International Journal on Emerging Technologies **12**(2): 245-250(2021)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Machine Learning and Deep Learning for Challenging Security of IoT: Analysis and Impact

Amir Ijaz[1], Saleem Raza[2], Naveed Imran[3], Mubashir Ali[4*] and Vaneeza Iman[4]
[1]Department of Computer Engineering, HITEC University, Taxila, Pakistan.
[2]Department of Electronic Engineering, Quaid-e-Awam University of Engineering, Science and Technology, Nawabshah, Pakistan.
[3]Department of Computer Science, University of Central Punjab, Lahore, Pakistan.
[4]Department of Software Engineering, Lahore Garrison University, Lahore, Pakistan.

(Corresponding author: Mubashir Ali)*
(Received 01 May 2021, Revised 01 June 2021, Accepted 23 June 2021)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Internet of Things (IoT) is an emerging technology that is expected to revolutionize the embedded systems, industry 4.0, and society 5.0. The IoT infrastructure is heterogeneous and will generate sensed data in exponential ratio. Wireless sensor networks, cloud computing, edge computing, and various other technologies lay the necessary foundation for IoT systems. Several challenges need to be addressed before IoT can be used on a large commercial scale. One of the prime challenges of IoT is security, which due to its heterogeneous and distributed nature which needs to be addressed. Emerging technologies, such as Machine learning (ML) and deep learning (DL) provide intelligence to IoT applications and set new benchmarks for security issues. In this paper, we analyze the role, impact, and contribution of ML and DL for IoT applications specifically focusing on IoT security. We discuss different techniques such as supervised learning, unsupervised learning, semi-supervised learning, reinforcement learning, and deep learning. Finally, we present the future research directions along with current challenges which need to be addressed.

Keywords: Machine Learning, Deep Learning, Internet of Things, Security, Privacy, Data Analysis.

I. INTRODUCTION

Internet of things (IoT) is the most recognizable technology in the current era with unlimited applications in all domains [1]. It brings revolution from medical to agriculture and education to no boundaries. IoT transferred the manual processes and systems to smart and automated systems[2]. Various sensors and smart devices are implemented within IoT systems which are producing sensed data in an exponential rate. Along with IoT, various other emerging and evolving technologies in recent years with more improvement to the internet protocols and computing systems made easier communication between different devices or computers. Internet protocols are used to send or receive data from one computer to another, every computer has its IP address which distinguishes it from another computer on the internet [3]. Whenever a computer sends or receives any type of information, this will possible only with the help of internet protocols. Almost twenty to fifty billion machines are presumed to relate to the Internet in 2021 [4]. We can say that IoT is our future. IoT is a combination of submerging technologies about wireless and wired communications, actuator devices, sensors, and the physical objects that are connected to the Internet [5]. Each object or system has its IP which distinguishes it from other objects or systems that are connected with the help of internet of things (IoT). Actuators convert an electrical signal to the physical action, task, or work [6]. IoT aims to connect all the devices through the internet. This will reduce the work of a man, as the computer will do the same job by itself instead of an individual. The main objective of computing is to simplify and improve human activities. IoT will collect all the information through different means, this information is not analyzed nor organized, when the information is elicited in raw the system will be able to analyze this raw information. By analyzing the raw information, the knowledge will be extracted. So, IoT needs efficient data processing technologies to present better services to users and to enhance the structure of overall IoT performance. IoT has taken over almost everything in our society like banking, meeting setting, e-learning, agriculture, industry, transportation, smart health, and businesses. As data is available in digital format, the security of data is the foremost concern in IoT systems.

Currently, IoT generates a huge amount of data. The field that use algorithms, processes, and scientific methods to collect knowledge from structured and unstructured data is known as data science [7]. Machine learning is an application of artificial intelligence which gives the ability to the system to automatically learn and improve from experience without being explicitly programmed [8]. Machine learning focuses on the development of computer programs that can access data and use it to learn for themselves. Machine learning is significantly adopted in numerous applications of IoT to fulfill the advanced requirements which are not possible with traditional methods. Optimized artificial intelligence and machine learning techniques are required by IoT to cope with challenging and complex tasks of the current technological era. Various technologies are providing basic infrastructure to IoT systems such as cloud computing, wireless sensor networks, edge computing, 4G and 5G communication. Owing to such heterogeneous use of technologies, data privacy and protection is primary apprehension by addressing the challenging security attacks. Mostly wearable and node devices are responsible for sensing and transferring data through smartphones which leads to leakage of information concerns. Further, it is challenging for IoT devices to

perform well under the low resourced environments such as short battery life, small memory and computation power for heavy streams of data. The heterogeneous nature of IoT systems exposes them to easy security breaches.

Security of IoT systems is more critical than other standalone systems. There is another truth that the IoT systems are more vulnerable, so appropriate techniques are required to examine and ensure the security of IoT systems. Huge sensed data and their processing, intelligent prediction, decision-taking of IoT systems and IoT security is the main problem which is faced and there is a need to address these problems to efficiently cope with future systems.

II. INTERNET OF THINGS

Internet of Things (IoT) aims to build an intelligent smarter environment and a convenient lifestyle by saving energy, effort and money [9]. It automates every process of life in smart ways. It enhances industry productivity by saving resources. In modern times, humans have started to depend more and more on technology. In fact, in 2008 the total connected devices on the internet exceeded the total population of humans. Devices like mobiles phones, sensors and actuators work together to handle tasks and their use will keep on increasing in newer more complex ways. We have entered an era where modern devices share data on through networks, and this helps to collect data easier. IoT refers to modern devices connected, to share information these devices include sensors, actuators and embedded systems having a microprocessor [10].

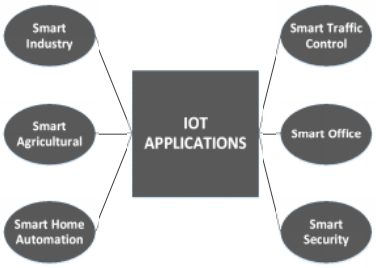

Fig. 1. IoT Applications.

The idea is to reduce human-to-human and human-to-machine interaction as much as possible and connect machines with networks to handle all the data exchanges themselves using machine-to-machine interaction. In IoT, data can be shared at short range using Wi-Fi, ZigBee, and Bluetooth or using a wide range of technologies like NB-IoT, LoRa, GSM, GPRS, CAT M1, Sigfox, WiMAX, 3G, 4G, LTE, and 5G. Every IoT device has its own uses and limitations. There should be a balance between processing power, energy consumption and cost, hence it is important to select the right device for the right scenario. IoT Infrastructure uses platforms like Thing Speak, Main flux, Things Board, Kaa, or Device Hive and protocols such as AMQP, XMPP, STOMP,MQTT, HTTP and CoAP [11]. IoT platforms offer capabilities like storing and analyzing data, managing nodes and monitoring, etc. IoT devices are low-end and cannot handle heavy data transmissions and processing. This calls for new techniques including cloud computing, edge computing and fog nodes. The idea is to provide something that has enough resources to handle heavy tasks and hence lowering the load on low-end IoT devices. Data obtained from devices can be stored on cloud servers where it can be analyzed by different machine learning techniques. This leads us to IoT applications which are nowadays widely used in smart city projects. As the number of devices and data has increased tremendously, researchers have taken interest in Machine Learning and have developed modern AI technologies to handle complex tasks [12].

A. Cloud Computing

Cloud computing is an evolving technology that provides ubiquitous, on-demand, convenient, reliable and secure network access to shareable resources that can easily be configured, used and managed with the help of cloud service providers, stated by the National Institute of Standards and Technology (NIST) [13].

It is an ultimate solution to the current need for advanced systems which work on the model of “Pay As You Go”. Users can access the high level of resources as per their needs with minimum budget and manageable efforts. Maximum IoT systems are integrated with different cloud services to efficiently process and store real time data. Now, special cloud services are available which are specially designed for IoT.

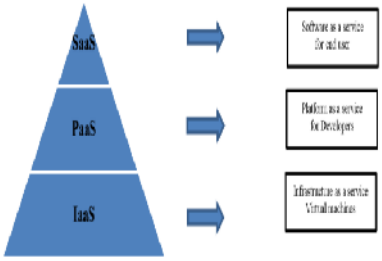

Fig. 2. Cloud Services [14].

B. Fog Computing

As cloud computing providing a number of benefits, there are few prime disadvantages that are faced by cloud services. Normally, the cloud data centers are centralized and far from users which requiring high network access resources known as latencies. The high latencies are normal for traditional applications such as web or enterprise systems, but in the context of real-time systems such as IoT and autonomous driving, it causes problems. These latest systems are developed with the help of edge nodes or devices which come with low resources but requiring low latencies. So in this situation, the fog computing is an ultimate solution which considers both cloud and edge nodes by addressing low latency issue. Fog computing is an extension of cloud computing and it is more secure than the cloud because it is not sharing all data into the cloud [15]. The personal data of edge nodes are kept to edge while the filtered data is forwarded to cloud. Fig. 3 shows the high-level deployment aspects of fog computing.

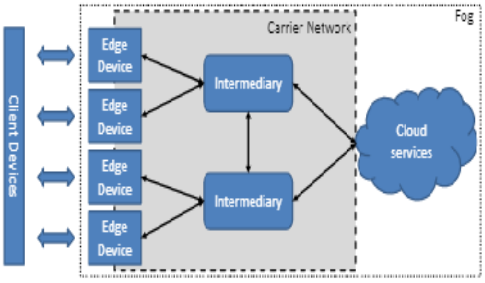

Fig. 3. Deployment Aspects of Fog Computing [16].

C. Edge Computing

The prime issue in cloud computing is end to end reliable communication of between end device and cloud. Further, the time taken for transfer of data from the mobile device to cloud, then processing on cloud and action back to the mobile device is high and cost big in terms of usable resources. Edge nodes refer to the endpoint devices which are connected in any system that collects the data and performs the actions [17]. Further, there is critical private information that is associated with edge nodes and the transfer of this information enhances the security challenges itself. In comparison to traditional systems, the IoT systems consist of many edge nodes [18].

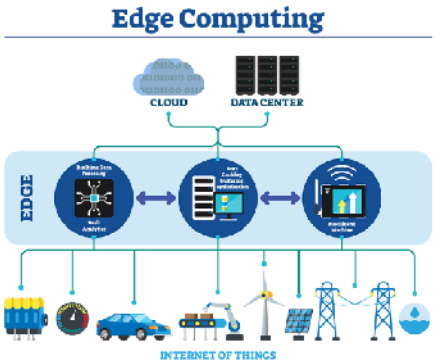

Fig. 4. Edge Computing Overview [19].

The marvelous advancement is seen in an system on chip embedded systems which are incorporated with full-fledged hardware compatibility and own operating system. Previously, the IoT nodes only collect the data and transfer it to the cloud but now due to the system on chip technology of end nodes, it enhances their capability of self-computing [20].

III. MACHINE LEARNING FOR IOT

The concept of machine learning (ML) has been around for a while. Machine learning is a sub domain of artificial intelligence [21]. ML helps computer systems in learning different tasks such as clustering, predictions, classification, pattern recognition etc. The Computer systems can be trained to analyze sample data by using different statistical models and algorithms [22, 23]. Sample data can be characterized by its features for measurable characteristics. The Machine learning algorithm is used to observe the correlation between features and output values which are also known as labels. As the machine learns and figures out how to identify new patterns and makes decisions on the basis of new data. IoT systems are integrated with autonomous manners and they need to take self-decisions in most cases. Currently, machine learning is the appropriate solution to IoT systems which brings intelligence and smartness in them.

Now, latest business format requires strong IoT connection, high privacy and security, full coverage, extreme high dependability, and very low waiting time. 5G with AI, IoT enhanced data transfer speed, best coverage and great flow rate, providing a solution to businesses [24]. The structure of IoT must be highly optimized. Flexibility, power utilizing, and solving problems must be recognizing for effective implementation of IoT. Flexibility problems are solved by establishing multi-hop routing protocols occupying greater range and are automatically modifiable [25]. The power utilizing problem is solved by using power gathering method [26], designing power-saving MAC [27] and cross-layer protocols. Managing large number of IoT data of all internet connected devices is tiresome job. Also, power efficiency of data centers need to be examined. So to solve these problems, artificial intelligence methods, novel fusion algorithms, ultra-modern temporal machine learning techniques and neural networks are necessary for autonomous decision and power saving [25]. Security of user data is one of the major problems in IoT structure. User data must be protected and managed by user itself. Many cryptographic algorithms are suggested for authentication but they consume lot of energy [28].

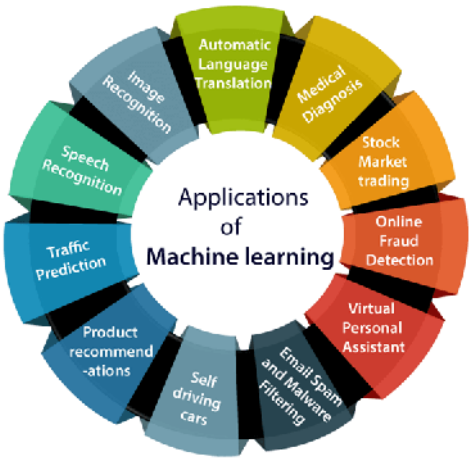

Fig. 5. Applications of Machine Learning [29].

A. Supervised Learning for IoT

Supervised learning copes with regression problems and uses algorithms like linear regression and random forest, to deal with problems such as life experience estimation, weather forecasting and population growth predictions. Algorithms such as a nearest neighbor, support vector machines, the forest can be used for classification problems such as speech recognition, digit recognition, and identity fraud detection and diagnostics [8, 30, 31]. Supervised learning can be classified into two phases namely training and testing phase. Data is given in the training phase and has labels. The algorithm tries to learn the relationship between Input and labels and tries to predict the correct output value of the data.

Supervised machine learning algorithms work on the basis of labelled data and perform adaptive filtering, localization, security handling, spectrum sensing and channel estimation in IoT networks. While the regression is used to predict the continuous numeric data in IoT traffic for highlighting trends. SVM face the low memory issues in the kernel which create a problem for modeling heavy datasets. Naïve Bayes is used to detection of spam and malware in IoT networks. Random forest performs well for large datasets where SVM faces issues. Random forest is also used for the identification of valid device categories from the white lists to pass the traffic and network data [32]. An intrusion detection system is developed with supervised machine learning techniques to handle unexpected intrusions [33]. Supervised learning is also used to examine the irregularities in IoT systems. A Neural network is used to detect invalid data nodes in the IoT network [34]. The Artificial neural network is used for threat assessment and mitigation in IoT networks [35].

B. Unsupervised Learning

Conditionality reduction problems can be solved by unsupervised learning. It is used for feature elicitation, data visualization or for discovering hidden structures. Unsupervised learning is used for clustering problems such as customer segmentation, targeted marketing and recommendation systems. If we compare this to supervised learning, labels are not available in unsupervised learning which tries to identify patterns on testing data and cluster the data for predicting future values [36,37].

C. Semi-supervised Learning

In semi-supervised learning both labeled and unlabeled data are used[38]. In simple terms, most of its working is like unsupervised learning with some of the improvements using labeled data.

D. Reinforcement Learning

In reinforcement learning problems are based on tuning parameters and the algorithm tries to predict the output. The output is then processed again and again till an optimal output is obtained [39]. This learning style is used in deep learning and neural networks [37]. Nowadays it is mainly used in AI gaming, robot navigation, real-time decisions and skill acquisitions.

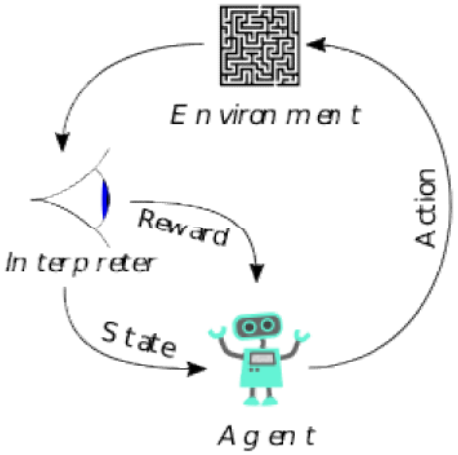

Fig. 6. Reinforcement Learning [40].

Computational power and speed are two major parameters that need to be considered when choosing a machine learning technique for a specific application. For example, in real-time analysis a technique that is fast enough to change the input data and produce the required results on time.

IV. DEEP LEARNING FOR IOT

Internet of things raised significant challenges in the context of data privacy and secured communication. Deep learning has appeared as the strongest backbone of artificial intelligence for modern systems [41]. Deep learning is widely used in robotics, computer vision, embedded systems and various other applications. Deep learning provides some key benefits in comparison to machine learning such as [42],

- No restriction on hidden layers of neural networks
- CNN and LSTM directly works with raw data
- Coping with big data challenges

Deep learning helps to efficiently analyze the huge, complicated and complex data which is generated by IoT infrastructure. Furthermore, deep learning helps the IoT to understand the complicated patterns of real-time data where machine learning stops. Deep learning providing state of the art mechanisms for

- Device identification in heterogeneous IoT environment via IMEI codes, images and radio fingerprinting [43], [44]
- Efficient extraction of service fingerprints in dynamic networks [45, 46]
- Integrity testing against hardware Trojan detection [47]
- Network behavior analysis in IoT [48]
- Federated learning for data security and privacy [49, 50]

V. CHALLENGES AND DIRECTIONS

As the IoT infrastructure is based on resource-constrained environment with distributed and heterogeneous nodes, it faces various challenges which need to address such as,

- Time efficiency and Memory efficiency
- Power constraints
- Need high adaptability due to heterogeneous nature
- Heterogeneous data.

VI. CONCLUSION

Internet of things enabling future generation automated systems with the help of various supporting technologies such as cloud computing, fog computing, edge computing and wireless sensor networks. IoT systems generating sensed data in huge volume which is also in dynamic nature like text, audio, video, images etc and need efficient analysis for decision making. IoT security is very critical and challenging due to its heterogeneous environment. Machine learning and deep learning are revolutionizing every domain and best candidates for addressing data analysis and security challenges in IoT. We have described the IoT with their supporting technologies. After that, we elaborated on the role and impact of machine learning and deep learning in IoT. Furthermore, we highlighted the current research challenges and future research directions.

REFERENCES

[1]. Ande, R., Adebisi, B., Hammoudeh, M., & Saleem, J. (2020). Internet of Things: Evolution and technologies from a security perspective. *Sustainable Cities and Society*, *54*, 101728.

[2]. Čolaković, A., & ialić, M. (2018). Internet of Things (IoT): a review of enabling technologies, challenges, and open research issues. *Comput Netw*, *144*, pp. 17–39.

[3]. P. Fraga-Lamas, T. Fernández-Caramés, M. Suárez-Albela, L. Castedo, and M. González-López, “A Review on Internet of Things for Defense and Public Safety,” *Sensors*, vol. *16*, no. 10, p. 1644, Oct. 2016, doi: 10.3390/s16101644.

[4]. M. A. Khan and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” *Futur. Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018, doi: 10.1016/j.future.2017.11.022.

[5]. M. Banerjee, J. Lee, and K. K. R. Choo, “A blockchain future for internet of things security: a position paper,” *Digit. Commun. Networks*, vol. 4, no. 3, pp. 149–160, Aug. 2018, doi: 10.1016/j.dcan.2017.10.006.

[6]. R. Tiwari, “An Overview of Internet of Things (IoT): From Literature Survey to Application Implementation Perspective,” *Int. Res. J. Eng. Technol.*, vol. 04, no. 01, pp. 575–582, 2017, [Online]. Available:

https://www.irjet.net/archives/V4/i1/IRJET-V4I197.pdf.
[7]. E. Oztemel and S. Gursev, “Literature review of Industry 4.0 and related technologies,” *J. Intell. Manuf.*, no. July, 2018, doi: 10.1007/s10845-018-1433-8.
[8]. J. Palmer and A. Chakravarty, “Supervised Machine Learning,” in *An Introduction to High Content Screening*, Hoboken, NJ, USA: John Wiley & Sons, Inc., 2015, pp. 231–245.
[9]. European Technology Platform on Smart Systems Integration, “Internet of Things in 2020,” *Internet Things 2020*, pp. 1–27, 2008.
[10]. S. Borkar and A. A. Chien, “The future of microprocessors,” *Commun. ACM*, vol. 54, no. 5, pp. 67–77, May 2011, doi: 10.1145/1941487.1941507.
[11]. R. Doshi, N. Apthorpe, and N. Feamster, “Machine learning DDoS detection for consumer internet of things devices,” in *Proceedings - 2018 IEEE Symposium on Security and Privacy Workshops, SPW 2018*, Aug. 2018, pp. 29–35, doi: 10.1109/SPW.2018.00013.
[12]. F. Zantalis, G. Koulouras, S. Karabetsos, and D. Kandris, “A review of machine learning and IoT in smart transportation,” *Futur. Internet*, vol. 11, no. 4, pp. 1–23, 2019, doi: 10.3390/FI11040094.
[13]. P. Mell and T. Grance, “The NIST definition of cloud computing,” 2011.
[14]. M. Ali, S. Malik, Z. Khalid, M. M. Awan, and S. Ahmad, “Security Issues , Threats And Respective Mitigation In Cloud Computing – A Systematic Review,” *Int. J. Sci. Technol. Res.*, vol. 9, no. 08, pp. 474–484, 2020.
[15]. C. Perera, Y. Qin, J. C. Estrella, S. Reiff-Marganiec, and A. V. Vasilakos, “Fog computing for sustainable smart cities: A survey,” *ACM Comput. Surv.*, vol. 50, no. 3, Jun. 2017, doi: 10.1145/3057266.
[16]. D. Bermbach *et al.*, “A Research Perspective on Fog Computing,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Nov. 2018, vol. 10797 LNCS, pp. 198–210, doi: 10.1007/978-3-319-91764-1_16.
[17]. Tadapaneni, N. R. (2016). Overview and Opportunities of Edge Computing. *Available at SSRN 3656806*.
[18]. Y. Ai, M. Peng, and K. Zhang, “Edge computing technologies for Internet of Things: a primer,” *Digit. Commun. Networks*, vol. 4, no. 2, pp. 77–86, Apr. 2018, doi: 10.1016/j.dcan.2017.07.001.
[19]. “Real-Life Use Cases for Edge Computing - IEEE Innovation at Work.” https://innovationatwork.ieee.org/real-life-edge-computing-use-cases/ (accessed Mar. 21, 2021).
[20]. N. Hassan, S. Gillani, E. Ahmed, I. Yaqoob, and M. Imran, “The Role of Edge Computing in Internet of Things,” *IEEE Commun. Mag.*, vol. 56, no. 11, pp. 110–115, Nov. 2018, doi: 10.1109/MCOM.2018.1700906.
[21]. J. Stajic, R. Stone, G. Chin, and B. Wible, “Artificial intelligence. Rise of the Machines,” *Science*, vol. 349, no. 6245, pp. 248–249, Jul. 2015, doi: 10.1126/science.349.6245.248.
[22]. X.-D. Zhang, “Machine Learning,” in *A Matrix Algebra Approach to Artificial Intelligence*, Singapore: Springer Singapore, 2020, pp. 223–440.
[23]. M. I. Jordan and T. M. Mitchell, “Machine learning: Trends, perspectives, and prospects,” *Science*, vol. 349, no. 6245. American Association for the Advancement of Science, pp. 255–260, Jul. 17, 2015, doi: 10.1126/science.aaa8415.
[24]. N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, D. I. Kim, and Z. Han, “Data Collection and Wireless Communication in Internet of Things (IoT) Using Economic Analysis and Pricing Models: A Survey,” *IEEE Commun. Surv. Tutorials*, vol. 18, no. 4, pp. 2546–2590, 2016, doi: 10.1109/COMST.2016.2582841.
[25]. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013, doi: 10.1016/j.future.2013.01.010.
[26]. K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, “Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT Scenarios,” *IEEE Access*, vol. 8. Institute of Electrical and Electronics Engineers Inc., pp. 23022–23040, 2020, doi: 10.1109/ACCESS.2020.2970118.
[27]. Q. Chi, H. Yan, C. Zhang, Z. Pang, and L. Da Xu, “A reconfigurable smart sensor interface for industrial WSN in IoT environment,” *IEEE Trans. Ind. Informatics*, vol. 10, no. 2, pp. 1417–1425, 2014, doi: 10.1109/TII.2014.2306798.
[28]. M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, “Strong authentication for RFID systems using the AES algorithm,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 3156, pp. 357–370, 2004, doi: 10.1007/978-3-540-28632-5_26.
[29]. “Applications of Machine Learning - Javatpoint.” https://www.javatpoint.com/applications-of-machine-learning (accessed Mar. 21, 2021).
[30]. S. Kotsiantis, “Supervised Machine Learning: A Review of Classification Techniques,” *Inform.*, vol. 31, p. 20, 2007.
[31]. R. Gentleman, W. Huber, and V. J. Carey, “Supervised Machine Learning,” *Bioconductor Case Stud.*, pp. 121–136, 2008, doi: 10.1007/978-0-387-77240-0_9.
[32]. Meidan, Y., Bohadana, M., Shabtai, A., Ochoa, M., Tippenhauer, N. O., Guarnizo, J. D., & Elovici, Y. (2017). Detection of unauthorized IoT devices using machine learning techniques. *arXiv preprint arXiv:1709.04647*.
[33]. F. Alam, R. Mehmood, I. Katib, and A. Albeshri, “Analysis of Eight Data Mining Algorithms for Smarter Internet of Things (IoT),” *Procedia Comput. Sci.*, vol. 98, pp. 437–442, Jan. 2016, doi: 10.1016/J.PROCS.2016.09.068.
[34]. J. Canedo and A. Skjellum, “Using machine learning to secure IoT systems,” *2016 14th Annu. Conf. Privacy, Secur. Trust. PST 2016*, pp. 219–222, 2016, doi: 10.1109/PST.2016.7906930.
[35]. E. Hodo *et al.*, “Threat analysis of IoT networks using artificial neural network intrusion detection system,” *2016 Int. Symp. Networks, Comput. Commun. ISNCC 2016*, Nov. 2016, doi: 10.1109/ISNCC.2016.7746067.
[36]. M. Khanum, T. Mahboob, W. Imtiaz, H. Abdul Ghafoor, and R. Sehar, “A Survey on Unsupervised Machine Learning Algorithms for Automation, Classification and Maintenance,” *Int. J. Comput. Appl.*, vol. 119, no. 13, pp. 34–39, 2015, doi: 10.5120/21131-4058.
[37]. J. Schmidhuber, “Deep Learning in neural networks: An overview,” *Neural Networks*, vol. 61. Elsevier Ltd, pp. 85–117, Jan. 01, 2015, doi: 10.1016/j.neunet.2014.09.003.
[38]. V. J. Prakash and D. L. M. Nithya, “A Survey on Semi-Supervised Learning Techniques,” Feb. 2014, doi: 10.14445/22312803/IJCTT-V8P105.
[39]. M. Taylor and P. Stone, “Transfer learning for reinforcement learning domains: A survey,” *J. Mach.*

Learn. Res., vol. 10, pp. 1633–1685.
[40]. L. P. Kaelbling, M. L. Littman, and A. W. Moore, "Reinforcement learning: A survey," *J. Artif. Intell. Res.*, vol. 4, pp. 237–285, 1996, doi: 10.1613/jair.301.
[41]. S. Li, T. Qin, and G. Social, "Blockchain-based digital forensics investigation framework in the Internet of Things and social systems," *ieeexplore.ieee.org*, Accessed: Sep. 02, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8777292/.
[42]. M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deep learning for IoT big data and streaming analytics: A survey," *IEEE Commun. Surv. Tutorials*, *20*(4), pp. 2923–2960, Oct. 2018, doi: 10.1109/COMST.2018.2844341.
[43]. L. Bondi, L. Baroffio, D. Güera, … P. B.-I. S., and undefined 2016, "First steps toward camera model identification with convolutional neural networks," *ieeexplore.ieee.org*, Accessed: Sep. 02, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7786852/.
[44]. J. Yu *et al.*, "Radio frequency fingerprint identification based on denoising autoencoders," *ieeexplore.ieee.org*, Accessed: Sep. 02, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8923325/.
[45]. L. Bai, L. Yao, S. Kanhere, X. W.-2018 I. 43rd, and undefined 2018, "Automatic device classification from network traffic streams of internet of things," *ieeexplore.ieee.org*, Accessed: Sep. 02, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8638232/.
[46]. S. Aneja, N. Aneja, and M. S. Islam, "IoT Device fingerprint using deep learning," *Proc. - 2018 IEEE Int. Conf. Internet Things Intell. Syst. IOTAIS 2018*, pp. 174–179, Jan. 2019.
[47]. H. Gao, L. Kuang, Y. Yin, B. Guo, K. D.-M. N. and Applications, and undefined 2020, "Mining consuming behaviors with temporal evolution for personalized recommendation in mobile marketing apps," *Springer*, Accessed: Sep. 02, 2021. [Online]. Available: https://link.springer.com/content/pdf/10.1007/s11036-020-01535-1.pdf.
[48]. Y. Meidan *et al.*, "N-BaIoT-Network-based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervasive Comput.*, vol. 17, no. 3, pp. 12–22, Jul. 2018, doi: 10.1109/MPRV.2018.03367731.
[49]. Y. Zhao, M. Li, L. Lai, N. Suda, D. C. preprint arXiv, and undefined 2018, "Federated learning with non-iid data," *arxiv.org*, Accessed: Sep. 02, 2021. [Online]. Available: https://arxiv.org/abs/1806.00582.
[50]. X. Wang, Y. Han, C. Wang, Q. Zhao, X. Chen, and M. Chen, (2019). "In-edge AI: Intelligentizing mobile edge computing, caching and communication by federated learning," *IEEE Netw.*, *33*(5), pp. 156–165, Sep. 2019, doi: 10.1109/MNET.2019.1800286.

How to cite this article: Ijaz, A., Raza, S., Imran, N., Ali, M. and Iman, V. (2021). Machine Learning and Deep Learning for Challenging Security of IoT: Analysis and Impact. *International Journal on Emerging Technologies, 12*(2): 245–250.