Int. J. Nonlinear Anal. Appl. 14 (2023) 5, 27–35
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2023.67512.4305

Review on machine learning and deep learning algorithms for IoT security

Harith Abdulkarim

Department of Computer Science, University of Kufa, Najaf, Iraq

(Communicated by Seyed Hossein Siadati)

Abstract

With its rapid expansion in more sectors, for instance, wearables, smart sensors, plus house devices, the Internet of Things (IoT) is drifted to have a significant influence on many parts of our life. IoT devices stand out for their connectivity, ubiquity, and low processing power. By 2025, there will likely be 30.9 billion devices adjoined to the Internet, since the count of IoT devices in use worldwide is growing quickly. This eruption about IoT devices, which in analogy to desktop PCs, can be quickly increased, has caused an increase in occurrences of IoT-based cyber intrusions. It is necessary to create new methods for identifying attacks launched from hacked IoT devices in order to address this challenge. The best detective control solution against attacks caused by IoT devices, in this context, uses machine and deep learning approaches. This paper attempts some analysis of technologies, threats arising from IoT devices, and intrusion detection system overview as they associate with IoT systems. The investigation of several machine learning plus deep learning concepts appropriate for identifying IoT devices linked with cyberattacks is also included in this paper.

Keywords: IoT, Machine Learning, Deep Learning, Cyber Security, Intrusion Detection
2020 MSC: 68T07

1 Introduction

The Internet of Things (IoT), a recent advancement along with computer and communication technology, has significantly outperformed the old method of detecting the immediate environment. IoT technology have aided in the creation of systems that really can enhance quality of life. IoT, one of the computer fields' technologies that is expanding the fastest, is predicted to have 30.9 billion devices through the year 2025 [1]. By 2025, IoT additionally relevant implementations are predicted to have a possible financial effect of 3.9$trillioninto$11.1 trillion annually [26]. By utilising the IoT's key technologies, such as communication networks, pervasive and everywhere computing, embedded systems, Internet protocols, sensor systems, and applications depending on AI, the gadgets can become intelligent objects [47]. The processing and communication are extended to additional IoT devices with differing specifications thanks to the pervasive interconnection of physically dispersed IoT devices [65]. These gadgets contain a variety of sensors that allow them to remotely collect real-time data from the actual devices. We can successfully manage IoT environments and develop intelligent decision systems thanks to the data that the devices collect. Connecting frequently utilised real-world gadgets with the net, however, furthermore prompts worries regarding cybersecurity dangers [7, 59]. For the security of IoT devices and versus assaults brought on by compromised IoT devices, it is necessary to design and create intelligent protection solutions.

Email address: haritha.alshimaysawe@student.uokufa.edu.iq (Harith Abdulkarim)

Received: December 2022 *Accepted:* March 2023

2 Background

2.1 IoT security attacks category

Protecting the Internet of Things is one of the main issues. IoT security is currently receiving tinier attention as the majority of major security initiatives are focused on safeguarding/securing traditional servers, workstations, and mobile [33]. The Confidentiality, Integrity, and Availability (CIA) trinity is regarded in cybersecurity as the core component of security measures through data technology and systems [54]. The same concept is being deployed in IoT and yet does not completely meet its needs because IoT is a unique ecosystem with constantly changing threats. Here are a few of the most well-known IoT assaults (for a taxonomy of IoT threats, see Fig. 1 [24]):

Jamming: such incursion takes place when malicious radio equipment obstructs proper information exchange and especially renders the equipment inoperable using launching a denial of service (DOS) assault [13].

Malicious code Injection Incursions: to gain complete control of an IoT environment, an attacker physically instals malicious code in one of its nodes [36].

Node Capture Attacks: by physically altering or tampering with an IoT component or device, an attacker can seize control of it [67].

Sleep Deprivation Attack / Resource Exhaustion: attackers achieve this by keeping the nodes awake so they may drain their batteries, this manages to shorten the node's lifespan and cause it to close down [61].

Sinkhole Attack: This attack aims to attract traffic in order to stop the ground station from receiving all of the data from nodes. As a result, it taints the data that devices send [28].

Wormhole Attack: In order to disrupt the network architecture and traffic flows, an attacker broadcasts all traffic across a virtual tunnel created between a binary of malicious nodes [45].

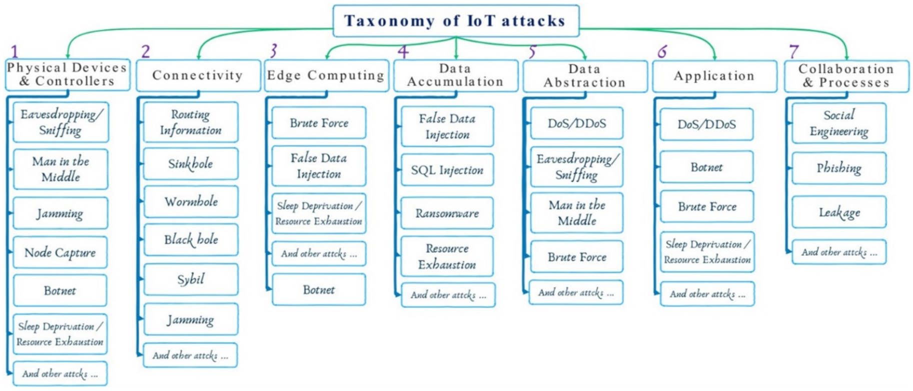


Figure 1: IoT attack classification

Black hole Attack: a malignant action taken by a cell which purports to have quickest route to the goal with the intention of dropping the traffic that has been received [3].

Sybil attack: it happens when an attacker impersonates several different nodes simultaneously, it takes place. The attacker can do this to get an abnormal level of control and lower the network's effectiveness [49].

Routing Information Attacks: To draw or fend off the network away from these chosen nodes, an attacker generates routing loops that are expanded or compressed [40].

False Data Injection: Threat actors take control of a jointed device and insert data to introduce misleading information into the outcomes of data aggregation, causing the collected data to wander from their true value and rendering the outcomes meaningless [63].

SQL Injection: Incursion takes place while a vicious SQL statement is entered into a field that is unsafe and will be evaluated by a SQL database. If successful, the attacker will get admission to the system. This threat is widespread across various system types, including IoT [50].

Ransomware: That is malware that completely seizes control over the system, encrypts its data, and only gives the user restricted access while demanding a ransom in exchange for restoring control of his object, if the user refuses to pay, the malware will destroy each of the system's data [64].

DoS/DDoS: Denial of Service occurs when an attacker tries to devalue a service by consuming its resources, bandwidth, or both. When attacks originate from several compromised nodes, they are referred to be distributed denial of service (DDoS) [57].

Botnet (zombies): comprise robots of compromised Internet-linked tools that are utilised to perform spread DDoS assaults, password cracking, keylogging, cryptocurrency extraction, also provide the assailant with the option of entering the equipment via command plus control (C&C) programs [9].

Eavesdropping/Sniffing attack: The majority of Internet of Things (IoT) equipment exchange information over wireless networks, which makes them susceptible to eavesdropping. Assailants can sense this information utilising specific applications [66].

Man in the Middle (MitM): This attack technique allows attackers to intercept, manipulate, change, or replace data transmission over two or more machines without the targets' knowledge [14].

Brute Force: Here, the attacker's goal is to determine valid credentials by employing thorough techniques to examine all potential passphrases in order to identify the right single or decrypt encoded data [12].

Social Engineering attacks: constitute emotional assaults directed at device users or administrators, i.e., humans instead of hardware [2].

Phishing Attacks: constitute social engineering assaults that will be readily and automatically used against numerous people [2].

Leakage attacks: these are carried out via authorised users who reveal confidential information or login credentials to others or to the internet [16].

3 DL and ML for internet things

3.1 Machine learning algorithms

3.1.1 Support vector machines (SVMs)

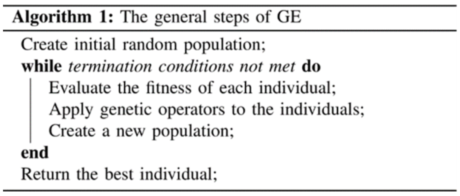
In 1963, Alexey Ya. Chervonenkis and Vladimir N. Vapnik developed the first SVM algorithm [55]. SVMs are applied to classification by dividing the attributes of the data into at least two categories, maximising the spacing among separating hyperplanes and the closest sample points of every category [58]. SVM is a frequently employed strategy for IoT security-related problems According to several studies [44, 27, 8, 29]. Recently, SVM was employed as a method to compromise device security in another area of research. The findings in [32, 22] demonstrated that ML techniques may defeat cryptographic defences, and that SVM is superior than the conventional approach in doing so. Another study in which a two-stage hybrid method was presented by Saba et al. [53] for the identification of malicious assaults in IoT networks. Along with well-known ML methods including support vector machine (SVM), ensemble classifier, and decision tree, a genetic algorithm (GA) was utilized to choose pertinent features (DT). The network's multi-class attack subcategories cannot be detected by the present systems. Additionally, the performance of the current system can be enhanced for multi-class and binary classification. Disadvantages of The SVM algorithm is difficult to choose the best kernels, as well as it takes a lot of memory and CPU time, also it takes more coding to solve problems with more than binary classification, and it performs poorly when dealing with massive data and tasks with numerous classifications.

3.1.2 k-nearest neighbors (KNN)

Is an algorithm that Evelyn Fix and Joseph Hodges first constructed in 1951 [17]. The K-Nearest Neighbor (kNN) method is one of the most widely used machine learning methods and a method with a strong theoretical foundation [25, 11, 48]. The fundamental tenet of the KNN classifier is that, inside the feature space, a sample belongs to a particular category if the majority of its k-nearest neighbors likewise do [35]. Assuming the IoT domain, a study [62] for the purpose identify the network traffic of IoT, supervised learning approaches including SVM, KNN, RF, Naive Bayes, and artificial neural networks (ANN) are effective. In more detail, they are able to recognize network intrusions and spoofing assaults. Multivariate correlation is required to detect Denial of Service (DoS) attacks. The model is 92% more accurate once it captures the geometrical relations in network traffic variables. The researchers came to the conclusion that, when deep learning was excluded, the RF performed best with malware detection and the KNN scored highest for network intrusion. KNN-based intrusion detection systems were developed by another study [34]. The proposed method showed effective and precise intrusion detection and was designed for utilize in identifying cells as malignant and benign within a wireless sensor network (WSN), a crucial component of IoT systems.

3.1.3 Grammatical Evolution(GE)

Grammatical Evolution was developed by Ryan and O'Neill in 1998 [52]. GE is a population-based optimization method that draws heavily on Darwinian evolution's mechanism of operation. It aims to create populations of potential solutions that are increasingly suited to the target environment [42]. The GE algorithm demonstrated a strong performance in identifying assaults that weren't present during training. The pseudocode of the GE algorithm is outlined in Fig. 2 [5].



```
Algorithm 1: The general steps of GE
  Create initial random population;
  while termination conditions not met do
      Evaluate the fitness of each individual;
      Apply genetic operators to the individuals;
      Create a new population;
  end
  Return the best individual;
```

Figure 2: Pseudo code of GE

Alyasiri et al. [5] , For detecting cyberattacks, the authors looked at a new grammatical evolution (GE) model. The Darwinian evolution-based population-based optimization algorithm GE. GE creates a grammar made out of rule expressions using the Backus-Naur Form notation. Over time, GE adapts to itself through crossover and mutation to provide fresh, presumably improved solutions. The IoT-MQTT dataset [23] and the Bot-IoT dataset were used to train and test the GE algorithm. Following their experiments on the Bot-IoT, GE achieved a binary classification accuracy score of 99.98%. Criticism. GE has faced considerable criticism in spite of its achievements. One problem is that GE's genetic operators do not attain high locality, which is a highly valued attribute of genetic operators in evolutionary algorithms, as a result of its mapping operation.

3.2 Machine learning algorithms

3.2.1 Convolutional neural networks (CNN)

Convolutional neural networks are based on the Neocognitron, which was introduced by Kunihiko Fukushima in the 1980's [18]. CNNs were developed in order to utilise less data than a conventional artificial neural network (ANN). Three ideas—sparse interaction, parameter sharing, and equivariant representation—are used to decrease the data parameters [19]. Figure 6 shows how CNN operates with extended IoT security.The key advantage of a CNN is this is most utilized in DL training approaches. Additionally, it makes it possible to automatically train high-performance features from the original information. Unfortunately, a CNN has a vast computational cost, making it challenging to instal it on devices with little money for onboard security. Spread architecture, however, can address this issue. A tiny deep neural network (DNN) is built and trained inside the design Utilizing just a small fraction of significant outcome categories on-board, only the deep classification is accomplished by finishing process of the algorithm's training toward the cloud level [15]. [39] suggested an Android malware detection approach based on CNN. By using CNN, it is no longer necessary to manually design features because the important features linked towards malware detection are learned automatically from the original data. The key to employing a CNN is that it can be trained to simultaneously learn appropriate features and perform classification, doing away with the extraction step necessary for classical ML and delivering an end-to-end concept [39]. However, attackers might make use of CNNs' powerful learning capabilities. A previous work [37] showed how well a CNN algorithm can be used to crack cryptographic systems.

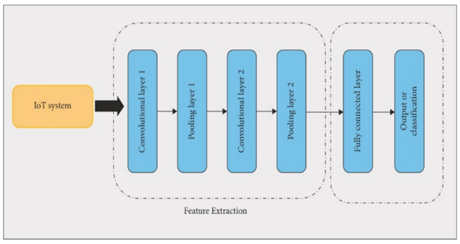


Figure 3: CNN for IoT protection

3.2.2 Recurrent Neural Networks (RNN)

David Rumelhart's work from 1986 served as the foundation for recurrent neural networks [51]. RNN is a biased DL technique that performs well in situations where data must be handled in a sequential manner. Its outcome is based on back-propagation rather than forward propagation, through contrast towards different neural networks [31, 21, 43]. An RNN includes a temporal layer for sequential data analysis, accompanied by learning concerning multi-dimensional variations in hidden recurrent components [41]. The neural network subsequently makes adjustments to these hidden units in response to the data it encounters, resulting in ongoing updates as well as the appearance of the neural network's existing state. Utilizing RNN approach, the neural network's present unrevealed by anticipating future concealed states as the triggering conditions of a prior undisclosed state. Fig. 4 describes how an RNN performs in a straightforward procedure. Here, neurons' outcomes are fed back toward the neurons in the layer below as feedback. RNNs are important in IoT safety systems, particularly network attack detection, because IoT settings are characterised by the creation of enormous volumes of sequential data, including network traffic flows. The use of an RNN for attack recognition has been proposed in earlier research [60] through network traffic behaviour analysis, and there has been observed that this approach yields useful results, especially for time series-based attacks. An IDS that employs cascaded filtering stages and deep multi-layered RNNs is proposed in another recent study [4]. Then, RNNs are taught to recognise frequent assaults made against IoT environments, such as R2L, Dos, U2R, and Probe. The design of IDS has also utilised long short-term memory (LSTM) network designs, a specific type of RNN. The ability to store data or cell state in order to subsequent use across the network is the primary characteristic of LSTM-based RNNs. They are suitable for performing analysis on temporal data that varies over time because of this property. In order to tackle issues with intrusion detection in period sequence data, LSTM networks are preferred. Researchers in [20, 46, 38, 56, 10, 68] have employed a variety of RNN types, including LSTM-based RNNs, for anomaly as well as intrusion identification in IoT networks. Although RNNs have shown promise in forecasting time series data, it is still difficult to identify anomalous traffic utilising predictions.

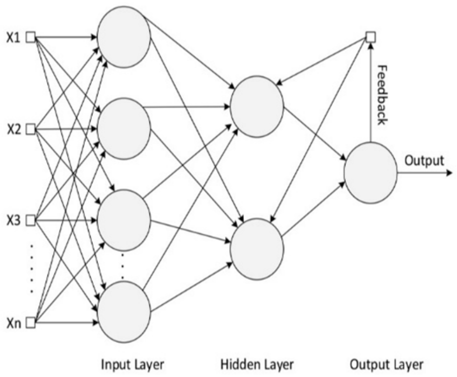


Figure 4: Illustration of RNN

3.2.3 Ensemble of DL networks (EDLNs)

It is possible for many DL algorithms to cooperate to outperform single algorithms when implemented alone. By combining generative, discriminative, or hybrid models, EDLNs can be created. When dealing with intricate issues that include high-dimensional features and uncertainty, EDLNs are frequently used. An EDLN is a collection of stacked individual classifiers that can be homogeneous Means(classifiers representing the exact similar family) either heterogeneous Means(classifiers representing various families) also is used to improve variety, accuracy, performance, as well as generalisation [30]. For instance, authors in [6] use SAE to extract features and regression layer using softmax activation function. The experiment's findings showed that, when compared to past work, our semi-supervised intrusion identification approach can detect attacks more accurately. Despite the fact that EDLNs have had remarkable success in a variety of applications, including the recognition of human activity, their use in IoT security requires further research. In particular, the potential for implementing lightweight homogenous either heterogeneous classifiers in a spread environment to enhance the precision plus effectiveness of an IoT safety system and address issues with computational complexity needs to be explored.

4 Recommended IOT security producers

Although previous IoT security problems have been resolved, more factors need to be taken into account, like the following recommendations.

- Regulating agencies should establish a recognised IoT cybersecurity framework depend on their knowledge of the sector, standards, and appropriate practises.
- To stop illegal communication, IoT devices shouldn't rely just on the network firewall.
- Analyzing the weaknesses of equipment connected to remote systems is crucial.
- Regularly updating the default login information and checking all linked devices are recommended.
- To reduce the number of sites of attack, IoT systems should be partitioned or separated.
- Threat intelligence needs to be tracked and communicated. Additionally, it is essential to scan every software to make certain that the network is secure.
- Security software must be installed, and objects plus containers must be included in order to digitally gate networks and devices.
- Threats must be monitored and information shared between individuals, organisations, and governments.
- Additional attack detection techniques, such as IP spoofing, DDoS, and so forth, may be used.
- Avoid connecting devices towards the network that have known security flaws or default passwords.
- Access credentials for controllers and device apps must be confirmed
- Devices and networks need to be patched and upgraded often.
- For access control, biometrics and strong validation should be used.
- quality encryption is required for Wi-Fi security.

Despite several efforts, the goal of protecting the IoT has not yet been achieved. IoT security remains a challenging issue. However, the deployment of snipping cybersecurity solutions powered by artificial intelligence may significantly dissuade intruders.

5 Conclusion

IoT devices have become more popular over the past ten years in all spheres of life thanks to their ability to transform things from a wide range of implementations into Internet hosts. Simultaneously time, IoT security flaws put users' protection and privacy in danger. Consequently, it is necessary to create more reliable protection solutions with IoT. One of the primary methods for IoT security is IDS that is ML plus DL based. The types of attacks against IoT devices were discussed. Also this paper referred to some research that used solutions related to the use of deep learning plus machine learning. This review paper seeks to supply researchers with concise yet valuable knowledge of the many protection concerns now existing encountered via IoT plus networks and potential remedies.

References

[1] *Global IoT and non-IoT connections 2010-2025*, https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/, Accessed Jan. 12, 2023.

[2] *Social engineering attacks on the internet of things - IEEE internet of things*, https://iot.ieee.org/newsletter/september-2016/social-engineering-attacks-on-the-internet-of-things.html, 2016, Accessed Jan. 13, 2023.

[3] S. Ali, M.A. Khan, J. Ahmad, A.W. Malik, and A. ur Rehman, *Detection and prevention of black hole attacks in IOT & WSN*, Third Int. Conf. Fog Mobile Edge Comput.(FMEC), IEEE, 2018, pp. 217–226.

[4] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, *Deep recurrent neural network for iot intrusion detection system*, Simul. Model. Pract. Theory **101** (2020), 102031.

[5] H. Alyasiri, J.A. Clark, A. Malik, and R. de Fréin, *Grammatical evolution for detecting cyberattacks in internet of things environments*, Int. Conf. Comput. Commun. Networks (ICCCN), IEEE, 2021, pp. 1–6.

[6] M.E. Aminanto and K. Kim, *Detecting active attacks in wi-fi network by semi-supervised deep learning*, Conf. Inf. Secur. Cryptography, 2017.

[7] L. Atzori, A. Iera, and G. Morabito, *The internet of things: A survey*, Comput. Networks **54** (2010), no. 15, 2787–2805.

[8] A. Azmoodeh, A. Dehghantanha, M. Conti, and Kim-Kwang R. Choo, *Detecting crypto-ransomware in iot networks based on energy consumption footprint*, J. Ambient Intell. Humaniz. Comput. **9** (2018), no. 4, 1141–1152.

[9] E. Bertino and N. Islam, *Botnets and internet of things security*, Computer (Long. Beach. Calif). **50** (2017), no. 2, 76–79.

[10] L. Bontemps, V.L. Cao, J. McDermott, and N.-A. Le-Khac, *Collective anomaly detection based on long short-term memory recurrent neural networks*, Int. Conf. Future Data Secur. Engin., 2016, pp. 141–152.

[11] P.B. Callahan and S.R. Kosaraju, *A decomposition of multidimensional point sets with applications to k-nearest-neighbors and n-body potential fields*, J. ACM **42** (1995), no. 1, 67–90.

[12] A.M. Chandrashekhar, S.T. Ahmed, and N. Rahul, *Analysis of security threats to database storage systems*, Int. J. Adv. Res. data Min. Cloud Comput. **3** (2015), no. 5.

[13] Y. Chen, Y. Li, D. Xu, and L. Xiao, *DQN-based power control for iot transmission against jamming*, IEEE 87th Vehicular Technol. Conf. (VTC Spring), 2018, pp. 1–5.

[14] M. Conti, N. Dragoni, and V. Lesyk, *A survey of man in the middle attacks*, IEEE Commun. Surv. Tutorials **18** (2016), no. 3, 2027–2051.

[15] E. De Coninck, M. Abdel-Nasser, S. Willocx, B. Peeters, P. Simoens, P. Demeester, and M. Van de Ginste, *Distributed neural networks for internet of things: The big-little approach*, Int. Internet Things Summit, 2015, pp. 484–492.

[16] D.E. Denning, *An intrusion-detection model*, IEEE Trans. Softw. Eng. (1987), no. 2, 222–232.

[17] E. Fix and J.L. Hodges, *Discriminatory analysis, nonparametric discrimination: Consistency properties*, Int. Statist. Rev. **57** (1989), no. 3, 238–247.

[18] K. Fukushima, *Neocognitron: A self-organizing neural network model for a mechanism of pattern recognition unaffected by shift in position*, Biol. Cybern. **36** (1980), no. 4, 193–202.

[19] I. Goodfellow, Y. Bengio, and A. Courville, *Deep learning*, MIT press, 2016.

[20] T. Guo, Z. Xu, X. Yao, H. Chen, K. Aberer, and K. Funaya, *Robust online time series prediction with recurrent neural networks*, IEEE Int. Conf. Data Sci. Adv. Analy. (DSAA), 2016, pp. 816–825.

[21] M. Hermans and B. Schrauwen, *Training and analysing deep recurrent neural networks*, Adv. Neural Inf. Process. Syst., vol. 26, 2013.

[22] A. Heuser and M. Zohner, *Intelligent machine homicide*, Int. Workshop Constructive Side-Channel Anal. Secure Design, Springer, 2012, pp. 249–264.

[23] H. Hindy, C. Tachtatzis, R. Atkinson, E. Bayne, and X. Bellekens, *Mqtt-iot-ids2020: Mqtt internet of things intrusion detection dataset*, 2020.

[24] I. Idrissi, M. Azizi, and O. Moussaoui, *Iot security with deep learning-based intrusion detection systems: A systematic literature review*, Fourth Int. Conf. Intell. Comput. Data Sci. (ICDS), 2020, pp. 1–10.

[25] A.M. Iliyasu and C. Fatichah, *A quantum hybrid pso combined with fuzzy k-nn approach to feature selection and cell classification in cervical cancer detection*, Sensors **17** (2017), no. 12, 2935.

[26] T. Reinbacher J. Diechmann, K. Heineke and D. Wee, *The internet of things: How to capture the value of IoT*, Tech. report, Technical Report, 2018.

[27] S.U. Jan, S. Ahmed, V. Shakhov, and I. Koo, *Toward a lightweight intrusion detection system for the internet of things*, IEEE Access **7** (2019), 42450–42471.

[28] G.W. Kibirige and C.s Sanga, *A survey on detection of sinkhole attack in wireless sensor network*, arXiv preprint arXiv:1505.01941 (2015).

[29] I. Kotenko, I. Saenko, and A. Branitskiy, *Framework for mobile internet of things security monitoring based on big data processing and machine learning*, IEEE Access **6** (2018), 72714–72723.

[30] L.I. Kuncheva, *Combining pattern classifiers: Methods and algorithms*, John Wiley & Sons, 2014.

[31] Y. LeCun, Y. Bengio, and G. Hinton, *Deep learning*, Nature **521** (2015), no. 7553, 436–444.

[32] L. Lerman, G. Bontempi, and O. Markowitch, *A machine learning approach against a masked AES*, J. Cryptographic Engin. **5** (2015), no. 2, 123–139.

[33] S. Li and L. Da Xu, *Securing the internet of things*, Syngress, 2017.

[34] W. Li, P. Yi, Y. Wu, L. Pan, and J. Li, *A new intrusion detection system based on KNN classification algorithm in wireless sensor network*, J. Electric. Comput. Engin. **2014** (2014).

[35] G. Liu, H. Zhao, F. Fan, G. Liu, Q. Xu, and S. Nazir, *An enhanced intrusion detection model based on improved kNN in WSNs*, Sensors **22** (2022), no. 4, 1407.

[36] J. Liu and W. Sun, *Smart attacks against intelligent wearables in people-centric internet of things*, IEEE Commun. Mag. **54** (2016), no. 12, 44–49.

[37] H. Maghrebi, T. Portigliatti, and E. Prouff, *Breaking cryptographic implementations using deep learning techniques*, Int. Conf. Secur. Privacy Appl. Cryptography Engin., 2016, pp. 3–26.

[38] P. Malhotra, L. Vig, G. Shroff, and P. Agarwal, *Long short term memory networks for anomaly detection in time series*, ESANN., vol. 89, 2015, pp. 89–94.

[39] N. McLaughlin, J. Martinez del Rincon, B.B. Kang, A.W.A. Wahab, H.J. Lee, and H. Kim, *Deep android malware detection*, Proc. Seventh ACM Conf. Data Appl. Secur. Privacy, 2017, pp. 301–308.

[40] M. Nawir, A. Amir, N. Yaakob, and O.B. Lynn, *Internet of things (IoT): Taxonomy of security attacks*, 3rd Int. Conf. Electronic Design (ICED), IEEE, 2016, pp. 321–326.

[41] H.F. Nweke, Y.W. Teh, M.A. Al-garadi, and U.R. Alo, *Deep learning algorithms for human activity recognition using mobile and wearable sensor networks: State of the art and research challenges*, Expert Syst. Appl. **105** (2018), 233–261.

[42] M. O'Neill and C. Ryan, *Grammatical evolution*, IEEE Trans. Evol. Comput. **5** (2001), no. 4, 349–358.

[43] R. Pascanu, C. Gulcehre, K. Cho, and Y. Bengio, *How to construct deep recurrent neural networks*, arXiv Prepr. arXiv1312.6026 (2013).

[44] D. Perez, M.A. Astor, D.P. Abreu, and E. Scalise, *Intrusion detection in computer networks using hybrid machine learning techniques*, XLIII Latin Amer. Comput. Conf.(CLEI), 2017, pp. 1–10.

[45] P. Pongle and G. Chavan, *Real time intrusion and wormhole attack detection in internet of things*, Int. J. Comput. Appl. **121** (2015), no. 9.

[46] Y. Qin, D. Song, H. Chen, W. Cheng, G. Jiang, and G. Cottrell, *A dual-stage attention-based recurrent neural network for time series prediction*, arXiv Prepr. arXiv1704.02971 (2017).

[47] R. Zaheer R. Khan, S.U. Khan and S. Khan, *Future internet: the internet of things architecture, possible applications and key challenges*, 10th Int. Conf. Front. Inf. Technol., 2012, pp. 257–260.

[48] B. Rajagopalan and U. Lall, *A k-nearest-neighbor simulator for daily precipitation and other weather variables*, Water Resources Res. **35** (1999), no. 10, 3089–3101.

[49] A. Rajan, J. Jithish, and S. Sankaran, *Sybil attack in IOT: Modelling and defenses*, Int. Conf. Adv. Comput. Commun. Inf.(ICACCI), IEEE, 2017, pp. 2323–2327.

[50] Syed Rizvi, Aaron Kurtz, Joshua Pfeffer, and Mohammad Rizvi, *Securing the internet of things (IoT): A security*

taxonomy for IoT, 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Engin. (TrustCom/BigDataSE), IEEE, 2018, pp. 163–168.

[51] D.E. Rumelhart, G.E. Hinton, and R.J. Williams, *Learning representations by back-propagating errors*, Nature **323** (1986), no. 6088, 533–536.

[52] C. Ryan, J.J. Collins, and M.O'N. Neill, *Grammatical evolution: Evolving programs for an arbitrary language*, Eur. Conf. Genetic Program., 1998, pp. 83–96.

[53] T. Saba, T. Sadad, A. Rehman, Z. Mehmood, and Q. Javaid, *Intrusion detection system through advance machine learning for the internet of things networks*, IT Profess. **23** (2021), no. 2, 58–64.

[54] S. Samonas and D. Coss, *The CIA strikes back: Redefining confidentiality, integrity and availability in security*, J. Inf. Syst. Secur. **10** (2014), no. 3.

[55] B. Schölkopf, Z. Luo, and V. Vovk, *Empirical inference: Festschrift in honor of Vladimir N. Vapnik*, Springer Science & Business Media, 2013.

[56] D.T. Shipmon, J.M. Gurevitch, P.M. Piselli, and S.T. Edwards, *Time series anomaly detection; detection of anomalous drops with limited features and sparse examples in noisy highly periodic data*, arXiv Prepr. arXiv1708.03665 (2017).

[57] K. Sonar and H. Upadhyay, *A survey: Ddos attack on internet of things*, Int. J. Eng. Res. Dev. **10** (2014), no. 11, 58–63.

[58] S. Tong and D. Koller, *Support vector machine active learning with applications to text classification*, J. Mach. Learn. Res. **2** (2001), no. Nov, 45–66.

[59] A. Torkaman and M.A. Seyyedi, *Analyzing iot reference architecture models*, Int. J. Comput. Sci. Softw. Eng. **5** (2016), no. 8, 154.

[60] P. Torres, C. Catania, S. Garcia, and C.G. Garino, *An analysis of recurrent neural networks for botnet detection behavior*, IEEE Biennial Cong. Argentina (ARGENCON), 2016, pp. 1–6.

[61] S. Vashi, J. Ram, J. Modi, S. Verma, and C. Prakash, *Internet of things (IoT): A vision, architectural elements, and security issues*, Int. Conf. I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2017, pp. 492–496.

[62] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, *Iot security techniques based on machine learning: How do iot devices use AI to enhance security?*, IEEE Signal Process. Mag. **35** (2018), no. 5, 41–49.

[63] L. Yang, C. Ding, M. Wu, and K. Wang, *Robust detection of false data injection attacks for data aggregation in an internet of things-based environmental surveillance*, Computer Networks **129** (2017), 410–428.

[64] I. Yaqoob, H. Alasmary, A. Alashaikh, E. Ahmed, H. Song, and J.J.P.C. Rodrigues, *The rise of ransomware and emerging security challenges in the internet of things*, Comput. Networks **129** (2017), 444–458.

[65] Y. Yang Y. Peng X. Wang Z. Yang, Y. Yue and W. Liu, *Study and application on the architecture and key technologies for IOT*, Int. Conf. Multimedia Technol., 2011, pp. 747–751.

[66] Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, *On secure wireless communications for iot under eavesdropper collusion*, IEEE Trans. Autom. Sci. Eng. **13** (2015), no. 3, 1281–1293.

[67] K. Zhao and L. Ge, *A survey on the internet of things security*, Ninth Int. Conf. Comput. Intell. Secur., 2013, pp. 663–667.

[68] L. Zhu and N. Laptev, *Deep and confident prediction for time series at uber*, IEEE Int. Conf. Data Min. Workshops (ICDMW), 2017, pp. 103–110.