International Journal for Modern Trends in Science and Technology
Volume 12, Special Issue 01, pages 67-71.
ISSN: 2455-3778 online
Available online at: http://ijmtst.com/ICRCSET2026.html
DOI: https://doi.org/10.5281/zenodo.19426924

An in-depth look at how machine learning and deep learning can be used to improve IOT security

V.Thrisanthi | G. Srinivasararao

Department of Computer Science and Engineering, Chalapathi Institute of Technology, Guntur, Andhra Pradesh, INDIA.

To Cite this Article
V.Thrisanthi & G. Srinivasararao (2026). An in-depth look at how machine learning and deep learning can be used to improve IOT security. International Journal for Modern Trends in Science and Technology, 12(SI01), 67-71. https://doi.org/10.5281/zenodo.19426924

Article Info
Received: 02 March 2026; Revised: 01 April 2026; Accepted: 04 April 2026.

KEYWORDS

Machine Learning, Gadgets, Security Challenges and Checks, Issues, Deep Learning, IoT.

ABSTRACT

Through the IoT, millions of smart devices may be networked together and set to automatically exchange information with one another.By 2022, the number of connected devices is projected to have reached 80 billion, making IoT one of the fastest-growing digital sectors. Furthermore, additional security concerns have arisen due to the interconnectedness of IoT devices and the many different fields that must work together to install such devices. The underlying weaknesses of IoT devices render useless the implementation of security mechanisms such as protection from cyber threats, authorization, access control, networking, and information protection.To protect the IoT ecosystem, it is necessary to improve upon current security checks. As a result of recent developments in Machine Learning and Deep Learning (ML-DL), artificial intelligence has moved from the realm of science fiction to that of everyday life in several crucial contexts. Therefore, ML-DL techniques play a crucial role in advancing the protection of IoT systems beyond just ensuring encrypted communications between IoT components.To better secure IoT devices, this analysishelps to give a complete overview of ML strategies and current breakthroughs in DL strategies. Vulnerabilities to the protection of the IoT are addressed, including those that have always been present as well as those that are relatively new. The merits, demerits, and overall viability of the ML/DL approach to IoT protectionare then described and analyzed. The use of ML/DL to enhance IoT security is explored, along with its advantages and disadvantages. These prospects and difficulties suggest avenues for future study.

INTRODUCTION

Everything in this modern world can be predicted using ML and DL approaches such as generating captions for images, weather forecasting, attrition prediction, rainfall prediction, stock market prediction, and fraud detection. Many individuals also use them to foresee future vulnerabilities and assaults in the Internet of Things [1][2] and Wireless Sensors Networks (WSN) [3], as well as in the housing market prediction, the spread of illness detection, financial fraud detection, and other areas.The IoT and other contemporary connectivity advancements have greatly expanded conventional environmental monitoring in remarkable ways. The IoT has the potential to gather, measure, and comprehend environmental data, hence enabling modernizations that enhance the living experience. This makes it possible to realize digital infrastructure by simplifying the new types of interactions between objects and people. With an approximated 50 million tech gadgets by the end of 2020, IoT is one of the quickest-emerging topics in the era of computational technology. E-healthcare, e-housing, e-transportation, and e-education are just a few examples of how IoT technology has improved these practical domains. However, additional privacy issues have emerged due to the interconnected and expansive architecture of the IoT network, which includes a wide range of moving parts in their implementation.

Hierarchical configurations are part of the complexity of IoT applications. Consequently, it is difficult to keep the safety standards up in an IoT device with such a large threat environment. To meet the need for safety, remedies should take a more comprehensive approach. Unfortunately, most IoT gadgets function best when left alone. The result is that an intruder may potentially get direct entry to these systems. Wi-fi connections are the standard method of connecting IoT systems, making them vulnerable to espionage attacks. Due to their restricted processing capacity and battery life, IoT systems cannot implement sophisticated safety protocols.

Spontaneously, Iot applications must continuously adapt and cope meticulously and consistently, with protection as a topmost issue, notably in segregated regions, because the IoT platform is also a component of aninfiltration-physical framework, with its sophisticated infrastructure frameworks as an outcome of restricted data processing, information exchange, and energy facilities as well as trustable interaction with a spatial realm. Furthermore, the IoT ecosystem introduces additional security vulnerabilities. The interrelated and linked ecosystems of the IoT provide such security vulnerabilities. As a result, the safety of the IoT network is more precarious than that of other electronic systems, and the conventional remedy may not work.

ML-DL are potent information extraction techniques for identifying "typical" and "unusual" actions based on the interplay of IoT modules and gadgets. To detect suspicious attacks in their early phases, it is possible to collect and analyze the input feed of each component of the IoT environment. In addition, ML-DL approaches may be useful for foreseeing upcoming undiscovered assaults by cognitively understanding current instances, which is especially relevant given that emerging threats are typically variations of earlier attempts. For this reason, IoT applications need to go beyond just enabling safe connections between devices to incorporateprotection-based insights made possible by DL/ML techniques which are shown in Fig.1.

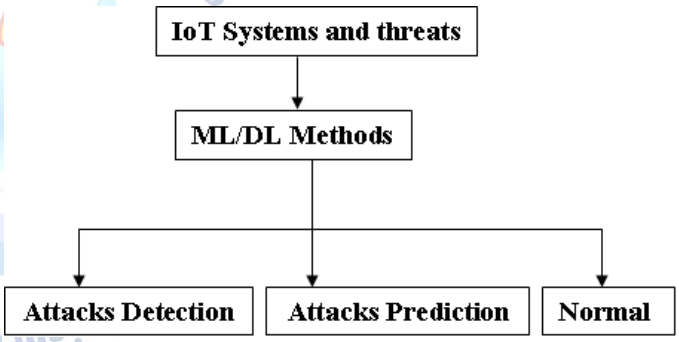

Fig. 1. Exemplification of how ML and DL may protect the Internet of Things.

RELATED WORKS

Several experts in the field have surveyed the state of IoT security to compile a useful resource for understanding the gaps in protection now present in IoT infrastructure and a plan for addressing them in forthcoming research. When it comes to IoT security, however, ML and DL have been largely overlooked in previous assessments. There are many ML and DL techniques employed by researchers towards IoT Security including Convolution Neural Networks (CNN), Ensemble Learning(EL), Principal Component Analysis (PCA), Random Forest (RF), Generative Adversarial Networks (GAN), Recurrent Neural Networks (RNN), Support Vector Machines (SVMs), K-Means, Ensemble DL Networks

(EDLN),K-nearest neighbor (KNN), Auto Encoders (AE), Deep Belief Network (DBN), Decision Tree (DT), Restricted Boltzmann Machines (RBM), Naive Bayes(NB) and Association Rules (ARs).In Fig.2, the taxonomy of ML-DL approaches to IoT safety is addressed. Table I summarizes findings from a survey of relevant current ML-DL approaches for the Internet of Things.

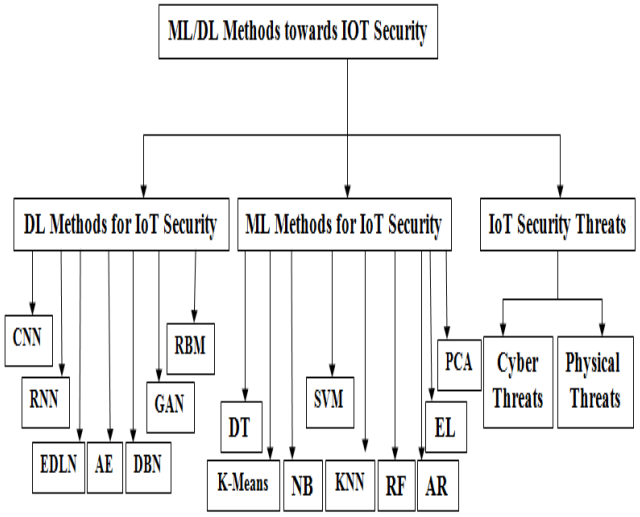

Fig. 2. Taxonomy of ML-DL Approaches to IoT Safety

TABLE I. SUMMARY OF RELEVANT CURRENT ML-DL APPROACHES FOR THE INTERNET OF THINGSSAFETY

Method	Merits	Drawbacks	Possible Use in the IoT Security
DT[4]	DT is an approach that is straightforward to understand and use.	Due to its building nature, DT needs substantial storage space. Only when there are few DTs involved do the procedures based on DTs become simple to understand.	Sources of infiltration and malicious traffic are identified.
SVM[5]	SVMs are well-known for their standardization abilities and their compatibility with data that has many feature properties but few sample points.	It might be challenging to choose the best kernel. SVM-based models are complex and challenging to comprehend and analyze.	Protecting smart grids from cyber threats like malware and incursion.
NB[6]	NB is well-liked because of its minimal training sample demand, straightforwardness, facile execution, and resistance to unnecessary characteristics.	Because of its feature-by-feature approach, NB misses out on valuable insights stemming from interrelationships between features.	Network Intrusion Detection.
KNN[7]	Intruders may be easily identified by using KNN, a common and efficient ML technique.	The best value of k changes from dataset to dataset, making it a potentially difficult and time-consuming task to determine.	Network Intrusion Detection.
RF[8]	Overfitting has little effect on RF. Unlike other methods, RF doesn't need picking features and may run on very little data.	Since RF relies on building several DTs, it may not be suitable for certain applications that operate in real-world scenarios considering the size of the necessary training dataset.	Threats like DDoS assaults and unapproved IoT gadgets may also be spotted.
AR[9]	The usage of AR algorithms is intuitive and uncomplicated.	The computations have a significant temporal complexity. Most AR techniques rely on very basic hypotheses about the connections and frequencies of variables. Such presumptions don't always hold up, particularly in security-related contexts.	Network Intrusion Detection.
EL[10]	Over-fitting is not a problem for EL, as it also minimizes variation. With its expanded collection of hypotheses and findings, EL is more flexible than a single classifier-based approach.	An EL method has a greater temporal overhead than an approach constructed around an individual predictor.	A threat, anomaly, and malware detection.
K-Means[11]	When creating the labeled data is a	When compared to supervised learning	An IoT solution

	significant challenge, it is often best to use an unsupervised approach. Since k-Means clustering may function with unlabeled data, it can be utilized to protect individuals' privacy in an IoT environment.	approaches, k-Means clustering performs poorly, especially when it comes to spotting previously seen attacks.	that can identify Sybil attacks and anonymize private data in industrial WSNs.
PCA[12]	In other words, PCA may accomplish dimensionality reduction, which in turn simplifies the model.	To create an efficient security strategy, PCA, a tool that transforms higher dimensions into lower dimensions, should be used in conjunction with various additional ML techniques.	In IoT settings, PCA may be used to reduce model features in realtime, making it suitable for usage in real-time detection systems.

ANALYSIS OF ML-DL SOLUTIONSFORIOT SAFETY AND PROTECTION

The challenges of utilizing ML and DL to improve protection, as well as the opportunities that may arise in the future,are focusedin this part. IoT networks are classified based on data, learning approaches, IoT contexts, opportunities to merge ML/DL with alternatives, computationally demanding problems, and the significance of safety vs. other trade-offs. Some of the open challenges are mentioned in Table II.

TABLE II. OPEN CHALLENGES

Context	Open challenges
Boosting the effectiveness of learning algorithms with augmented IoT security data.[13]	Data augmentation often requires domain expertise, and its primary difficulty lies in the generation of fresh instances that maintain the proper data skewness for each class. In light of this issue, appropriate techniques for augmenting IoT security data to boost the classification accuracy of learning algorithms should be explored.[14]
Availability of Datasets about security.[15]	The fundamental goal and problem in the bigger picture of using ML and DL for IoT protection are how to obtain or generate an appropriate, acceptable, accurate, and excellently trained dataset that includes a variety of plausible intrusion patterns. The enormous volumes of data generated by IoT gadgets make data quality control in real-time data streaming challenging.
How to Protect the Internet of Things withlow-Quality Data.[16]	To protect IoT systems that deal with massive amounts of streaming, diverse, and noisy data, it is necessary to create effective multi-modal DL models.[17]

CONCLUSION

New advancements, from hardware to information transfer to mobile and cloud architectures, all must be protected and integrated to meet the stringent standards for protecting IoT components. The development of ML and DL has made the establishment of several potential, analytical, and useful techniques that may be deployed in several IoT devices to improve security. Many potential dangers and entry points for Internet of Things attacks are addressed in this work. The paper provides a thorough analysis of how ML and DL techniques may be used in the topic of IoT protection. Last but not least, a comprehensive set of problems, obstacles, and forthcoming developments regarding the employment of ML and DL in efficiently safeguarding IoT components are addressed.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Rao, K. Venkateswara, et al. "A Study on Defensive Issues and Challenges in Internet of Things." High-Performance Computing and Networking: Select Proceedings of CHSN 2021 (2022): 591-601.

[2] Venkateswara Rao, K., D. Srilatha, and L. Mary Gladence. "Disease prediction and diagnosis implementing fuzzy neural classifier based on IOT and Cloud." Int J Adv Sci Technol 29.5 (2020): 737-745.

[3] Vivek, Kolla, et al. "An Efficient Triple-Layered and Double Secured Cryptography Technique in Wireless Sensor Networks." 2021 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER). IEEE, 2021.

[4] Al-Garadi, Mohammed Ali, et al. "A survey of machine and deep learning methods for Internet of Things (IoT) security." IEEE Communications Surveys & Tutorials 22.3 (2020): 1646-1685.

[5] Deorankar, Anil V., and Shiwani S. Thakare. "Survey on anomaly detection of (IoT)-internet of things cyberattacks using machine learning." 2020 fourth international conference on computing methodologies and Communication (ICCMC). IEEE, 2020.

[6] Babu, Meenigi Ramesh, and K. N. Veena. "A survey on attack detection methods for IoT using machine learning and deep learning." 2021 3rd International Conference on signal processing and Communication (ICPSC). IEEE, 2021.

[7] Gopalakrishna, Nikhil Krishna, et al. "If security is required": Engineering and Security Practices for Machine Learning-based IoT Devices." 2022 IEEE/ACM 4th International Workshop on Software Engineering Research and Practices for the IoT (SERP4IoT). IEEE, 2022.

[8] M. T. Mahmood, S. R. A. Ahmed, and M. R. A. Ahmed, "Using Machine Learning To Secure IOT Systems," 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Istanbul, Turkey, 2020, pp. 1-7, doi: 10.1109/ISMSIT50672.2020.9254304.

[9] S. Malik and R. Chauhan, "Securing the Internet of Things using Machine Learning: A Review," 2020 International Conference on Convergence to Digital World - Quo Vadis (ICCDW), Mumbai, India, 2020, pp. 1-4, doi: 10.1109/ICCDW45521.2020.9318666.

[10] M. Mamdouh, M. A. I. Elrukhsi and A. Khattab, "Securing the Internet of Things and Wireless Sensor Networks via Machine Learning: A Survey," 2018 International Conference on Computer and Applications (ICCA), Beirut, Lebanon, 2018, pp. 215-218, doi: 10.1109/COMAPP.2018.8460440.

[11] K. M S, R. R. G and S. Karthik, "Streamlining Load Scheduling in Cloud Computing: A Thorough Performance Assessment and Development of Effective Methods for Design," 2024 International Conference on Advances in Modern Age Technologies for Health and Engineering Science (AMATHE), Shivamogga, India, 2024, pp. 1-7, doi: 10.1109/AMATHE61652.2024.10582239.

[12] Sai Srinivas Vellela, Roja D, NagaMalleswara Rao Purimetla, SyamsundaraRao Thalakola, Lakshma Reddy Vuyyuru, Ramesh Vatambeti, Cyber threat detection in industry 4.0: Leveraging GloVe and self-attention mechanisms in BiLSTM for enhanced intrusion detection, Computers and Electrical Engineering,Volume 124, Part A,2025,110368,ISSN 00457906,https://doi.org/10.1016/j.compeleceng.2025.110368.

[13] S. S. Vellela, L. R. Vuyyuru, K. B. S. K, N. MalleswaraRaoPurimetla, L. Dalavai and M. V. Rao, "A Novel Approach to Optimize Prediction Method for Chronic Kidney Disease with the Help of Machine Learning Algorithm," 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), Gautam Buddha Nagar, India, 2023, pp. 1677-1681, doi: 10.1109/IC3I59117.2023.10397974.

[14] Kavitha Mettupalayam Subramaniam, Ramachandra Rao Goli, Karthik Subburathinam, Srihari Kannan,Optimization of pyrolysis parameters for enhanced biochar production from agricultural biomass: A study on energy efficiency and carbon sequestration potential,Science of The Total Environment, Volume 1015,2026,181362,ISSN 00489697,https://doi.org/10.1016/j.scitotenv.2026.181362.

[15] K. K. Kumar, S. G. B. Kumar, S. G. R. Rao and S. S. J. Sydulu, "Safe and high secured ranked keyword searchover an outsourced cloud data," 2017 International Conference on Inventive Computing and Informatics (ICICI), Coimbatore, India, 2017, pp. 20-25, doi: 10.1109/ICICI.2017.8365348.

[16] R. K. Yarava, G. R. C. Rao, Y. Garapati, G. C. Babu and S. D. V. Prasad, "Analysis on the Development of Cloud Security using Privacy Attribute Data Sharing," 2022 First International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), Trichy, India, 2022, pp. 1-5, doi: 10.1109/ICEEICT53079.2022.9768608.

[17] K. K. . Kommineni and A. . Prasad, "A Review on Privacy and Security Improvement Mechanisms in MANETs", Int J Intell Syst Appl Eng, vol. 12, no. 2, pp. 90–99, Dec. 2023.

[18] Kommineni, K.K., Prasad, A. Enhancing Data Security and Privacy in SDN-Enabled MANETs Through Improved Data Aggregation Protection and Secrecy. Wireless Pers Commun 139, 855–882 (2024). https://doi.org/10.1007/s11277-024-11635-w

[19] "Blockchain-Enabled Secure Data Aggregation for SDN-Enabled Ad-Hoc Networks," International Journal of Intelligent Engineering and Systems, vol. 18, no. 5, pp. 704–717, Jun. 2025, doi: https://doi.org/10.22266/ijies2025.0630.49.

[20] K. K. Kommineni, P. Ande, "Blockchain-driven key management and privacy-preserving data Aggregation Scheme for SDN-enabled MANETs," International Journal of Intelligent Engineering and Systems, vol. 18–18, no. 9, pp. 601–615, 2025, doi: 10.22266/ijies2025.1031.39.