Machine Learning-Based Intrusion Detection for IoT Botnet Attacks: A Comprehensive Review

[1]Arvind Yadav, [2]Prof.Sakshi Tiwari, Prof. Onkar Nath Thakur, Prof. Rakesh Tiwari
[1]Research Scholar, Department of Computer Science Engineering, Technocrats institute of Technology & Science Bhopal (M.P.) India
[2,3,4] Professor, Department of Computer Science Engineering, Technocrats institute of Technology & Science Bhopal (M.P.) India
arvindup89@gmail.com , sakshitripathi0710@gmail.com , er.onkarthakur@gmail.com , rakeshtiwari80@gmail.com

* Corresponding Author: Arvind Yadav

Abstract:

The recent upsurge of the Internet of Things (IoT) in smart homes, healthcare, industrial automation, and smart cities has widened the possibilities of cyber threats such as IoT botnet attacks in particular. IoT settings are left helpless by resource limitation, weak patterns of authentication, default passwords, and a very occasional uptaking of patch updates," making IoT devices highly susceptible to botnet-led attacks of gargantuan amplitude, such as DDoS, malware proliferation, and data theft. Security controls such as signature / rule-based intrusion detection still remain predominantly ineffective against up-to-the-state IoT threats as they cannot keep pace with the ever-dynamic scenario of IoT dangers and fail to scale as necessary.Machine learning (ML) has emerged as a hopeful solution for smart, adaptive, and automated intrusion detection in IoT settings. This review provides an all-inclusive analysis of ML-based IoT botnet detection approaches, including supervised, unsupervised, and semi-supervised learning approaches. Important elements criticizly analyzed entail features of engineered characteristics, behavior of traffic, dataset characteristics, and assessment metrics for performance, etc. The aim is to include how edge and fog computing would cascade into the detection of botnet detection in real-time and with low latency, taking under consideration the strictly related issue of resource constraints.This paper also, however, points out present challenges ranging from class imbalance, high false alarm rates, lack of scalability and limitations on deployment on constrained IoT devices Synthesizing current research trends and recognizing open gaps in research, the review offers useful insights to researchers and practitioners aspiring to build effective, lightweight, and robust ML-based intrusion detection frameworks to secure the Internet of Things networks of the upcoming generations.

Keywords:*IoT Security, Botnet Attacks, Intrusion Detection System, Machine Learning, Anomaly Detection, Edge Computing*.

I.INTRODUCTION

The Internet of Things (IoT) is an emerging paradigm where physical objects, devices, sensors, and machines are interconnected through the internet to select data, share data, and act on data with little or no human intervention [1]. IoT is designed for the fluid data interchange between heterogeneous devices using embedded sensors, software, and network connectivity in very intelligent, automated, and data-driven learning environments [2].

IoT now bears the promise of being a technological torchbearer for modern cyber-physical systems, thereby enabling real-time monitoring, control, and real-time decision-making across numerous realms such as smart homes, healthcare, industrial automation, transportation, agriculture, and smart cities [3]. It’s clashing with cloud computing, edge computing, artificial intelligence, and machine learning has boosted its retrospective and predictive capacities, thus solidifying the integration of IoT with these transformative areas [4]. In an IoT ecosystem, the devices continue to generate staggering quantities of data which traverse a wire-line or wireless communication network to centralized or distributed processing platforms. These platforms interpret data to draw decisions, perform response automation, and further fine-tune the performance of the system [5]. Nevertheless, as the IoT device spread speedily, grinding against security, a number of stumbling blocks are posed. Owing to a lack of resources, most of the IoT devices run insufficient security practices and are deployed with default credentials and, further, outdated firmware [6]. With such vulnerabilities as this, the IoT networks seem to form very attractive targets for cyber-attacks that may involve, for example, massive attacks through a botnet propagation space, or from compromised devices. Hence, it is important to understand the primary modules and internal characteristics of IoT gadgets for designing consistent security frameworks. Our research endeavors to use machine learning techniques to confront IoT botnet threats by implementing prevention and detection mechanisms simultaneously [7]. Figure1 represents Intrusion Detection System

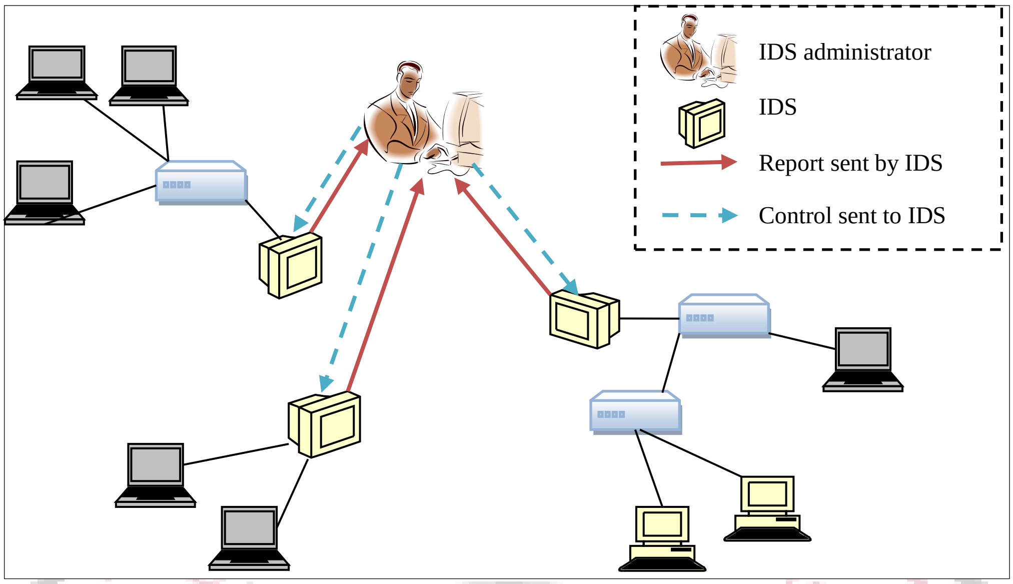

Figure 1: Intrusion Detection System [8]

The key components include:

Sensors and Actuators: Sensors collect physical data such as temperature, humidity, motion, light, and pressure, while actuators perform certain actions as commanded [8].

IoT Devices: Embedded systems comprising sensors, processors, and communication modules which communicate with the environment.

Communication Networks: Used for transmitting data using a number of protocols, (such as Wi-Fi, Bluetooth, ZigBee, LoRaWAN, LTE, and 5G).

Gateways: Deliver data aggregation and protocol translation while serving as an interface between IoT devices and cloud platforms [9].

Data Processing Platforms: Cloud, fog, or edge computing platforms that store, process, and analyze IoT data.

Application Layer: User-facing applications imparting visualization, monitoring control, and analytics services. UNYES

a. Characteristics of IoT Devices

Table 1: Characteristics of IoT Devices [8]-[9]

Characteristic	Description
Resource Constraints	Limited processing power, memory, and energy capacity
Heterogeneity	Diverse hardware architectures, operating systems, and communication protocols
Scalability	Ability to support a large number of interconnected devices
Autonomous Operation	Minimal human intervention during normal operation
Real-Time Data Generation	Continuous sensing and transmission of real-time data
Interconnectivity	Seamless communication between devices and systems
Mobility	Support for mobile and dynamic network environments
Context Awareness	Ability to sense and respond to environmental conditions
Low Power Consumption	Optimized for energy-efficient operation
Security Vulnerability	Susceptibility to attacks due to weak authentication and encryption
Remote Accessibility	Devices can be accessed and managed remotely
Dynamic Topology	Network structure changes as devices join or leave

b. Growth and Applications of IoT Systems

As the Internet of Things (IoT) technologies advance at lightning speed, the physical world intermingles with the digital. Pushing IoT to be widely deployed across various sectors is the lowering price of sensors, wireless communication, cloud computing, and artificial intelligence [10]. The increasing scale and complexity of IoT deployments intensify security challenges in instances of botnet-based cyber-attacks, which demand stringent protective and detection actions.

Smart Homes and Smart Cities: -The IoT-controlled appliances art and smart thermostats, lighting systems, surveillance cameras, and voice-activated assistants, which make homes smart [11]. The primary aim is the augmentation of the comfort, efficiency, and safety level. These appliances facilitate remote monitoring and control of home appliances through applications running on mobile phones or on-line services. IoT-based automation leads to self-adaptive control based on user actions and environmental conditions, while energy management systems help manage electricity consumption by observing real-time usage patterns. Integrated with sensor and cameras, smart security systems become burglary detectors and real-time averters. [12]

Industrial IoT (IIoT): Industrial Internet of Things (IIoT) integrates sensors, machines, and control systems within industrial environments to enhance the productivity, efficiency, and reliability of operations [13]. IIoT enables real-time monitoring of manufacturing processes, equipment health, and production quality. Predictive maintenance systems analyze sensor data to identify potential equipment failures before they occur. This reduces downtime and maintenance costs. Industrial automation systems leverage IoT data to optimize workflows and resource allocation [14].

Healthcare and Wearable IoT : Health IoT networks offer caregivers interlinked medical systems, equipment, and wearables for keeping lots of health details of their patients and remotely providing medical help, for example, in a hospital [15]. Wearables, like smartwatches, fitness bands, or biosensors, can record data with health conditions like heart rate, pressure, and oxygenation for a whole host of physiological parameters.

c. IoT Network Architecture

The IoT network architecture provides the structural framework for communication, data exchange, and intelligent processing among connected IoT devices. The architecture generally follows a layered model wherein the sensing, communication, and application functionalities are treated differently to provide the much-needed scalability, interoperability, and manageability [16]. The IoT architecture supports an uninterrupted flow of data from the physical sensors to higher-level applications, leveraging less resource-consuming communication mechanisms. It also brings together the cloud, edge, and fog computing paradigms to process massive amounts of data effectively [17]. Each layer of the architecture is vested with distinct responsibilities and therefore different security needs. It is essential for a secure design of ML-driven countermeasures for detecting and preventing botnet attacks to have a good understanding of IoT network architecture [18].Figure 2 represents the Principle of Detection

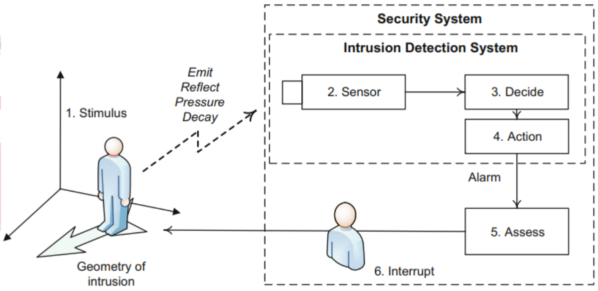

Figure 2: The Principle of Detection [19]

Perception Layer: -The perception layer is the lowest layer in the IoT architecture and functions as the gateway between the physical world and the digital one. It senses, gathers, and digitizes real-world data via a set of diverse sensors and actuators. Some commonly used sensing devices are temperature sensors [19], humidity sensors, motion detectors, cameras, and RFID tags.

Network Layer: -Analyzing data from perception has its advantages, but it is the intermediary layer that facilitates and manages this data. The network layer grants wireless or wired connectivity utilizing communication technologies such as Wi-fi, Bluetooth, ZigBee, LoRaWAN, LTE, and 5G [20]. Its primary duty is ensuring stable, flexible, and effective data delivery throughout a diverse range of networks.

Application Layer: -The applications layer provides user-oriented services and interfaces that enable the user to interact with IoT systems. It utilizes information received from lower layers to deliver meaningful insights, visualizations, and control functionalities [21]. Common IoT applications may consist of smart home management systems, healthcare monitoring platforms, industrial control dashboards, and smart city services.

Edge and Fog Computing in IoT: -In edge and error computing, they both extend the tradition of IoT architecture and position computation closer to the data origin. While edge computing conducts computation on the device itself and nearby gateway, fog computing renders an intermediary between the edge nodes and the cloud servers [22]. They save latency, conserving bandwidth usage, and break away from a model of centralized cloud reliance.

d. Botnet Attacks in IoT Environments

Botnet attacks have given birth to one of the most critical IoT security threats where major vulnerabilities are still associated with the advent of these devices. IoT botnet is a sinister chain of IoT devices compromised, manipulated remotely to systematically perform harmful operations by an attacker [23]. These attacks are for representative warnings from problems built on-device weaknesses, namely weak authentication mechanisms, defaults, excesses in processing capacity or seldom firmware updates.

IoT botnets are primary used to lead large-scale Distributed Denial-of-Service (DDoS) attacks, data exfiltration attacks, and malware propagation campaigns [24]. While traditional bot-botnets were based mostly on personal computers, IoT botnets utilize devices such as cameras, routers, smart TVs, and sensors to a great extent, continuously or intermittently connected to the internet. Their great interconnectedness makes them perfect candidates for botnet clones.

The scale and intensity of IoT botnet attacks are increased all the more by the numerous devices involved. The compromised devices can unleash vast volumes of malicious data, capable of doing a denial of service attack on servers and significant infrastructures [25]. These activities are responsible for some of the largest DDoS incidents to date, hindering Internet services, financial institutions, and government systems.

Botnets in IoT, because they generate inter-node communication in small and low-attention traffic patterns, are very challenging to monitor. Furthermore, attackers enhance their botnet malware to refrain from signature grey listing. Once the span-installed and inter-connected-device supported view of IoT environment is considered, it has in fact proven impossible to secure the security management of all devices [26]. Therefore, it would be imperative to come up with intelligent, adaptive, machine learning-based approaches to prevent or accurately detect attacks from IoT botnets.

An IoT botnet refers to a series of interconnected IoT devices that have been infected with malicious software and are controlled by a remote operator-referred to as the botmaster. These infected devices are referred to as bots or zombies, and they collectively perpetrate cyber assaults which are unknown to the owners of the devices [27].

IoT botnets commonly exploit vulnerabilities caused by weak passwords, open ports, or outdated firmware in order to enter devices. Once on a network, the bot makes contact with a command and control server for directions [28]. These commands may result in harmful actions such as a DDoS attacks, seeking unprotected devices through scanning, or taking out confidentially preserved information.

e. Common IoT Botnet Families

Table 2: Common IoT Botnet Families [28]

Botnet Family	Targeted Devices	Attack Type	Key Characteristics
Mirai	Cameras, routers, DVRs	DDoS	Uses default credentials, high traffic floods
Bashlite (Gafgyt)	IoT routers, cameras	DDoS	IRC-based C&C, TCP/UDP floods
Mozi	Routers, gateways	DDoS	P2P-based C&C using DHT
Reaper (IoTroop)	Smart devices	DDoS	Exploits software vulnerabilities
Hajime	Routers	Worm-like	Decentralized, self-propagating
VPNFilter	Network routers	Espionage, DDoS	Multi-stage malware
Okiru	ARC-based IoT devices	DDoS	Mirai variant, multi-architecture
Satori	IoT devices	DDoS	Rapid exploitation techniques

Centralized C&C architectures are the ideal model for IoT botnets. By way of those mechanisms, command and control entities correspond with both the botmaster and the corrupted devices [29]. The infrastructure for C&C allows blame-ridden royalties in the sense of dispatching commands, upgrading viral codes adlibitum, and setting the infamous course of impending strikes. Botnets in the traditional spirit had better go for atomized segments communicating back to a head end of a centralized component, with all of them separately talking to the server [30]. Centralized C&C architectures are easy to implement but easy to take down when the server is discovered. Decontrol the limitation, with current IoT botnets using decentralized C&C mechanisms like peer-to-peer (P2P) communication and distributed hash tables (DHTs). They make a more resilient botnet, and disrupting such networks becomes more of a sophisticated plot.

II. MACHINE LEARNING TECHNIQUES FOR IOT BOTNET DETECTION

In recent studies, numerous machine learning practices have been adopted to cope with the IoT botnet strikes. Time-series-based sequential learning frameworks aimed to conceal real-time and arranged- IoT traffic herein, which could help early spotting of the odd noisy behavior indicating botnet activities [1]. This study indicates that the sequence model especially succeeds in reflecting time dependencies within network traffic. However, in the absence of much evaluation on a huge simulated dataset, it provides limited applicability to real-world- IoT deployments. So far, there has been no validation exercise within large, heterogeneous IoT networks.

In order to address the issue of real datasets, a botnet detection framework meant for IoT is verified using the MedBIoT dataset, which presented a decision system of machine learning classifiers concluding ensemble as the best in high-performance detection and accuracy [2]. The findings also underscored the importance of careful feature selection and preprocessing in effectively and dramatically improving the classifier's performance. While the implementation has some accuracy limitations in healthcare IoT applications, the lack of real-time deployment considerations can impede its operation in truly dynamic settings.

Intrusion detection in domains that cannot accommodate latencies and other resource-related constraints has found an increasing sphere of priority in the IoT world. For the real-time detection of intrusion, a distributed architecture deployed near the edges made proper use of edge devices by distributing computation across them enhancing accuracy and effective resource usage. However, there is a scalability issue, interoperability issues, and issues of deployment at scale. An elucidation of these domain-specific deep learning models is illustrated by Anomaly-Based Detection, which has been applied in practice through deep learning architectures and achieved high precision and recall in their attempts at intrusion detection [7]. These models are more broadly applicable and computationally very intensive at-the-edge counterparts.

Promising initial observations have emerged in using deep learning for securing UAV-enabled IoT networks, in particular in the detection of drone incidents within high accuracy [5]. However, continuous monitoring introduces a considerable processing and storage overhead, making lightweight detection mechanisms more practical. Research has further examined results for reinforcement learning for intrusion detection in IoT, accentuating good points related to reducing false positives and energy efficiency [6]. Though offering such benefits, most reinforcement learning models have not been validated to be true, especially in real-world settings of IoT.

Traffic behavior-based botnet detection algorithms using machine learning classifiers gained much attention, based on the effectiveness of tree-based models achieving high rates of detection with low false alarm ratios [7]. However, while three models in contrast, static models can no longer keep pace because botnet behaviors are ever-evolving, thus entailing adaptive learning and online learning strategies. As for the deep learning cybersecurity studies at large, the convolutional and recurrent neural network-based methods gained great inspiration to analyze the network traffic patterns [8]. Nevertheless, problems such as data imbalance, interpretability, and the computational power involved have limited their applications, while integrations are sought alongside explainable AI techniques.

Essentially, it is mentioned in the subtle suspension-theories of entity in topology, when the possibility of the existence of different types of entities wholly scrolls up and upwards. This study was designed to cope with five problems: `Any posits graduate courses in ontology are an uphill battle,' which differs its courses from others in linguistics; some holds on to beliefs in which ontological commitments assert the ontological status of linguistic entities, while some focus on a third view of the entities resistant to change in the areas of linguistic studies (52). The Kansai University Course had been voted 'lecture of authenticity,' 'privacy,' 'ciphers in sets,' 'writers writing,' and 'construction project management' by graduate students.

Comparative evaluations of machine learning and deep learning intrusion detection systems consistently show that Deep Learning is a superior candidate for detecting complex large-scale attacks [12]. It is further observed that automated AI-driven intrusion detection and response frame modules may be able to reduce false alarms and increase the speed of mitigation activities [13], (however) which may be mitigated owing to scalability properties that are data-dependent. Security in cloud-integrated IoT environments had appeared to be more promising with the aid given to use blockchain, evolutionary algorithms, and post-quantum cryptography to solve issues [14], but the question of scalability and computational tractability remains.

Systems with more secure methods, such as tamper-resistant mechanisms for organic materials and sensors that enhance integrity and anomaly detection for IoT, are being slowed down by deployment complexity. According to the vulnerability and threat modeling frameworks for IoT risk identification, updates are crucial in real-time for the obtained [16] effect. Studies into the adoption of IDS stress organizational factors and usability as primary determinants in enterprise IoT security [17].

Systematic reviews of deep learning-based detection systems have proven the high precision of these detection models as opposed to their traditional counterparts [18], facets like interpretation and computation constraints pose still serious hurdles. Their importance within multiclassifier experiments again confirmed feature selection and optimization, while increasingly comprehensive taxonomies around ML-based IDS models and data sets and real-time deployment are heterogeneous. remarkable to scale, remain a difficult challenge [20].

The titles in the detection network are divided into two groups: signature-based and anomaly-based, and the last variation is technically challenging due to high resource requirements for the system. Works, which have focused extensively on the anomaly approach of deep learning IDS detection, provide improved accuracy together with few false positives [21]. Based on analyses by machine learning experts, there would be greater emphasis on hybrid learning methods, building a way to adaptive learning techniques in order to achieve an increase in the effectiveness of monitoring [22]. Various solutions submitted, that are protocol oriented, attempted to detect IoT-enabled MQTT traffic with an accuracy, despite the fact that there were hurdles in mounting them on resource-constrained devices [23]. Research works into network-based IDS predictions have always primarily noted a lack of standardized dataset calibration evaluation metrics [24].

In all these studies, there are also successful results to show that fog and edge-based intrusion detection systems can outperform even large systems on their own. The exception lies in the capacity of IoT heterogeneity. Literature surveyed found strong class imbalanced data, the impenetrability of feature extraction, and energy efficiency as critical impediments and recommended hybridized architectures, namely ML–DL [26]. IoMT-based IDS models scored very highly on detection accuracy, depending on regular and stable traffic patterns [[27]]. In all probable measures ensembles performed admirably against single classifiers in anomaly detection [28], mutation of CNN–LSTM effectively captured the spatial and temporal-related traffic features at the expense of computation [29]. As a consequence, recent reviews suggest that deep learning and ensemble techniques bring about the greatest detection rate, but that limitations in resource capacity require lightweight, adaptive, and scalable systems capable of preventing intrusion in real-life settings of IoT applications [30].

Table 3: Summary of Machine Learning and Deep Learning-Based IoT Intrusion Detection Systems

Ref	Technique	Dataset Used	Key Results / Performance	Limitations
[1]	Sequential ML architecture	IoT network traffic datasets	Accuracy: 97.8%, F1-Score: 97.5%, early detection, low false positives	Simulated data, limited real-world generalization
[2]	ML classifiers, ensemble models	MedBIoT	Accuracy: 98.2%, Precision: 97.9%, F1-Score: 98.0%	Scalability challenges for large IoT networks
[3]	Distributed AI architecture	TON_IoT	Accuracy: 96.5%, F1-Score: 96.0%, improved resource efficiency	Complex deployment in heterogeneous IoT environments
[4]	Deep learning anomaly detection	Healthcare IoT datasets	Accuracy: 98.1%, Recall: 97.6%, Precision: 97.9%	May not generalize beyond healthcare IoT, edge resource constraints
[5]	Deep learning IDS for drones	UAV network datasets	Accuracy: 97.2%, F1-Score: 96.8%, real-time detection	High computational requirements for continuous monitoring
[6]	Reinforcement learning for IoT security	Survey / Multiple IoT datasets	Adaptive threat mitigation, energy-efficient detection	Many approaches lack real-world validation
[7]	ML classifiers (Decision Tree, RF)	IoT network traffic	Accuracy: 95.8%, F1-Score: 95.5%, early botnet detection	Limited adaptability to evolving botnets
[8]	Deep learning (CNN, RNN)	Mobile network datasets	Accuracy: 96.9%, F1-Score: 96.5%, improved anomaly detection	Data imbalance, resource overhead, interpretability issues
[9]	Hybrid ML + user behavior analysis	Smart home IoT datasets	Accuracy: 97.4%, F1-Score: 97.1%, reduced false alarms	Dependent on consistent user behavior, scalability issues
[10]	Supervised learning framework	IoT healthcare datasets	Accuracy: 97.6%, Precision: 97.3%, Recall: 97.5%	Computational overhead on edge devices
[11]	Data science & ML overview	Multiple IoT datasets	Accuracy range: 94–97%, insights on anomaly detection	Large-scale data management and real-time analysis challenges
[12]	ML & DL techniques IDS	IoT network datasets	Accuracy: 96.8%, F1-Score: 96.3%, DL outperformed ML	High computational cost, model interpretability
[13]	AI-based orchestration	IoT datasets	Accuracy: 95.5–96.7%, improved detection & reduced response time	Dependent on accurate data, complex integration
[14]	Review: blockchain, post-quantum crypto	Multiple IoT case studies	Not numeric; highlights key IoT security gaps	Scalability and computational constraints
[15]	Tamper-evident security for sensors	Smart sensing IoT datasets	Accuracy: 96.2%, anomaly detection improved	Deployment complexity, resource overhead
[16]	IoTVT model (vulnerability mapping)	IoT sensor datasets	Detection rate: 95%, improved mitigation of high-risk components	Dataset dependency, real-time updates needed
[17]	Correlational study on IDS adoption	Survey of IT professionals	Adoption determinants identified (usefulness, ease of use)	Survey-based bias, limited generalizability
[18]	Systematic review on DL IDS	Multiple IoT datasets	Deep learning outperformed traditional ML (Accuracy: ~96%)	Interpretability and computational overhead
[19]	Experimental comparison of ML classifiers	Network datasets	Accuracy range: 94–96%, feature selection impacts performance	Dataset specificity, adaptability issues
[20]	Taxonomy of ML-based IDS	IoT datasets	Ensemble effectiveness highlighted, Accuracy ~95–97%	Scalability, interpretability, real-time deployment

III. FEATURE ENGINEERING AND TRAFFIC ANALYSIS IN IOT NETWORKS

Feature engineering and traffic analysis complement intrusion detection systems (IDS) to handle issues such as the Internet of Things (IoT) [11]. Given the diverse nature of IoT devices, the network traffic varies with the means of communication, data rates, and peculiarities specific to the needs of the protocol. The generation of effective features can convert crude traffic data into sensible representations, thereby enhancing the potential of learning for machine learning and deep learning models. Commonly extracted features include packet-level attributes (such as packet size, time, and type of the protocol), flow-level features [14]. These features establish the demarcation between normal behavior and exceptions or malign acts.

Traffic analysis in IoT surroundings mainly looks for any deviation from established behavioral base-lines. Many IoT devices produce traffic that is periodic and therefore predictable. Behavioral profiling is one of the effective approaches to detect botnet activity and intrusion attempts [15]. Hence, sudden anomalies between traffic volume, unusual communication endpoints, failed connection attempts repeatedly, and synchronized traffic bursts across devices are a good indicator of an attack, be it DDoS or malware in action. Hence, a myriad of hardware installations that are entirely reliant on variable threats in and out of the network should be looked into, typically employing (DDD) techniques [20]. As far as the selection of features is another high-level step, reduction of dimensions, such as correlation analysis path, principal component analysis, mutual information, and ad-hoc convex optimization. Potential metrics for selecting features involve optimizing feature sharing computations or even measurements largely: cross-validation. Selecting multiple features is of paramount importance [21].

Protocol-aware traffic analysis also becomes more crucial in IoT systems where lightweight protocols especially MQTT, CoAP, and HTTP are in use. Observing protocol-specific features has been contributing largely to the effectiveness at intrusion detection with a reduction in false alarms [22]. While encrypted traffic, the class imbalance, and changing attack patterns pose different hurdles in the way, the research in the future should focus on automated feature learning with deep learning, encourage adaptive feature selection, and foster lightweight traffic analysis schemes suitable for real-time deployment to resource-constrained IoT networks [25].

IV. INTERNET OF THINGS: ARCHITECTURE AND SECURITY CHALLENGES

The Internet of Things (IoT) refers to a network of interconnected physical devices embedded with sensors, actuators, communication modules, and processing capabilities that enable them to collect, exchange, and act on data autonomously. A typical IoT architecture is commonly structured into layered models, most notably the three-layer and five-layer architectures [26]. The three-layer architecture consists of the perception layer, network layer, and application layer. The perception layer includes sensors and actuators responsible for data acquisition from the physical environment. The network layer ensures reliable data transmission using communication technologies such as Wi-Fi, ZigBee, Bluetooth Low Energy, LoRaWAN, and cellular networks. The application layer delivers end-user services across domains such as smart homes, healthcare, transportation, and industrial automation. Extended architectures introduce middleware, processing, and business layers to support data analytics, device management, and decision-making [27].

Despite its transformative potential, IoT architecture faces significant security challenges due to its distributed and heterogeneous nature. Resource-constrained devices often lack sufficient computational power, memory, and energy to implement strong cryptographic mechanisms, making them vulnerable to attacks [28]. Weak authentication, default credentials, and insecure firmware updates further expose IoT systems to threats such as botnets, spoofing, and unauthorized access. Network-level vulnerabilities enable attacks including Distributed Denial-of-Service (DDoS), man-in-the-middle, and traffic analysis attacks, while application-layer threats target data privacy, integrity, and service availability [29].

Additionally, the massive scale of IoT deployments complicates centralized security management and monitoring. Interoperability issues among diverse devices and protocols create security gaps that attackers can exploit. The absence of standardized security frameworks and the difficulty of applying timely patches exacerbate these risks [30]. Consequently, ensuring IoT security requires multi-layered defense mechanisms, incorporating secure device design, robust communication protocols, and intelligent intrusion detection systems capable of adapting to evolving threat landscapes [31].

V. CONCLUSION AND FUTURE WORK

In this review, various machine learning and deep learning–based techniques have been examined to address the growing security challenges in Internet of Things (IoT) networks. Machine learning and deep learning-based intrusion detection systems have been recognized as viable solutions for enhancing IoT security mechanisms. This security mechanism employs sophistication such as automatic, adaptive, and behavior-based detection of threats. These researchers have described that through the feature engineering of traffic and real-time analysis, they identify intrusions in complex attack patterns mostly not detected by static signature-based systems. With the rise of edge and fog computing, the detection of intrusions becomes more effective in real-time, while at the same time reducing latency and accommodating higher bandwidths. There are several important advances in the field, yet not all of the problems have been solved, including increased false-positives, data imbalance, and lack of real validation on field data, scalability issues, and the computational-engram burden placed by deep learning models on resource-constrained devices. The lack of standardized datasets and evaluation frameworks, in turn, severely complicates fair comparisons and practical deployments. Therefore, future security solutions for IoT must work toward developing lightweight, explainable, and energy-efficient detection models that can work effectively in dynamic and heterogeneous environments. By overcoming these challenges, intelligent intrusion detection systems will play a key role in the realization of secure, reliable, and trustworthy IoT networks in next-generation applications.

REFERENCES

[1] Soe, Yan Naung, et al. "Machine learning-based IoT-botnet attack detection with sequential architecture." *Sensors* 20.16 (2020): 4372.

[2] Guerra-Manzanares, Alejandro, et al. "Using MedBIoT dataset to build effective machine learning-based IoT BotNet detection systems." *International Conference on Information Systems Security and Privacy*. Cham: Springer International Publishing, 2020.

[3] Moustafa, Nour. "A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets." *Sustainable Cities and Society* 72 (2021): 102994.

[4] Ahmad, Usman, et al. "A novel deep learning model to secure internet of things in healthcare." *Machine intelligence and big data analytics for cybersecurity applications*. Cham: Springer International Publishing, 2020. 341-353.

[5] Ramadan, Rabie A., et al. "Internet of drones intrusion detection using deep learning." *Electronics* 10.21 (2021): 2633.

[6] Uprety, Aashma, and Danda B. Rawat. "Reinforcement learning for iot security: A comprehensive survey." *IEEE Internet of Things Journal* 8.11 (2020): 8693-8706.

[7] Vaibhaw, Jay Sarraf, and P. K. Pattnaik. "Early Detection of Botnet Based Attacks Using Various Classification Techniques on Traffic Behavioral Features." *International conference on smart computing and cyber security: strategic foresight, security challenges and innovation*. Singapore: Springer Nature Singapore, 2021.

[8] Rodriguez, Eva, et al. "A survey of deep learning techniques for cybersecurity in mobile networks." *IEEE Communications Surveys & Tutorials* 23.3 (2021): 1920-1955.

[9] Alghayadh, Faisal Yousef. *A hybrid intrusion detection system for smart home security based on machine learning and user behavior*. Diss. Oakland University, 2021.

[10] Hussain, Faisal, et al. "A framework for malicious traffic detection in IoT healthcare environment." *Sensors* 21.9 (2021): 3025.

[11] Sarker, Iqbal H. "Data science and analytics: an overview from data-driven smart computing, decision-making and applications perspective." *SN Computer Science* 2.5 (2021): 377.

[12] Hindy, Hanan. *Intrusion Detection Systems Using Machine Learning and Deep Learning Techniques*. Diss. Abertay University, 2021.

[13] Zheng, Yifeng, et al. "Towards IoT security automation and orchestration." *2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. IEEE, 2020.

[14] Balogh, Stefan, et al. "IoT security challenges: cloud and blockchain, postquantum cryptography, and evolutionary techniques." *Electronics* 10.21 (2021): 2647.

[15] Sniatala, Pawel, Sundararaja S. Iyengar, and Sanjeev Kaushik Ramani. *Evolution of Smart Sensing Ecosystems with Tamper Evident Security*. Springer International Publishing, 2021.

[16] Nicho, Mathew, and Shini Girija. "IoTVT model: A model mapping IoT sensors to IoT vulnerabilities and threats." *2021 20th International Conference on Ubiquitous Computing and Communications (IUCC/CIT/DSCI/SmartCNS)*. IEEE, 2021.

[17] Paiola, Marcos. *Factors that Impact Information Technology Security Professionals' Intent to Use Intrusion Detection Systems: A Correlational Study*. Diss. Capella University, 2021.

[18] Lansky, J., Ali, S., Mohammadi, M., Majeed, M. K., Karim, S. H. T., Rashidi, S., ... & Rahmani, A. M. (2021). Deep learning-based intrusion detection systems: a systematic review. *IEEE Access*, *9*, 101574-101599.

[19] Hidayat, Imran, Muhammad Zulfiqar Ali, and Arshad Arshad. "Machine learning-based intrusion detection system: an experimental comparison." *Journal of Computational and Cognitive Engineering* 2.2 (2023): 88-97.

[20] Jamalipour, Abbas, and Sarumathi Murali. "A taxonomy of machine-learning-based intrusion detection systems for the internet of things: A survey." *IEEE Internet of Things Journal* 9.12 (2021): 9444-9466.

[21] Alsoufi, Muaadh A., et al. "Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review." *Applied sciences* 11.18 (2021): 8383.

[22] Kocher, Geeta, and Gulshan Kumar. "Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges." *Soft Computing* 25.15 (2021): 9731-9763.

[23] Khan, Muhammad Almas, et al. "A deep learning-based intrusion detection system for MQTT enabled IoT." *Sensors* 21.21 (2021): 7016.

[24] Kumar, Satish, Sunanda Gupta, and Sakshi Arora. "Research trends in network-based intrusion detection systems: A review." *Ieee Access* 9 (2021): 157761-157779.

[25] Alzubi, Omar A., et al. "Optimized machine learning-based intrusion detection system for fog and edge computing environment." *Electronics* 11.19 (2022): 3007.

[26] Adnan, Ahmed, et al. "An intrusion detection system for the internet of things based on machine learning: Review and challenges." *Symmetry* 13.6 (2021): 1011.

[27] Kulshrestha, Priyesh, and T. V. Vijay Kumar. "Machine learning based intrusion detection system for IoMT." *International Journal of System Assurance Engineering and Management* 15.5 (2024): 1802-1814.

[28] Abdelmoumin, Ghada, Danda B. Rawat, and Abdul Rahman. "On the performance of machine learning models for anomaly-based intelligent intrusion detection systems for the internet of things." *IEEE Internet of Things Journal* 9.6 (2021): 4280-4290.

[29] Qazi, Emad Ul Haq, Muhammad Hamza Faheem, and Tanveer Zia. "HDLNIDS: hybrid deep-learning-based network intrusion detection system." *Applied Sciences* 13.8 (2023): 4921.

[30] Kikissagbe, Brunel Rolack, and Meddi Adda. "Machine learning-based intrusion detection methods in IoT systems: A comprehensive review." *Electronics* 13.18 (2024): 3601.