A Comprehensive Survey to Prediction of Botnet Attacks and Prevent Attacks using Integration Framework of Deep Learning, Blockchain Technology

Bhagyalaxmi B S[1], Ashwini M S[2], Yashodha H R[3]

[1]Senior Scale Lecturer, Department of Computer Science & Engineering, Government Polytechnic for Women,Ramanagara
[2]Senior Scale Lecturer, Department of Computer Science & Engineering, Government Polytechnic, Channapatna
[3]Lecturer, Department of Computer Science & Engineering, Government Residential Women's Polytechnic, Shivamogga

Abstract

Many devices which are connected digitally (IoT) has become part of our daily use in modern life, revolutionizing areas such as smart homes, healthcare, organizations, agricultural areas and transportation. However, the rapid expansion of connected devices has significantly increased the hazard of malicious bot activities, bullying the safety of IoT networks. To address these challenges, researchers have explored the use of Intelligent Machine learning (ML) and Deep Neural network learning (DL) methods for detecting and mitigating botnets, alongside Blockchain technology for enhancing data integrity and securing decentralized communication. This organized review explores the integration of ML, DL, and Blockchain technologies in IoT botnet detection, focusing on target datasets, performance metrics, and datasets preprocessing strategies. By analyzing primary research published between 2018 and 2023, the analysis highlights the few issues of existing approaches, identifies key advancements, and outlines research areas for developing robust, scalable, and secure frameworks for IoT botnet detection and prevention.

Keywords: IoT, Machine Learning, Deep Learning, Blockchain, Metrics

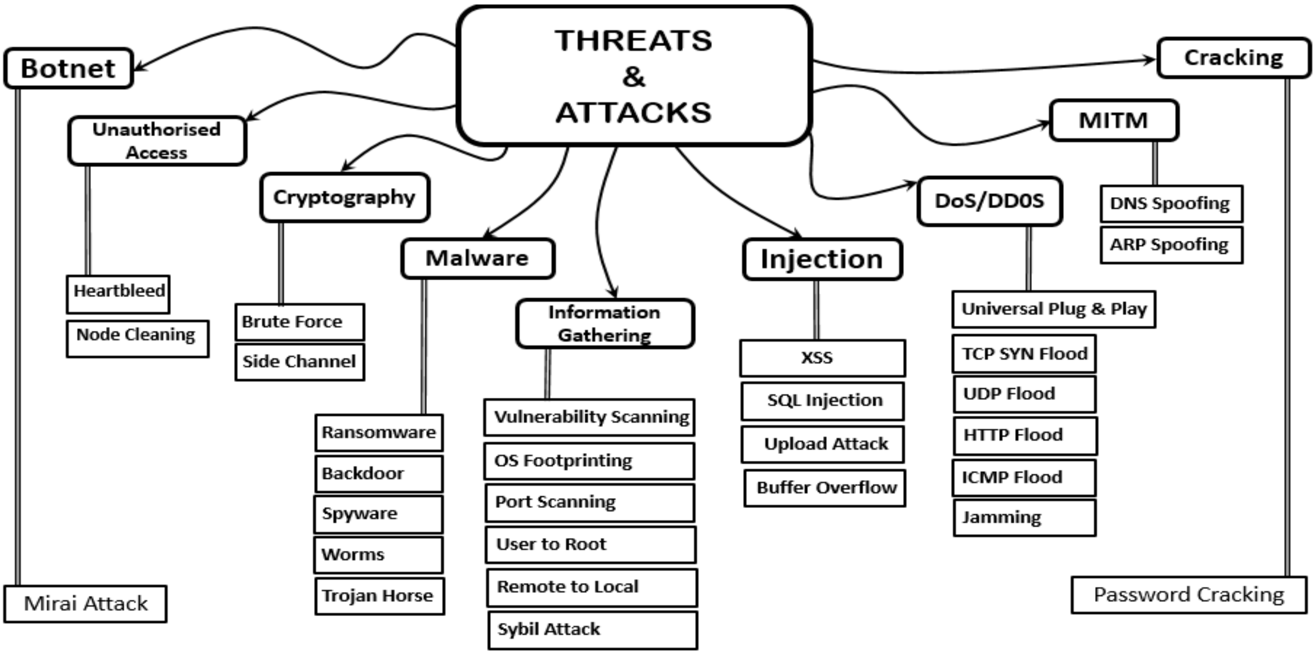
1. Introduction

The Internet, which was first developed as a means of digital interacting and exchanging information, has drastically changed the world. Significant interconnections between countries have been cultivated as a result of high speed internet connection in vital domains like governance, economics, defence, trade, and intercultural contacts. Interconnected networks, devices, and users are the fundamental elements of the Internet [1]. Internet technologies have been continuously evolving due to advancements in computer technologies and the evolving capabilities of various user groups. However, significant security issues have been brought about by the growth in the past few years and broad use of these technologies. In order to protect people's and organizations' digital information, a lot of research has been done to create strong cybersecurity infrastructures [2].

Cybercriminals remotely manipulate networks of compromised devices, or "botnets [3] , also known as the "botmasters" or "bot herder." With the help of specialized software, the attacker can control these infiltrated devices which could include personal computer systems, servers and or IoT’s devices without owner's knowledge or approval. Once the malware has been installed, the device is changed into a "bot" or "zombie," which joins the botnet, a wider network of linked devices. Malicious operations including Distributed Denial of Service (DDoS) assaults, email spamming, stealing information, mining bitcoins, and spreading more ransomware are all frequent uses of such network of bots. These Internet of Things gadgets, which frequently have default login information and lower security protections can be subject to the attacks. In our daily lives the use of smart devices have become common use [4], which are more targeted to security attacks. In today's world, networking and cybersecurity are essential for quick communication across the global and very easy to approach the confidential data stored in the devices through cloud based services [5]. Global connections are facilitated by platforms like, e-mail, digital via communication, and E-communication tools, though cybersecurity safeguards like security gateways, anti-malware software, and multifactor verification guard compared to identity theft, cyberattacks and Phishing mails. Many organizations such as healthcare industry, where protecting patient privacy and safeguarding medical information are critical [6], the precautions of safeguarding are especially important. Similar to this, the economic service sector mostly depend on high performance security measures to protect sensitive client data and transactions.

Cyberattacks are increasingly targeting IoT devices, frequently without the owners' knowledge. It is possible to breach these devices and add them to a "botnet," which is a collection of hacked machines. The increasing use of IoT device vulnerabilities to support botnet operations, especially their crucial role in planning Distributed Denial of Service assaults, is highlighted in the CUJO AI [2022–2023] IoT Botnet Report [7]. In order to improve the connected devices security towards such cyber hazards, this trend emphasizes the urgent necessity to put strong cybersecurity frameworks and cutting-edge threat mitigation techniques into place. Figure 1.1 illustrates the different attacks and threats in various areas.

Figure 1.1 Various Attacks and Threats [8]



The formation of trustworthy botnets prediction algorithms and architecture is essential to assure the protection and secrecy of IoT Inter-networks, systems, and also users confidential information. The total number of devices connected is increasing at an e rate due to the increasing in amalgamation and prevalence of IoT skills, due to which there will be increase in cybercriminals attacks and takes advantage of their weaknesses [9]. IoT networks are predominantly susceptible to bot-nets, which have the capability to cause serious harm like Long-term disruptions to services, substantial revenue losses, and private data breaches [10]. Additionally, these networks can steal sensitive and private information from hacked connected Internet of devices, leading to identity theft, fraud, and spying. [11]. In IoT networks, Intelligent Machine Learning (ML), Deep Neural Network learning (DL) and BlockChain techniques [12,13] have proven to be real and efficient tools for predicting, analysing and undetectable attacks powered by botnets.

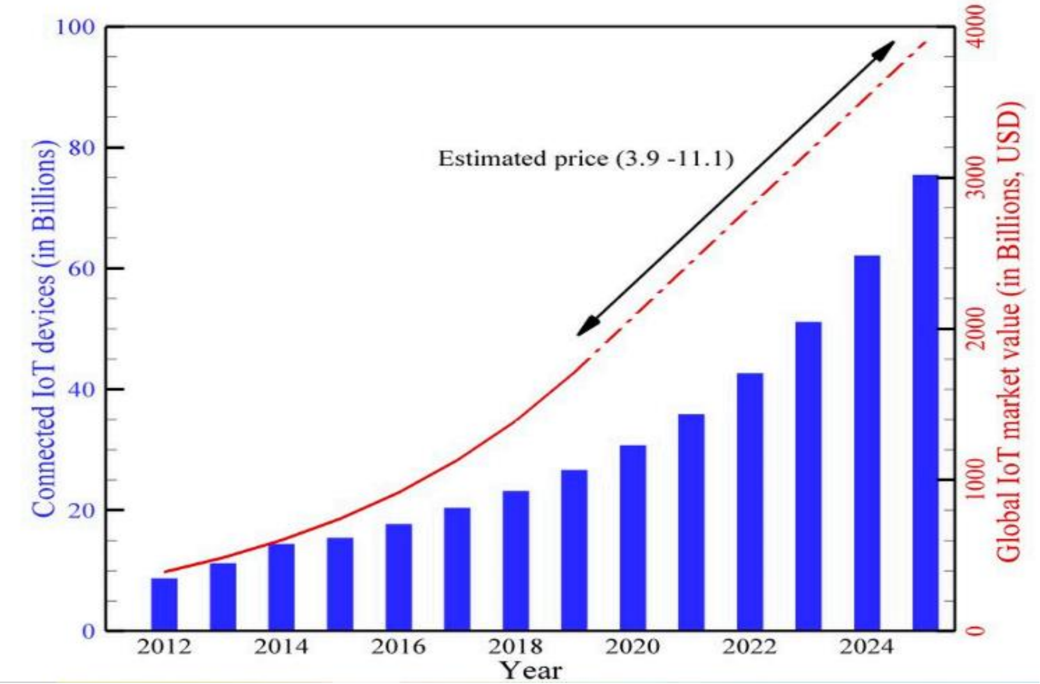
1.1 Importance of Intelligent Machine Learning, Deep Neural Networks and BlockChain Technologies

Enormous installation and deployment of interconnected digital devices across various domains have made the security level challenging. The traditional measures to detect the various attack in the digital communications where various devices are connected has its own drawbacks [14]. The drawbacks of traditional approaches can be over by using advanced technologies like Intelligent Machine Learning, Deep Neural Network and BlockChain, to predict and analyze the different digital communication attacks. IoT security has been demonstrated to be significantly improved by machine learning (ML) methods. Machine Learning frameworks can find attributes, abnormalities, and possible security coercions by analyzing the massive volumes of data produced by IoT devices. To detect intrusions, categorize malicious activity, and predict security events in IoT environments, methods like RF, decision trees, BI-LSTM, Convolution neural network, and GAN have been discussed for security measures [15]. Proactive threat identification, real-time surveillance, and flexible defence tactics are made possible by integrating machine learning algorithms into Internet of Things security systems [16]. There are chances to improve quality of life and tackle the aforementioned difficulties by utilizing IoT intelligent services. In order to improve cybersecurity, Intelligent machine learning (ML) and deep neural learning (DL) algorithms are essential since they tackle issues including malware categorization, spam prevention, and intrusion detection [17]. For detecting flaws in IT devices where confidential data are stored, methods like random forests, support vector machines (SVM) , naive Bayes, decision trees, and deep belief networks have been extensively researched . In order to detect anomalous behaviour in network traffic, models that combine multi-layer SVMs with deep feature extraction have been employed. Large-scale datasets such as NSL-KDD have been subjected to intrusion detection using deep belief networks [18], whereas recurrent neural networks (RNNs) improve detection accuracy in spite of processing difficulties [19].

Blockchain technologies are useful for tackling security threats and privacy issues while providing excellent services because of features like transparency, decentralization, trustlessness, and immutability. Future sustainable smart cities are expected to be greatly aided by IoT, which is expected to be a major driver of Internet-based and service-oriented computing in both existing (4G/5G) and emerging (6G) wireless networks. Blockchain technology enhances IoT systems' security, transparency, and immutability by functioning as a decentralized ledger that safely logs confirmed security events. This solution enables professional analysis and feedback by guaranteeing an unalterable and visible record of security occurrences within the IoT ecosystem. Research done from 2016 to 2022 looked into Blockchain’s potential for cybersecurity in addition to its original application in cryptocurrencies like Ethereum and

Bitcoin. Applications included lowering cybercrime and building safe networks for communication and information exchange [20]. Blockchain technology increases reliability by making tampering highly computational because each block has a unique hash linked to the one before it [21]. Because every block in a blockchain has a unique hash linked to the one before it, tampering is more difficult to do, which makes the system more reliable. To reduce FDIA in smart grids, researchers proposed models that combine blockchain with smart contracts and layered architectures to ensure safe data flow, transaction validation, and fraud detection [21]. Strong cybersecurity frameworks were made possible by these models, which made use of Blockchain's features to establish decentralized security mechanisms, facilitate safe data sharing, and enhance peer-to-peer performance on networks. The botnet attacks projected until 2024 are depicted in Figure 1.2.

Figure 1.2 Valuation of the Botnet Attacks till 2024



The following sections of the study in structured as: the review of the literature of the work done on the importance of technologies in the prediction of cyber security in section II, some of the research related works in the field of cyber security in section III, Issues related to the state of work done is given, in the section IV gives performance metrics to measure the attacks efficiently, section with section V the conclusion and with the references.

2. Review of the Literature works

The increasing risks triggered by bots, the requirement for efficient prediction systems, and the promise of BlockChain technologies to improve safety in IoT ecosystems are the driving forces behind this review paper. The hazards and vulnerabilities of widespread botnet attacks are becoming more noticeable as IoT networks grow. While deep neural network learning (DL) and Intelligent Machine Learning (ML) approaches have shown great potential in addressing these issues, blockchain technology enhances detection frameworks with decentralized security, transparency, and immutability. To comprehend cutting-edge ML/DL and blockchain-based techniques, assess their efficacy, pinpoint their drawbacks, and investigate potential future research avenues, a thorough evaluation of the body of existing literature is important. In order to support the creation of reliable and effective IoT botnet detection solutions, this work aims to give researchers, practitioners, and policymakers a thorough understanding of these technologies.

This study [22] successfully addressed the difficulties in detecting unseen botnets that can avoid conventional Rule-Based techniques by introducing a multi-layered machine learning perceptron framework for botnet identification. By combining behaviour-based analysis with flow-based features in its filtering and classification modules, the framework makes it possible to study packet headers even in enclosed situations, such as VPN tunnels. With a high F1 measure of 92% and a decrease False-Negative rate with 1.5%, the suggested method demonstrated the effectiveness of Intelligent Learning systems in botnets prediction and emphasized the significance of behaviour examination in identifying contemporary botnet attacks.

A deep learning-based intrusion detection (ID) framework for Industrial IoT (IIoT) was presented by the authors [20]. Data from TCP/IP packets is processed and verified by the framework using a hybrid rule-based feature selection technique. In addition to the feature selection method, a deep feedforward neural network was employed for training. With a false positive rate (FPR) of 1.0% for the NSL-KDD dataset and an accuracy and detection rate of 99.0%, performance assessments outperformed alternative approaches. Based on the UNSW-NB15 dataset, the framework obtained a 98.9% accuracy rate, a 99.9% detection rate, and a 1.1% FPR. Similarly, using the Aegean AWID dataset, which was generated from a SOHO 802.11 wireless network, researchers in [24] suggested intrusion detection systems (IDS) for wireless networks. Using a variety of devices, including PCs, workstations, tablets, smartphones, and smart TVs, the dataset was gathered with an emphasis on the Media Access Control layer. Nevertheless, the dataset is limited in its applicability to IoT-specific applications because it excludes data from IoT devices.

Khacha et al. [25] proposed an innovative intrusion detection system (IDS) utilizing deep learning methodologies. Specifically, the system integrates Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) algorithms for detecting and categorizing intrusions. In this research, a contemporary dataset known as Edge-IIoT, comprising real network traffic data from Industrial IoT (IIoT) and IoT applications, was employed for evaluation.

Alabsi et al. [16] presented a method for identifying IoT network assaults by combining two Convolutional Neural Networks (CNNs). Important features that point to IoT assaults are extracted from raw network traffic data using the original CNN technique. These collected properties are used by the second CNN to develop a trustworthy detection system that can precisely identify IoT assaults. The researchers presented a novel deep learning-based intrusion detection system (DL-IDS) [17]. This method makes use of the Stacked-Deep Polynomial Network (SDPN) and the Spider Monkey Optimizer (SMO) technology. While the SDPN technique classifies the data as either normal or abnormal, the SMO chooses the most pertinent features from the datasets.

The researchers presented ForChaos, a lightweight detection technique made especially for Internet of Things devices, in [26]. This method detects floods and Distributed Denial of Service (DDoS) assaults by using chaotic perception and predictive techniques. The algorithm's ability to effectively analyze abnormal patterns in network data through the integration of chaotic perception gives it the ability to detect anomalies in real time with little computing overhead, which makes it ideal for IoT contexts with limited resources.

The authors of [27] put out a unique strategy based on the Reversible Sketch (CRT-RS) method in conjunction with the Chinese Remainder Theorem (CRT). This novel architecture improves the system's capacity to detect unusual keys linked to criminal activity or undesired network traffic sources in addition to compressing and combining massive amounts of network traffic. Utilizing the CRT-RS technique, the solution solves the scalability issues commonly encountered in high-volume network systems by guaranteeing effective traffic processing and anomaly detection.

In order to secure IoT device authentication and preserve data integrity in a decentralized [28] setting presented a blockchain-based system. Utilizing Blockchain's built-in features, their strategy aims to provide a reliable and impenetrable system for confirming device IDs and maintaining data accuracy across dispersed IoT networks. Blockchain technology was also used in a study [29] to create an immutable IoT data record which ensures the transparent and trustworthy data communications. By guaranteeing that every interaction with data generated by the Internet of Things can be monitored and verified, this method improves confidence in data transfers. Nevertheless, the scope of collective hazard intellect in IoT safety is not completely explored in either study, which focuses primarily on data integrity and device authentication.

Shi et al. [30] in their study explores a BlockChain frameworks aimed at facilitating Encrypted and auditable data communication across IoT devices. Their research underscored the significance of decentralized decision-making protocols and secure, tamper-proof data retention as foundational components for building trust and improving the dependability of IoT ecosystems. The framework primarily targeted by preserving the data privacy and data integrity when the exchange of information within interconnected Internet of Devices.

Table 1.1: State-of-art on various Botnet attacks

Year/ref	Survey	Vector of Attack
2023 [33]	Mirai botnet scans over six years by examining the Mirai signature (TCP.seq == IP.dst) in the TCP packets of the MAWI datasets traces.	Mirai botnet targeted on Telnet port 23
2022 [34]	Discuss on Current trends and challenges on botnet attacks such as DDoS, malware, Ransomware, phishing. Also survey on large number of articles to detect, prevent the botnet attacks in various fields IoT Botnet, Mobile botnet, VANET botnets	Browsers, extensions, smartphones and online clipboards, IoT devices, Blockchain structures, Automobiles. Author explores the promising technique to avoid various botnet attack such as Quantum computing to combat Mirai, SMTP analysis, ML, DL , mitigation based attacks
2021 [35]	Artificial Intelligence-based solutions show more promising in detection of various botnet attacks. Apart from this an Integrating machine learning with blockchain and SDN, Deep Learning are explored in detection and prevention of botnets .	IoT botnet detection techniques, botnet phases, and various malicious activity scenarios are all explored

2021 [36]	This study works on the how the data sets play a crucial role in the various networks attacks and emphasising how such datasets improves the training rate of Intelligent Machine Learning-based algorithms.	In this article, two major solutions found in the literature for preventing IPS, DDoS attacks are Intrusion Detection (IDS) attacks.

El Bekkali et al. [31] explores a BlockChain-powered framework specifically designed for IoT devices, focusing on authenticating and securing the important information. Their approach tackled critical challenges such as scalability and interoperability, which are frequently encountered in large-scale IoT environments. The proposed architecture offered an efficient method for authenticating devices and tracing the origin and lifecycle of data, thereby reinforcing the security and dependability of IoT deployments.

Threatening internet security, botnets under the control of bot-herders enable a variety of cyberattacks, including spam, phishing, and DDoS. Large, balanced datasets are necessary for the detection and mitigation of these assaults, but machine learning (ML) and deep learning (DL) are essential. DL methods can improve detection and address class imbalance. Data transmissions are made more secure by blockchain technology, which offers a decentralized, tamper-resistant record. Because it is distributed, it is reliable because it would take more than 50% of the network for an attacker to change the blockchain, and cryptographic safeguards guard against fraud and manipulation.

Table 1.2: The state-of-art on various techniques applied in prediction of Botnet attacks

Article	**Technologies Discussed**	**Data Set used and the prediction**	**Limitations**
2024 [37]	Ensemble network-based Intrusion Detection System (NIDS)	The dataset N-BaIoT is applied to evaluate the suggested IDS model, containing Mirai and BASHLITE botnet malware targeting 9 various types IoT device .	The proposed model faces challenges with imbalanced data, a restricted range of botnet attack types, uncertain applicability across varied IoT environments, and susceptibility to device-specific vulnerabilities.
2024 [38]	Convolutional Neural Network -Pelican Optimization System	The Bot-IoT of 43 network traffic variables and 3 label categories for 11-class classification are included. Experiments demonstrated that the CNN-POA model formed with high efficiency compared to several metaheuristic algorithms, achieving 99.5% accuracy.	Future work includes simplifying the algorithm to reduce computational complexity and analyzing network attack datasets to identify key features for addressing heterogeneous platform issues.

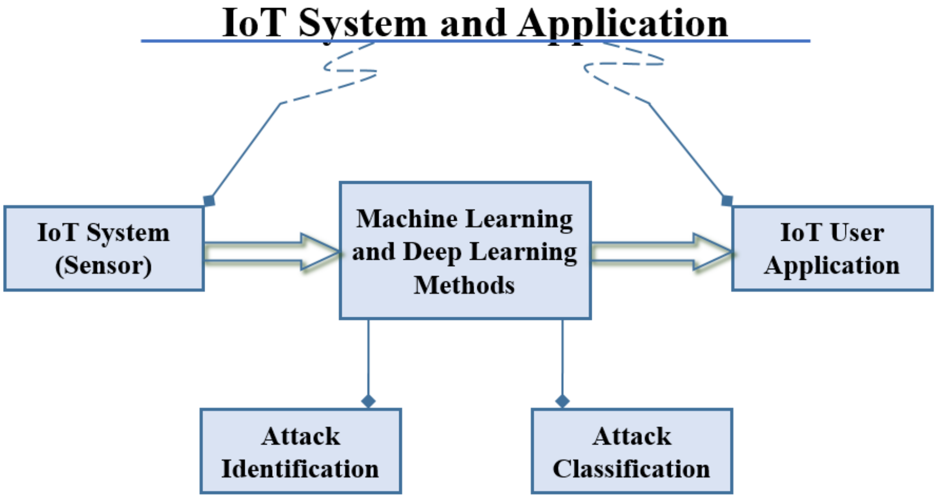
2023 [39]	Intelligent Machine Learning and Deep neural Network Learning algorithms	NSL-KDD, KDD-CUP'99	DL techniques, though superior for large data in DDoS detection, face challenges with evolving IDS defences and limited IPv6 application, necessitating a new detection model.

3. The Issues with Review Discussed in the Previous Sections is Shown Below

The analysis surveys and state-of-art of the existing works shown in the table 1.1 and 1.2. few issues are addressed below with the general architecture for the prediction of botnet attacks which is shown in the figure 1.3.

- Botnets are constantly changing, so there is a need to develop deep learning models that can adapt to new botnet types and attacks. These models should be robust against adversarial attacks and able to generalize well to new, unseen data.
- Imbalanced data is a challenge, and solutions are needed to create additional samples for the less-represented classes, ensuring the model can learn and predict rare botnet attack patterns accurately.
- Traditional methods struggle with issues like packet loss, low energy efficiency, long computation times, and difficulty in improving detection accuracy. Therefore, hybrid models are necessary to enhance botnet attack detection accuracy.
- Emerging technologies like Blockchain, combined with machine learning and deep learning, can help address specific classification challenges. The selected model should process large amounts of data effectively, with carefully adjusted hyperparameters to optimize performance and avoid underfitting.

Figure 1.3 General Architecture for Botnet Predictions using Various Technologies



3.1 Performance Metrics in Prediction of botnet attacks [32]

The metrics used to assess intrusion detection (ID) systems' performance are described in this section. Metrics like accuracy and false alarm rate are used to assess how well four machine learning models identify botnet attacks. In this case, true positives (TP) denote situations in which the classifier accurately detects an assault. When an attack is wrongly categorized as normal, it is known as a false negative (FN).

A false positive (FP) happens when a harmless event is mistakenly classified as an assault by the classifier. Cases where the classifier correctly identifies a typical occurrence are represented by true negatives (TN). A number of additional evaluation criteria are also used by researchers, including as recall, accuracy, precision, false alarm rate, and true negative rate. The false alarm rate (FAR) is defined as the ratio of samples erroneously classified as attacks to all other samples and is calculated as shown in equation 1.

$$\mathrm{FAR} = \frac{\mathrm{FP}}{(\mathrm{TN}+\mathrm{FP})} \qquad (1)$$

Accuracy, on the other hand computes the ratio of correct results to the total number of predictions of input samples and is determined using as shown in equation 2.

$$\mathrm{Accuracy} = \frac{(\mathrm{TP}+\mathrm{TN})}{(\mathrm{TP}+\mathrm{TN}+\mathrm{FP}+\mathrm{FN})} \qquad (2)$$

4. Conclusion

A thorough analysis of the several Deep Neural Learning and Intelligent Machine Learning algorithms used to identify and counteract botnet assaults in the framework of Internet of Things (IoT) networks has been given by this survey on prediction. Additionally, it emphasized how Blockchain technology may be integrated to improve the confidentiality of information and offer a decentralized method for safe exchange of information on threats. Through an analysis of primary research conducted between 2018 and 2023, we were able to identify critical assessment metrics that are crucial for evaluating the effectiveness of detection mathematical models, including precision, recall, efficacy, false positives rate, and the percentage of false alarms. Blockchain may further reinforce safety measures by guaranteeing data confidentiality and transparency, even though ML and DL techniques show promising results in botnet detection, according to our analysis of various datasets, evaluation techniques, and pre-processing strategies. Challenges including dataset constraints, computational complexity, and the requirement for more reliable integration of different technologies still exist despite the developments. In order to create botnet detection systems for IoT environments that are more precise, scalable, and effective, future research should concentrate on resolving these issues and utilizing the complementary capabilities of ML, DL, and Blockchain-based technologies.

References

1. Pan, J., Paul, S., & Jain, R. (2011). A survey of the research on future Internet architectures. In IEEE Communications Magazine (Vol. 49, Issue 7). https://doi.org/10.1109/MCOM.2011.5936152
2. Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. Computers and Security, 56. https://doi.org/10.1016/j.cose.2015.10.006
3. Debicha, I., Cochez, B., Kenaza, T., Debatty, T., Dricot, J. M., & Mees, W. (2023). Adv-Bot: Realistic adversarial botnet attacks against network intrusion detection systems. Computers and Security, 129. https://doi.org/10.1016/j.cose.2023.103176
4. Gul, F., Mir, I., Abualigah, L., Sumari, P., & Forestiero, A. (2021). A consolidated review of path planning and optimization techniques: Technical perspectives and future directions. In Electronics (Switzerland) (Vol. 10, Issue 18). https://doi.org/10.3390/electronics10182250
5. Abualigah, L., Falcone, D., & Forestiero, A. (2023). Swarm Intelligence to Face IoT Challenges.

Computational Intelligence and Neuroscience, 2023(1). https://doi.org/10.1155/2023/4254194

6. Fang, J. (2023). Security Evaluation Method of Distance Education Network Nodes Based on Machine Learning. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 13655 LNCS. https://doi.org/10.1007/978-3-031-20096-0_22
7. Gelgi, Metehan, Yueting Guan, Sanjay Arunachala, Maddi Samba Siva Rao, and Nicola Dragoni. "Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques." Sensors 24, no. 11 (2024): 3571
8. Aldhaheri, A., Alwahedi, F., Ferrag, M. A., & Battah, A. (2024). Deep learning for cyber threat detection in IoT networks: A review. In Internet of Things and Cyber-Physical Systems (Vol. 4). https://doi.org/10.1016/j.iotcps.2023.09.003
9. Pan, X., & Yamaguchi, S. (2022). Machine Learning White-Hat Worm Launcher for Tactical Response by Zoning in Botnet Defense System. Sensors, 22(13). https://doi.org/10.3390/s22134666
10. Shi, C., Liu, J., Liu, H., & Chen, Y. (2017). Smart User authentication through actuation of daily activities leveraging wifi-enabled IoT. Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), Part F129153. https://doi.org/10.1145/3084041.3084061
11. Singh, R., Singh, J., & Singh, R. (2017). Fuzzy based advanced hybrid intrusion detection system to detect malicious nodes in wireless sensor networks. Wireless Communications and Mobile Computing, 2017. https://doi.org/10.1155/2017/3548607
12. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2019). LSB: A Lightweight Scalable Blockchain for IoT security and anonymity. Journal of Parallel and Distributed Computing, 134. https://doi.org/10.1016/j.jpdc.2019.08.005
13. Durani, H., Sheth, M., Vaghasia, M., & Kotech, S. (2018). Smart Automated Home Application using IoT with Blynk App. Proceedings of the International Conference on Inventive Communication and Computational Technologies, ICICCT 2018. https://doi.org/10.1109/ICICCT.2018.8473224
14. Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications, 38. https://doi.org/10.1016/j.jisa.2017.11.002
15. Muneer, S. M., Alvi, M. B., & Farrakh, A. (2023). Cyber Security Event Detection Using Machine Learning Technique. International Journal of Computational and Innovative Sciences, 2(2).
16. Kaushik, P. (2023). Unleashing the Power of Multi-Agent Deep Learning: Cyber-Attack Detection in IoT. International Journal for Global Academic & Scientific Research, 2(2). https://doi.org/10.55938/ijgasr.v2i2.46
17. Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018). Machine Learning and Deep Learning Methods for Cybersecurity. IEEE Access, 6. https://doi.org/10.1109/ACCESS.2018.2836950
18. Zhou, A., Li, Z., & Shen, Y. (2019). Anomaly detection of CAN bus messages using a deep neural network for autonomous vehicles. Applied Sciences (Switzerland), 9(15). https://doi.org/10.3390/app9153174
19. Das, R., & Sandhane, R. (2021). Artificial Intelligence in Cyber Security. Journal of Physics: Conference Series, 1964(4). https://doi.org/10.1088/1742-6596/1964/4/042072
20. Ghosh, P. K., Chakraborty, A., Hasan, M., Rashid, K., & Siddique, A. H. (2023). Blockchain Application in Healthcare Systems: A Review. In Systems (Vol. 11, Issue 1).

https://doi.org/10.3390/systems11010038

21. Tran, C. H., Bui, T. K., & Pham, T. V. (2022). Virtual machine migration policy for multi-tier application in cloud computing based on Q-learning algorithm. Computing, 104(6). https://doi.org/10.1007/s00607-021-01047-0
22. Kumari, A., Sukharamwala, U. C., Tanwar, S., Raboaca, M. S., Alqahtani, F., Tolba, A., Sharma, R., Aschilean, I., & Mihaltan, T. C. (2022). Blockchain-Based Peer-to-Peer Transactive Energy Management Scheme for Smart Grid System. Sensors, 22(13). https://doi.org/10.3390/s22134826
23. Ibrahim, W. N. H., Anuar, S., Selamat, A., Krejcar, O., Gonzalez Crespo, R., Herrera-Viedma, E., & Fujita, H. (2021). Multilayer Framework for Botnet Detection Using Machine Learning Algorithms. IEEE Access, 9. https://doi.org/10.1109/ACCESS.2021.3060778
24. Awotunde, J. B., Chakraborty, C., & Adeniyi, A. E. (2021). Intrusion Detection in Industrial Internet of Things Network-Based on Deep Learning Model with Rule-Based Feature Selection. Wireless Communications and Mobile Computing, 2021. https://doi.org/10.1155/2021/7154587
25. Kolias, C., Kambourakis, G., Stavrou, A., & Gritzalis, S. (2016). Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset. IEEE Communications Surveys and
26. Khacha, A., Saadouni, R., Harbi, Y., & Aliouat, Z. (2022). Hybrid Deep Learning-based Intrusion Detection System for Industrial Internet of Things. ISIA 2022 - International Symposium on Informatics and Its Applications, Proceedings. https://doi.org/10.1109/ISIA55826.2022.9993487
27. Procopiou, A., Komninos, N., & Douligeris, C. (2019). ForChaos: Real time application DDoS detection using forecasting and chaos theory in smart home IoT network. Wireless Communications and Mobile Computing, 2019. https://doi.org/10.1155/2019/8469410
28. Jing, X., Yan, Z., Jiang, X., & Pedrycz, W. (2019). Network traffic fusion and analysis against DDoS flooding attacks with a novel reversible sketch. Information Fusion, 51. https://doi.org/10.1016/j.inffus.2018.10.013
29. Alzubi, J. A. (2021). Blockchain-based Lamport Merkle Digital Signature: Authentication tool in IoT healthcare. Computer Communications, 170. https://doi.org/10.1016/j.comcom.2021.02.002
30. Al-Omrani, E. N., & Humayun, M. (2023). Securing Electronic Health Records (EHR) from Tampering Using Blockchain. Lecture Notes in Networks and Systems, 761 LNNS. https://doi.org/10.1007/978-3-031-40579-2_38
31. Shi, J., Zeng, X., & Han, R. (2022). A Blockchain-Based Decentralized Public Key Infrastructure for Information-Centric Networks. Information (Switzerland), 13(5). https://doi.org/10.3390/info13050264
32. Cha, J., Singh, S. K., Pan, Y., & Park, J. H. (2020). Blockchain-based cyber threat intelligence system architecture for sustainable computing. Sustainability (Switzerland), 12(16). https://doi.org/10.32890/JICT2018.17.3.8260
33. Padhiar, S., & Patel, R. (2023). Performance evaluation of botnet detection using machine learning techniques. International Journal of Electrical and Computer Engineering, 13(6). https://doi.org/10.11591/ijece.v13i6.pp6827-6835
34. Affinito, A., Zinno, S., Stanco, G., Botta, A., & Ventre, G. (2023). The evolution of Mirai botnet scans over a six-year period. Journal of Information Security and Applications, 79. https://doi.org/10.1016/j.jisa.2023.103629
35. Ahmad, S., Jha, S., Alam, A., Alharbi, M., & Nazeer, J. (2022). Analysis of Intrusion Detection Approaches for Network Traffic Anomalies with Comparative Analysis on Botnets (2008-2020). In

Security and Communication Networks (Vol. 2022). https://doi.org/10.1155/2022/9199703

36. Wazzan, M., Algazzawi, D., Bamasaq, O., Albeshri, A., & Cheng, L. (2021). Internet of things botnet detection approaches: Analysis and recommendations for future research. In Applied Sciences (Switzerland) (Vol. 11, Issue 12). https://doi.org/10.3390/app11125713
37. Booij, T. M., Chiscop, I., Meeuwissen, E., Moustafa, N., & Hartog, F. T. H. D. (2022). ToN_IoT: The Role of Heterogeneity and the Need for Standardization of Features and Attack Types in IoT Network Intrusion Data Sets. IEEE Internet of Things Journal, 9(1). https://doi.org/10.1109/JIOT.2021.3085194
38. Wardana, A. A., Kołaczek, G., Warzyński, A., & Sukarno, P. (2024). Ensemble averaging deep neural network for botnet detection in heterogeneous Internet of Things devices. Scientific Reports, 14(1). https://doi.org/10.1038/s41598-024-54438-6
39. Thota, S., & Menaka, D. (2024). Botnet detection in the internet-of-things networks using convolutional neural network with pelican optimization algorithm. Automatika, 65(1). https://doi.org/10.1080/00051144.2023.2288486
40. Al-Shareeda, M. A., Manickam, S., & Saare, M. A. (2023). DDoS attacks detection using machine learning and deep learning techniques: analysis and comparison. Bulletin of Electrical Engineering and Informatics, 12(2). https://doi.org/10.11591/eei.v12i2.4466