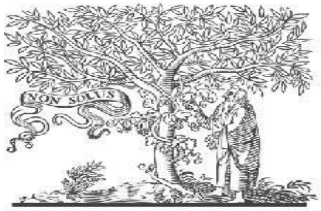
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 28 Aug 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 08

10.48047/IJIEMR/V12/ISSUE 08/58

Title **A Comprehensive Review of Machine Learning based Intrusion Detection System in Internet of Things**

Volume 12, ISSUE 08, Pages: 384-391

Paper Authors **Dr. K. Jayarajan, Dr. T. Poongothai**

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

A Comprehensive Review of Machine Learning based Intrusion Detection System in Internet of Things

Dr. K. Jayarajan[1], Dr. T. Poongothai [2]

[1]Professor, Department of IT, Malla Reddy Engineering College for Women, Secunderabad, India.

[2] Lecturer, Department of Computer Engineering, Government Polytechnic College Kadathur,Tamilnadu, India

Abstract

The Internet of Things (IoT) is a brand-new paradigm that unifies the Internet with actual physical things from several domains, including home automation, business processes, environmental monitoring, and human health. It increases the prevalence of Internet-connected gadgets in our daily lives, bringing with it concerns linked to security issues in addition to many positive effects. Due to the vast diversity of IoT devices, limited computational resources, and protocols and standards, secured communication is a common difficulty. Even with certain security precautions, IoT networks are extremely susceptible to a variety of threats due to their enormous attack surface. Designing protection measures is therefore required for identifying attackers. However, due to the IoT's unique features including resource-constrained devices, distinct protocol stacks, and standards, applying typical IDS approaches to it is challenging. A number of issues with traditional IDS, such as the high false alarm rate and low detection accuracy, are brought out, just as they are in literature. Because of the computational limitations and inherent resources of IoT systems, it cannot be secured directly by using traditional security techniques. ML techniques integrated with IDS enable real-time detection of both unknown and known attacks on IoT devices. In this article, a thorough analysis of traditional Deep Learning (DL) and Machine Learning (ML) methodologies as well as cutting-edge technologies for intrusion detection in the Internet of Things is done. Our goal is to discover emerging trends, open issues, and promising areas for future research. In this review, various attack detection approaches are clearly discussed along with their advantages and disadvantages.

Keywords: Internet of Things (IoT), Intrusion Detection System (IDS), Machine Learning (ML), Deep Learning (DL).

Introduction

The potential for integrating smart objects into our daily activities through the Internet has increased with the development of various technology areas such as sensors, automatic identification and tracking, embedded computing, wireless communications, broadband Internet access, and distributed services. The Internet of Things is the confluence of the Internet with intelligent devices that can converse and interact with one another (IoT). IoT is one of the most significant player in the Information and Communication

Technology (ICT) in forthcoming years. By 2025, the IoT research team at Cisco anticipated there would be an average of 75.3 billion actively connected devices [1]. IoT technology differs from conventional Internet technology in that human intervention is not required during data sharing between systems. The need for data network bandwidth has expanded along with the growth of IoT devices. The majority of IoT devices, however, have resource limitations, making it difficult to implement conventional security techniques for system protection against assaults. When it comes time to process sensitive data, the IoT gadget raises serious problems.

IoT systems can gather and interpret data remotely in real-time thanks to a variety of sensors that are incorporated in them. They can create sophisticated decision-making systems and successfully manage IoT environments thanks to the data collected by the sensors. Users' capacity to remotely manipulate their devices makes them vulnerable to a variety of dangers. Methods for ensuring data confidentiality and authentication, access control inside the IoT network, privacy and trust among users and things, and the enforcement of security and privacy regulations are implemented for improving IoT security. Securing IoT devices is complex due to the following characteristics such as heterogeneity, unpredictable nature of physical environment and heavily distributed nature.

Despite the fact that there have been a number of review studies published in the literature since 2017, none of them specifically used ML approaches for IDS in IoT. Therefore, this paper provides a detailed discussion on various work related with ML in Intrusion Detection System for IoT. Following a survey of relevant research articles in ML, the following perspectives are contributed to the audience.

1. First, an IoT system has been provided with taxonomy of various layers. Additionally, IoT security and several potential attacks have been discussed along with their potential layer-by-layer implications.
2. This survey focuses on the literature related to machine learning (ML)-based security solutions for Internet of Things (IoT).
3. The authors discuss potential issues or restrictions with ML-based IoT system security as well as their future plans for research.

The remainder of the paper is structured as follows: Section 2 provides an overview of IoT security, focusing on IoT layers and the significance of IoT security; Section 3 discusses ML in IoT security, highlighting various machine learning and deep algorithms and IoT security solutions; Section 5 presents inferences that are drawn from literature. Section 6 analyses the research challenges in ML-based IDS of IoT; Section 7 concludes the survey and includes recommendations for the future.

Security issues in Internet of Things

IoT systems are made up of networked mechanical, electronic, or other objects that may transport data over a network without the need for human-to-human or human-to-computer interaction. IoT systems connect

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

to diverse devices or things using unique network address schemes. Due to resource limitations, the majority of Internet-connected IoT devices are vulnerable to cyberattacks since their security measures are inadequate. However, the majority of IoT systems run independently across unreliable network connections and the Internet, which exposes the network to cyberattacks.

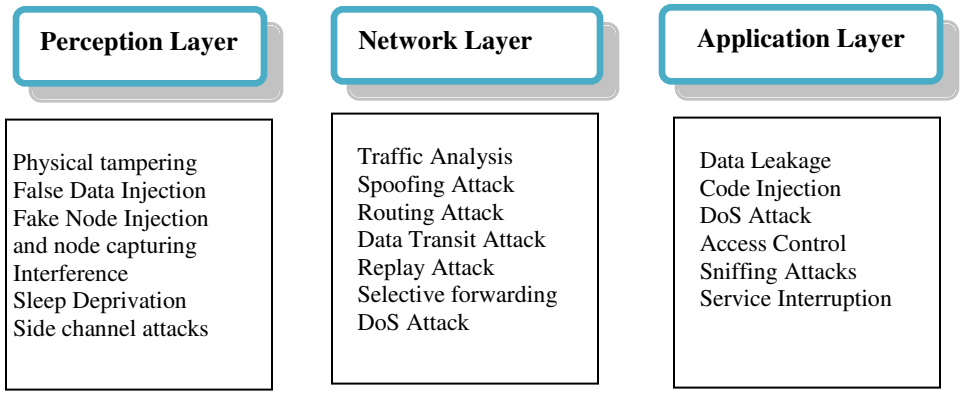
To safeguard IoT devices, a variety of security mechanisms must be put in place. The physical design of IoT devices, however, hinders their computational capacity and prevents the use of sophisticated security protocols. A threat/attack occurs when an unauthorised user gains access to a system and discloses private information without the associated user's consent.

To provide the taxonomy of IoT attacks, a layered architecture of IOT is presented. Generalized architecture of IOT consists of three layers namely perception, network and application layers [6,7]. Basic security issues and mechanisms are listed in Table1.

Table 1. Basic security issues and mechanisms in IOT

SNo	IoT Layer	Security issues	Security Mechanisms
1	Application Layer	Data Sharing, Cloud Application Vulnerability, Privacy and authentication	Privacy protection and key management
2	Network Layer	Integrity, Availability & Confidentiality, Congestion Attack	Authentication and encryption
3	Perception Layer	Physical damage, Storage vulnerabilities, Resilience to Node capture and Jamming attack	Encryption and key agreement, Sensor data protection

Figure 1 shows the various layers as well as common attacks that occur at each layer and also with some attacks occurring on more than one layer.



Intrusion Detection System for Internet of Things

Intrusion Detection System using ML Techniques

One of the artificial intelligence techniques known as machine learning (ML) enables devices to learn from their experience rather than being explicitly programmed [8]. ML can operate in dynamic networks without the aid of a person or challenging mathematical formulae. For IoT security needs, ML approaches have significantly evolved in the last several years. Therefore, by examining the behaviour of the devices, ML techniques can be utilised to detect various IoT attacks at an early stage. For IoT devices with limited resources, appropriate solutions can also be offered utilising various ML algorithms.

The experimental results showed that the proposed ensemble method outperformed existing ensemble methods and SVM, BN, and MC mechanisms using data sources from the DNS and HTTP protocols. The architecture of developing the ensemble method-based NIDS in lower overhead compared to other approaches.

Mohamed et al. [10] developed a Random Forest (RF) and Neural Network for detecting IoT intrusions (NN). IDS concentrated on ML techniques that may be offered as a service on IoT systems. RF was employed as a classifier to detect intrusions, and then a NN classifier was utilised to detect the classification of invaders. The Raspberry Pi 3 will act as the main computer for all applications of the offered solutions. The system acts as a bridge between the endnode layer and top-level application layer. Due to sensors' relatively low computational power, this service is better suited for safeguarding IoT network end nodes by keeping an eye on and monitoring unusual activity. An RF and NN-based cloud-based intrusion detector is the second component. The system in question is used to gather IoT traffic, extract features, and then classify the extracted features. The data point is described as radio frequency interference or non-use (RF).

Utilizing NN, the observed intrusion is categorised. The experimental results show that while the suggested model successfully detects intrusions, intruder categorization suffers from low precision and high bias.

Additionally, binary differential mutation is used to broaden the diversity of people. Random forest (RF) is optimised for flow classification by updating the weight of each sample after repeatedly creating each tree, and making the final determination using a weighted voting process. The performance of this approach is evaluated with precision, recall, F-score and false positive rate. The result of two-stage intrusion detection system is compared with decision tree, Adaboost, RF, SVM and GDBT. The results demonstrated that this model achieved a greater accuracy and lower overhead.

For IoT networks, Anthi et al.[13] created a three-layer Intrusion Detection System (IDS) that uses a supervised technique to identify a range of common network-based intrusions. This system provides three primary functions such as 1) Identify and

profile each connected IoT system's routine behaviour. 2) Spot malicious packets on the network while an attack is occurring. 3)Classify various attack types that have already been launched. This IDS architecture mainly focuses on the 4 attacks namely Denial of Service (DoS), Man-In-The-Middle(MITM)/Spoofing,
Reconnaissance, and Replay.

The evaluation findings show that the proposed ILECA outperforms other well-known algorithms in terms of detection accuracy and real-time characteristics.

Additionally, the Scikit-Learn tool has been used to build a number of well-known algorithms, including Decision Trees, k-Nearest Neighbor, Support Vector Machines, etc., in order to discover the best classification model appropriate for the IoT environment.

Using three different data sets, including the KDD99, NSL-KDD, and UNSW-NB15 datasets, this study's comparative analysis of feature selection techniques and their effects on various classification algorithms is presented.

Intrusion Detection System using DL Techniques

Diro and Chilamkurti. [16] designed a deep learning based distributed attack detection mechanism that incorporate the distribution features of IoT. Accuracy, detection rate, false alarm rate, and other performance measures have been used in the evaluation process to demonstrate the superiority of deep models over shallow models. This deep model performance was compared to that of a centralised detection system, which evaluated the distributed attack detection, as opposed to typical ML techniques. When compared to centralised detection systems, distributed attack detection systems perform better using a DL model.

Otoum[17] suggested a new deep learning-based intrusion detection system (DL-IDS) to identify security risks in IoT environments in order to address the difficulties associated with protecting IoT devices. Although there are several IDSs described in the literature, they all suffer from deficiencies in learning and data set management, which have a significant impact on how accurately attacks are detected.

In experiments, a processed dataset is employed, and the suggested strategy produces good classification accuracy.

Using a feature selection technique, non-essential variables are found in the data and eliminated. This has no impact on how accurate the prediction model is. Principal Component Analysis (PCA), which is implemented here as the Random Forest (RF) technique due to its adaptability, is frequently employed in machine learning (ML) algorithms.

Self-normalizing neural networks (SNN) and feedforward neural networks were used by the authors in [24] to investigate vulnerability detection against adversarial assaults (FNN). The Bot-IoT dataset was utilised. The results of the experiment showed that the average precision, recall, and F1 score was 0.95% and the maximum accuracy for FNN was 95.1%. However, it was discovered that SNN 9% was more resistant to adversarial attacks than FNN in terms of feature normalisation. Although

feature normalisation of the Bot-IoT dataset increased resilience, it had an adverse effect on SNN accuracy, which dropped to under 50%, which is deemed inappropriate for real-world security demands.

Inferences from the Literature

IDS provides important network-level solutions for resolving these problems and safeguarding Internet-connected frameworks. But it is crucial to understand how to transform conventional IDS into intelligent IDS, which is similar to intelligent IoT. Using IDS, the feature selection issue is solved. This paper discussed about how machine learning techniques are used to identify anomalies in network intrusion detection systems. Different ML techniques can be used with Swarm Optimization techniques in the Network Intrusion Detection System to improve the performance of the intrusion detection system and to detect abnormalities in the future. Using deep autoencoders, anomalous network traffic coming from infected IoT devices is found. Usage of various deep learning techniques also discussed for the detection of attacks in IoT.

DDoS assaults use up bandwidth on modern IoT devices. Consequently, a preventative strategy has been suggested to improve network and IoT device cyber security. The anomaly detection technique is only used when the attack signature is likely to occur. An adaptive intrusion detection and prevention system has been launched for the IDPIoT. This improves security and the expansion of Internet-connected devices. The investigation of current intrusion detection systems leads to the recommendation of IDPIoT, which enhances security and network- and host-based functionality.

Current Challenges in implementing ML and DL based IDS in IoT

Issues with real-time updates, infrastructure, data security, and algorithms that limit computing Networks powered by IoT face threats from exploitation and privacy leaks. The goal of data augmentation approaches was to produce datasets that were more precise and trustworthy for ML and DL model training. For IoT network security, a strong software infrastructure must be created.

Aside from that, adding machine learning algorithms to an IoT system makes the system's computations more difficult. Systems are slowed down as a result. Therefore, using artificial intelligence algorithms is required to lessen complexity. Actually, the majority of users are unaware of how, where, or with whom their personal information has been disclosed. The essential security practises of authentication, encryption, and security updates are followed by all IoT devices. To preserve message security, IoT devices must encrypt messages before sending them via the cloud. However, while building IoT devices, privacy protection must be the first priority. Since many improvements still need to be made, this study will be expanded as additional work to give comprehensive security, privacy, and cyber-attack frameworks in IoT-based innovative ecosystems.

Conclusion

IoT networks are frequently the target of serious attacks. IoT dangers have increased over the past few years, and large-scale malicious attacks have been launched as a result.

IDS is an essential security defence measure to have in IoT setups. Therefore, typical security countermeasures like authentication and encryption are insufficient. IoT device features present highly particular issues. IDS offers important network-level solutions for resolving these problems and safeguarding Internet-connected frameworks. However, as in literature, various problems are raised in traditional IDS, like the high false alarm rate. In IoT, for intrusion detection, a detailed study of traditional DL and ML techniques and recent technologies is presented in this review.

References

1. Jurcut, A., Niculcea, T., Ranaweera, P. *et al.* Security Considerations for Internet of Things: A Survey. *SN COMPUT. SCI.* 1, 193 (2020). https://doi.org/10.1007/s42979-020-00201-3
2. L. Xiao, X. Wan, X. Lu, Y. Zhang and D. Wu, "IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?," in IEEE Signal Processing Magazine, vol. 35, no. 5, pp. 41-49, Sept. 2018, doi: 10.1109/MSP.2018.2825478.
3. N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques," in IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2671-2701, thirdquarter 2019, doi: 10.1109/COMST.2019.2896380.
4. Zeadally, Sherali, and Michail Tsikerdekis. "Securing Internet of Things (IoT) with machine learning." International Journal of Communication Systems, Vol.33, No.1, 2020.
5. I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu and W. Ni, "Anatomy of Threats to the Internet of Things," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1636-1675, Secondquarter 2019, doi: 10.1109/COMST.2018.2874978.
6. Z. Bakhshi, A. Balador and J. Mustafa, "Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models," 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), 2018, pp. 173-178, doi: 10.1109/WCNCW.2018.8368997.
7. M. Serror, S. Hack, M. Henze, M. Schuba and K. Wehrle, "Challenges and Opportunities in Securing the Industrial Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 17, no. 5, pp. 2985-2996, May 2021, doi: 10.1109/TII.2020.3023507.
8. Yadhav Dheeraj, Machine Learning: Trends, Perspective, and Prospects Machine Learning: Trends, Perspective, and Prospects, Vol. 349,Issue.6245,pp.255-260, 2020.
9. N. Moustafa, B. Turnbull and K. -K. R. Choo, "An Ensemble Intrusion Detection Technique Based on Proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4815-4830, June 2019, doi: 10.1109/JIOT.2018.2871719.

10. Mohamed, T., Otsuka, T., Ito, T. (2018). Towards Machine Learning Based IoT Intrusion Detection Service. In: Mouhoub, M., Sadaoui, S., Ait Mohamed, O., Ali, M. (eds) Recent Trends and Future Technology in Applied Intelligence. IEA/AIE 2018. Lecture Notes in Computer Science(), vol 10868. Springer, Cham. https://doi.org/10.1007/978-3-319-92058-0_56.

11. Khraisat, Ansam, Iqbal Gondal, Peter Vamplew, Joarder Kamruzzaman, and Ammar Alazab. 2019. "A Novel Ensemble of Hybrid Intrusion Detection System for Detecting Internet of Things Attacks" Electronics, vol. 8, no. 11: 1210. https://doi.org/10.3390/electronics8111210

12. J. Li, Z. Zhao, R. Li and H. Zhang, "AI-Based Two-Stage Intrusion Detection for Software Defined IoT Networks," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2093-2102, April 2019, doi: 10.1109/JIOT.2018.2883344.

13. E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos and P. Burnap, "A Supervised Intrusion Detection System for Smart Home IoT Devices," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 9042-9053, Oct. 2019, doi: 10.1109/JIOT.2019.2926365.

14. Zheng, Dehua, Zhen Hong, Ning Wang, and Ping Chen. 2020. "An Improved LDA-Based ELM Classification for Intrusion Detection Algorithm in IoT Application" Sensors, vol. 20, no. 6: 1706. https://doi.org/10.3390/s20061706

15. Fenanir, Samir & Semchedine, Fouzi & Baadache, Abderrahmane, A Machine Learning-Based Lightweight Intrusion Detection System for the Internet of Things. Revue D Intelligence Artificielle, Vol.33, No. 3, pp.203-211, 2019.

16. Abebe Abeshu Diro, Naveen Chilamkurti, Distributed attack detection scheme using deep learning approach for Internet of Things,Future Generation Computer Systems, Vol. 82,2018,pp.761-768 .

17. Otoum, Yazan & Liu, Dandan & Nayak, Amiya. (2019). DL-IDS: a deep learning–based intrusion detection framework for securing IoT. Transactions on Emerging Telecommunications Technologies, vol.33, no3, pp.1-14.