A Review on IoT Cyber-Attacks Detection Challenges and Solutions

Marwa Jawad Kathem[*], Tayseer Salman Atia[**]

[*] College of Engineering, Al-Iraqia University, Saba'a Abkar Complex, Baghdad, Iraq
Email: marwajk86@gmail.com
https://orcid.org/0009-0000-3719-429X

[**] College of Engineering, Al-Iraqia University, Saba'a Abkar Complex, Baghdad, Iraq
Email: tayseer.Salman@aliraqia.edu.iq
https://orcid.org/0000-0002-1552-569X

Abstract

The Internet of Things (IoT) has recast the way we interact with technology and the world around us. The IoT is almost everywhere in our daily lives, and this huge growth in using the IoT increases the need for implementing a high level of security framework for this technology. This study presents an analysis of some of the recent IoT cyber-attack detection systems to provide an evaluation of these systems and useful future research directions in this field. This analysis is introduced along with an overview of the IoT's security challenges and solutions and the types of security attacks in the IoT environment. Although the most recent approaches to cyber-attack detection have high percentages of attack detection accuracy, these classical DL models that were learned with local datasets need more enhancement to maintain privacy and data storage when involved in networks of cooperative nodes in IoTs. Furthermore, current techniques still lack the ability to provide a generalization for new attacks, cover the binary and multiclass classifications of cyber-attacks, and develop feature selection algorithms to reduce dataset dimension.

Keywords- IoT security, Fog/edge computing, machine learning, deep learning, cyber-attacks.

I. INTRODUCTION

The Internet of Things (IoTs) is one of the rapidly developed technologies works on a strategy of connecting electronic/mechanical devices, sensors, and objects to be communicated with each other and sharing data over the internet. Our daily life is enhanced with use of IoT technology since it's used is varied from smart homes, smart cities and wearable devices to industrial machinery and different areas including healthcare services, automotive, agriculture and smart farming, and smart grid [1 - 3].This huge growth of using IoT in our daily life increases the need for securing this technology and studying the challenges and solutions related to this issue.

Different architectures have been proposed to model the structure of IoT such as: three-layer architecture, middleware architecture, SOA-Based architecture, and five-layer architecture [4]. There is no one model can used to all suggested architectures, but the "Three Based Architecture" presented in [5] is one of the greater architectures that could be used to describe the structure of IoT.
This architecture, as it shown in Figure 1, has the three layers [5]:

1. IoT layer: the layer in which all the IoT system devices are placed including sensors, actuators, smart devices, entities, and end-users.
2. Fog layer: the layer of Fog (edge) devices which have the responsibility of managing and processing all data related to IoT system devices which are grouped in this layer.
3. Cloud layer: this layer contains different servers in which multiple processes are done. Servers of cloud layer include cloud server, data server, application server; and data centres and operation centres.

This study aims to present an analysis for some of recent IoT cyber-attacks detection systems along with providing an overview of IoTs security challenges and solutions, and types of security attacks in IoT environment. Moreover, this review is done to address the limitation of the available DL techniques used for cyber-attack detection in IoT environments. According to the analysis of the most

recent available studies, useful information and future research directions is provided to be used by researchers interested in the field of this study.

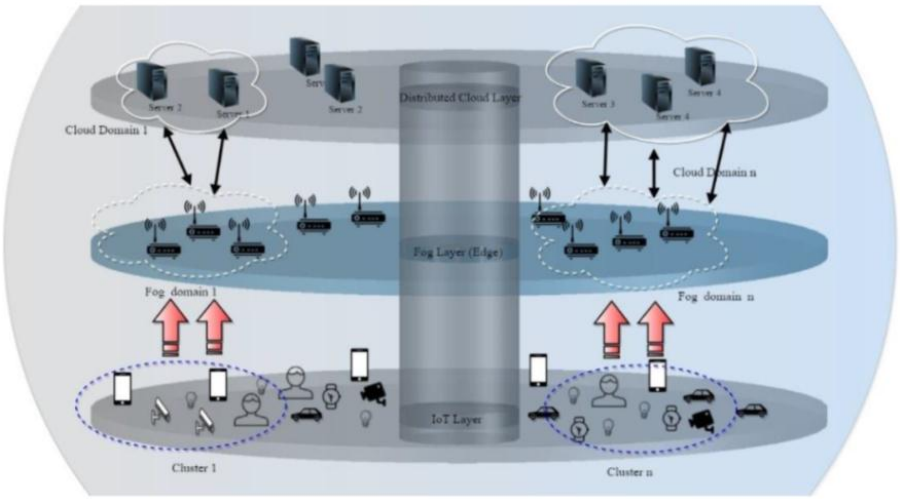

Fig 1. The IoT three-based architecture layered

II. IoTS SECURITY CHALLENGES AND SOLUTIONS

The growth and wide use of IoT technology in different areas of our daily lives has increased the need for implementing it with a high level of security. Implementing security for IoT has limitations and challenges since the data processing in IoT needs a reliable security mechanism and a light weight version of cryptographic algorithm fit the resource limited devices "things" connected in IoT environment [6].
Different mechanisms of security solution in IoT environment are proposed in literature including: block-chain, cloud, fog/edge computing and machine learning.

A. Block-chain based solutions

A block-chain is a peer-to-peer (P2P) network decentralized and distributed framework that is able to record and track assets and transactions through the network. It uses blocks of data arranged in chain, as it shown in Figure 2, to store full history of all transactions. The basic structure of each block in a block-chain has two parts, the header and the list of transactions as the body part. The header of a block holds information related to block size, version number, timestamp, and transactions number. To have efficient data verification, the structure uses "Merkle tree hashing" to identify the value of each block. Other fields of header nonce and difficulty target are used for specifying "proof-of-work algorithm" and "number of leading zeros" respectively [7].
Authentication and integrity of data in the block-chain are proved by using elliptic curve cryptography (ECC) along with SHA-256 hashing. Block-chain could be implemented as permissioned network or permission-less network. A permissioned network is the most private and the best implementation of block-chains in terms of privacy and access control [7].

B. Fog/edge computing based solutions based solutions

Fog computing represent an extend approach of cloud computing to the edge of the network, providing a mechanism of management and computation for devices at the edge of the IoT network. The structure of fog computing provide many advantages such as: Low latency, Geographical and large-scale distribution, Mobility and location awareness, Flexibility and heterogeneity, Scalability [8]. The nodes of fog layer are close to the limited resources devices of IoT with support of different real-time services to these devices.
An example that is showing architecture of Cloud-Fog is presented in Figure 3 [9]. According to the provided structure, fog nodes have a horizontal distribution along with location awareness related to the fog devices, and a vertical construction shows how part of processing in fog computing is distributed to the edge nodes of the network [9].

C. Machine learning based solutions

Machine learning (ML) is one of the subsets related to artificial intelligence (AI). The advances in the techniques of ML participate in using it in attacks detection for security solutions in IoT [10]. ML uses algorithms including (supervised, unsupervised, semi supervised and reinforcement) to train machines and help devices to learn and work in automated machine [11].
Deep learning (DL) is also an approach for machine learning in which several layers of processing are combined including inputs, hidden, and output layers, to give the ability of learning from data. Learning from large datasets makes DL better in performance than

traditional ML. Multilayer Perceptron (MLP) and Convolutional Neural Network are the most used algorithms among DL algorithms [11]. The structure of an ANN model with multiple processing layers to represent a MLP is shown in Figure 4. The connection of nodes from one layer to another is set with weight that is adjusted using a "Backpropagation" technique. MLP structure is computationally costly model since it provides flexibility in tuning the "hyperparameters" including the number of iterations, hidden layers, and neurons [11].

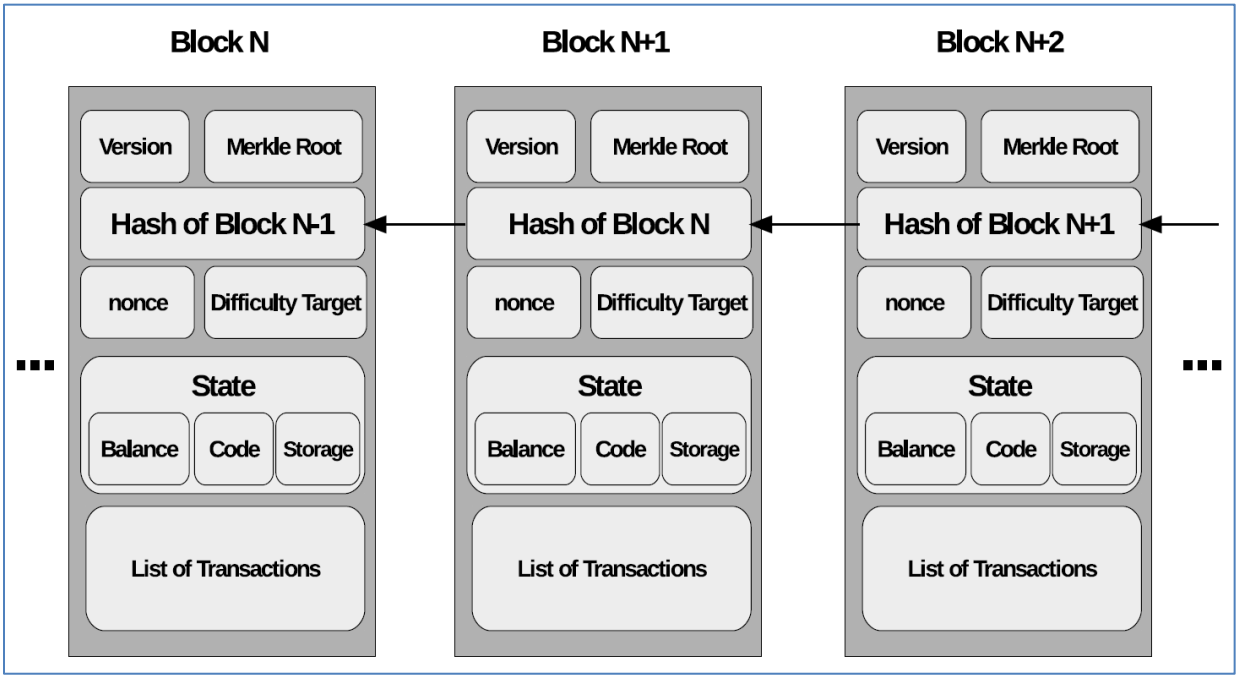

Fig 2. Block-chain design Structure

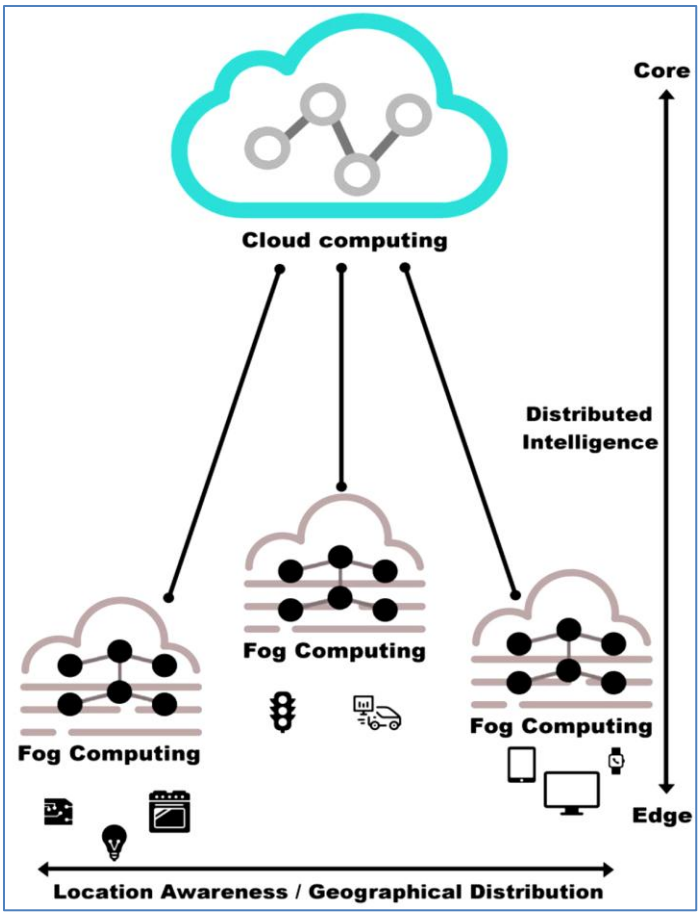

Fig 3. Cloud-Fog architecture

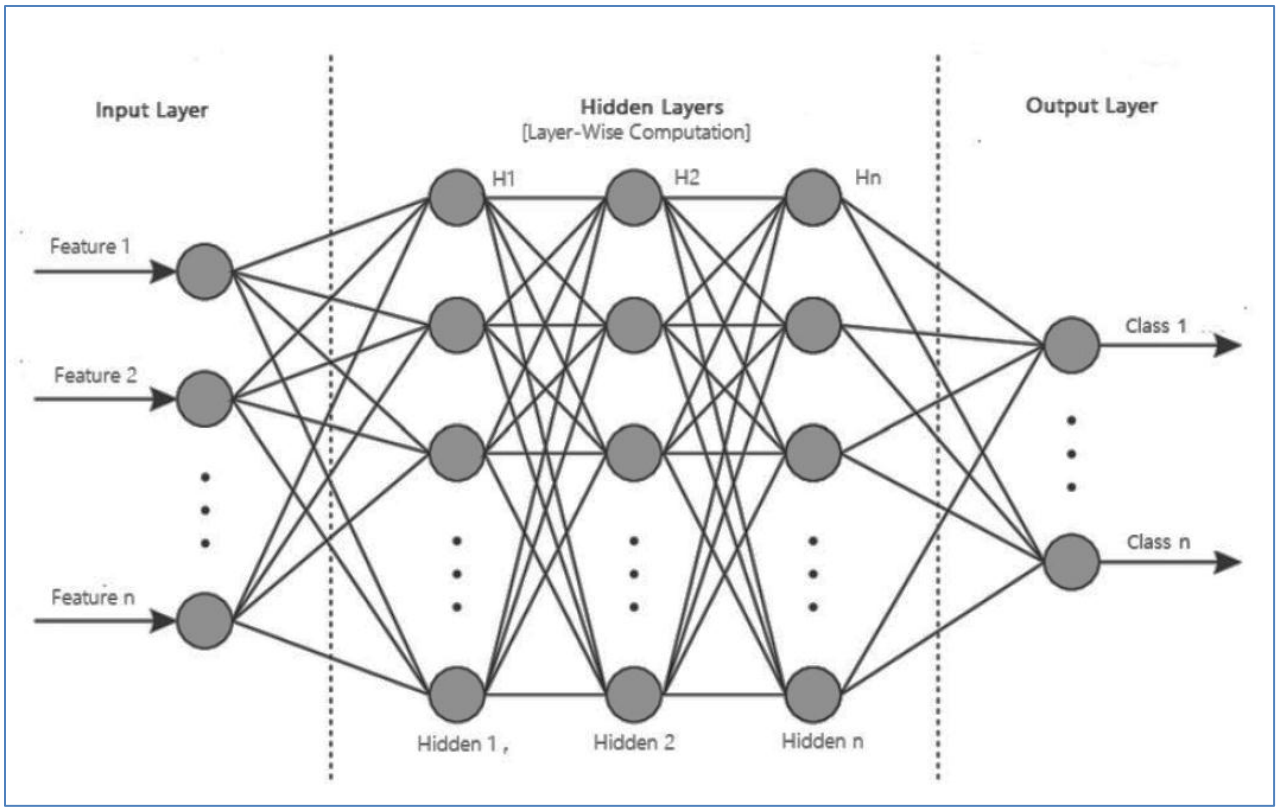

Fig 4. A structure of an ANN model with multiple processing layers

III. SECURITY ATTACKS IN IoT ENVIRONMENT

In IoT environment, devices are targeted by different types of attacks. One of the best known classification for the security attacks in IoT is the four domains classification which are: physical attacks, network attacks, software attacks and data attacks [12]. Figure 5 shows the classifications of attacks in IoT which are briefly described below [12]:

A. Physical attacks

It is a class of IoT attacks in which the attacker be close physically to IoT network and its devices to generate attack with one of physical attacks including: Tampering, Malicious Code Injection, RF Interference/Jamming, Fake Node Injection, Sleep Denial Attack, Side Channel Attack and Permanent Denial of Service (PDoS).

B. Network Attacks

In this class of attacks, IoT Network is exploited to attacks without having to be close to the network. Different network attacks could be done such as: Traffic Analysis Attack, RFID Spoofing, RFID Unauthorized Access, Routing Information Attacks, Selective Forwarding, Sinkhole Attack, Wormhole Attack, Sybil Attack, Man in the Middle Attack (MiTM), Replay Attack and Denial/Distributed Denial of Service (DoS/DDoS) Attacks.

C. Software Attacks

It is a major type of attacks targeting the communication interface of IoT devices using different types of software attacks including: Virus, Worms, Trojan Horses, Spyware, Adware, and Malware. The best examples for software attacks in reality are: the mirai botnet and the jeep hack.

D. Data Attacks

It is a class of attacks aim to manipulating or hacking the database resources of IoT network using different form including: data inconsistency, unauthorized access, and data Breach.

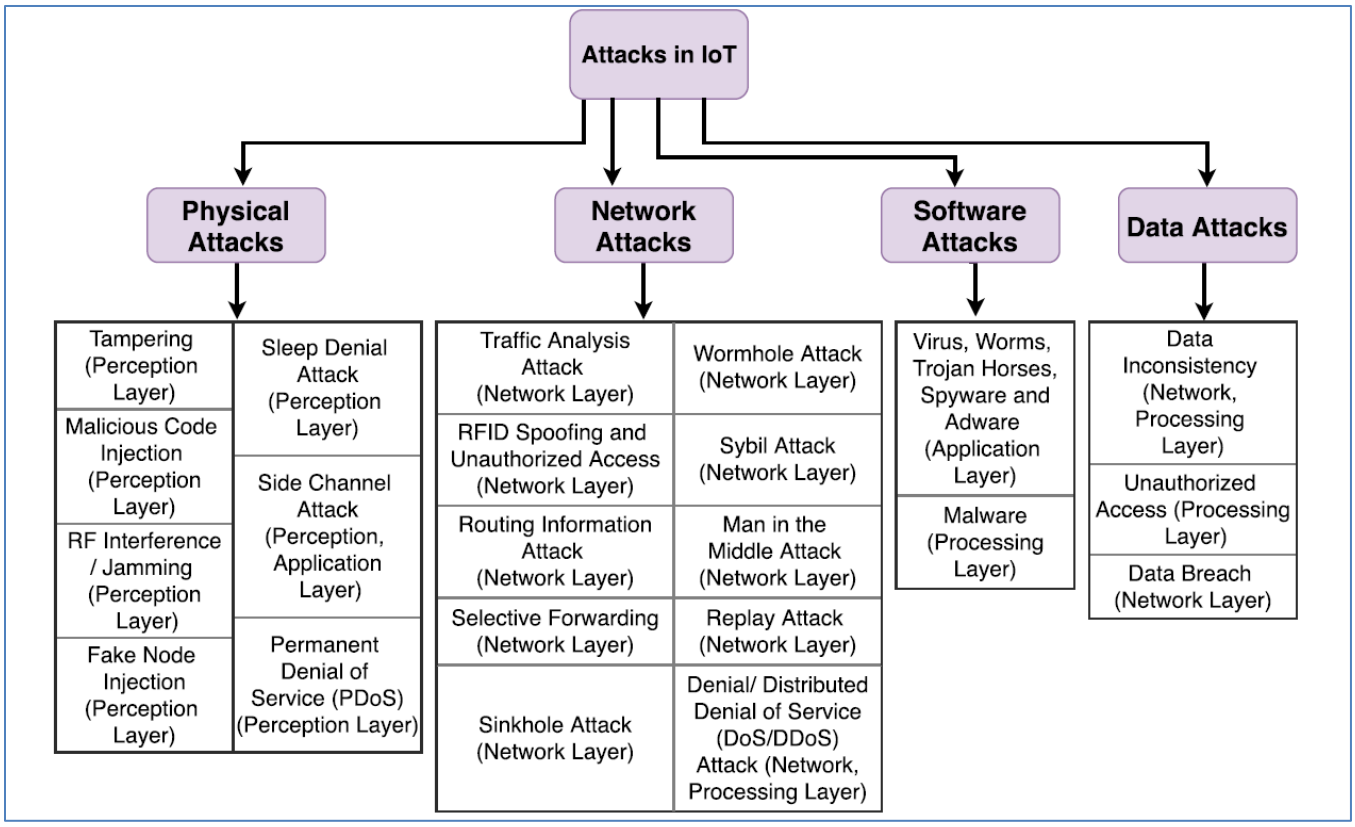

Fig 5. The classifications of attacks in IoT environment

IV. DETECTION TECHNIQUES BASED ON DL

In recent years, there has been an increasing amount of studies on developing methods for solving IoT cyber-attacks detection. In a study in 2020, Yi-Wen Chen, et al. [13] provided a method to detect and block DDoS attacks in SDN controlled environments based on techniques of machine learning. Decision trees as a supervised learning tool are used to do the process of DDoS attack detection while the attack blocking phase is done on an SDN controller in a real IoT environment. The suggested algorithm used by this study was able to achieve accuracy and F1-score of over 97%.

Yizhen Jia, et al. [14] (2020), suggested two machine learning models to identify and classify DDoS attacks, which are LSTM and CNN models. Authors in this study use the suggested machine learning models to build an IoT defense design named as "FlowGuard". The study uses a dataset created by combining dataset generated by DDoS simulators with the known CICDDoS2019 dataset. The provided design reached attack identification accuracy of 98.9% and attack classification of 99.9%.

Another study by Mahmoud Said Elsayed, et al. (2020), [15] proposed Deep Learning (DL) based intrusion detection system to detect DDoS attacks in SDN environments named as "DDoSNet". The Authors of this study use combined learning techniques of Recurrent Neural Network (RNN) with auto-encoder. Training and evaluation of the model suggested by this study are done with the use of CICDDoS2019 dataset. Suggested DDoSNet has an accuracy of 99%.

An approach for detection and classification of malware based on deep learning is presented by Gueltoum Bendiab, et al. (2020), [16]. ResNet50 architecture is used by the authors of this study to implement the suggested approach. A dataset construction is done by authors to create a testing dataset of 1000 PCAP files for attack and non-attack of different traffic sources. The testing of the proposed use of ResNet50 showed accuracy in detection of malware traffic of 94.50%.

A security framework application for IoT networks to provide DDoS attack detection is proposed by JALAL BHAYO, et al. (2020) [17]. The authors build a C-DAD (Counter-based DDoS Attack Detection) application to be used in providing a service of attack

detection. The testing of the proposed application and framework focused on discussing detection time. A minimum time related to minimum use of memory resources and CPU power.

Another framework of attack detection is presented by Mahdi Hassan Aysa, et al. (2020) [18]. Authors build a proposed framework to detect abnormal defense activities. Different algorithms of data mining and machine learning including (LSVM, Neural Network, and Decision tree) are used for detection of DDOS features. Open source software named WEKA is used to learn the selected machine learning algorithms with standard dataset of two DDoS attack types. According to the authors of this study, the best result of accuracy is achieved by combining random forest and decision tree for attack detection.

Faisal Hussain, et al. [19] (2020), used a method to deal with network traffic by encoding it into images then train them with ResNet. The dataset selected to test the work done by this study is CICDDoS2019. A binary classification of DoS and DDoS showed an accuracy of 99.99% while multi-classification of eleven type's of DoS and DDoS showed an accuracy of 87%.

In a study in 2021, G.C. Amaizu, et al. [20] a framework to detect DDoS attack in 5G and B5G is presented. Two combined deep learning models are used to build the framework presented by this study and Pearson Correlation Coefficient (PCC) is used as a feature extraction algorithm to optimize model accuracy and reduce complexity. The testing of the presented framework with CICDDoS2019 to detect DDoS attacks achieved an accuracy of 99.66% and a loss of 0.011.

Akshat Gaurav, et al. [21] (2021) suggested a method for DDoS attack detection in the fog layer of IoT architecture. Authors build their work with use of Omnet++ simulator. Identification of malicious IoT devices is done with the use of clustering along with entropy-based methods. According to the authors of this study, an efficient architecture is achieved with recognized values including precision rate and low traffic in detection of DDoS attack traffic.

A fog layer based framework for anomaly detection in IoT networks is considered by Deepak Kumar Sharma, et al. [22] (2021). Continuous ranked probability score (CRPS) is used to build the algorithm suggested by this study. DARPA99 dataset is used in the process of evaluating the proposed architecture. Results of this study showed the ability of the proposed algorithm in identification of DDoS attacks correctly.

In a study in 2022, Kumar Saurabh, et al. [23] intended DDoS attack detection framework named "NFDLM". ANN optimized version and mutual correlation is used in designing the suggested framework. Mutual correlation's role is to build the phase of feature selection. The study presented more than one model to compare ANN based models with LSTM based models. The evaluation of the framework is done on the BoT-IoT dataset. The accuracy of detection for the main model (ANN based) in this study was 99%.

Parul Gahelot, et al. [24] (2023) presented an intelligent method of detecting DDoS attacks on IoT networks. Authors proposed a CNN model in their study for detecting DDoS attack. The suggested CNN structure was tested on self-generated dataset provided in the study. The proposed model achieved an accuracy rate of 99.98% in detecting DDoS attacks.

A DL detection method of brute force attacks on IoT is suggested by Ahmed Otoom, et al. (2023) [25]. The authors used two DL methods (i.e. hold out validation and 5-fold cross validation) to have more accurate binary classification to brute force attacks provided in MQTT-IoT-IDS2020 dataset. Two subsets from the dataset are used in the WEKA workbench for testing the proposed classifiers, which are the Bi-flow feature set and Uni-flow feature Set. The best accuracy achieved by this study is 99.56% on Bi-flow feature set and 99.67% on Uni-flow feature set.

Another DL technique for detecting botnet attacks is provided by Muhammad Nadeem, et al. (2023) [26]. Five DL methods were simulated in this work and CNN was selected as the best model among them. Proposed methods were tested on self-generated datasets based on the SDN network. The best result of accuracy achieved by the CNN model was 99% for normal flows and 97% for attack flows.

Table 1 summarizes a comparison of the studies mentioned previously. As described in the table, the analysis covers all important aspects related to attack types, processing methods, datasets used, results, and environments used. Although these studies achieve their design goal, the following issues are not considered:

1. Most studies in this field have only been carried out for attacks detection (i.e. Binary classification) and attacks identification with Multi-class classification was not considered.
2. Feature selection, which is playing a key role in enhancing the accuracy and speed of the model training.
3. A framework of decentralized or centralized learning are not discussed when local models involved in networks of cooperative nodes of IoTs.

Table 1. Summary of detection techniques.

Ref. No	Attack type	Processing method	Dataset used	Results	Environment
[13]	DDoS	Decision Tree (Supervised learning)	self-generated dataset	97% in both accuracy and F1-score.	IoT Environment
[14]	DDoS	LSTM's following by CNN	CICDDoS2019	over 98.9% in identification, and 99.9% in classification	edge servers
[15]	DDoS	Recurrent Neural Network (RNN)	CICDDoS2019	High evaluation in terms of recall, precision, F-score, and accuracy	SDN environments
[16]	Malware	ResNet-50	self-generated dataset	Accuracy of 94.50%.	visual representation of the collected network traffic
[17]	DDoS	C-DAD programmable solution	self-generated dataset with Cooja simulator	Minimizing the time of attack detection with a tolerable impact on CPU and memory.	SDN environments and IoT controller
[18]	Botnet DDoS	LSVM learning and Decision tree with WEKA (S/W)	dataset collected from IoT Sensor Devices	Good accuracy in detecting attacks.	Wireless IoT network
[19]	DOS / DDoS	CNN (ResNet)	CICDDoS2019	99.99% accuracy. 87% precision	IoT Environment
[20]	DDoS	DNN and Pearson Correlation Coefficient (PCC)	CICDDoS2019	Accuracy of 99.66%	B5G network

[21]	DDoS	Per-trained model	Training dataset required	Efficiently detects the DDoS attack traffic.	Fog Layer
[22]	DDoS	Continuous ranked probability score (CRPS)	DARPA99	Efficiently detects the DDoS attack traffic.	fog-empowered IoT networks
[23]	Botnet DDoS	ANN with mutual correlation as feature selection	BoT-IoT	Achieves approximately 99% accuracy	IoT Environment filter based : lightweight
[24]	Botnet DDoS	CNN model	self-generated dataset	Accuracy of 99.98%	IoT Environment
[25]	brute force	DL methods hold out validation 5-fold cross validation with WEKA (S/W)	MQTT-IoT-IDS2020 dataset Bi-flow feature set Uni-flow feature set	Accuracy of 99.56% on Bi-flow feature set Accuracy of 99.67% on Uni-flow feature set	IoT Environment
[26]	Botnet DDoS	five DL methods (best selected is CNN model(	self-generated dataset	99% for normal flows and 97% for attack flows.	SDN-supported environment

V. DISCUSSION

This review addresses the limitation of the available DL techniques used for cyber-attack detection in IoT environments [13-26]. Most of the recent available studies provide DL systems with high percentages of attack detection accuracy. On the other hand we can identify important issues related to these available approaches.

In the available studies and approaches there is still lack in providing a generalization of the developed models for new attacks (i.e. zero-day attack). Most of the developed DL models do a job of detection by providing only the binary classification of cyber-attacks like in [13], [15]-[26]. Furthermore, there is a need for developing feature selection algorithms which reduce the dimension of datasets, leading to improvement in accuracy and speed of DL models.

Another important issue related to the IoT DL models used for applications on edge nodes, is the need to implement an efficient and secure framework of decentralized or centralized learning that guarantees the privacy of data.

VI. CONCLUSION

Studying the security challenges and solutions related to cyber-attack security of IoT is very important in supporting the growth of IoT technology. The present study was designed to determine and evaluate the security systems in IoT environment. The IoT architecture, the IoTs security challenges and solutions, and types of security attacks in the IoT environment have been discussed in this study. The study focused on analysis of various research works available in the literature, which suggested different security systems for IoT.

Most recent approaches provide a classical DL technique with high percentages of attack detection accuracy. However, these classical DL models that learned with local datasets need more enhancement for maintaining privacy and data storage when involved in networks of cooperative nodes of IoTs. Furthermore, current techniques still have lack in providing a generalization for new attacks, covering the binary and multiclass classifications of cyber-attacks and developing feature selection algorithms to reduce dataset dimension.

REFERENCES

[1] R. P. Singh, M. Javaid, A. Haleem, and R. Suman, “Internet of things (IoT) applications to fight against COVID-19 pandemic,” Diabetes & Metabolic Syndrome: Clinical Research & Reviews, vol. 14, no. 4, pp. 521–524, 2020. doi:10.1016/j.dsx.2020.04.041.

[2] N. Hossein Motlagh, M. Mohammadrezaei, J. Hunt, and B. Zakeri, “Internet of things (IoT) and the Energy Sector,” Energies, vol. 13, no. 2, p. 494, 2020. doi:10.3390/en13020494.

[3] F. Alshehri and G. Muhammad, "A Comprehensive Survey of the Internet of Things (IoT) and AI-Based Smart Healthcare," in IEEE Access, vol. 9, pp. 3660-3678, 2021, doi: 10.1109/ACCESS.2020.3047960.

[4] L. Kakkar, D. Gupta, S. Saxena, and S. Tanwar, “IoT architectures and its security: A Review,” Lecture Notes in Networks and Systems, pp. 87–94, 2021. doi:10.1007/978-981-15-9689-6_10.

[5] W. Kassab and K. A. Darabkh, “A–Z survey of internet of things: Architectures, protocols, applications, recent advances, future directions and recommendations,” Journal of Network and Computer Applications, vol. 163, p. 102663, 2020. doi:10.1016/j.jnca.2020.102663.

[6] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, “A survey on internet of things security: Requirements, challenges, and solutions,” Internet of Things, vol. 14, p. 100129, 2021. doi:10.1016/j.iot.2019.100129.

[7] M. A. Khan and K. Salah, “IoT security: Review, Blockchain Solutions, and open challenges,” Future Generation Computer Systems, vol. 82, pp. 395–411, 2018. doi:10.1016/j.future.2017.11.022.

[8] G. Peralta et al., “Fog computing based efficient IoT scheme for the industry 4.0,” 2017 IEEE International Workshop of Electronics, Control, Measurement, Signals and their Application to Mechatronics (ECMSM), 2017. doi:10.1109/ecmsm.2017.7945879.

[9] E. Guardo, Alessandro Di Stefano, Aurelio La Corte, M. Sapienza, and Marialisa Scatá, “A Fog Computing-based IoT Framework for Precision Agriculture,” vol. 19, no. 5, pp. 1401–1411, Sep. 2018, doi: https://doi.org/10.3966/160792642018091905012.

[10] S. M. Tahsien, H. Karimipour, and P. Spachos, “Machine learning based solutions for security of internet of things (IoT): A survey,” Journal of Network and Computer Applications, vol. 161, p. 102630, 2020. doi:10.1016/j.jnca.2020.102630.

[11] I. H. Sarker, “Machine learning: Algorithms, real-world applications and Research Directions,” SN Computer Science, vol. 2, no. 3, 2021. doi:10.1007/s42979-021-00592-x.

[12] J. Sengupta, S. Ruj, and S. Das Bit, “A comprehensive survey on attacks, security issues and blockchain solutions for IoT and Iiot,” Journal of Network and Computer Applications, vol. 149, p. 102481, 2020. doi:10.1016/j.jnca.2019.102481.

[13] Y. -W. Chen, J. -P. Sheu, Y. -C. Kuo and N. Van Cuong, "Design and Implementation of IoT DDoS Attacks Detection System based on Machine Learning," 2020 European Conference on Networks and Communications (EuCNC), Dubrovnik, Croatia, 2020, pp. 122-127, doi: 10.1109/EuCNC48522.2020.9200909.

[14] Y. Jia, F. Zhong, A. Alrawais, B. Gong and X. Cheng, "FlowGuard: An Intelligent Edge Defense Mechanism Against IoT DDoS Attacks," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9552-9562, Oct. 2020, doi: 10.1109/JIoT.2020.2993782.

[15] M. S. Elsayed, N. -A. Le-Khac, S. Dev and A. D. Jurcut, "DDoSNet: A Deep-Learning Model for Detecting Network Attacks," 2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Cork, Ireland, 2020, pp. 391-396, doi: 10.1109/WoWMoM49955.2020.00072.

[16] G. Bendiab, S. Shiaeles, A. Alruban and N. Kolokotronis, "IoT Malware Network Traffic Classification using Visual Representation and Deep Learning," 2020 6th IEEE Conference on Network Softwarization (NetSoft), Ghent, Belgium, 2020, pp. 444-449, doi: 10.1109/NetSoft48620.2020.9165381.

[17] J. Bhayo, S. Hameed and S. A. Shah, "An Efficient Counter-Based DDoS Attack Detection Framework Leveraging Software Defined IoT (SD-IoT)," in IEEE Access, vol. 8, pp. 221612-221631, 2020, doi: 10.1109/ACCESS.2020.3043082.

[18] M. H. Aysa, A. A. Ibrahim, and A. H. Mohammed, “IoT Ddos attack detection using machine learning,” 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), 2020. doi:10.1109/ismsit50672.2020.9254703.

[19] F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad and G. A. Shah, "IoT DoS and DDoS Attack Detection using ResNet," 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, 2020, pp. 1-6, doi: 10.1109/INMIC50486.2020.9318216.

[20] G. C. Amaizu, C. I. Nwakanma, S. Bhardwaj, J. M. Lee, and D. S. Kim, “Composite and efficient ddos attack detection framework for B5G Networks,” Computer Networks, vol. 188, p. 107871, 2021. doi:10.1016/j.comnet.2021.107871.

[21] A. Gaurav, B. B. Gupta, C. -H. Hsu, S. Yamaguchi and K. T. Chui, "Fog Layer-based DDoS attack Detection Approach for Internet-of-Things (IoTs) devices," 2021 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2021, pp. 1-5, doi: 10.1109/ICCE50685.2021.9427648.

[22] D. K. Sharma et al., “Anomaly detection framework to prevent ddos attack in fog empowered IoT Networks,” Ad Hoc Networks, vol. 121, p. 102603, 2021. doi:10.1016/j.adhoc.2021.102603.

[23] K. Saurabh, T. Kumar, U. Singh, O. P. Vyas and R. Khondoker, "NFDLM: A Lightweight Network Flow based Deep Learning Model for DDoS Attack Detection in IoT Domains," 2022 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 2022, pp. 736-742, doi: 10.1109/AIIoT54504.2022.9817297.

[24] P. Gahelot, P. K. Sarangi, and L. Rani, “Intelligent detection of ddos attack in IOT Network,” Mobile Radio Communications and 5G Networks, pp. 173–184, 2023. doi:10.1007/978-981-19-7982-8_15.

[25] A. F. Otoom, W. Eleisah, and E. E. Abdallah, “Deep learning for accurate detection of brute force attacks on IOT Networks,” Procedia Computer Science, vol. 220, pp. 291–298, 2023. doi:10.1016/j.procs.2023.03.038.

M. W. Nadeem, H. G. Goh, Y. Aun and V. Ponnusamy, "Detecting and Mitigating Botnet Attacks in Software-Defined Networks Using Deep Learning Techniques," in IEEE Access, vol. 11, pp. 49153-49171, 2023, doi: 10.1109/ACCESS.2023.3277397.