International Journal of Integrative Research (IJIR)
Vol.1, No.7, 2023: 423-428

An Investigation into Deep Learning and Machine Learning Approaches for Securing the Internet of Things (IOT)

A.Y.Gital[1*], A.A.Ibrahim[2], H.Sunusi[3]
Department of Computer Science, Abubakar Tafawa Balewa University, Bauchi State
Corresponding Author: A.Y.Gital ali62209@gmail.com

ARTICLEINFO

Keywords: Internet of Things, Deep Learning, Machine Learning, Security

Received : 5 June
Revised : 20 June
Accepted : 24 July

ABSTRACT

The study explores machine learning and deep learning (ML) (DL) model helped in solving IoT the computation problem, which led to the adoption of many domains for its application in the problem-solving task. Solving a specific problem, this has led to the idea that deep and machine learning (DL) (ML) are two powerful approaches to data. Therefore, the purpose of this article is to provide a systematic review of "Scanning Machines and Deep Learning Methods for Internet of Things (IOT) Security and Privacy" on the current state of research on IoT and its joint venture with DL. This technique uses discrepancy privacy to prevent the adversary from understanding the use cases used to build the target model. The paper concluded that algorithms deep learning and machine learning were only developed recently and are not intended for use in cryptographic applications. However, for researchers who can implement cryptography, deep learning and machine learning can be used to implement cryptography.

DOI: https://doi.org/10.59890/ijir.v1i7.81
ISSN-E: 2988-2184
https://journal.multitechpublisher.com/index.php/ijir

INTRODUCTION

The Internet of Things (IoT) is a network of gadgets that are all linked to each other. Each device has a unique number that lets it automatically collect and send data over the network. IoT devices are used in many different fields and businesses, including customer, business, and government uses. There are billions of IoT gadgets around the world that all aim to do the same thing. As they become more common in our daily lives, their underlying security problems are getting more attention. Deep learning (DL) and machine learning (ML) as an Internet of Things (IoT) model helped solve the problem better because they were easy to compute. This led to many fields using it to solve problems. Getting a certain problem fixed This led to the idea of deep learning (DL) and techniques based on machine learning (ML) for studying and exploring data to find "abnormal" and "normal" behavior in components. IoT parts are all linked to each other in their surroundings. Also, DL/ML methods can be very helpful in finding new threats, which are often just modified versions of old ones. This is because they can learn from past attacks and find new threats that haven't happened yet. So, for safe and effective systems, IoT systems must be able to move from controlled contact between devices and information based on cybersecurity to ML and DL technologies. Ray and others (2016) But symmetric encryption, inequality privacy, trusted implementation, and ecology are four ways to deal with the limits of security and privacy problems in DL and ML from different angles. Secure reciprocal computing is the DL and ML protection technique that is used the most. Differential secrecy is used in this method to keep the opponent from knowing the use cases that were used to build the model being attacked. Encrypted multiparty processing and symmetrical encryption techniques are used to keep training and test data safe. On the one hand, these methods make processing much harder and require a different approach for each type of neural network. On the other hand, they allow secure running environments that use hardware-dependent security and seclusion to protect private data and training code.

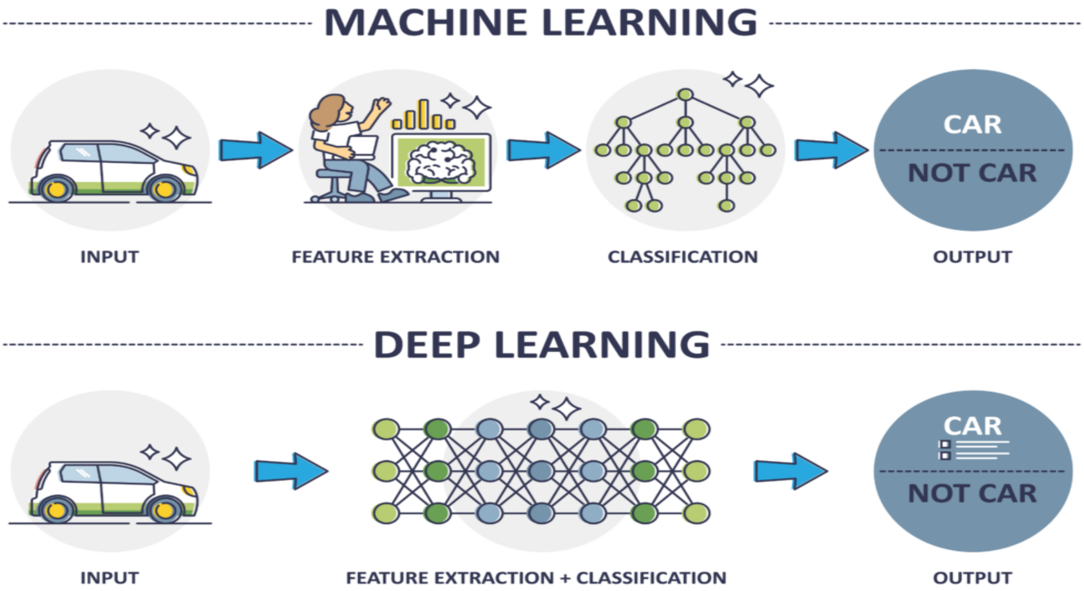
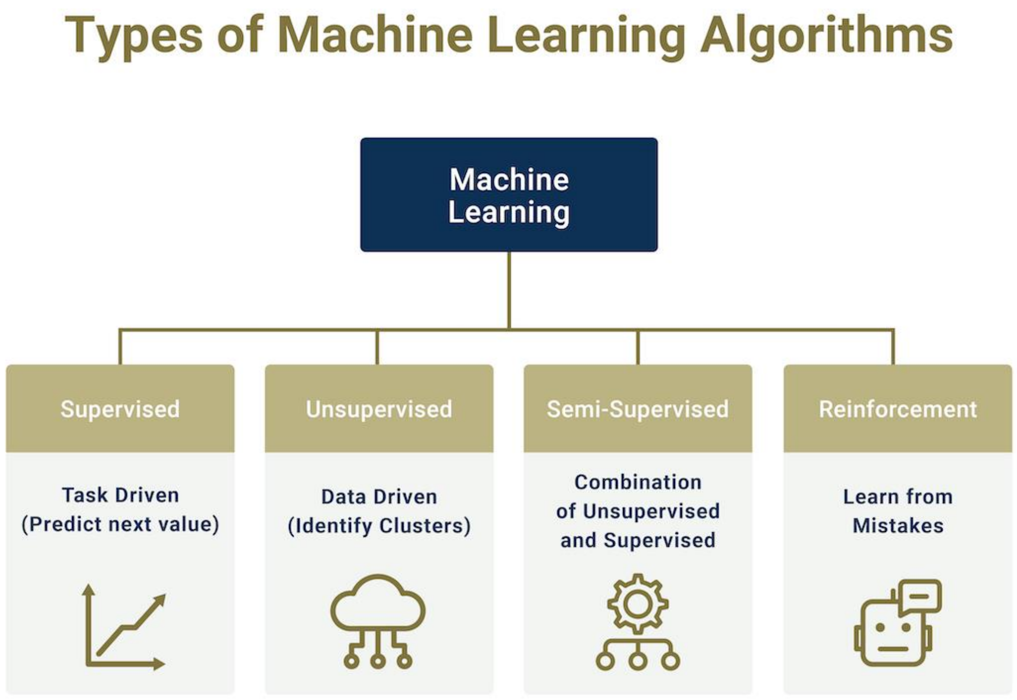


Figure 1. Machine Learning and Deep Learning
Source: Basu, 2020


Types of Machine Learning Algorithms
Machine Learning
Supervised
Task Driven (Predict next value)
Unsupervised
Data Driven (Identify Clusters)
Semi-Supervised
Combination of Unsupervised and Supervised
Reinforcement
Learn from Mistakes

Even though security and privacy are intertwined, privacy cannot exist without security while security cannot exist without privacy. While privacy is primarily focused on protecting your privacy in relation to your personal information, confidentiality safeguards the information's accessibility, integrity, and confidentiality. Privacy is important when processing personal data, while information security focuses on preventing unauthorized access to information sources. Any information pertaining to an individual may be considered personal data, including name, login credentials, address, social security number, bank account information, etc. Different IoT situations and applications might result in more complex and catastrophic attacks like Mirai because of the vulnerability of IoT equipment. It might be challenging to identify the appropriate security options for IoT devices. Data fed into an IoT system can be analyzed and aggregated to display standard interface patterns for early detection of malicious activity. The field of IoT includes public transportation, car sharing, vehicle recognition, accident prediction and inference among other activities covered in this article. The purpose of this document is to make it more complete and comprehensive. Therefore, the purpose of this article is to provide a systematic overview of the current state of research on Internet of Things (IoT) scanners for privacy and security, as well as learning methodologies. "The deep". Learn more about IoT and conquering DL.

LITERATURE REVIEW

Many researchers conduct IoT security studies to provide specific insights into current security vulnerabilities and the future direction of IoT systems. However, most of his current research on IoT security is less concerned with ML and DL implementations of IoT security. Current research presents and evaluates challenges related to encryption, access control, authentication, cybersecurity, and application security in IoT systems. Kumar et al. (2017) focuses on the security of IoT communications after reviewing the security problems and solutions of the IoT communications system. Numerous studies and reviews refer to IoT security to provide guidance for future challenges. A lot of research has focused on IoT security, but none of it has focused on the implementation of DL or ML for IoT security. According to Kumar et al. (2017) reviewed a number of works aimed at improving and regulating access control, authentication, application security, cryptography, and cybersecurity in environments. A study by Safar et al. (2018) explores IoT communications security issues and solutions. Likewise, Zhao et al. (2013) on an IoT intrusion detection system. Furthermore, the IoT framework for regulatory approaches and regulatory issues can define security and privacy requirements (Bengio et al., 2015). A decentralized IoT environment also includes privacy and security. Various challenges also affected this activity. Although there are many issues to explore, researchers believe that the distributed IoT approach offers several privacy and security benefits.

METHODOLOGY

ML or DL discretion concerns remain unresolved in a universally accepted manner. To protect against hostile attacks, several security processes have been proposed, which can be distributed into three categories: model resilience enhancement, input processing, and malware recognition.

RESULTS AND DISCUSSION

The goal of preprocessing is to reduce the model's dependence on immunize activity by performing operations such as randomization, image transformation, and noise reduction that normally do not require updating or retraining the model. Regulation, adversarial training, trait reduction, as well as other techniques to enhance model rigidity through model retraining and modification, belong to the second group. Adaptive noise reduction and Image transformation detection are patterns of third scale detection mechanisms that can be implemented prior to the first prototypical layer. In the point of view, no protective strategy can completely protect against adversarial conditions, although several defense mechanisms have been proposed. To combat hostile situations, opponent training is currently the most effective technique. For toxic attacks, there are two basic defenses. The initially is an odd selection method, which removes outliers from the related set. The second phase is to improve the neural network's resistance to contamination from contaminated samples. In addition, a number of surveys on IoT applications and improvements by DL technologies have been done in the literature. However, most of these tend to focus on a specific aspect of DL and/or IoT. For example, a survey on big data analytics in the Internet of Things. Also consider an assessment of how computer vision plays a major role in the ground transportation system. While examining DL patterns in the field of IoT, this is not an exhaustive survey that covers all current research publications on the fields of IoT and learning. An important review dedicated to optimizing IoT systems through DL has been conducted, but mainly focuses on traffic situation prediction and traffic sign recognition tasks. With the proliferation of connected devices, gathering the ever evolving sanctuary standards of the Internet of Things can be challenging. Solutions must take the complete system into account in order to deliver the necessary degree of security. However, the majority of IoT devices can function without human input. Then an unauthorized person can physically access these peripherals (Abomhara et al., 2015).

CONCLUSIONS

Security requirements for IoT devices are becoming increasingly complex as multiple technologies from hardware connection and wireless links to cloud architectures and mobile, need to be protected and integrated with additional machineries. Advancements in ML then DL have created several powerful analytics technologies that to improve IoT security. This study examines several IoT attack surfaces and IoT security threats. To provides an inclusive overview of the applicability of ML and DL approaches in IoT security. We then compare the strengths and weaknesses of these technologies and their application to IoT security. Next, we look at the ML and DL methods that enable the essential IoT covers (i.e. knowledge, application layers and network). In short, there has been a lot of study with many DL models in different IoT fields, but there are still many problems, future directions and challenges in the use of DL. Please use DL. Use ML and DL to effectively secure managed, classified, and secure IoT systems. Teaching strategies; How to improve machine learning algorithms that use diverse IoT data effectively, how to build strong detection simulations, and how to use models to make sure privacy and security are maintained.

Some security trade-offs in applications for the Internet of Things and the simultaneous assimilation of ML and DL with block chain technology for IoT sanctuary; Finally, ML and DL for IoT sanctuary in a collaborative, consistent, and interdependent ecosystem of IoT systems. The goal of this review is to give a practical director that may inspire researchers to improve the security of IoT structures, from the rudimentary step of allowing safe communication between IoT components to the more advanced step of constructing end-to-end intelligent IoT systems.

The paper concludes that deep learning and machine learning algorithms have only been developed recently and are not intended for use in cryptographic applications. However, researchers who can perform cryptography can use machine and deep learning to implement cryptography. Similarly, Alaba (2017) taught DL algorithms to decode cipher frames and concluded that DL will. Machine learning algorithms and logical operations have been replaced by CNN algorithms. The ability of RNNs to learn to decode has been previously demonstrated. Decoding the fuzzy machine on RNNs with a 3,000-unit LSTM is possible thanks to the detailed analysis of the encoder's internal representations.

The thorough study in this work shows that deep learning algorithms like RNN can recognize polyalphabetic ciphers and decode them for cryptanalysis. Research in machine learning and deep learning may hasten the development of the Internet of Things. The endpoints of IoT devices must be protected because of the huge number of intelligent objects that are linked to them. Key avenues for future IoT DL research are also indicated, and the proven advantages of IoT DL models are highlighted.

REFERENCES

Diro A. and N. Chilamkurti, (2018). Leveraging LSTM networks for attack detection in to things communications. IEEE Communications Magazine, vol. 56, no. 9, pp. 124–130.

E. A. Safar, R. Natalizio, Y. Challal, and Z. Chtourou, (2018). A Road Map for Security Challenges in the Internet of Things. Digit Commun Netw. ,vol. 4, no.2, pp.118 – 137.

F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, (2017). Internet of Things Security: A survey, J. Netw. Comput. Appl., vol. 88,pp. 10 –28.

J. S. Kumar, and D. R. Patel, (2017). A Survey on Internet of Things: Security and privacy Issues, ”Int. J. Comput. Appl., vol. 90.

K. Zhao and L. Ge, (2013). A survey on the Internet of Things Security. InProc. IEEE 9th Int. Conf. Computer Intell. Security (CIS), Dec. 2013. pp. 663 – 667, doi:10.1109/CIS.2013.145.

M. A. bomharaand G.M.Klien, (2015). Cyber security and the internet of things: Vulnerabilities threats, intruders and attacks. Journal of Cyber Security and Mobility, vol. 4, no. 1, pp.65–88.

R. I. Lee, L. Sha, and J. Stankovic, (2010). Cyber Physical Systems: The Next Computing Revolution, in Proceedings of the Design Automation Conference pp. 731 – 736 IEEE, Anaheim, CA, USA.

S. A. Sicari, L. A. Rizzardi, Grieco, and A. CoenPorisini, (2015). Security privacy and trust in Internet of Things: The Road a Head. Comput Netw, vol. 76, pp.146 – 164.

S. Y. Jin, and A. Raychowdhury, (2016) Changing computing paradigm with internet of things: a tutorial introduction, IEEE Design & Test, vol. 33, no.2, pp.76 – 96.

Y. Bengio, and G. Hinton, (2015). Deep learning Nature, vol. 521, no. 7553, p.436.