Deep learning-based Internet of Things intrusion detection

Wisam Mohammed Abed[1*]

[1*]Department of Preparation and Training of Computer Science and Information Systems, Ministry of Education, Directorate of Anbar Education, Ramadi, Iraq
E-mail: [1*] wisammohammed17@yahoo.com,

ABSTRACT

A number of models use deep learning to find new ways to infiltrate more secure networks and identify Internet of Things (IoT) attacks. The nature of IoT data and its growing applications, which make attacks more common, has increased the need for the development of an intrusion detection system to quickly identify and categorize attacks. Malicious assaults are always developing and changing. In this research, we investigate how to distinguish between legitimate and malicious behavior while analyzing network data for new threats in order to identify abnormalities and intrusions. This study analyzes earlier work and evaluates the efficacy of previous studies utilizing two fresh types of current traffic data (For example, Bot-IoT and CSE-CIC-IDS2018 datasets). We provide accuracy tests for intrusion detection in various systems to assess performance.

Keywords: deep learning (DL) , Internet of Things (IoT) ,intrusion detection system (IDS) ,Bot-IoT, CSE-CIC-IDS2018

1. Introduction

Critical national infrastructures rely on supervisory control, data acquisition, and industrial control systems to manage their production utilizing the Internet of Things (IoT). Hospitals, transmission and distribution companies for electricity, water and gas, and other sectors of the national infrastructure are all now at risk from cyber-attacks and security issues. Protection has emerged as a crucial concern for safeguarding networks, information, and electronic communications in order to combat these electronic assaults and security issues . In order to protect the network using multiple defensive lines, Additionally, serving as a second line of protection against different threats is the Intrusion Detection System (IDS)[1] . Based on particular rules that outline certain attack patterns or typical system behavior, IDSs discriminate between normal and malicious behaviors . To get higher performance, IDS must fulfill time efficiency, high accuracy, and minimal complexity. Through knowledge discovery, data mining contributes to greater accuracy in unique forms of intrusion and exhibits more resilient behavior than traditional IDSs [2].

The dataset is a crucial element in enhancing the effectiveness of intrusion detection techniques and the need for a trustworthy dataset with examples of both benign behavior and different types of assaults . The IoT's potential for integrating artificial intelligence (AI) to make life simpler has transformed all spheres of existence by making everything smart. [3]. Poor network protocols and a dearth of mathematical analytic methods that are adequately trustworthy hamper the IoT, which causes a surge in attacks. The robust elements in the detection of IoT assaults are

addressed, along with a variety of study approaches and their obstacles. By reviewing prior studies and assessing the model, robust variables are employed to assess these assaults. Deep learning performance using two new real-world traffic datasets Listed below are these components. Factors like "high accuracy rate," "high detection rate," and "low false alarm rate" have an influence on how effective NIDS is. We have made the following contributions to this work:

-We examine prior NIDS studies that used deep learning techniques.

-For intrusion detection, we provide two new actual networks and IoT datasets for intrusion.

-We compare the performances of several deep learning models using various network and Internet of Things data.

2. Materials and Methods (Networks ids (NIDS))

Dependence on worldwide networks while engaging in various commercial, academic, and social activities led to technological growth. Numerous problems with Internet security have emerged as a consequence of the growing usage of computer networks. Therefore, maintaining the security of Internet-connected devices is crucial to guaranteeing system availability and integrity . Network traffic is often recorded in packet and stream formats. Packet-level network traffic is typically recorded by copying ports to network devices, and its data comprises payload data. Flow-based data contains only network connection metadata [4].

For passive traffic collection and analysis, managing networks, analyzing user information networks and services, and quickly identifying security vulnerabilities are important tools . Using firewalls and authentication techniques, one may provide systems protection and prevent unauthorized access. However, these systems, however, these methods lose the ability to monitor network traffic, especially in the case of internal attacks carried out by enraged employees who use their right to network access to cause destruction . Figure (1) illustrates the steps for installing network security.

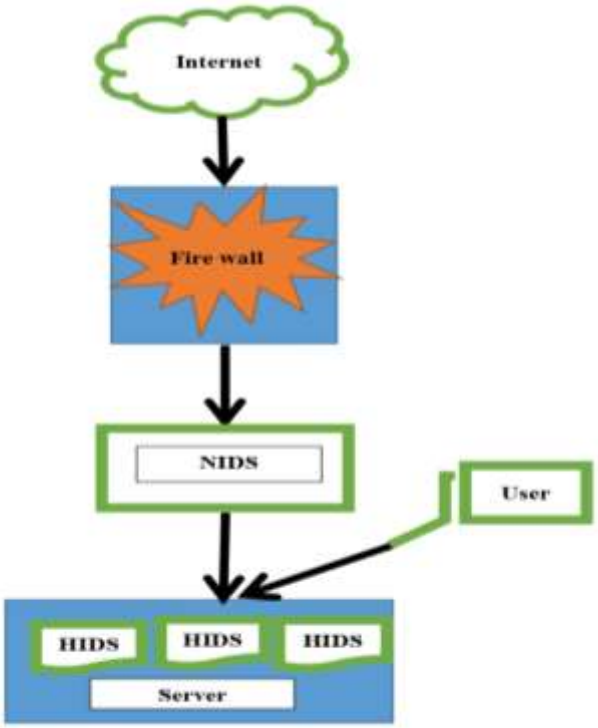

Figure 1. Intrusion Detection System

IDSs are capable of performing two distinct tasks: intrusion alerting, which serves as the initial task and finds harmful activity inside the system; and site security office (SSO), which takes appropriate action in response to the alert. IDSs are categorized using the phrases "anomaly-based detection," "signature-based detection," and "specification-based detection" [5]. The IDS categories are shown in the figure(2).

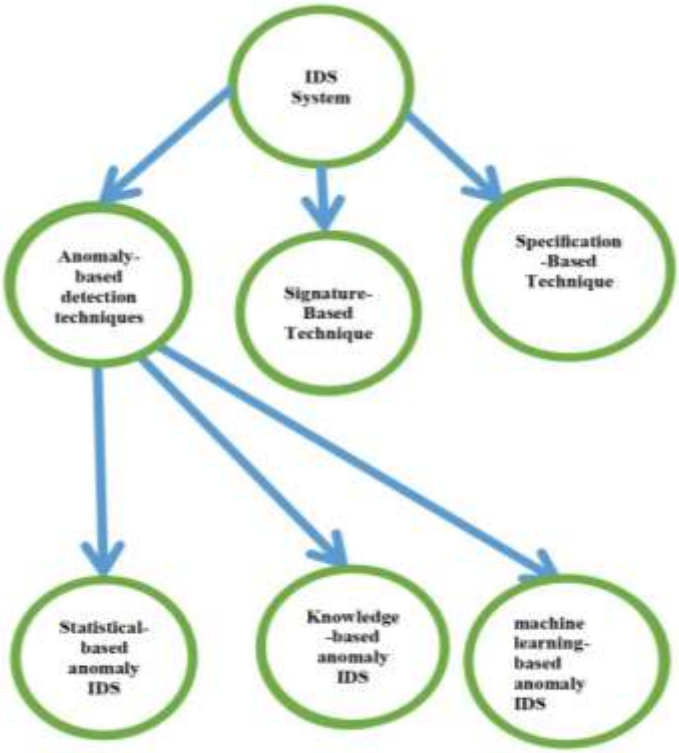

Figure 2 . Types of IDS system

2.1. Anomaly-based detection' techniques

Approaches, which generally relate to statistical data, rely on the conceptualization of a normal or legitimate profile that is acquired under the normal settings of the network without assaults. As a result, this study focused on IDS based on an anomaly. The subject of this investigation's current sub-classification is as follows:

- Statistical-based anomaly IDS: It continuously collects data from traffic statistical characteristics and compares them to the typical functioning of a newly created stochastic traffic model . The difference in patterns between the two statistical models—the one that is now being recorded from the network and the typical one that is stored—notifies an attack.
- Knowledge-based anomaly IDS: Experts define the connection's behavior or add several laws as an expert system to the fuzzy-based system to identify attacks and normal behavior. This system's inputs will be rule-based, and it sometimes uses heuristics or UML to define how assaults behave [6].
- An anomaly IDS based on machine learning : It builds an explicit or implicit model of the observed patterns. According to prior studies, these models need to be updated often to support intrusion detection efficacy.

2.2. Signature-Based Technique

Misuse or knowledge-based detection is a kind that compares the attack's signature to the existing traffic. If a match is discovered, there is a report of an assault; otherwise, there is no attack. This method differs from others in that

it requires continual signature updates and has a low false alarm rate [7].

2.3. Specification-Based Technique

This kind relies on comparing the memorized and predefined specifications with the criteria or specifications to identify a certain program's functioning and alert the user to any criterion violations . This research focuses on anomaly-based NIDS, which is taken into account since it aids in the detection of emerging dangers in IoT. The NIDS examines network traffic and finds fresh and undiscovered assaults. The feature set design is critical for identifying network traffic [8], a persistent research issue.

3. Techniques to Designnids

These techniques give general algorithms to build efficient NIDS based on AI and define the most popular machine learning (ML) and deep learning (DL) algorithms. Both supervised and unsupervised algorithms are essential for classification [9].Supervised algorithms employ user data that is extracted from known and labeled data. Contrarily, unsupervised algorithms draw relevant details and traits from unlabeled input. Some of the most well-known machine learning (ML) applications include K-Nearest Neighbor, the Bayesian approach, decision trees (DT), support vector machines (SVM), and principal component analysis. Examples of DL include recurrent neural networks, long-term RNNs, bi-directional RNNs, gated recurrent units, and generative adversarial networks.

3.1. Machine Learning Techniques(ML)

A subfield of AI called machine learning (ML) allows computers to automatically acquire useful knowledge gleaned from large datasets. Many security issues may be solved by using intelligence approaches with IoT networks and devices. From a security perspective, several current ML/DL approaches using IoT were examined . Big data's difficulties with intrusion detection prompted the development of feature selection with high classification efficiency and lower computing costs [10]. A database of HMM templates and two architectures that can identify and follow the development of assaults in real time were constructed using Hidden Markov Models (HMM), one of the statistical machine learning approaches , and they demonstrated a range of performance. The DT classifier has used the "Cuttlefish algorithm" (CFA) and "Feature grouping based on linear correlation coefficient" (FGLCC) methods. By combining the two techniques, the dimensionality reduction methodology was combined with the "information gain" (IG) method, PCA, and intrusion detection [11].

3.2. Deep Learning Techniques(DL)

A subset of the ML is represented by the multi-hidden layer artificial neural network known as the DL. In several areas, including object identification, language translation, and voice recognition, DL is more effective and accurate than ML. It has a deep structure and the capability to self-learn from the dataset to provide the output depending on key attributes. The DL techniques are used to suggest NIDS remedies after an assessment of recent findings. ML has the capacity to self-learn from data without the requirement for human understanding or programmed directives. Therefore, ML differs from DL in that it can be comprehended from raw data such as text, but DL is given access to additional data, increasing predicted accuracy [12].

Deep learning, which offers the related definitions for IDS, explanations for various IDS kinds, and its applications, is a crucial component of improving IDS performance . The sparse auto-encoder and soft max regression have been used in NIDS to evaluate the efficacy of anomaly detection using the benchmark network intrusion dataset NSL-KDD. SDN demonstrated the ability to construct a strong, secure network while also increasing the possibility of an attack. Emerging security flaws in the IoT architecture's layers have been highlighted by a survey on the subject [13].IDS finds it difficult to deal with enormous data, but deep learning's capacity for handling massive data makes this difficulty more manageable. As opposed to machine learning, deep learning can automatically extract features without the requirement for feature engineering [14].

Therefore, in the most recent study of DL with network anomaly detection , deep learning viability in network traffic analysis has been

shown and also explored. Some IDSs that applied deep learning algorithms for intrusion detection demonstrated their limitations, advantages, and disadvantages . A hybrid model combining RNN and "Restricted Boltzmann Machines" is given (RBM).Without the use of feature engineering, this hybrid approach detects fraudulent traffic by classification [15]. The intrusion detection technique recommended on the basis of CNN carries out complicated features automatically in constantly changing contexts, which is thought to be crucial in detecting network intrusions . Due to the black-box nature of DNNs, which prevents transparency of the DNN-IDS, which is essential for establishing confidence, the DNN-IDS demonstrated better user trust and was more communicative. By training DNN-IDS, the user represented input attributes that are crucial for identifying every kind of incursion [16].

A novel IDS was characterized by the phrase "hierarchical spatial-temporal features-based IDS" (HAST-IDS). HAST-IDS first represented spatial characteristics via low-level network traffic that was learnt using deep CNNs, and subsequently, high-level temporal features were learned using LSTM . The accuracy and precision of three models—a "vanilla deep neural net" (DNN), a "Self-Taught Learning" (STL) method, and an RNN-based LSTM—are compared . Many deep learning algorithms have been employed for IDS. Using "Bi-directional LSTMRNN" (BLSTMRNN), a novel deep learning system presented a design inside the youth network for identifying attacks [17].

The design of "Particle Swarm Optimisation" (PSO) employing learning factors and adaptive inertia weight is part of the structure of DBN's network optimized by offering a new structure. Then, the PSO is developed by using fish swarm behavior . The suggested system made use of the Deep Learning approach, which improved the accuracy with which assaults were identified and decreased the number of irrelevant characteristics [18]. It has been suggested that Scale-Hybrid-IDS-Alert Net (SHIA) is a hybrid DNN framework that successfully monitors host-level events and network traffic in real time. This SHIA is on the lookout for potential cyber-attacks . Multiple auto encoders have been incorporated with convolutional and RNNs in a unique AE-based deep neural network architecture that elicits associated knowledge of the anticipated relationships between the key characteristics (spatial-features) and their timely development (temporal-features) [19]. In order to get consistent traffic characteristics and identify the browser using nonlinear multiclass classification methods, DeepCNN has proposed a novel system .

The challenges posed by many traffic tunnels are addressed by a source identification method that uses DL [20] to identify the several video sources in a single encrypted channel. The proposed method is based on a picture that classifies encrypted network data with high accuracy. It initially transforms the session's first few non-zero payload sizes into gray scale images before performing the desired classification of encrypted network data. It then classifies the transformed grayscale pictures using CNNs. The DL category utilized for attack detection is shown in Figure (3).

3.3. OTHER(NIDS)TECHNIQUES

Swarm intelligence, genetic algorithms, data mining, and other techniques are used to build NIDS. This section discusses the research on these subjects. Effective approaches are applied to swiftly discover and classify data flows. Effective approaches include data mining and swarm intelligence. After authentication and encryption, the networks for the Internet of Things have been protected. Their cyber security defenses, however, are still poor. As a result, anomaly-based detection methods are used to reduce the likelihood of various attack types . The Bayesian networks (BN) and C4.5 were used to classify attacks by the classifier in the feature selection technique, which made use of the firefly algorithm [21].

The "Deep Belief Network"-based intrusion detection model, which was enhanced by a genetic algorithm over numerous rounds of the GA, was subject to several sorts of assaults. The proposed technique combined the fuzzy aggregation approach with the DBNs, and the training set was separated into varied subsets

to minimize sample size and unbalanced samples using the modified density peak clustering algorithm (MDPCA) . The hybrid approach utilizes AdaBoost for IDS anomaly screening. ABC algorithms offer a high detection rate (DR) and a low false positive rate (FPR) [22].

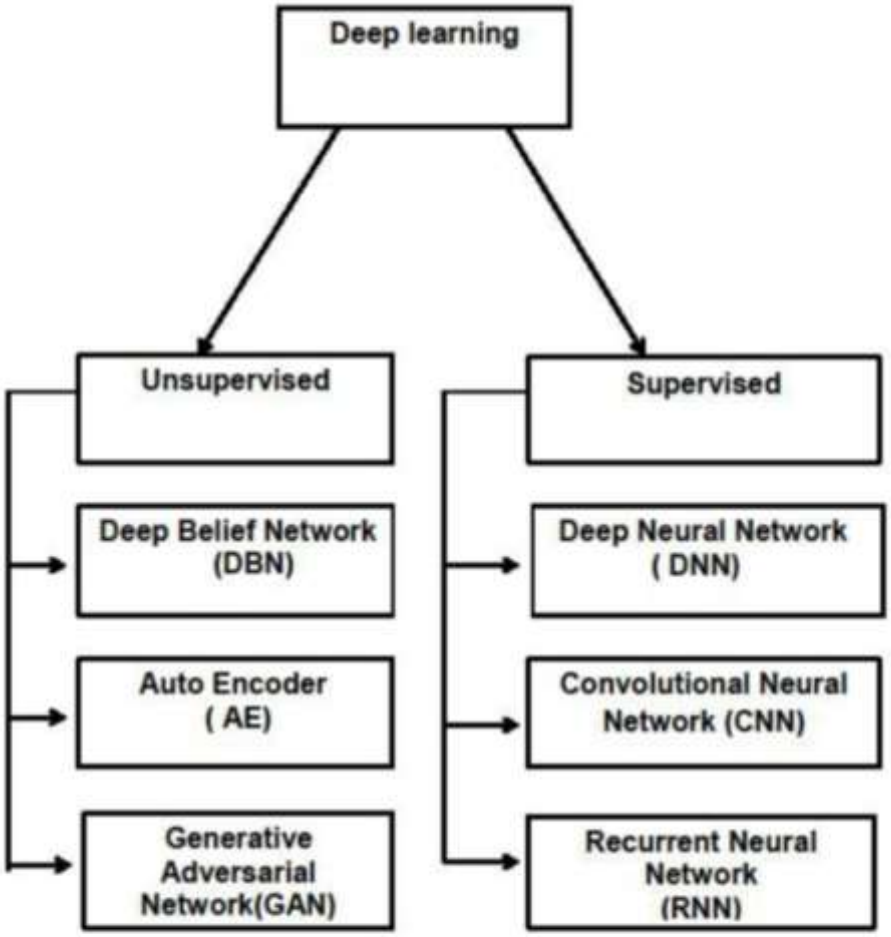

Figure 3. General clsssification of deep learning

4. IDS AND IOT

Research on IoT for IDS is given in this section. Furthermore, a distributed attack detection paradigm for the Internet of Things is offered . IDSs recommend utilizing AdaBoost-based algorithms as a learning strategy to identify odd activities. These IDSs were used in specialized botnet attacks that targeted the "Domain Name System" (DNS), the "Hypertext Transfer Protocol" (HTTP), and the "Message Queue Telemetry Transport" (MQTT) [23].The "Hybrid IDS" (HIDS) group uses both an SVM classifier with One-Class and A C5 may be used as a classifier to identify well-known invasions. A comprehensive analysis revealed that in order to create a successful intrusion detection system for the IoT, accuracy and performance overheads must be compromised [24].

The recommended method makes use of DL to identify IoT botnets effectively. Using network-based approaches and deep packet inspection techniques, the aberrant activity was detected as botnet attacks on network traffic . The model of specification-based IoT intrusion

detection suggests defending against previously unknown threats and attacks with a higher degree of detection accuracy [25]. This has produced defenses against these dangers and assaults as well as effective performance (low memory and communication overhead). Using block chain technology, a novel solution to IoT intrusion detection is proposed. Local agents and a central component that organizes the information (alerts) gleaned from these agents make up the technique [26]. In IoT networks, a deep learning-based method has been used to identify physical layer attacks. The emphasis of this study is primarily on attacks in which the attacker tries to include the victim's IoT device in the radio frequency (RF) transmission . An analytic study for IDSs depends on three factors: computation cost, privacy, and energy consumption [27].

It is advised to create a new IDS that uses machine learning techniques to find abnormalities in IoT. Using the platform-provided "security as a service" for detection has been employed in the IoT to simplify the cooperation across protocols . Deachlayer presented and examined risk analysis related to security threats. IoT protocols' practical methods and their restrictions are listed . By using a machine learning technique for intrusion detection, the new model has employed PCA to decrease the dimensions from a large number of features to a small number in the dataset [28]. This paper explains why the KDD99 and NSLKDD data sets do not provide findings that are acceptable due to three key problems: they lost the contemporary attack patterns; they lost the modern scenarios of traffic streams; and they lost the dispersed sets of training. and testing are challenging. To solve these concerns, the newly created UNSW-NB15 dataset was used . The "variantGRU" automatically learns packet payloads using network header characteristics. For in-network intrusion detection, new approaches called "E-GRU" and "E-BinGRU" have never before been used [29]. The typical IDS for an IoT context is shown in Figure (4).

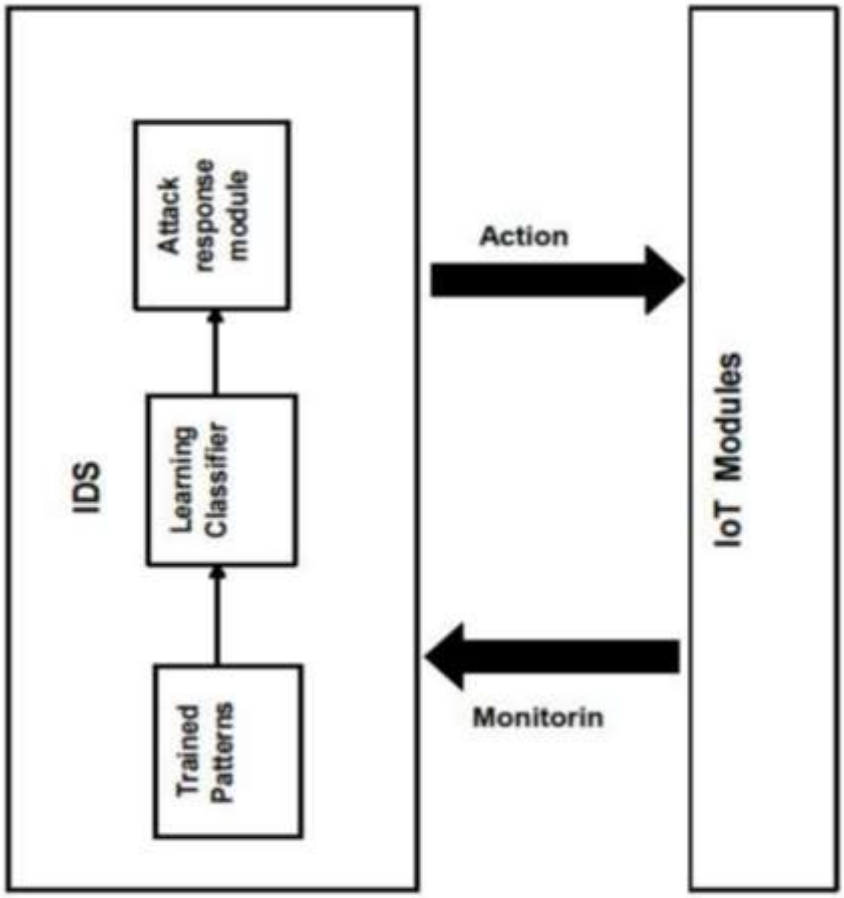

Figure 4 . An IOT environment's typical intrusion detection system

5. Nidsoniotusing Deep Learning

The use of Dl It has become increasingly useful due to advancements in neural network methods. Due to its capacity to extract information at a high level, deep learning is thought to be the most adaptable in identifying new assaults. The tests show that distributed attack detection systems utilizing deep learning are superior to centralized attack detection systems . This work has shown a few smart city issues based on house automation systems and using UCI data sets from temperature sensors and pictures of individual walkways [30]. In order to demonstrate the notion and the new detection framework's scalability, simulation is used. The detection options promote interoperability amongst IoT protocols and are offered as a service . The suggested solution was developed by using AI to identify botnet assaults that are brought on by growing threats. In the "Amazon Web Services" (AWS) environment, the Canadian "Institute for Cyber Security" (CIC) produced the real-time IDS dataset (CSE-CIC-IDS2018) in 2018 . An attack-detection system is demonstrated by using BLSTMRNN as deep learning technology inside the network. The lightweight distributed security solution has shown the ability to design IoT architectures, analyze ML and DL methods for IoT and cyber security, and assess networks (LSTM and GRU) for each layer in the IDS dataset's architecture [31].

6. Public Datasets

The database type used for information extraction is essential since it supports the detection model's functionality. A variety of cyber security datasets are used for intrusion detection, which can be divided into seven main categories with their respective subtypes as follows:

"Network traffic-based," "electrical network-based," "internet traffic-based," "virtual private network-based," "android apps-based," "IoT traffic-based," and "internet-connected devices-based" are all terms used to describe

how data is collected from networks. The CSE-CIC-IDS 2018 dataset and the Bot-IoT dataset, two new real-time traffic datasets, will be the main subjects of this study.

6.1. Network Traffic - Based dataset(CSE-CIC-IDS2018 DATASET)

The CICIDS2018 dataset was created jointly by the Institute for Cyber Security (CIC) and the Communications Security Establishment (CSE) [32].CICIDS2018 addresses seven types of attacks: brute force, infiltration, web attacks, DoS, DDoS, and botnets. These attacks are applied against a large number of forward and reverse-calculated protocols and network topologies. The CIC Flow Meter is a tool that adds 80 characteristics to the CICDS 2017 dataset by gathering them from the network's generated traffic. This dataset comes in PCAP and CSV formats. AI first uses the PCAP format rather than the CSV format for describing new features [33].

6.2. Iot Traffic - Based Dataset (BOT-IOT DATASET)

The database depicts the typical IoT network traffic together with different types of assaults. The Bot-IoT database contains information on attacks against the IoT environment, including key logging, OS and service scanning, DDoS, DoS, and data exfiltration. Koroniotis et al. [34] offered the Bot-IoT as a new dataset to allow comparison of IoT settings with older datasets.

7. Conclusion

The IoT confronts several difficulties and security risks, and there are ongoing, novel, and diverse assaults that have a detrimental impact on smart systems and the delivery of associated services. As a result, it is necessary to implement a system to identify network intrusions and assaults. Deep learning is more effective than machine learning because it can handle large amounts of data, identify new incursions, enable the capacity to self-learn, and recognize zero-day assaults. The most current research on detecting models and integrating models to assist in intrusion detection and datasets is highlighted in this review. The models promote the adoption of new datasets since they support the efficient functioning of the detection model. Examples of these new datasets are the Bot-IoT dataset and the CSECIC-IDS2018.

8. Acknowledgements

The authors would like to thank the Ministry of Education/Directorate of Anbar Education, Preparation and Training Department, their facilities, which helped improve the quality of this work.

References

1. A. Ahmim, M. Derdour, and M. A. Ferrag, “An intrusion detection system based on combining probability predictions of a tree of classifiers,” Int. J. Commun. Syst, vol. 31, no. 9, pp. 3547–3547, 2018.
2. B. Stewart, L. Rosa, L. A. Maglaras, T. J. Cruz, M. A. Ferrag, and P. Simões, “A novel intrusion detection mechanism for scada systems which automatically adapts to network topology changes,” EAI Endorsed Trans. Ind. Netw. Intell. Syst, no. 10, pp. 4–4, 2017.
3. Akashshukla and A. Himanshosharma, “Future of Internet of Things: Trends, Challenges & Insight To Artificial Intelligence,” International Journal of Advanced Research in Computer, vol. 9, no. 2, 2018.
4. M. H. Prasantagogoi and Bhuyan, 2012.
5. H. Liao, C. R. Lin, Y. Lin, and K. Tung, “Journal of Network andComputer Applications Intrusion detection system,” J. Netw. Comput, vol. 36, pp. 16–24, 2013.
6. M. Petkovic, I. Basicevic, D. Kukolj, and M. Popovic, “Evaluation of takagi-sugeno-kang fuzzy method in entropy-based detection of DDoS attacks,” Comput. Sci. Inf. Syst, vol. 15, pp. 139–162, 2018.
7. A. H. Hamamoto, L. F. Carvalho, L. H. Sampaio, T. Abrão, and M. L. Proença, “Network anomaly detection system using genetic algorithm and fuzzy logic,” Expert Syst. Appl, vol. 92, pp. 390–402, 2018. 8.Shawqm,Mehibs,H.Soukaena,andHashim,“ ProposedNetworkIntrusionDetectionSyste mInCloudEnvironmentBasedonBackPropag ation Neural Network,” Journal of Babylon university/Pure and Applied Sciences, vol. 26, no. 1, 2018.

8. M. W. Berry, M. A. Yap, and B. W, Supervised and Unsupervised Learning for Data Science. New York, NY: Springer, 2019.
9. T. M. Richardzuech and Khoshgoftaar, "A survey on feature selection for intrusion detection," in 21st ISSAT International Conference on Reliability and Quality in Design, 2015.
10. A. Fadisalo, A. Bounassif, and Essex, "Dimensionality Reduction with IG-PCA and Ensemble Classifier for Network Intrusion Detection," Computer Networks, 2018.
11. F. Gottwalt, E. Chang, T. Dillon, and Corrcorr, "A Feature Selection Method for Multivariate Correlation Network Anomaly Detection Techniques," Computers&security.
12. M. F. Elrawy, A. I. Awad, F. A. Hesham, and Hame, "Intrusion detection systems for IoT-based smart environments: a survey," Journal of Cloud Computing :Advances, Systems and Applications, 2018.
13. K. Kim and Muhamaderzaaminanto, 2017.
14. C. Li1, J. Wang1, and X. Ye1, "Using a Recurrent Neural Network and Restricted Boltzmann Machines for Malicious Traffic Detection," NeuroQuantology, vol. 16, no. 5, pp. 823–831, 2018.
15. M. Kasunamarasinghe and Manic, 2018.
16. D. H. B. Roy and Cheung, "A Deep Learning Approach for Intrusion Detection in Internet of Things using Bi-Directional Long Short-Term Memory Recurrent Neural Network," 28th international Telecommunication Network Communication Conference (ITANC), 2018.
17. V. Kanimozhi and P. Jacob, "UNSW-NB15 Dataset Feature Selection and Network Intrusion Detection using Deep Learning," International Journal of Recent Technology and Engineering (IJRTE), vol. 7, no. 5S2, 2019.
    19.D.G.PalmieriandF,"Networktrafficclassificationusingdeepconvolutionalrecurrentautoencoderneuralnetworksforspatial-temporalfeatures extraction," Journal of Network and Computer Applications, pp. 102890–102890, 2021.
18. Y. Shi, D. Feng, and Y. Cheng, "A natural language-inspired multilabel video streaming source identification method based on deep neural networks," Signal Image and Video Processing, pp. 1–8, 2021.
19. Selvakumarb and K. Muneeswaran, "Firefly algorithm based Feature Selection for Network Intrusion Detection," Computers & Security, 2018.
20. Mazinim, Shirazib, and I. Mahdavi, "Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoostalgorithms," Journal of King Saud University - Computer and Information Sciences, 2018.
21. N. Moustafa, B. Turnbull, and K. R. Choo, "An Ensemble Intrusion Detection Technique Based on Proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things," IEEE Internet of Things Journal, vol. 6, pp. 4815–4830, 2019.
22. J.Arshad,M.A.Azad,andR.Amad,"KhaledSalah, MamounAlazabandRaziIqbal"AReviewofPerformance,EnergyandPrivacyofIntrusion Detection Systems for IoT," Electronics, vol. 2020, pp. 9040629–9040629.
23. V. Sharma, I. You, K. Yim, I. Chen, and J. Cho, "BRIoT: Behavior Rule Specification-Based Misbehavior Detection for IoT-Embedded CyberPhysical Systems," IEEE, vol. 7, pp. 118556–118580, 2019.
24. 26. D. Li, L. Deng, M. Lee, and H. Wang, "IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning," Int. J. Inf. Manag, vol. 49, pp. 533–545, 2019.
25. M. A. Junaidarshad, K. Azad, W. Salah, Jie, and M. Raziiqbal, 2018.
26. S. Zhao, W. Li, T. Zia, and A. Y, "A Dimension Reduction Model and Classifier for Anomaly-Based Intrusion Detection in Internet of Things," IEEE. 15th Intl Conf on Dependable, Autonomic and Secure Computing, 2017. Y. Yiranhao and J. Sheng, 2019.
27. N. Rakesh, "Performance analysis of anomaly detection of different IoT datasets using cloud micro services," International Conference on Inventive Computation Technologies (ICICT), pp. 1–5, 2016.
28. M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber

security intrusion detection: approaches, datasets, and comparative study," Journal of Information Security and Applications, vol. 50, pp. 102419–102419, 2020. C.-C.-I. Dataset, 2019.

29. N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the internet of things for network forensic ana- lytics: Bot-IoT dataset," Fut. Gener. Comput. Syst, vol. 100, pp. 779–96, 2019. [34] Bot-Iot and Dataset, 2019.