Knowledge Engineering on Internet of Things through Reinforcement Learning

Wasswa Shafik
Computer Engineering Dept
Yazd University
Yazd, Iran

Seyed Akabr Mostafavi
Computer Engineering Dept
Yazd University
Yazd, Iran

ABSTRACT
Reinforcement learning (RL) is a new research area practical in the internet of things (IoT) where it addresses a broad and relevant task through about making decisions. RL enables interaction of devices and with the environment through a probabilistic approach using the response from its own actions and experiences. RL permits the machine and software agent to attain its behavior constructed on feedback from the environment. The IoTs extends to devices to the internet like smart electronic devices that can network and interconnect with others over through connectivity of remote resources being supervised and meticulous. In this paper, we examine the main four RL techniques including Markov Decision Process (MDP), Learning Automata (LA), artificial neural network (ANN), Q-learning in relation to its applicability in IoT, challenges and link them to state of art solutions. This review provides a summarized analysis of RL techniques that researchers can use to identify current bottlenecks in IoT and suggest models that are in line with the move.

Keywords
Internet of Things; Markov Decision Process; Learning Automata; Artificial neural networks; Q-learning

1. INTRODUCTION
Reinforcement Learning (RL) is a part of the Machine Learning (ML) techniques decide supervised, semi-supervised and unsupervised which is also a division of Artificial Intelligence (AI). Social media platforms that embedded on the Internet of Things devices nowadays utilize RL for instance automatically tag people and identify common objects like landmarks in uploaded pictures among more. Different numbers of the algorithm that tackle this applicability and automatic recovery of data are considered with times of learning and are now available [1].

IoT extends of Internet connectivity into carnal devices and ordinary items include connected contact Lenses, digital inter-device connectivity and Autonomous Self-Healing Systems, Smart Lock and Smart Mirror. Embedded with electronics, Internet connectivity, and other forms of hardware, these strategies can interconnect and interrelate with others over the Internet, and they can be remotely monitored and controlled. RL examines, evaluates a detailed sort of problem, and all its resolutions are referred to as RL algorithms. It is applied in many categories of technology phenomena like detecting the premature onset of an infection, fraud detection, resource optimization, programmed or self-driving cars, facial recognition, high volume trading among more with real-valued function [2].

Lively programming that trains algorithms by means of a system of return and consequence. The learning holds approximately studying patterns to the approach of data detection including categorize, predict, identify, and detection among others. This kind of automated learning scheme indicates that there is little requirement for a human expert who knows about the domain of submission. This will be spent designing a resolution, due to no necessity for hand-crafting complex sets of rules. RL solves percurrent problems of correlating instantaneous actions with the delayed returns they produce [3].

These algorithms are predictable to perform better more ambiguous, real-life environments through selecting from an arbitrary number of possible actions, rather than from the limited options of phenomena. Reinforcement learning is iterative, an attempt to model a complex probability distribution of rewards in relation to a very large number of state-action pairs [4].

Due to the limited perception, regularly impossibilities to determine the current state is the problem is this reward. This also affects the performance of the set of rules, and much work has been done to recompense this Perceptual Aliasing. Issues like applicable rules might be intuited, but are not easily designated by unpretentious logical rules, potential outputs are defined but which action to take is dependent on diverse circumstances which cannot be predicted, accuracy is supplementary significant than interpretation or interpretability [5].

RL is challenged with memory extensivity to store values of each state, since the problems are a times complex, solving this involves observing value approximation techniques, like neural networks. There are many connotations of introducing these imperfect value estimations and research tries to minimize their influence on the quality and the authentication enhancement where IoT is managed and maintained using this machine language [6] entity as illustrated in figure1.

Summarized operations with RL entails the following steps including Involvement that is an initial state from which the prototypical will flinch, Productivity here many imaginable productions as there are assortment of solution to a particular problem, Training based upon the input, The archetypal will reappear a state and the user will resolve to recompense or discipline the prototypical based on its output. An illustration of this type of learning procedure is denoted by one step over the next to provide a clear understanding of this artificial intelligence in figure 2.

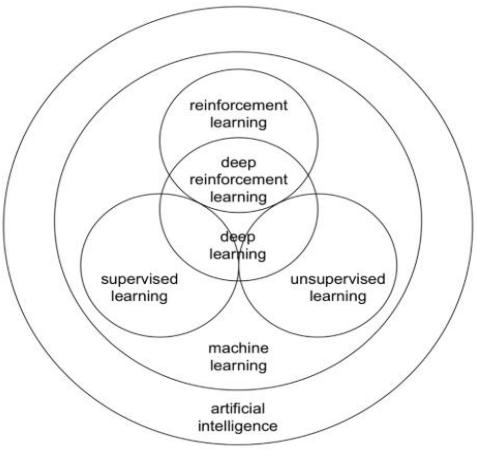

Fig. 1. Applicability of IoT Systems

Due to the limited perception, regularly impossibilities to determine the current state is the problem in this area of research, this affects the performance of the set of rules. Issues like applicable rules might be intuited, but are not easily designated by unpretentious logical rules, potential outputs are defined but which action to take is dependent on diverse circumstances which cannot be predicted, accuracy is supplementary significant than interpretation or interpretability [7].

The model keeps continues to learn at any time. The best solution is decided based on the maximum reward perhaps large environments the model of the environment is known, but an analytic solution is not available. At only, an imitation model of the environment is given and to accomplish the only way to accumulate information about the setting is to interact through it.

We observed that it is a significant issue to carry out a study on this new arena in artificial intelligence that is influenced by a numerous issues that are not classified to provide clear view on these issues and offer researchers summarized information about for reinforcement techniques in computing so that will avail the assumption of behaviors agents, current tailbacks and most models development. Hot issues in this study were tackled and presented in a simplified way in table 1. Most issues were seen learning delay detection and intrusions since reinforcement learning is developing toward connectivity so that continually leads to the need to carry out this study in devices that connect to the internet. This paper exclusively covers the following areas as summarized:

1. An inclusive and in-depth systematic survey of the main reinforcement learning techniques in IoTs.
2. Designate current state-of-the-art results solutions on IoT networks with a close focus on the reinforcement learning techniques in the IoTs.
3. Examine and describe the relationship between IoTs and the reinforcement learning techniques based on application, issues, and resolutions.
4. Provide summarized table 1 that categorizes these reinforcement learning techniques in different phenomena that cut across in resolutions, identified independent challenges.

The rest of this paper is structured as follows. In section 2 we provided related work. In section 3, we present the methodology of data collection. In Section 4, shows reinforcement techniques in summary. In Section 5, lights the bottlenecks classification and availing left-outs within the models and with a summary in table 1 together with state of the art. Lastly comes the conclusion of the paper and displays our future work.

2. RELATED WORK

In this section, we discuss different areas where RL techniques have been applied with the ability of the machines to practice and learning is recognized as algorithms. Within the security phenomena and its associated challenges including attacks[8], confidentiality and integrity, physical access within the IoTs analysis on the standard and natural policy gradients on actor-critics [9], huge or big data processing in learning [10], user simulation techniques for RL example dialogue management strategies [11], robotic systems during learning, node discovery within IoTs scenarios [12], content-aware computing with close focus on the learning and data screening analytics [13].

The procedures of machines to practice, learn are recognized as algorithms. Different algorithms are acquired in dissimilar traditions or behaviors. As data regarding observed comebacks to the environment are provided to the "machine" the algorithm's concert improves in the return increases intelligence over time like authentication frameworks. Security and its associated challenges attacks, confidentiality and integrity, physical access within the IoTs, multi-agents of RL, safety in RL direction, analysis on the standard and natural policy gradients on actor-critics, huge or big data processing in learning, user simulation techniques for RL of example dialogue management strategies, node discovery within IoTs scenarios, content-aware computing with close focus on the learning, data screening analytics were considered in this study [14].

An intelligent algorithm based on IoTs, sensor cognitive study as also significant, IoT based security solutions were sorted, data analysis in general machine learning. The combination of all these studies provided a clear path to the analysis of the RL techniques [15].

3. METHODOLOGY

A comprehensive literature search was entirely done for the current papers over the use of popular databases including IEEE Xplore, science direct, google scholar plus more associated web pages that are written in English based. The keywords during the search included RL, application of IoT, RL computing, classification review on RL, applications, and algorithms. These keywords were used in combination with the initial collection of research material.

Only papers considered relevant virtual on classification techniques, applications, challenges, and solutions were included in this survey. We only riveted commonly used classification techniques that include Artificial Neural Networks (ANN), Learning automata (LA), Markov Decision Process (MDP), and Q-Learning (QL). Different a combined classification based on the applications, issues, and current solutions are presented.

4. REINFORCEMENT LEARNING TECHNIQUES

In this section, RL techniques are presented and summarized. The machine is provided with a set of acceptable actions, rules, and potential end states. By smearing the rules, exploring different actions and detecting resulting reactions the machine learns to adventure the rules to generate the

desired result. Accordingly, determining what sequence of actions, in what surroundings, resolves to an optimized result. Mathematical algorithms and programming in space search, statistical and dynamic programming to estimate the utility of different learning aspects [16]. RL necessitated a lot of data, consequently, it is relevant in domains where simulated data is readily available identical to gameplay, robotics. Other areas include text mining or text summarization engines, dialogue agent trade transaction, health care and navigations [17]. Therefore, the four major techniques of RL is briefly explained below:

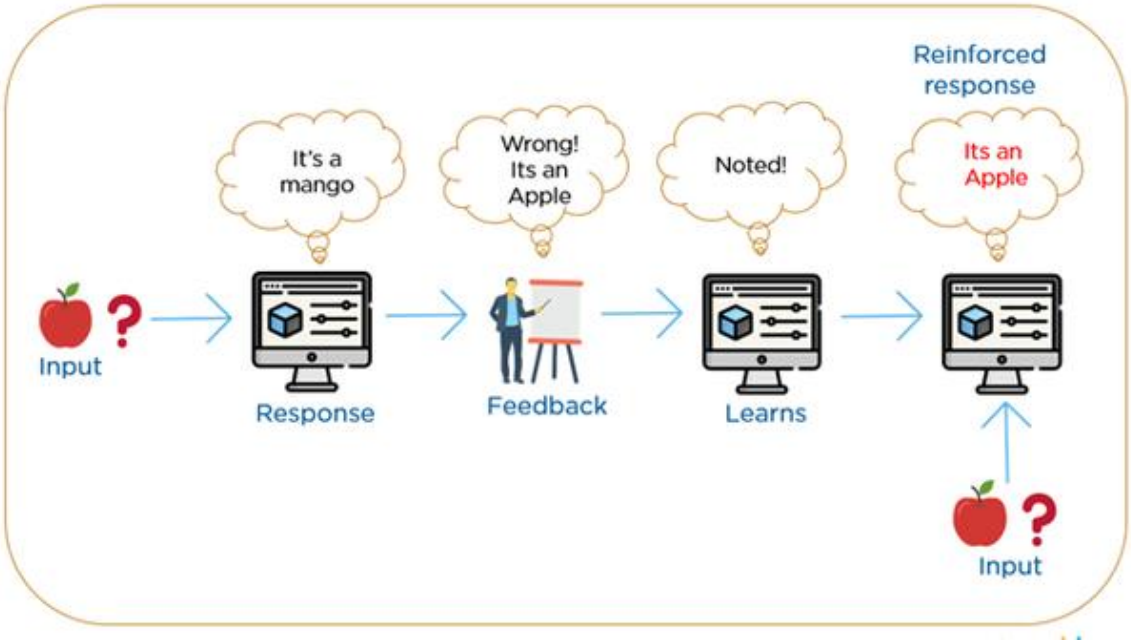

Fig. 2. Reinforcement learning with the use of IoT devices

4.1 Artificial Neural Networks (ANN)

Neural networks are sometimes called connectionist systems that use computational algorithms and capable of pattern recognition. RL is accessible as systems of interconnected "neurons" which can compute values from inputs. It is based on a collection of connected nodes called artificial neurons that loosely model the neurons in a biological brain [18]. ANN is currently used including feedforward neural network, radial basis function neural network, Recurrent Neural Network (RNN) Long Short-Term Memory, Convolutional neural networks, and Modular Neural Networks. Some of the advantages of these techniques include the ability to work with incomplete knowledge, fault tolerance, having a distributed memory, Parallel processing capability, ability to make machine learning [19].

4.2 Learning Automata

Early learning techniques that use adaptive decision-making with unit situated in a random environment that absorbs the optimal action over frequent relations with its environment. The arrangements are selected according to an explicit probability distribution which is efficiently constructed on the situation response on the automation obtains by execution a specific accomplishment [20]. LA managed a multipart, highly non-linear, indefinite and half-finished have to delicate and interactive exchange with the environment where they operate [21].

4.3 Markov Decision Process (MDP)

MDP has an isolated time stochastic control procedure providing a mathematical framework for modeling verdict creation in situations where outcomes are partly random and partly under the control of a result maker. The resolution for an MDP is a policy that designates the superlative action for each state in the MDP called the optimal policy found through a variety of methods, like dynamic programming. The difference between LA and Q-learning is that the former technique neglects the memory of Q-values, but updates the action possibility straight to find the learning result. LA is a learning scheme with a rigorous proof of convergence [22].

4.4 Q-Learning

The penalty area of QL is to absorb a policy, which expresses an agent pardon's action to take under what surroundings does not even necessitate a model of the environment and it can grip difficulties with stochastic transitions and plunders, deprived of necessitating adaptations [20]. QL holds different variants including deep Q-learning, double Q-learning, delayed Q-learning and the greedy Q-learning used in the combination with function approximation and convergence is guaranteed even when function approximation is used to estimate the action values is an advantage [23].

5. CLASSIFICATION OF RL TECHNIQUES, CHALLENGES, AND STATE OF THE ART SOLUTIONS

The most important classification techniques have been discussed in the above section with their basic merits. Within this section, we show some vital IoT benefits that RL has put forward in relation to application, issues, and solutions for most current models. Advancement in reinforcement learning technique that varieties practice of really sophisticated neural networks [24, 25]. To apply one of the four types of reinforcement every time the behavior occurs is named a Continuous Schedule. These types include positive reinforcement, negative reinforcement, punishment, and extinction. Studies have shown that positive reinforcement is vivid and works better. Below we discuss and present reinforcement learning categories based on the application and are arranged according to the impact during the learning

process.

Table 1 A: Classification of Reinforcement Learning Issues and State of the Art Solution

Technique	Issue-Based	Ref	State of the art solutions
ANN	Prediction of the performance	[26]	Precognitive ANN algorithm
	Classification of capability	[27]	Hybrid NN for document classification
	tolerance related acquisition	[28]	Management models based on Biases
	IoT crime forensics	[39]	Reinforced forensics detection
	fraud detection in IoT application	[40]	A neural-fuzzy model
			An automated GIS- ANN model
LA	Predicting Software Defects on IoTs	[41]	Development of the LA predicting models.
	Prediction of behavioral changes	[42]	Computation and data-driven modeling
	signature verification	[43]	Deep learning driven detection models
	analysis and decisions	[44]	Design Deep generating model
	auto-selection of IoT task	[45]	A predictive model based on ANN
	traffic incident detection	[46]	Wave font cellar LA modeling
	telecommunication	[47]	Use of Botnet Detection
	Internet networks	[48]	Ensure distributed learning models
	Reinforcement Recognition	[49]	Development of the LA predicting models.
	Short-term traffic forecasting	[50]	Probabilistic methodologies

5.1 Products Referencing

RL has permitted nowadays a product-based endorsement system since models can identify those products in which that purchaser drives be attentive and standpoints to acquisitions. The RL algorithm recognizes concealed patterns amongst substances and emphases on an alliance of similar products into bands. An RL model of this decision procedure would permit a program to brand approval to a purchaser and motivate product purchases sideways with section detail is used by social media to acclamation users to connect with other operators.

5.2 Health Analyses

The special attachment we all have in the field of medicine, RL has improved the patient's health with minimum expense injection. Considering a case of RL is making near-flawless detects, commendation superlative medicines, forecast readmissions and recognize high-risk patients. Completely these calculations are based on the dataset of anonymized patient records and symptoms displayed by a patient.

5.3 Lifetime Dissection and Rate prediction

Prediction actually one of the main challenges faced by any IoT application. IoT state of affairs has a huge number of devices relevant data from various foundations like website visitors and lead data. By the use of data mines and RL, a precise prediction for individual IoT offers and incentives can be proficient through the use of RL in eradicating all sorts of guesswork complicated in the data-driven set-up of IoT like the pattern of behavior by a user identifying chances of conversion to paid variety can be forecast.

Table 2B. A: Classification of Reinforcement Learning Issues and State of the Art Solution

Technique	Issue-Based	Reference	State of the art solutions
MDP	Reinforcement Recognition	[51]	Filter models
	Short-term traffic forecasting	[52]	Code retrieval
	long-term traffic flow forecasting	[53]	Multi-period decision-making models
	Data classification	[54]	A Self-supervised Approach
	Speech and text recognition	[55]	Automating keystroke-level modeling
	Face recognition	[56]	Hidden Markov modeling
QL	IoT decision and processing division	[35]	Q-Learning model for decision making
	IoT decision and processing division	[8]	Handoff based RL modeling
	IoT Induction detection	[43]	Deep computation model
	IoT fault diagnosis		Distant supervision relation extractor
	Navigational IoT detection	[42]	Fault data management

5.4 Economic Investigation

Unresolved to large data volumes, nature quantitative and precise historical data, RL so used in monetarist bearing of mind an occasion of RL in backing comprises algorithmic interchange, selection management, fraud detection and loan guaranteeing, RL enables continual taxations of data for detection and analysis of incompatibilities and gradations to progress the precision of models, directions and sentiment analysis.

5.5 Predictive Maintenance

Counteractive and precautionary preservation observes are expensive and uncreative, RL planning is built on the authenticity of historical IoT device data, self-motivated analysis situation, workflow commencement tool, and processes reply circlet. RL algorithm obtains the affiliation amongst sensor fluctuations and value in feeler moralities to antique failures.

5.6 Identical Recognition

IoT devises vision harvests symbolic statistics from images or duplicates and high-dimensional facts. RL encompasses dynamic learning, data mines, database evidence detection and pattern recognition, image recognition technology, healthcare mentioned but a few. In table 1b and 2b above, we present a summarized table of current state-of-the-art solutions to other RL challenges.

An RL representative learns by interacting with its environment. The agent receives rewards by accomplishment correctly and penalties for performance inaccurately. The agent learns without interference from a human by maximizing its reward and minimizing its penalty. These algorithms are predictable to perform better more ambiguous, real-life environments through selecting from an arbitrary number of possible actions, rather than from the limited options of phenomena. RL is iterative, a challenge to archetypal a complex probability distribution of plunders in relative to an identical large quantity of state-action pairs.

6. ACKNOWLEDGMENTS

This research has been supported by Yazd University. The authors would like to recognize the support and remarks shared with them from the Computer Engineering department members to attain this paper quality.

7. REFERENCES

[1] C. H. Liu, Q. Lin, and S. Wen, “Blockchain-enabled Data Collection and Sharing for Industrial IoT with Deep Reinforcement Learning,” IEEE Transactions on Industrial Informatics, 2018.

[2] J. Chen, S. Chen, Q. Wang, B. Cao, G. Feng, and J. Hu, “iRAF: a Deep Reinforcement Learning Approach for Collaborative Mobile Edge Computing IoT Networks,” IEEE Internet of Things Journal, 2019.

[3] Y. Wei, F. R. Yu, M. Song, and Z. Han, “Joint Optimization of Caching, Computing, and Radio Resources for Fog-Enabled IoT Using Natural Actor-Critic Deep Reinforcement Learning,” IEEE Internet of Things Journal, 2018.

[4] M. Mohammadi, A. Al-Fuqaha, M. Guizani, and J.-S. Oh, “Semisupervised deep reinforcement learning in support of IoT and smart city services,” IEEE Internet of Things Journal, vol. 5, no. 2, pp. 624–635, 2018.

[5] A. Singla and A. Sharma, “Physical Access System Security of IoT Devices using Machine Learning Techniques,” Available at SSRN 3356785, 2019.

[6] C. H. Liu, Q. Lin, and S. Wen, “Blockchain-enabled Data Collection and Sharing for Industrial IoT with Deep Reinforcement Learning,” IEEE Transactions on Industrial Informatics, 2018.

[7] S. Yousefi, F. Derakhshan, and A. Bokani, "Mobile Agents for Route Planning in the Internet of Things Using Markov Decision Process," in 2018 IEEE International Conference on Smart Energy Grid Engineering (SEGE), 2018, pp. 303–307.

[8] P. Sun, J. Li, M. Z. A. Bhuiyan, L. Wang, and B. Li, "Modeling and clustering attacker activities in IoT through machine learning techniques," Information Sciences, vol. 479, pp. 456–471, 2019.

[9] A. Singla and A. Sharma, "Physical Access System Security of IoT Devices using Machine Learning Techniques," Available at SSRN 3356785, 2019.

[10] P. Punithavathi, S. Geetha, M. Karuppiah, S. H. Islam, M. M. Hassan, and K.-K. R. Choo, "A lightweight machine learning-based authentication framework for smart IoT devices," Information Sciences, vol. 484, pp. 255–268, 2019.

[11] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," arXiv preprint arXiv:1904.05735, 2019.

[12] I. Grondman, L. Busoniu, G. A. Lopes, and R. Babuska, "A survey of actor-critic reinforcement learning: Standard and natural policy gradients," IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 42, no. 6, pp. 1291–1307, 2012.

[13] J. Qiu, Q. Wu, G. Ding, Y. Xu, and S. Feng, "A survey of machine learning for big data processing," EURASIP Journal on Advances in Signal Processing, vol. 2016, no. 1, p. 67, 2016.E. K. Wang, T.-Y. Wu, C.-M. Chen, Y. Ye, Z. Zhang, and F. Zou, "Malpas: Markov decision process based adaptive security for sensors in the internet of things," in Genetic and Evolutionary Computing, Springer, 2015, pp. 389–397.

[14] Mostafavi, M. Dehghan, "Game-theoretic Bandwidth Procurement Mechanisms in Live P2P Streaming Systems", Multimedia Tools and Applications, vol. 75, no. 14, pp. 8545-8568, 2016.

[15] S. Mostafavi, M. Dehghan, "Game-theoretic Auction Design for Bandwidth Sharing in Helper-assisted P2P Streaming", International Journal of Communication Systems, vol. 29, no. 6, pp. 1057-1072, 2016.

[16] S. M. Matinkhah and W. Shafik, "A Study on Financial Pricing and Applications models on 5G," in 4th international Mathematical Conference and Modelling, pp. 52.

[17] W. Shafik and S. M. Matinkhah, "Admitting New Requests in Fog Networks According to Erlang B Distribution," in 2019 27th Iranian Conference on Electrical Engineering (ICEE), 2019, pp. 2016–2021.

[18] S. M. Matinkhah, W. Shafik, and M. Ghasemzadeh, "Emerging Artificial Intelligence Application: Reinforcement Learning Issues on Current Internet of Things." in 2019 16th international Conference in information knowledge and Technology(ikt2019), pp. 2019 ICIKT10_062.

[19] S. Mostafavi and W. Shafik, "Fog Computing Architectures, Privacy and Security Solutions," J. Commun. Technol. Electron. Comput. Sci., vol. 24, pp. 1–14, 2019.

[20] W. Shafik, S. M. Matinkhah, and M. Ghasemazade, "Fog-Mobile Edge Performance Evaluation and Analysis on Internet of Things," J. Adv. Res. Mob. Comput., vol. 1, no. 3.

[21] W. Shafik and S. M. Matinkhah, "How to use Erlang B to determine the blocking probability of packet loss in a wireless communication," in presented at the 13th Symposium on Advances in Science & Technology, 2018.

[22] W. Shafik and S. M. Matinkhah, "Privacy Issues in Social Web of Things," in 2019 5th International Conference on Web Research (ICWR), 2019, pp. 208–214.

[23] S.-H. Zahiri, "Learning automata-based classifier," *Pattern Recognition Letters*, vol. 29, no. 1, pp. 40–48, 2008.

[24] B. Braune, S. Diehl, A. Kerren, and R. Wilhelm, "Animation of the generation and computation of finite automata for learning software," in *International Workshop on Implementing Automata*, 1999, pp. 39–47.

[25] K. S. Narendra and M. A. Thathachar, "Learning automata-a survey," *IEEE Transactions on systems, man, and cybernetics*, no. 4, pp. 323–334, 1974.

[26] A. K. Ghosh, C. Michael, and M. Schatz, "A real-time intrusion detection system based on learning program behavior," in *International Workshop on Recent Advances in Intrusion Detection*, 2000, pp. 93–109.

[27] C. L. Giles, C. B. Miller, D. Chen, H.-H. Chen, G.-Z. Sun, and Y.-C. Lee, "Learning and extracting finite state automata with second-order recurrent neural networks," *Neural Computation*, vol. 4, no. 3, pp. 393–405, 1992.

[28] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *Journal of Network and Computer Applications*, vol. 84, pp. 25–37, 2017.

[29] A. Abduvaliyev, A.-S. K. Pathan, J. Zhou, R. Roman, and W.-C. Wong, "On the vital areas of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 1223–1237, 2013.

[30] R. Zhao, R. Yan, Z. Chen, K. Mao, P. Wang, and R. X. Gao, "Deep learning and its applications to machine health monitoring: A survey," *arXiv preprint arXiv:1612.07640*, 2016.

[31] S. Misra, P. V. Krishna, H. Agarwal, A. Saxena, and M. S. Obaidat, "A learning automata-based solution for preventing distributed denial of service in Internet of things," in *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, 2011, pp. 114–122.

[32] M. Weisman *et al.*, "Machine Learning and Data Mining for IPv6 Network Defence," in *International Conference on Cyber Warfare and Security*, 2018, pp. 681–XVI.

[33] W. Jiang, C.-L. Zhao, S.-H. Li, and L. Chen, "A new learning automata-based approach for online tracking of event patterns," *Neurocomputing*, vol. 137, pp. 205–211, 2014.

[34] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad hoc networks*, vol. 11, no. 8, pp. 2661–2674, 2013.

[35] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *Journal of network and computer applications*, vol. 42, pp. 120–

134, 2014.

[36] M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, and M. Guizani, "A survey of machine and deep learning methods for internet of things (IoT) security," *arXiv preprint arXiv:1807.11023*, 2018.

[37] K. Zaheer, M. Othman, M. H. Rehmani, and T. Perumal, "A Survey of Decision-Theoretic Models for Cognitive Internet of Things (CIoT)," *IEEE Access*, vol. 6, pp. 22489–22512, 2018.

[38] L. Cao, G. Weiss, and S. Y. Philip, "A brief introduction to agent mining," *Autonomous Agents and Multi-Agent Systems*, vol. 25, no. 3, pp. 419–424, 2012.

[39] O. B. Sezer, E. Dogdu, and A. M. Ozbayoglu, "Context-aware computing, learning, and big data in internet of things: a survey," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 1–27, 2018.

[40] C. Gomez, A. Shami, and X. Wang, "Machine Learning Aided Scheme for Load Balancing in Dense IoT Networks," *Sensors*, vol. 18, no. 11, p. 3779, 2018.

[41] F. M. Al-Turjman, "Information-centric sensor networks for cognitive IoT: an overview," *Annals of Telecommunications*, vol. 72, no. 1–2, pp. 3–18, 2017.

[42] M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1996–2018, 2014.

[43] K. Ye, "Key Feature Recognition Algorithm of Network Intrusion Signal Based on Neural Network and Support Vector Machine," *Symmetry*, vol. 11, no. 3, p. 380, 2019.

[44] J. Abreu, L. Fred, D. Macêdo, and C. Zanchettin, "Hierarchical Attentional Hybrid Neural Networks for Document Classification," *arXiv preprint arXiv:1901.06610*, 2019.

[45] K. Wang, "Network data management model based on Naïve Bayes classifier and deep neural networks in heterogeneous wireless networks," *Computers & Electrical Engineering*, vol. 75, pp. 135–145, 2019.

[46] P. F. Fantoni, "A neuro-fuzzy model applied to full range signal validation of PWR nuclear power plant data," *INTERNATIONAL JOURNAL OF GENERAL SYSTEM*, vol. 29, no. 2, pp. 305–320, 2000.

[47] M. Kahng, N. Thorat, D. H. P. Chau, F. B. Viégas, and M. Wattenberg, "GAN Lab: Understanding Complex Deep Generative Models using Interactive Visual Experimentation," *IEEE transactions on visualization and computer graphics*, vol. 25, no. 1, pp. 310–320, 2019.

[48] D. Popa, F. Pop, C. Serbanescu, and A. Castiglione, "Deep learning model for home automation and energy reduction in a smart home environment platform," *Neural Computing and Applications*, pp. 1–21, 2019.

[49] S. Baruah, "Botnet Detection: Analysis of Various Techniques," *International Journal of Computational Intelligence & IoT*, vol. 2, no. 2, 2019, pp 7-14.

[50] A. Mollalo, L. Mao, P. Rashidi, and G. E. Glass, "A GIS-Based Artificial Neural Network Model for Spatial Distribution of Tuberculosis across the Continental United States," *International journal of environmental research and public health*, vol. 16, no. 1, p. 157, 2019.

[51] R. V. McCarthy, M. M. McCarthy, W. Ceccucci, and L. Halawi, "Predictive Models Using Neural Networks," in *Applying Predictive Analytics*, Springer, 2019, pp. 145–173.

[52] A. Rezvanian, B. Moradabadi, M. Ghavipour, M. M. D. Khomami, and M. R. Meybodi, "Introduction to Learning Automata Models," in *Learning Automata Approach for Social Networks*, Springer, 2019, pp. 1–49.

[53] A. Rezvanian, B. Moradabadi, M. Ghavipour, M. M. D. Khomami, and M. R. Meybodi, "Wavefront Cellular Learning Automata: A New Learning Paradigm," in *Learning Automata Approach for Social Networks*, Springer, 2019, pp. 51–74.

[54] S. Matwin, L. Tesei, and R. Trasarti, "Computational modelling and data-driven techniques for systems analysis," *Journal of Intelligent Information Systems*, pp. 1–3, 2019.

[55] S. Misra, P. V. Krishna, V. Saritha, H. Agarwal, and A. Ahuja, "Learning automata-based multi-constrained fault-tolerance approach for effective energy management in smart grid communication network," *Journal of Network and Computer Applications*, vol. 44, pp. 212–219, 2014.

[56] I. Erev and G. Barron, "On adaptation, maximization, and reinforcement learning among cognitive strategies.," *Psychological review*, vol. 112, no. 4, p. 912, 2005.