ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24OCT580

Overview of Cyber Attacks Classification and Detection in IoT using CNN-Deep Reinforcement Learning

Katikam Mahesh[1*]
Scholar at Andhra University College of Engineering (AUCE(A), Visakhapatnam-530003, Andhra Pradesh, India, in the Department of Computer Science and Systems Engineering
https://orcid.org/0009-0000-0707-1117

Dr. Kunjam Nageswara Rao[2]
Professor at Andhra University College of Engineering (AUCE(A), Visakhapatnam – 530003, Andhra Pradesh, India, in the Department of Computer Science and Systems Engineering.
https://orcid.org/ 0009-0005-2779-0238

Coresopinding Author: Katikam Mahesh[1*]

Abstract:- Millions of digital devices total the Internet of Things (IoT), and this allows very easy interaction from users connecting the devices. IoT is one of the tech sectors that is expanding most rapidly, but it can also be very vulnerable to hazards. Infections and abnormal placement on the Internet of Things (IoT) framework is an increasing threat in the field of technology. In view of the growing IoT foundation usage across all industries, attacks and dangers on these systems have also grown proportional. Leveraging typical machine learning methods, cyber-attack detection plays a critical role in avoiding damage from cyberattacks on IoT devices. IoT Cyber Attacks are Not Detected by ANN Artificial Neural Networks Using Deep Learning Techniques CNN-DRL (Convolutional Neural Networks-Deep Reinforcement Learning) Hybrid Approach: Detects Attacks, including Distributed Denial of Service (DDoS), Zero-day, and Eavesdropping Attacks.

Keywords:- *Cyber Attacks, Internet of Things (IoT), Convolutional Neural Networks, Deep Reinforcement Learning.*

I. INTRODUCTION

Deep learning employs algorithms that, by examining data with a logical structure, try to draw conclusions that people would. Deep learning uses neural networks, multi-layered structures of algorithms that can detect patterns and classify data in the same way as people can, to do this.Our brains attempt to draw similarities among newly gained information and what we already know. Neural networks are utilized in deep learning to carry out the same idea. Big amounts of unstructured, data without labels are all that deep learning systems need in order to learn on their own and produce elegant, accurate forecast models.

II. CLASSIFICATION OF CYER ATTACKS IN IOT

A. Physical Attacks

IoT device hardware be the target of physical attacks. Attackers may trigger malfunctions or criminal data access via tampering devices, messing with sensors, or having unauthorized physical access to the devices.

- *Zero-Day Attacks*

This attack subtype relies on an undetected flaw in IoT devices or software. These vulnerabilities can be highly effective and tough to guard against because attackers make use of them before developers have a chance to issue patches.

- *Eavesdropping Attacks*

Attackers maintain a watch on the way IoT devices and communication channels interact with others, with the goal of stealing user credentials or sensitive data. To counter this threat, secure communication protocols and proper encryption are required.

- *Data Injection Attacks*

Malicious codes and commands are be employed by attackers to attack poorly protected systems.

- *Replay Attacks*

Through the application of malicious instructions, an approved info packet gets modified to carry off this attack. Electronic equipment receive malicious packets passed on through them under the disguise of totally legitimate information packets.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24OCT580

B. Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks.

Attackers flood IoT systems with a great deal of traffic, leaving them unresponsive or unusable, disrupting vital services and inflicting financial and reputational damages. This is done by taking advantage of flaws in the security protocols of IoT devices.

C. Botnet Attacks

Attackers take over weakly secured IoT devices to build botnets. These botnets can be used for various malicious activities, such as sending out spam emails, launching DDoS attacks, or spreading malware.

D. Man-in-the-Middle (MitM) Attacks

Attackers can eavesdrop on sensitive data or insert mal icious things via MitM crimes.This type of attack targets we ak authentication, weak encryption, and unsafe network con nections.

E. Malware Attacks Attacks

Malicious software compromising their operation and spreading to other devices in the network. Since ransomware can turn down devices and demand payment to release them, attacks on the web of Things, or IoT, devices are growing progressively troubling.

F. Credential Attacks

Attackers use default or weak passwords to access IoT devices with authority. Once inside, they change the settings of the device, take advantage of sensitive data, or use the device as a stepping stone to get onto a broader network.

G. Firmware Attacks

By rewriting the firmware, attackers take over the workings of the device and are potentially allowed to control it remotely or provide unauthorized access.

H. Side-Channel Attacks

Attackers using side channel take employ of data that is exposed if the device is working regularly, such as patterns of power use or electromagnetic emissions. IoT attacks like these have the capacity for exposing encryption keys and other personal information.

I. Encryption Attacks

If the user's IoT device is not encrypted, then attackers can install and modify their algorithms and take over your device. In regard to the significance of encryption in IoT devices, this is a crucial detail to remember.

J. Brute Force Password Attack

Software that can make a large number of password combinations is used in this attack, and the attacker distributes these to a targeted user base. The attack targets accounts that have a weak password securing them. As a result, the attacker is free to steal confidential data, spread malware, and carry any other actions.

III. RELATED WORKS

The art of incorporating machine learning has been the focus of numerous studies in the past and a number of professional works on the use of machine intelligence and data-mining techniques for intrusion detection have been published [1]. But almost all of these earlier studies have only employed machine learning methods to identify intruders in conventional networks. As a result, in this work, we are expanding this field of study by particularly using machine learning to recognize attacks in the conditions of Numerous studies has already concentrated on the art of incorporating machine learning 2], and a number of professional works on the utilization of data-mining and machine intelligence methods in security detection have been published [3]. However, nearly all of these prior studies have solely utilized machine learning techniques to detect intrusions via conventional networks. As a result, we extend this area of research in this work by specifically deploying machine learning to identify attacks under certain conditions of

We looked at a number of books and compiled them in Table I to analyze recent research on the subject of attack detection using machine learning in IoT networks. The datasets, detection strategies, and learning approaches have been provided for each research. We explored the usage of various machine learning approaches and datasets when choosing these studies. The studies provide evidence that machine learning techniques can achieve success for attack detection. From the works discussing the issue of using machine learning for IoT security, the detection methodologies can be categorized as unsupervised methods [6], [7], [8], [14] and supervised methods [9], [10], [11], [11, [12]

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24OCT580

Table 1: Summery of Related Works

Ref.	Year	Detection approach		
		Signature	Anomaly	ANN
[9]	2018		✓	✓
[10]	2018		✓	
[8]	2016	✓		
[12]	2018		✓	
[14]	2019		✓	
[19]	2016		✓	✓
[13]	2017		✓	
[20]	2015		✓	
[15]	2017	✓		
[21]	2018		✓	✓
[18]	2018		✓	
[16]	2017		✓	✓
[22]	2019		✓	✓
[23]	2019		✓	
[24]	2019		✓	
[17]	2019	✓		✓

IV. PROPOSED METHDOLOGY

CNN, our suggested method for feature selection and threat detection on Internet of Issues networks. CNN utilizes the features of a dual convolutional neural network architecture. Our approach is to automatically choose interesting elements from IoT network traffic data by utilizing CNN's features. In order to identify the most useful characteristics to correctly classify network traffic as either attack or regular, CNN-CNN consists of two separate CNN models that cooperate in some way. One model is used for feature selection, and the other is used for attack detection.

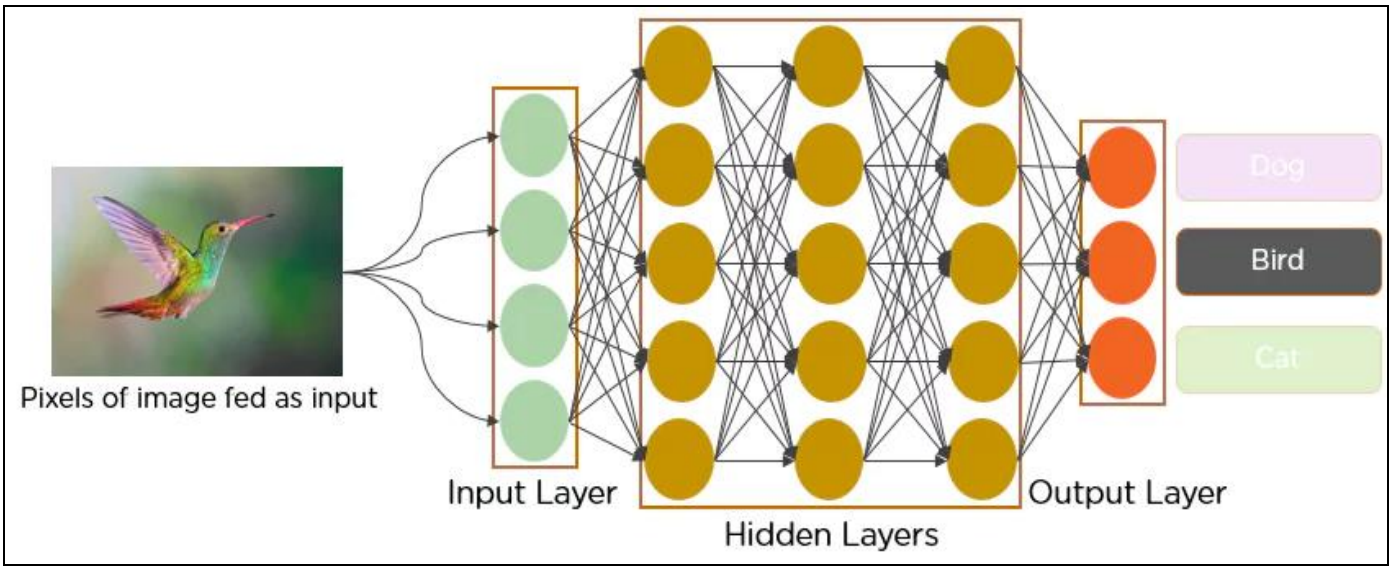

Fig 1: CNN For Attack Detection

Convolutional neural networks are distinguished from other neural networks by their superior performance with image, speech, or audio signal inputs. They have three main types of layers, which are:

- Convolutional layer
- Pooling layer
- Fully-connected (FC) layer

DRE deep reinforcement learning Within the field of machine learning, a new research area is called While neural networks have made recent advances in fields such as time series, computer vision, and machine translationNeural network deep learning. Many of DRL achievements can be attributed to extending earlier RL work to high-dimensional situations. This is brought about by neural networks' strong function approximation capabilities and their ability to learn

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24OCT580

low-dimensional feature representations. Unlike tabular and typical nonparametric approaches, DRL may successfully conquer the curse of dimensionality through representation learning [7]. Convolutional neural networks (CNNs), for example, can be employed as parts of reinforcement learning (RL) agents, enabling them to learn directly from high-dimensional, raw visual inputs. Training deep neural networks to approximate the optimal policy π* and/or the optimal value functions V*, Q*, and A* is the broad foundation for deep learning via reinforcement (DRL).

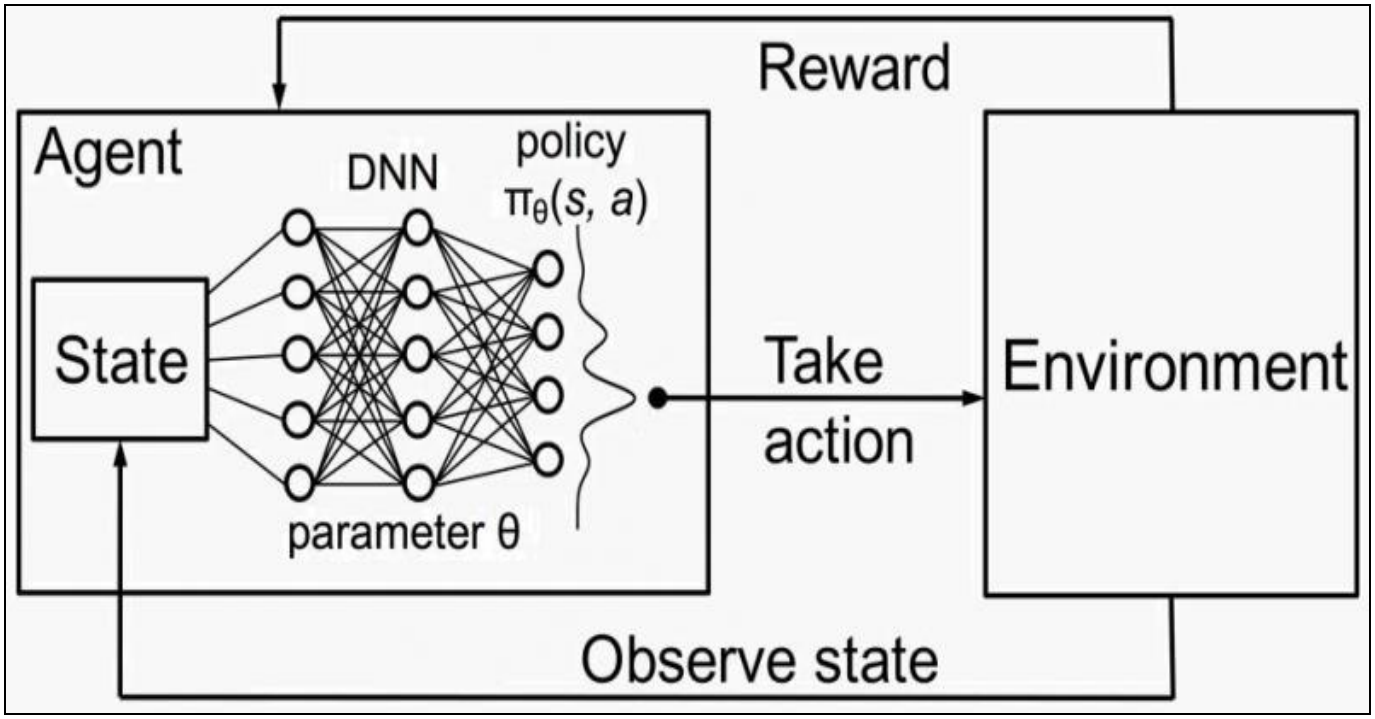

Fig 2: DRE for Attack Classification

➢ *Data Preprocessing*

The process of changing raw data into a format that is suitable to machine learning is known as data preparation. To get ready for machine learning, data is collected from many sources and scrubbed. It might not be in a suitable form, have sounds and missing data, or both.

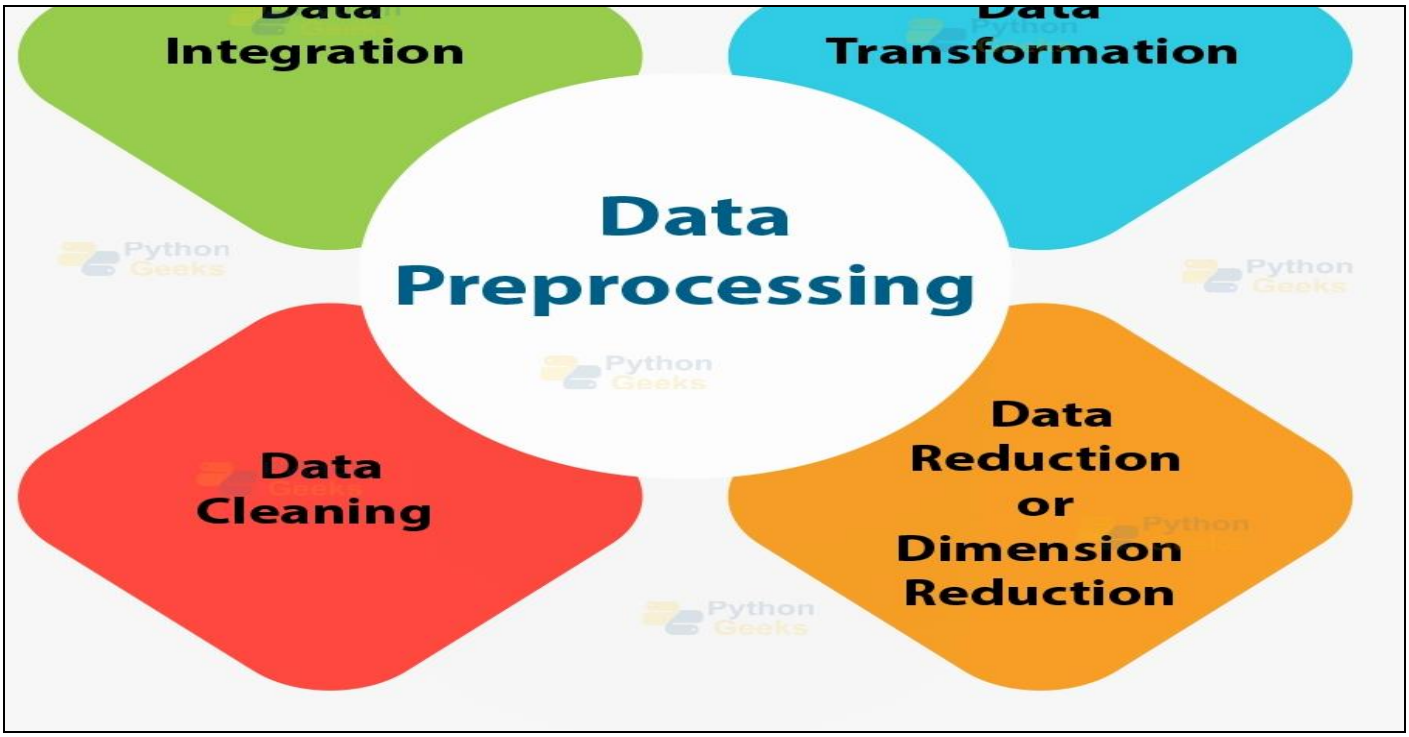

Fig 3: Data Preprocessing Stages

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24OCT580

V. RESULTS

df= pd.read_csv(r'C:\Users\qures\Downloads\sample.csv')
print(df)

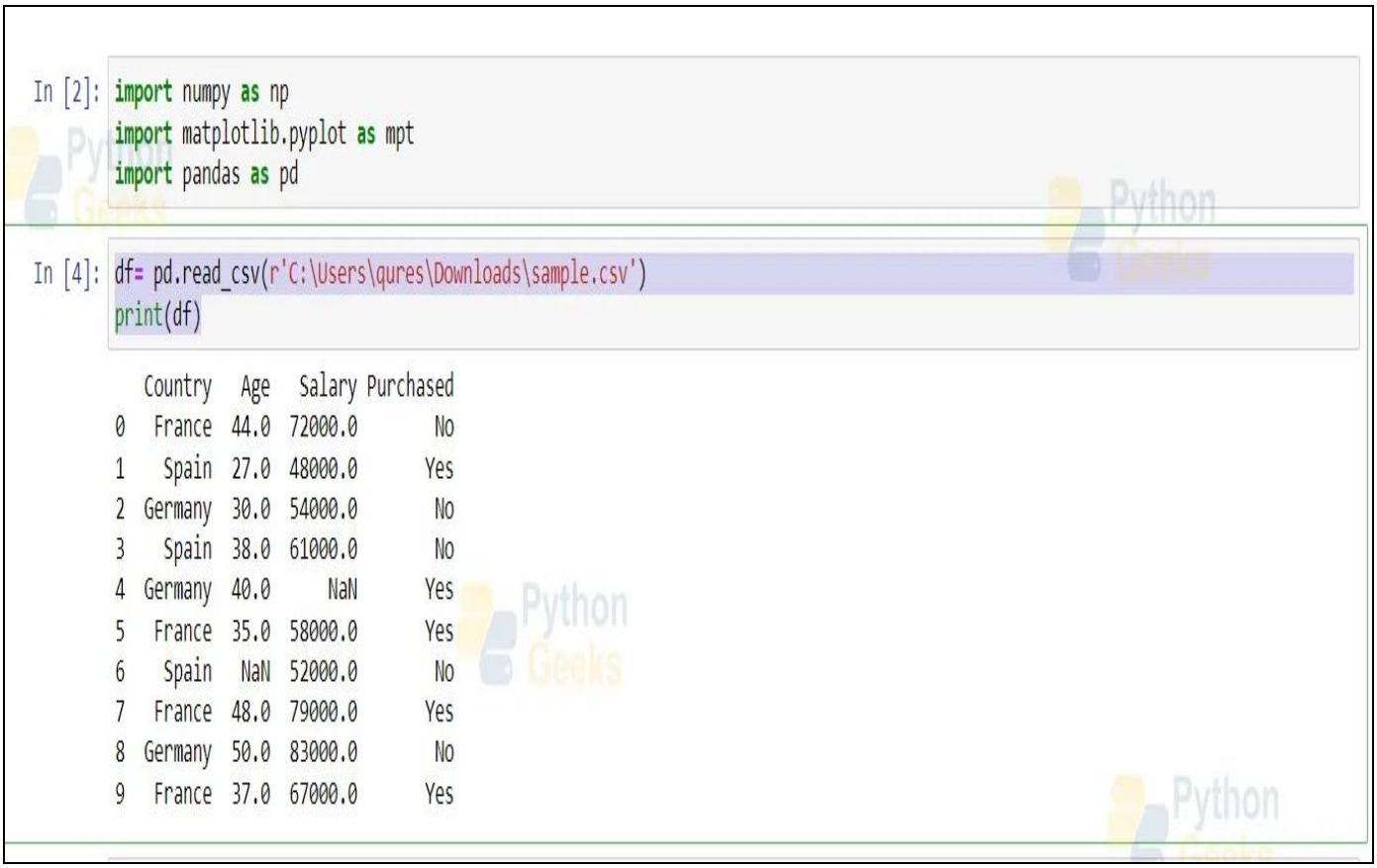

Fig 4: Data Set Importing to Classify Attacks

VI. CONCLUSION

The Internet of Things (IoT) is a system made up of millions of digital devices and people can easily interact with the devices by connecting them. One of the digital sectors that is expanding the fastest is IoT, but it may also be very hazardous. A increasing hazard in the sphere of technology is the Internet of Things (IoT) buildings that can be damaged by infections and faulty duty. Growing adoption of internet of things in various industries has led to a proportional rise in attacks and dangers on these systems. Cyber-attack detection, which makes utilization of basic machine learning methods, is critical for avoidance of damage from cyberattacks on Iot of Things devices. I.T. Artificial Neural Networks (also called ANN Do Not Detect Cyberattacks Using Deep Learning The techniques Convolutional neural networks-deep reinforcement learning (CNN-DRL) hybrid approach: Detect attacks, such as eavesdropping, zero-day, and distributed denial of service (DDoS) attacks.In future Classifly more Attcks Using Advanced Deeop Learnig Technques.

ACKNOWLEDGEMENT

I would like to express my profound gratitude to Dr. Kunjam Nageswara Rao Professor Department of Computer Science and System Engineering in Andhra University Andhra Pradesh, Visakhapatnam India, for giving Guidance and Support to Review and Given suggestion.

- *Author Contribution*

All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by Katikam Mahesh, Dr Kunjam Nageswara Rao, and all authors commented on previous versions of the manuscript.

- *Conflicts of Interest*

The authors declare no conflicts of interest

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24OCT580

REFERENCES

[1]. G. Eason, B. Noble, and I.N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551, April 1955. (*references*)

[2]. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[3]. I.S. Jacobs and C.P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.

[4]. K. Elissa, “Title of paper if known,” unpublished.

[5]. R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[6]. Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, “Kitsune: an ensemble of autoencoders for online network intrusion detection,” arXiv preprint arXiv:1802.09089, 2018.

[7]. X. Yuan, C. Li, and X. Li, “Deepdefense: identifying ddos attack via deep learning,” IEEE International Conference on Smart Computing (SMARTCOMP), pp. 1–8, 2017.

[8]. Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, “N-baiot—network-based detection of iot botnet attacks using deep autoencoders,” IEEE Pervasive Computing, vol. 17, no. 3, pp. 12–22, 2018.

[9]. M. A. Ferrag and L. Maglaras, “Deepcoin: A novel deep learning and blockchain-based energy exchange framework for smart grids,” IEEE Transactions on Engineering Management, 2019.

[10]. Y. Meidan, M. Bohadana, A. Shabtai, M. Ochoa, N. O. Tippenhauer, J. D. Guarnizo, and Y. Elovici, “Detection of unauthorized iot devices using machine learning techniques,” arXiv preprint arXiv:1709.04647, 2017.

[11]. N. Koroniotis, N. Moustafa, E. Sitnikova, and J. Slay, “Towards developing network forensic mechanism for botnet activities in the iot based on machine learning techniques,” International Conference on Mobile Networks and Management, pp. 30–44, 2017.

[12]. Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, “Rule generation for signature-based detection systems of cyber-attacks in iot environments,” Bulletin of Networking, Computing, Systems, and Software, vol. 8, no. 2, pp. 93–97, 2019.

[13]. V. H. Bezerra, V. G. T. da Costa, S. B. Junior, R. S. Miani, and B. B. Zarpelao, “One-class classification to detect botnets in iot devices,” Anais do XVIII Simposio Brasileiro em Seguranc¸a da Informac¸ ´ ao e ˜ de Sistemas Computacionais, pp. 43–56, 2018.

[14]. E. Hodo, X. Bellekens, A. Hamilton, P.-L. Dubouilh, E. Iorkyase, C. Tachtatzis, and R. Atkinson, “Threat analysis of iot networks using artificial neural network intrusion detection system,” International Symposium on Networks, Computers and Communications (ISNCC), pp. 1–6, 2016.