low-power and lossy networks: A focus on core operations. *IEEE Communications Surveys Tutorials* **21**(2): 1607–1635.

[40] Higginbotham, S. (2018) Wi-fi vs. internet of things [internet of everything]. *IEEE Spectrum* **55**(4): 22–22.

[41] Qiao, L., Zheng, Z., Cui, W. and Wang, L. (2018) A survey on wi-fi halow technology for internet of things. In *2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2)*: 1–5.

[42] Li, S., Xu, L.D. and Zhao, S. (2018) 5g internet of things: A survey. *Journal of Industrial Information Integration* **10**: 1–9.

[43] Jameel, F., Hamid, Z., Jabeen, F., Zeadally, S. and Javed, M.A. (2018) A survey of device-to-device communications: Research issues and challenges. *IEEE Communications Surveys Tutorials* **20**(3): 2133–2168.

[44] Iglesias-Urkia, M., Orive, A., Urbieta, A. and Casado-Mansilla, D. (2019) Analysis of coap implementations for industrial internet of things: a survey. *Journal of Ambient Intelligence and Humanized Computing* **10**: pages2505–2518.

[45] Çorak, B.H., Okay, F.Y., Güzel, M., Şahin Murt and Ozdemir, S. (2018) Comparative analysis of iot communication protocols. In *2018 International Symposium on Networks, Computers and Communications (ISNCC)*: 1–6.

[46] Ansari, D.B., Atteeq-Ur-Rehman and Mughal, R.A. (2018) Internet of things (iot) protocols: A brief exploration of mqtt and coap. *International Journal of Computer Applications* **179**(27): 9–14.

[47] Gündoğan, C., Kietzmann, P., Lenders, M., Petersen, H., Schmidt, T.C. and Wählisch, M. (2018) Ndn, coap, and mqtt: a comparative measurement study in the iot. *Proceedings of the 5th ACM Conference on Information-Centric Networking* : 159–171.

[48] Yassein, M.B., Shatnawi, M.Q., Aljwarneh, S. and Al-Hatmi, R. (2017) Internet of things: Survey and open issues of mqtt protocol. In *2017 International Conference on Engineering MIS (ICEMIS)*: 1–6.

[49] Pardo-Castellote, G. (2003) Omg data-distribution service: architectural overview. In *23rd International Conference on Distributed Computing Systems Workshops, 2003. Proceedings.*: 200–206.

[50] Auliva, R.S., Sheu, R.K., Liang, D. and Wang, W.J. (2018) Iiot testbed: A dds-based emulation tool for industrial iot applications. In *2018 International Conference on System Science and Engineering (ICSSE)*: 1–4.

[51] Ahemd, M.M., Shah, M.A. and Wahid, A. (2017) Iot security: A layered approach for attacks and defenses. In *2017 International Conference on Communication Technologies (ComTech)*: 104–110.

[52] Adat, V. and Gupta, B.B. (2018) Security in internet of things: issues, challenges, taxonomy, and architecture. *Telecommunication Systems* **67**: 423–441.

[53] Chen, K., Zhang, S., Li, Z., Zhang, Y., Deng, Q., Ray, S. and Jin, Y. (2018) Internet-of-things security and vulnerabilities: Taxonomy, challenges, and practice. *Journal of Hardware and Systems Security* **2**: 97–110.

[54] Kumar, S., Sahoo, S., Mahapatra, A., Swain, A.K. and Mahapatra, K. (2017) Security enhancements to system on chip devices for iot perception layer. In *2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*: 151–156.

[55] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H. and Zhao, W. (2017) A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal* **4**(5): 1125–1142.

[56] Deogirikar, J. and Vidhate, A. (2017) Security attacks in iot: A survey. In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*: 32–37.

[57] Zhang, K., Liang, X., Lu, R. and Shen, X. (2014) Sybil attacks and their defenses in the internet of things. *IEEE Internet of Things Journal* **1**(5): 372–383.

[58] Gupta, B.B., Arachchilage, N.A.G. and Psannis, K.E. (2018) Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems* **67**: 247–267.

[59] Rizvi, S., Orr, R., Cox, A., Ashokkumar, P. and R.Rizvi, M. (2020) Identifying the attack surface for iot network. *Internet of Things* **9**: 1–30.

[60] Berger, S., Bürger, O. and Röglinger, M. (2020) Attacks on the industrial internet of things – development of a multi-layer taxonomy. *Computers and Security* : 1–41.

[61] Patel, C. and Doshi, N. (2018) Security challenges in iot cyber world. In A., H.A.E.M.A.S.S. [ed.] *Security in Smart Cities: Models, Applications, and Challenges* (Springer, Cham), chap. Lecture Notes in Intelligent Transportation and Infrastructure, 171–191.

[62] Alqassem, I. and Svetinovic, D. (2014) A taxonomy of security and privacy requirements for the internet of things (iot). In *2014 IEEE International Conference on Industrial Engineering and Engineering Management*: 1244–1248.

[63] Oh, S.R. and Kim, Y.G. (2017) Security requirements analysis for the iot. In *2017 International Conference on Platform Technology and Service (PlatCon)*: 1–6.

[64] Zhou, J., Cao, Z., Dong, X. and Vasilakos, A.V. (2017) Security and privacy for cloud-based iot: Challenges. *IEEE Communications Magazine* **55**(1): 26–33.

[65] Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A. and Kikiras, P. (2015) On the security and privacy of internet of things architectures and systems. In *2015 International Workshop on Secure Internet of Things (SIoT)*: 49–57.

[66] Minoli, D., Sohraby, K. and Kouns, J. (2017) Iot security (iotsec) considerations, requirements, and architectures. In *2017 14th IEEE Annual Consumer Communications Networking Conference (CCNC)*: 1006–1007.

[67] Elaguech, M., Kchaou, A., Youssef, W.E.H., Othman, K.B. and Machhout, M. (2019) Performance evaluation of lightweight block ciphers in soft-core processor. In *2019 19th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*: 101–105.

[68] Xiao-Mei, L. and Yong, Q. (2019) Research on led lightweight cryptographic algorithm based on rfid tag of internet of things. In *2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*: 1717–1720.

[69] Avoine, G., Bingöl, M.A., Carpent, X. and Yalcin, S.B.O. (2013) Privacy-friendly authentication in rfid systems: On sublinear protocols based on symmetric-key cryptography. *IEEE Transactions on Mobile Computing* **12**(10): 2037–2049.

[70] Wang, C., Wang, D., Tu, Y., Xu, G. and Wang, H. (2020) Understanding node capture attacks in user authentication schemes for wireless sensor networks. *IEEE Transactions on Dependable and Secure Computing* : 1–1.

[71] SWEENEY, L. (2002) k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* **10**(5): 557–570.

[72] Ozdemir, S. and Xiao, Y. (2011) Integrity protecting hierarchical concealed data aggregation for wireless sensor networks. *Computer Networks* **55**: 1735–1746.

[73] Acharya, R. and Asha., K. (2008) Data integrity and intrusion detection in wireless sensor networks. In *2008 16th IEEE International Conference on Networks*: 1–5.

[74] Mo, Y., Kim, T.H.J., Brancik, K., Dickinson, D., Lee, H., Perrig, A. and Sinopoli, B. (2012) Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE* **100**(1): 195–209.

[75] Airehrour, D., Gutierrez, J. and Ray, S.K. (2016) Secure routing for internet of things: A survey. *Journal of Network and Computer Applications* **66**: 198–213.

[76] Kamble, A., Malemath, V.S. and Patil, D. (2017) Security attacks and secure routing protocols in rpl-based internet of things: Survey. In *2017 International Conference on Emerging Trends Innovation in ICT (ICEI)*: 33–39.

[77] Zhu, Y. and Zhou, D. (2020) Security technology of wireless sensor network based on ipsec. In O., X.Z.P.R.H.M.L.G. [ed.] *Cyber Security Intelligence and Analytics* (Springer, Cham), **1146**, chap. Advances in Intelligent Systems and Computing, 92–97.

[78] Cervantes, C., Poplade, D., Nogueira, M. and Santos, A. (2015) Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things. In *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*: 606–611.

[79] Liu, Y., Ma, M., Xiong, N.N., Liu, A. and Zhu, Y. (2020) Design and analysis of probing route to defense sink-hole attacks for internet of things security. *IEEE Transactions on Network Science and Engineering* **7**(1): 356–372.

[80] Taghanaki, S.R., Jamshidi, K. and Bohlooli, A. (2019) Deem: A decentralized and energy efficient method for detecting sinkhole attacks on the internet of things. In *2019 9th International Conference on Computer and Knowledge Engineering (ICCKE)*: 325–330.

[81] Tahir, S., Bakhsh, S.T. and Alsemmeari, R.A. (2019) An intrusion detection system for the prevention of an active sinkhole routing attack in internet of things. *International Journal of Distributed Sensor Networks* **15**: 1–10.

[82] Ahmad, Z., Abbasi, M.H., Khan, A., Mall, I.S., Khan, M.F.N. and Sajjad, I.A. (2020) Design of iot embedded smart energy management system. In *2020 International Conference on Engineering and Emerging Technologies (ICEET)*: 1–5.

[83] Langendörfer, J.M.B..A.S..M.V.M..D.G..P. (2015) Smartie project: Secure iot data management for smart cities. In *2015 International Conference on Recent Advances in Internet of Things (RIoT)*: 1–6.

[84] Novo, O. (2019) Scalable access management in iot using blockchain: A performance evaluation. *IEEE Internet of Things Journal* **6**(3): 4694–4701.

[85] Chen, L., Thombre, S., Järvinen, K., Lohan, E.S., Alén-Savikko, A., Leppäkoski, H., Bhuiyan, M.Z.H. *et al.* (2017) Robustness, security and privacy in location-based services for future iot: A survey. *IEEE Access* **5**: 8956–8977.

[86] Zhang, P., Nagarajan, S.G. and Nevat, I. (2017) Secure location of things (slot): Mitigating localization spoofing attacks in the internet of things. *IEEE Internet of Things Journal* **4**(6): 2199–2206.

[87] Gope, P., Amin, R., Islam, S., Kumar, N. and Bhalla, V.K. (2018) Lightweight and privacy-preserving rfid authentication scheme for distributed iot infrastructure with secure localization services for smart city environment. *Future Generation Computer Systems* **83**: 629–637.

[88] Ahmed, F. (2019) Self-organization: A perspective on applications in the internet of things. In KC., L.X.W. [ed.] *Natural Computing for Unsupervised Learning* (Springer, Cham), chap. Unsupervised and Semi-Supervised Learning, 51–64.

[89] Athreya, A.P. and Tague, P. (2013) Network self-organization in the internet of things. In *2013 IEEE International Workshop of Internet-of-Things Networking and Control (IoT-NC)*: 25–33.

[90] Rao, T.A. and ul Haq, E. (2018) Security challenges facing iot layers and its protective measures. *International Journal of Computer Applications* **179**: 1–5.

[91] Nurse, J.R., Creese, S. and Roure, D.D. (2017) Security risk assessment in internet of things systems. *IT Professional* **19**(5): 20–26.

[92] Wang, T. (2019) The information security risk assessment model based on improved electre method. *Proceedings of the 2019 7th International Conference on Information Technology: IoT and Smart City* : 570–574.

[93] Maheshwari, N. and Dagale, H. (2018) Secure communication and firewall architecture for iot applications. In *2018 10th International Conference on Communication Systems Networks (COMSNETS)*: 328–335.

[94] Gupta, N., Naik, V. and Sengupta, S. (2017) A firewall for internet of things. In *2017 9th International Conference on Communication Systems and Networks (COMSNETS)*: 411–412.

[95] Gaurav, A., Kumar, S.S. and Chetan, A. (2017) International journal of advanced research in computer science. *International Journal of Advanced Research in Computer Science* **8**: 499–50.

[96] Taher, K.A., Jisan, B.M.Y. and Rahman, M.M. (2019) Network intrusion detection using supervised machine learning technique with feature selection. In *2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST)*: 643–646.

[97] Ernst, J., Hamed, T. and Kremer, S. (2018) A survey and comparison of performance evaluation in intrusion detection systems. In K, D. [ed.] *Computer and Network Security Essentials* (Springer, Cham), 555–568.

[98] Hubballi, N. and Suryanarayanan, V. (2014) False alarm minimization techniques in signature-based intrusion detection systems: A survey. *Computer communications* **49**: 1–17.

[99] Bhuyan, M.H., Bhattacharyya, D.K. and Kalita, J.K. (2014) Network anomaly detection: Methods, systems and tools. *IEEE Communications Surveys Tutorials* **16**(1): 303–336.

[100] Patcha, A. and Jung-MinPark (2007) An overview of anomaly detection techniques: Existing solutions

and latest technological trends. *Computer Networks* **51**: 3448–3470.

[101] P.García-Teodoro, J.Díaz-Verdejo, G.Maciá-Fernández and E.Vázquez (2009) Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers and Security* **28**: 18–28.

[102] Aydin, M.A., Zaim, A.H. and Ceylan, K.G. (2009) A hybrid intrusion detection system design for computer network security. *Computers and Electrical Engineering* **35**: 517–526.

[103] Alem, S., Espes, D., Martin, E., Nana, L. and Lamotte, F.D. (2019) A hybrid intrusion detection system in industry 4.0 based on isa95 standard. In *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*: 1–8.

[104] Chandak, T., Ghorpade, C. and Shukla, S. (2019) Effective analysis of feature selection algorithms for network based intrusion detection system. In *2019 IEEE Bombay Section Signature Conference (IBSSC)*: 1–5.

[105] Shin, M.S., Kim, E.H. and Ryu, K.H. (2004) False alarm classification model for network-based intrusion detection system. In Yang Z.R., Yin H., E.R. [ed.] *Intelligent Data Engineering and Automated Learning* (Springer, Berlin, Heidelberg), **3177**, chap. Lecture Notes in Computer Science, 259–265.

[106] Kim, D.S. and Park, J.S. (2003) Network-based intrusion detection with support vector machines. In HK, K. [ed.] *Information Networking* (Springer, Berlin, Heidelberg), **2662**, chap. Lecture Notes in Computer Science, 747–756.

[107] Rice, T.R., Seppala, G., Edgar, T., Choi, E., Cain, D. and Mahserejian, S. (2019) Development of a host-based intrusion detection and control device for industrial field control devices. In *2019 Resilience Week (RWS)*, **1**: 105–111.

[108] Ali, F.A.B.H. and Len, Y.Y. (2011) Development of host based intrusion detection system for log files. In *2011 IEEE Symposium on Business, Engineering and Industrial Applications (ISBEIA)*: 281–285.

[109] Vokorokos, L. and Baláž, A. (2010) Host-based intrusion detection system. In *2010 IEEE 14th International Conference on Intelligent Engineering Systems*: 43–47.

[110] Rajput, D. and Thakkar, A. (2019) A survey on different network intrusion detection systems and countermeasure. In N., S.N.P.L.N.H.H.P.N. [ed.] *Emerging Research in Computing, Information, Communication and Applications* (Springer, Singapore), **906**, chap. Advances in Intelligent Systems and Computing, 497–506.

[111] Benkhelifa, E., Welsh, T. and Hamouda, W. (2018) A critical review of practices and challenges in intrusion detection systems for iot: Toward universal and resilient systems. *IEEE Communications Surveys Tutorials* **20**(4): 3496–3509.

[112] Wang, Z. and Zhu, Y. (2017) A centralized hids framework for private cloud. In *2017 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*: 115–120.

[113] Ahmim, A., Maglaras, L., Ferrag, M.A., Derdour, M. and Janicke, H. (2019) A novel hierarchical intrusion detection system based on decision tree and rules-based models. In *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*: 228–233.

[114] Khan, Z.A. and Herrmann, P. (2017) A trust based distributed intrusion detection mechanism for internet of things. In *2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)*: 1169–1176.

[115] Bernieri, G. and Pascucci, F. (2019) Improving security in industrial internet of things: A distributed intrusion detection methodology. In C., A. [ed.] *Security and Privacy Trends in the Industrial Internet of Things* (Springer, Cham), chap. Advanced Sciences and Technologies for Security Applications, 161–179.

[116] Yu-Fang Zhang, Zhong-Yang Xiong and Xiu-Qiong Wang (2005) Distributed intrusion detection based on clustering. In *2005 International Conference on Machine Learning and Cybernetics*, **4**: 2379–2383 Vol. 4.

[117] Ghaeini, H.R. and Tippenhauer, N.O. (2016) Hamids: Hierarchical monitoring intrusion detection system for industrial control systems. *roceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy* : 103–111.

[118] Sedjelmaci, H., Senouci, S.M. and Ansari, N. (2018) A hierarchical detection and response system to enhance security against lethal cyber-attacks in uav networks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* **48**(9): 1594–1606.

[119] Hajisalem, V. and ShahramBabaie (2018) A hybrid intrusion detection system based on abc-afs algorithm for misuse and anomaly detection. *Computer Networks* **136**: 37–50.

[120] Midi, D., Rullo, A., Mudgerikar, A. and Bertino, E. (2017) Kalis — a system for knowledge-driven adaptable intrusion detection for the internet of things. In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*: 656–666.

[121] A.Prayati, Ch.Antonopoulos, T.Stoyanova, T.Stoyanova, C.Koulamas and G.Papadopoulos (2010) A modeling approach on the telosb wsn platform power consumption. *Journal of Systems and Software* **83**: 1355–1363.

[122] Levis, P., Madden, S., Polastre, J., Szewczyk, R., Whitehouse, K., Gay, A.W.D., Hill, J. *et al.* (2005) Tinyos: An operating system for sensor networks. In E., W.W.R.J.A. [ed.] *Ambient Intelligence* (Springer, Berlin, Heidelberg), 115–148.

[123] Sheikh, N.U., Rahman, H., Vikram, S. and AlQahtani, H. (2018) A lightweight signature-based ids for iot environment. *Cryptography and Security* : 1–4.

[124] Li, W., Tug, S., Meng, W. and YuWang (2019) Designing collaborative blockchained signature-based intrusion detection in iot environments. *Future Generation Computer Systems* **96**: 481–489.

[125] Thing, V.L.L. (2017) Ieee 802.11 network anomaly detection and attack classification: A deep learning approach. In *2017 IEEE Wireless Communications and Networking Conference (WCNC)*: 1–6.

[126] Moustafa, N., Turnbull, B. and Choo, K.R. (2019) An ensemble intrusion detection technique based

on proposed statistical flow features for protecting network traffic of internet of things. *IEEE Internet of Things Journal* **6**(3): 4815–4830.

[127] Moustafa, N. and Slay, J. (2015) Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set). In *2015 Military Communications and Information Systems Conference (MilCIS)*: 1–6.

[128] Yavanoglu, O. and Aydos, M. (2017) A review on cyber security datasets for machine learning algorithms. In *2017 IEEE International Conference on Big Data (Big Data)*: 2186–2193.

[129] Prabavathy, S., Sundarakantham, K. and Shalinie, S.M. (2018) Design of cognitive fog computing for intrusion detection in internet of things. *Journal of Communications and Networks* **20**(3): 291–298.

[130] Mliki, H., Kaceam, A.H. and Chaari, L. (2019) Intrusion detection study and enhancement using machine learning. In A., K.S.C.F.C.B.N.H.K. [ed.] *Risks and Security of Internet and Systems* (Springer, Cham), **2026**, chap. Lecture Notes in Computer Science, 263–278.

[131] Krishnaveni, S. and Sivamohan, P.V.K.J. (2020) Anomaly-based intrusion detection system using support vector machine. In B., D.S.L.C.D.S.P. [ed.] *Artificial Intelligence and Evolutionary Computations in Engineering Systems* (Springer, Singapore), **1056**, chap. Advances in Intelligent Systems and Computing, 723–731.

[132] Bostani, H. and Sheikhan, M. (2017) Hybrid of anomaly-based and specification-based ids for internet of things using unsupervised OPF based on mapreduce approach. *Computer Communications* **98**: 52–71.

[133] Choudhary, S. and Kesswani, N. (2019) Cluster-based intrusion detection method for internet of things. In *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*: 1–8.

[134] Jaber, A.N. and Rehman, S.U. (2020) Fcm–svm based intrusion detection system for cloud computing environment. *Cluster Computing* .

[135] Li, J., Qu, Y., Chao, F., Shum, H.P.H., Ho, E.S.L. and Yang, L. (2019) Machine learning algorithms for network intrusion detection. In L., S. [ed.] *AI in Cybersecurity* (Springer, Cham), **151**, chap. Intelligent Systems Reference Library, 151–179.

[136] Khaled, A.A.U. and El-Sayed, M.E.A. (2018) Intrusion detection taxonomy and data preprocessing mechanisms. *Special Section: Soft Computing and Intelligent Systems: Techniques and Applications* **35**(3): 1369–1383.

[137] Liu, C., Liu, Y., Yan, Y. and Wang, J. (2020) An intrusion detection model with hierarchical attention mechanism. *IEEE Access* : 1–1.

[138] Taher, K.A., Jisan, B.M.Y. and Rahman, M.M. (2019) Network intrusion detection using supervised machine learning technique with feature selection. In *2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST)*: 643–646.

[139] Aljawarneh, S., Aldwairi, M. and Yassein, M.B. (2018) Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *Journal of Computational Science* **25**: 152–160.

[140] Labani, M., Moradi, P., Ahmadizar, F. and Jalili, M. (2018) A novel multivariate filter method for feature selection in text classification problems. *Engineering Applications of Artificial Intelligence* **70**: 25–37.

[141] Abdi, H. and Williams, L.J. (2010) Principal component analysis. *WIREs Computational Statistics* **2**: 433–459.

[142] Candès, E.J., Li, X., Ma, Y. and Wright, J. (2009) Robust principal component analysis? *Journal of the ACM* **11**: 1–39.

[143] Hall, M.A. (2000) Correlation-based feature selection of discrete and numeric class machine learning. In *2000 Working Papers* (University of Waikato, Department of Computer Science), chap. Computer Science Working Papers.

[144] Chormunge, S. and Jena, S. (2018) Correlation based feature selection with clustering for high dimensional data. *Journal of Electrical Systems and Information Technology* **5**: 542–549.

[145] Eid, H.F., Hassanien, A.E., hoon Kim, T. and Banerjee, S. (2013) Linear correlation-based feature selection for network intrusion detection model. In A.I., A. and K., H.A.B. [eds.] *Advances in Security of Information and Communication Networks* (Springer, Berlin, Heidelberg), **381**, chap. Communications in Computer and Information Science, 240–248.

[146] Raileanu, L.E. and Stoffel, K. (2004) Theoretical comparison between the gini index and information gain criteria. *Laura Elena Raileanu and Kilian Stoffel* **41**: 77–93.

[147] Roobaert, D., Karakoulas, G. and Chawla, N.V. (2006) Information gain, correlation and support vector machines. In L.A., G.I.N.M.G.S.Z. [ed.] *Feature Extraction* (Springer, Berlin, Heidelberg), **207**, chap. Studies in Fuzziness and Soft Computing, 463–470.

[148] Aydin, M., Butun, I., Bicakci, K. and Baykal, N. (2020) Using attribute-based feature selection approaches and machine learning algorithms for detecting fraudulent website urls. In *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*: 0774–0779.

[149] Choi, S.H. and Chae, H.S. (2014) Feature selection using attribute ratio in nsl-kdd data. *International Conference Data Mining, Civil and Mechanical Engineering, Bali, Indonesia* .

[150] Hutter, M. (2002) Fitness uniform selection to preserve genetic diversity. In *Proceedings of the 2002 Congress on Evolutionary Computation. CEC'02 (Cat. No.02TH8600)*, **1**: 783–788 vol.1.

[151] Syswerda, G. (1989) Uniform crossover in genetic algorithms. *Proceedings of the 3rd International Conference on Genetic Algorithms* : 2–9.

[152] Srinivas, M. and Patnaik, L.M. (1994) Genetic algorithms: a survey. *Computer* **27**(6): 17–26.

[153] Srinivas, M. and Patnaik, L.M. (1994) Adaptive probabilities of crossover and mutation in genetic algorithms. *IEEE Transactions on Systems, Man, and Cybernetics* **24**(4): 656–667.

[154] Hinterding, R. (1995) Gaussian mutation and self-adaption for numeric genetic algorithms. In *Proceedings of 1995 IEEE International Conference on Evolutionary Computation*, **1**: 384–.

[155] higeyoshi Tsutsui and Fujimoto, Y. (1993) Forking genetic algorithm with blocking and shrinking modes (fga). *the 5th International Conference on Genetic Algorithms, Urbana-Champaign, IL, USA* : 206–215.

[156] Oosthuizen, G. (1987) Supergran: a connectionist approach to learning, integrating genetic algorithms and graph induction. *Genetic algorithms and their applications:proceedings of the second International Conference on Genetic Algorithms* : 132–139.

[157] Mauldin., M.L. (1984) Maintaining diversity in genetic search. *AAAI-84 Proceedings* : 247–250.

[158] links open overlay panelCarol A.Ankenbrandt, A. (1991) An extension to the theory of convergence and a proof of the time complexity of genetic algorithms. *Foundations of Genetic Algorithms* **1**: 53–68.

[159] Mirjalili, S. (2019) Genetic algorithm. In *Evolutionary Algorithms and Neural Networks* (Springer, Cham), **780**, chap. Studies in Computational Intelligence, 43–55.

[160] İpek Uysal, E., Demircioğlu, G., Kale, G., Bostanci, E., Güzel, M.S. and Mohammed, S.N. (2019) Network anomaly detection system using genetic algorithm, feature selection and classification. In *2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*: 1–5.

[161] Zhang, X., Zhang, Q., Chen, M., Sun, Y., Qin, X. and Li, H. (2018) A two-stage feature selection and intelligent fault diagnosis method for rotating machinery using hybrid filter and wrapper method. *Neurocomputing* **275**: 2426–2439.

[162] Bansal, J.C. (2018) Particle swarm optimization. In J., B., P., S. and N., P. [eds.] *Evolutionary and Swarm Intelligence Algorithms* (Springer, Cham), **779**, chap. Studies in Computational Intelligence, 11–23.

[163] Lalit, K. and Kumari, B.K. (2019) An improved bpso algorithm for feature selection. In U., K.A.T., I., S. and N., S. [eds.] *Recent Trends in Communication, Computing, and Electronics* (Springer, Singapore), chap. Lecture Notes in Electrical Engineering, 505–513.

[164] Dong, C. and LixinZhao (2019) Sensor network security defense strategy based on attack graph and improved binary pso. *Safety Science* **117**: 81–87.

[165] Singh, A., Thakur, N. and Sharma, A. (2016) A review of supervised machine learning algorithms. In *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*: 1310–1315.

[166] Harikrishnakumar, R., Dand, A., Nannapaneni, S. and Krishnan, K. (2019) Supervised machine learning approach for effective supplier classification. In *2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA)*: 240–245.

[167] Collins, M., Schapire, R.E. and Singer, Y. (2002) Logistic regression, adaboost and bregman distances. *Machine Learning* **48**: 253–285.

[168] Hsu, C.W. and Lin, C.J. (2002) A comparison of methods for multiclass support vector machines. *IEEE Transactions on Neural Networks* **13**(2): 415–425.

[169] Drucker, H., Donghui Wu and Vapnik, V.N. (1999) Support vector machines for spam categorization. *IEEE Transactions on Neural Networks* **10**(5): 1048–1054.

[170] Hearst, M.A., Dumais, S.T., Osuna, E., Platt, J. and Scholkopf, B. (1998) Support vector machines. *IEEE Intelligent Systems and their Applications* **13**(4): 18–28.

[171] Amor, N.B., Benferhat, S. and Elouedi, Z. (2004) Naive bayes vs decision trees in intrusion detection systems. *Proceedings of the 2004 ACM symposium on Applied computing* : 420–424.

[172] Lowd, D. and Domingos, P. (2005) Naive bayes models for probability estimation. *Proceedings of the 22nd international conference on Machine learning* : 529–536.

[173] Dudani, S.A. (1976) The distance-weighted k-nearest-neighbor rule. *IEEE Transactions on Systems, Man, and Cybernetics* **SMC-6**(4): 325–327.

[174] C.Bezdek, J., K.Chuah, S. and DavidLeep (1986) Generalized k-nearest neighbor rules. *Fuzzy Sets and Systems* **18**: 237–256.

[175] Safavian, S.R. and Landgrebe, D. (1991) A survey of decision tree classifier methodology. *IEEE Transactions on Systems, Man, and Cybernetics* **21**(3): 660–674.

[176] Abraham, A. (2005) Artificial neural networks. In Sydenham, P.H. and Thorn, R. [eds.] *Handbook of Measuring System Design* (John Wiley and Sons), chap. AI Signal Processing Techniques, 901–908.

[177] Celebi, M.E. and Aydin, K. [eds.] (2016) *Unsupervised Learning Algorithms* (Springer, Cham).

[178] Han, G., Wang, H., Guizani, M., Chan, S. and Zhang, W. (2018) Kclp: A k-means cluster-based location privacy protection scheme in wsns for iot. *IEEE Wireless Communications* **25**(6): 84–90.

[179] Bharti, A.K., Verma, N. and Verma, D.K. (2019) Cluster analysis of iot data based on mapreduce technique. *International Journal of Research and Analytical Reviews (IJRAR)* **6**: 262–269.

[180] Steinley, D. (2010) K-means clustering: A half-century synthesis. *British Journal of Mathematical and Statistical Psychology* **59**: 1–34.

[181] Tamposis, I.A., Theodoropoulou, M.C., Tsirigos, K.D. and Bagos, P.G. (2018) Extending hidden markov models to allow conditioning on previous observations. *Journal of Bioinformatics and Computational Biology* **16**(5): 1–17.

[182] Zheng, Y., Jeon, B., Sun, L., Zhang, J. and Zhang, H. (2018) t-hidden markov model for unsupervised learning using localized feature selection. *IEEE Transactions on Circuits and Systems for Video Technology* **28**: 2586–2598.

[183] Li, J., Qu, Y., Chao, F., Shum, H.P., Ho, E.S. and Yang, L. (2019) Machine learning algorithms for network intrusion detection. In L., S. [ed.] *AI in Cybersecurity* (Springer, Cham), **151**, chap. Intelligent Systems Reference Library, 151–179.

[184] Hamamoto, A.H., Hamamoto, A.H., Carvalho, L.F., Sampaio, L.D.H., Abrao, T. and Proenca, M.L. (2018) Network anomaly detection system using genetic algorithm and fuzzy logic. *Expert Systems with Applications* **92**: 390–402.

[185] Wang, X., Wen, J., Alam, S., Jiang, Z. and Wu, Y. (2016) Semi-supervised learning combining transductive support vector machine with active learning. *Neurocomputing* **173**: 1288–1298.

[186] McLachlan, G.J., Lee, S.X. and Rathnayake, S.I. (2019) Finite mixture models. *Annual review of statistics and its application* **6**: 55–378.

[187] Devi, E.R. and Suganthe, R. (2020) Enhanced transductive support vector machine classification with grey wolf optimizer cuckoo search optimization for intrusion detection system. *Special Issue: Special Issue on Advances in Metaheuristic Optimization Algorithms (AMOA2018)* **32**: 1–11.

[188] Chaaboun, N., Mosbah, M., Zemmari, A. and Faruki, P. (2019) Network intrusion detection for iot security based on learning techniques. *IEEE Communications Surveys Tutorials* **21**(3): 2671–2701.

[189] Idhammad, M., Afdel, K. and Belouch, M. (2018) Semi-supervised machine learning approach for ddos detection. *Applied Intelligence* **48**: 3193–3208.

[190] Azeez, N.A., Bada, T.M., Misra, S., Adewumi, A., der Vyver, C.V. and Ahuja, R. (2020) Intrusion detection and prevention systems: An updated review. In N., S., A., C. and V., B. [eds.] *Data Management, Analytics and Innovation* (Springer, Singapore), **1042**, chap. Advances in Intelligent Systems and Computing, 685–696.

[191] Ahmim, A., Maglaras, M.A.F.L., Derdour, M., Janicke, H. and Drivas, G. (2020) Taxonomy of supervised machine learning for intrusion detection systems. In A., K. and P., K.E.T. [eds.] *Strategic Innovative Marketing and Tourism* (Springer, Cham), chap. Springer Proceedings in Business and Economics, 619–628.

[192] da Costa, K.A., Papa, J.P., Lisboa, C.O., Munoz, R. and de Albuquerque, V.H.C. (2019) Internet of things: A survey on machine learning-based intrusion detection approaches. *Computer Networks* **151**: 147–157.

[193] Kumar, D., Shen, K., Case, B., Garg, D., Alperovich, G., Kuznetsov, D., Gupta, R. *et al.* (2019) All things considered: An analysis of iot devices on home networks. In *28th USENIX Security Symposium (USENIX Security 19)* (Santa Clara, CA: USENIX Association): 1169–1185. URL https://www.usenix.org/conference/usenixsecurity19/presentation/kumar-deepak.

[194] Patel, C. and Doshi, N. (2019) Security challenges in iot cyber world. In A., H., M., E., S., A. and A., S. [eds.] *Security in Smart Cities: Models, Applications, and Challenges* (Springer, Cham), chap. Lecture Notes in Intelligent Transportation and Infrastructure, 171–191.

[195] Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C. and Faruki, P. (2019) Network intrusion detection for iot security based on learning techniques. *IEEE Communications Surveys Tutorials* **21**(3): 2671–2701.

[196] Ahmad, M., Younis, T., Habib, M.A., Ashraf, R. and Ahmed, S.H. (2019) A review of current security issues in internet of things. In M., J., F., K. and M., A. [eds.] *Recent Trends and Advances in Wireless and IoT-enabled Networks* (Springer, Cham), chap. EAI/Springer Innovations in Communication and Computing, 11–23.

[197] Zheng, S.D.X., Jolfaei, A., Yu, D., Ostovari, P. and Bashir, A.K. (2019) A survey of security and privacy issues in the internet of things from the layered context. *CoRR* **abs/1903.00846**. URL http://arxiv.org/abs/1903.00846. 1903.00846.

[198] Deng, L., Li, D., Yao, X., Cox, D. and Wang, H. (2019) Mobile network intrusion detection for iot system based on transfer learning algorithm. *Cluster Computing* **22**: 9889–9904.

[199] Benkhelifa, E., Welsh, T. and Hamouda, W. (2018) A critical review of practices and challenges in intrusion detection systems for iot: Toward universal and resilient systems. *IEEE Communications Surveys Tutorials* **20**(4): 3496–3509.

[200] Zhang, N., Demetriou, S., Mi, X., Diao, W., Yuan, K., Zong, P., Qian, F. *et al.* (2017) Understanding iot security through the data crystal ball: Where we are now and where we are going to be. *CoRR* **abs/1703.09809**. URL http://arxiv.org/abs/1703.09809. 1703.09809.

[201] Zarpelão, B.B., Miani, R.S., Kawakani, C.T. and de Alvarenga, S.C. (2017) A survey of intrusion detection in internet of things. *Journal of Network and Computer Applications* **84**: 25–37.