Cyber Attacks in SDN-Based IoT Environment: A Review

Yusra Sh. Ajaj[*], Bilal R. Al-Kaseem[**], Yousif Al-Dunainawi[***]

[*] Department of Computer Engineering, College of Engineering, Al-Iraqia University, Baghdad, Iraq
Email: yusra.sh.ajaj@gmail.com
https://orcid.org/0009-0001-1544-4179

[**] Department of Communication Engineering, College of Engineering and Information Technology, AlShaab University, Baghdad, Iraq
Email: bilal.al-kaseem@alshaab.edu.iq
https://orcid.org/0000-0001-8264-6339

[***] Department of Information Security Engineering, College of Engineering and Information Technology, AlShaab University, Baghdad, Iraq
Email: yousif@alshaab.edu.iq
https://orcid.org/0000-0003-1293-3345

Abstract

As the Internet of Things (IoT) continues to grow, integrating Software-Defined Networking (SDN) has brought numerous benefits to IoT deployments. However, this convergence also introduces new challenges in terms of cybersecurity. This review paper explores the landscape of cyber-attacks in SDN-based IoT environments, providing an overview of the various attack vectors, vulnerabilities, and potential security risks associated with this emerging paradigm. This paper examines the unique characteristics of SDN-based IoT networks and their implications for cybersecurity. It delves into different types of cyber-attacks that can target SDN-based IoT deployments, including port scanning, Operating System (OS) fingerprinting, fuzzing, Denial-of-Service (DoS), and Distributed Denial-of-Service (DDoS) attacks. In addition, this paper examines the existing research and case studies that leverage Deep Learning (DL) techniques for cyber-attack detection and prevention in SDN-based IoT environments. It highlights the advantages of using DL, including its ability to learn complex patterns and adapt to evolving attack strategies. This paper emphasizes the need for robust datasets and the importance of feature selection and preprocessing techniques to enhance the effectiveness of DL models in the context of SDN-based IoT security. It also discusses the integration of DL with other security measures, such as encryption and access control, to provide a comprehensive defense mechanism. In summary, this review paper contributes to understanding how Artificial Intelligence (AI) can enhance the security of SDN-based IoT environments. It serves as a valuable resource for researchers and practitioners in the field of cyber security, exploring the current research, obstacles, and potential solutions for using DL to identify and mitigate cyber-attacks in SDN-based IoT settings.

Keywords- Artificial Intelligence (AI), Cybersecurity Improvement, Internet of Things (IoT), Software Defined Networking (SDN).

I. INTRODUCTION

The Internet of Things (IoT) refers to a vast network of interconnected physical devices, vehicles, appliances, and other objects embedded with sensors, software, and network connectivity that enables them to collect and exchange data. These devices, Internet-enabled devices, sometimes known as “smart” or “connected” gadgets, are constantly exchanging data with one another and with centralized servers, creating an ecosystem of data-driven interactions and automation [1][2]. The main characteristics of the IoT environment include [3][4]:

1. Connectivity: IoT devices can send and receive data because they are linked to local or global networks.
2. Sensing and Actuating: IoT devices use sensors and actuators to gather information about their surroundings and respond accordingly.
3. Data Processing and Analytics: IoT systems employ various data processing and analytics techniques to extract meaningful insights from the collected data.
4. Automation and Control: With the data collected from IoT devices, processes and control of physical items or systems are possible.

IoT architecture comprises various layers and components that work together to enable seamless communication and data exchange. The following are examples of common components found in an IoT system [1][4]:

- Devices and Sensors: These are physical items with sensors, actuators, and networking modules built to gather and send data.
- Connectivity: IoT devices utilize various technologies and communication protocols, such as Wi-Fi, Bluetooth, ZigBee, or cellular networks, to establish connections with each other and the internet.
- Cloud Infrastructure: IoT data is often processed, stored, and analyzed in cloud-based platforms that provide scalability, computational power, and data management capabilities.

- Edge Computing: To overcome latency and bandwidth limitations, IoT systems leverage edge computing, where data processing and analysis occur closer to the devices or at the edge of the network.
- Applications and Services: IoT applications and services leverage the processed data to provide real-time insights, automation, monitoring, and control functionalities.

IoT technology finds applications across various industries and domains, offering numerous benefits [5][6]:

1. Smart Homes and Building Automation: IoT enables home automation, energy management, security systems, and efficient building operations.
2. Industrial Automation and Manufacturing: IoT facilitates intelligent monitoring, predictive maintenance, supply chain optimization, and process automation in factories and industrial settings.
3. Healthcare and Telemedicine: IoT devices make it possible to provide tailored healthcare, manage medications, and do remote patient monitoring.
4. Smart Cities: IoT contributes to smarter urban planning, traffic management, waste management, energy optimization, and environmental monitoring.
5. Agriculture and Farming: IoT helps optimize irrigation, crop monitoring, livestock tracking, and automated farming processes.
6. Logistics and Transportation: IoT provides intelligent transportation systems, fleet management, vehicle tracking, and logistics optimization.

The applications of IoT are diverse and continually expanding, transforming industries and enhancing efficiency, productivity, and quality of life. However, these interconnected systems also present significant cybersecurity challenges that must be addressed to ensure IoT deployments' secure and reliable operation [7].

Software-Defined Networking (SDN) is an architectural approach that separates the control plane from the data plane in computer networks [8]. In traditional architectures of networks, networking components like switches and routers have a close coupling between the control plane as well as the data plane. SDN introduces a centralized control plane called the SDN controller, which provides a global view and control over the network. In an SDN architecture, high-level decision-making regarding how traffic on the network must be forwarded, and corresponding network device configurations are made by the control plane [9]. It defines network policies, routing rules, and other configuration parameters. On the other hand, the data plane handles the actual forwarding of network packets based on the instructions received from the control plane. Integrating SDN and IoT has brought significant advancements in network management and control. To guarantee the safe operation of IoT deployments, nevertheless, this convergence also presents new cybersecurity challenges [10].

The IoT encompasses many interconnected devices that collect, transmit, and process data. These devices often have limited computing resources and may lack robust security measures. On the other hand, SDN offers centralized control and programmability of network infrastructure, allowing for efficient management and dynamic adaptation to changing network conditions. To secure SDN-based IoT environments, it is crucial to understand the unique cybersecurity considerations they present, and the key aspects to consider are listed below [10][11]:

- Expanded Attack Surface: By interconnecting disparate devices and protocols, the combination of SDN and IoT increases the attack surface. Vulnerabilities in each IoT device and the overall network must be addressed because of the increased risk of cyberattacks.
- IoT Device Security: IoT devices often have resource constraints, making them susceptible to attacks such as device spoofing, unauthorized access, or data tampering. Ensuring secure device authentication, encryption, and firmware updates is essential to protect against these threats.
- Network Infrastructure Security: SDN controllers and switches are critical components in an SDN-based IoT environment. They need to be protected against attacks such as control plane manipulation, protocol vulnerabilities, or malicious software injection. Implementing secure communication protocols, access control mechanisms, and regular security updates are crucial for maintaining the integrity and availability of the network infrastructure.
- Data Protection: There is a lot of sensitive information being generated and transmitted by IoT devices. Data privacy and security must be prioritized. Data should be protected at every stage of its existence by using encryption, safe data storage, and access control measures.
- Threat Intelligence and Monitoring: Continuous monitoring and threat intelligence gathering are essential in identifying and mitigating emerging cyber threats. Intrusion detection systems, anomaly detection techniques, and network traffic analysis can help detect and respond to potential security incidents promptly.
- Security Policy and Compliance: Establishing comprehensive security policies and ensuring compliance with industry standards and regulations are crucial in maintaining a secure SDN-based IoT environment. Routine security audits, assessments of exposure, and incident response strategies can prevent potential security breaches.
- Collaboration and Knowledge Sharing: Cybersecurity in SDN-based IoT environments requires collaboration between network operators, IoT device manufacturers, and security experts. Sharing knowledge, best practices, and threat intelligence can help identify and address vulnerabilities effectively.

Organizations can harness the benefits of this convergence while minimizing risks by addressing the unique cybersecurity challenges posed by the integration of SDN and IoT. A comprehensive security approach encompassing device security, network infrastructure protection, data privacy, and continuous monitoring is essential to ensure the resilience and integrity of SDN-based IoT environments in the face of evolving cyber threats.

The remaining sections of the paper are as follows: Section II highlights the main threats affecting the performance of the IoT environment. While Section III provides a brief description of the main attacks in an SDN-based IoT environment. Section IV introduces the main artificial intelligence techniques. On the other hand, Section V and Section VI review the state-of-the-art research and findings, respectively. Finally, Section VII concludes the current work.

II. THREAT LANDSCAPE IN SDN-BASED INTERNET OF THINGS ENVIRONMENT

The widespread adoption of the IoT has introduced a complex and evolving threat landscape. IoT devices, networks, and infrastructure face various security risks that can compromise data integrity, privacy, and system functionality. Understanding the threat landscape is crucial for developing effective cybersecurity strategies in the IoT domain. This section explores some prominent threats that pose significant challenges to IoT security [12][13].

1. Malware and Botnets: Malware, including viruses, worms, and ransomware, poses a significant threat to IoT systems. Malicious software can infect vulnerable devices, exploiting their processing power, network connectivity, or data resources for malicious purposes. In recent years, botnets have emerged as a severe concern, wherein IoT devices are compromised and harnessed to form vast networks of "zombie" devices under attackers' control. These botnets can be utilized for distributed denial-of-service (DDoS) attacks, data theft, or other malicious activities.
2. Unauthorized Access and Control: IoT devices often lack robust authentication and authorization mechanisms, making them susceptible to unauthorized access and control. Attackers may exploit weak passwords, default credentials, or vulnerabilities in device firmware to gain unauthorized entry. Once compromised, adversaries can manipulate device settings, intercept sensitive data, or use the compromised devices as entry points into the broader network.
3. Physical Attacks: Physical attacks on IoT devices are another significant concern. Attackers may tamper with devices or their physical connections to gain unauthorized access, extract data, or compromise device functionality. Physical attacks can be particularly challenging to detect and mitigate since they may not rely on traditional network-based attack vectors.
4. Data Breaches and Privacy Violations: The vast amount of data generated by IoT devices increases the risk of data breaches and privacy violations. IoT devices often collect and transmit sensitive information, such as personal data, location data, or user behavior patterns. If proper security measures are not in place, this data can be intercepted, manipulated, or stolen, leading to privacy breaches, identity theft, or unauthorized surveillance.

These are just a few examples of the threats that IoT systems face. The dynamic nature of the IoT ecosystem, the sheer number of devices, and the heterogeneity of technologies contribute to an ever-evolving threat landscape. As IoT deployments continue to expand and interconnect, the potential for new and sophisticated threats increases. Organizations and individuals must adopt a comprehensive approach to IoT security to address these threats effectively. This includes implementing robust authentication mechanisms, encryption protocols, intrusion detection systems, and security monitoring practices. Additionally, regular security updates and patches should be applied to mitigate vulnerabilities, and user awareness and education about IoT security risks are crucial to ensure responsible and secure IoT device usage. By understanding the diverse range of threats that exist in the IoT landscape, stakeholders can proactively implement security measures to protect IoT systems, safeguard data integrity, and preserve user privacy.

III. CYBER ATTACKS IN SDN-ENABLED IOT ENVIRONMENT

Cyber-attacks in SDN-based IoT settings pose serious risks to the safety and reliability of all IoT devices and networks involved. As the integration of SDN and IoT continues to advance, new attack vectors and vulnerabilities must be understood and addressed. This section sets the stage for exploring the landscape of cyber-attacks in SDN-based IoT environments, highlighting the complexities and risks associated with this convergence [14][15].

- **Denial-of-Service (DoS) Attack**

A denial-of-service (DoS) attack is any concerted effort to render an operating system or network resource useless to its intended audience by flooding it with fake requests or otherwise abusing its vulnerabilities. The objective is to soak up so much of the system's resources that its intended audience can no longer access the service. In most cases, a single attacker will launch a Denial of Service assault on a single target by flooding it with overwhelming requests or traffic. The kind of DoS Attacks that are typically used include:

- Transmission Control Protocol/Internet Protocol (TCP/IP) Attacks: These attacks exploit vulnerabilities in the underlying TCP/IP protocol stack, such as TCP SYN flooding or ICMP flooding, to consume network resources and disrupt communication.
- Application Layer Attacks: These attacks target specific applications or services running on the targeted system, overwhelming them with excessive requests or exploiting application vulnerabilities. Examples include HTTP floods, DNS amplification attacks, and Slowloris attacks.

- **Distributed Denial-of-Service (DDoS) Attack**

(DDoS) attacks are similar to DoS attacks but involve multiple attacking sources, often compromised computers or devices forming a botnet under the control of an attacker. DDoS attacks amplify the impact of an attack by distributing the attack traffic across a network of compromised devices, making it more challenging to mitigate. DDoS attacks can be categorized into several types:

- Volumetric Attacks: These attacks flood the target system or network with an overwhelming volume of traffic, consuming its available bandwidth and resources. Examples include UDP floods or ICMP floods.
- Protocol Attacks: Protocol attacks exploit network protocol or service vulnerabilities to overwhelm the target. Examples include SYN floods, DNS floods, or NTP amplification attacks.
- Application Layer Attacks: The applications layer of DDoS attacks take advantage of security flaws or flood the targeted service with too many requests. Attacks such as HTTP flooding, HTTPS flooding, and application-level attacks are all examples.

- **Port Scanning Attack**

Port scanning is the process of systematically scanning a range of ports on a device or network to identify which ports are open or closed and potentially vulnerable to attack. Each port represents a specific network service or application running on a device. By identifying open ports, an attacker can gain insights into the services or applications running on the device, potentially exposing vulnerabilities or weaknesses that can be exploited. Port scanning in SDN-based IoT networks can expose potential vulnerabilities and weaknesses in network devices. To address this security concern, implementing strong device-level security measures, monitoring network traffic, leveraging intrusion detection systems, and adopting network segmentation can help mitigate the risks associated with port scanning activities. By combining these measures with continuous security monitoring and proactive response mechanisms, organizations can enhance the security posture of their SDN-based IoT networks.

- **Operating System (OS) Fingerprinting Attack**

OS fingerprinting is a technique used to identify the operating system running on a device connected to a network. In SDN-based IoT networks, OS fingerprinting plays a significant role in understanding devices' composition, vulnerabilities, and potential security risks. By analyzing network communication patterns and specific characteristics of network packets, OS fingerprinting can provide valuable insights for network administrators and security professionals. It's important to note that OS fingerprinting techniques should be used ethically and with proper authorization. Unauthorized OS fingerprinting or using the collected information for malicious purposes can violate privacy and security standards.

- **Fuzzing Attack**

Fuzzing is a technique to discover vulnerabilities and security flaws in software systems by sending malicious or unexpected inputs to target applications or network protocols. In the context of SDN-based IoT networks, fuzzing attacks can pose significant risks to the security and stability of the network infrastructure and connected IoT devices. Fuzzing attacks aim to identify vulnerabilities in software and network protocols. Attackers attempt to trigger unexpected behavior or crashes that can reveal security weaknesses by sending malformed or unexpected inputs to target systems. Fuzzing attacks in SDN-based IoT networks target the applications running on IoT devices and the communication protocols used for network management and control. Fuzzing attacks in an SDN-based IoT network can severely affect IoT devices. If successful, these attacks can cause devices to malfunction, crash, or exhibit unexpected behavior. Attackers can leverage such vulnerabilities to gain unauthorized control over IoT devices, leading to potential privacy breaches, data theft, or even physical harm in critical IoT deployments.

IV. AI TO IMPROVE SECURITY IN SDN- ENABLED IOT ENVIRONMENT

The integration of SDN and the IoT has opened up new opportunities for optimizing network management and enhancing the capabilities of IoT deployments. However, this convergence also introduces unique security challenges that require advanced techniques to mitigate cyber threats. In order to increase the security and resilience of SDN-based IoT settings, Artificially Intelligence (AI), Machine Learning (ML), as well as Deep learning (DL) have emerged as potent technologies.

AI refers to the broader concept of machines mimicking human intelligence to perform tasks intelligently. ML, a subset of AI, involves training algorithms to learn patterns and make predictions from data without being explicitly programmed. DL, in turn, is a specific approach within ML that utilizes deep neural networks to extract complex features and patterns from data [16].

When applied in the context of SDN-based IoT security, AI, ML, and DL offer several benefits. Firstly, they enable more efficient anomaly detection by learning normal patterns of network behavior and identifying deviations that may indicate malicious activity. These techniques can detect unusual or suspicious activities by analyzing network traffic, device behavior, and system logs, providing early warnings for potential security breaches. Secondly, AI, ML, and DL techniques facilitate intrusion detection and prevention by continuously analyzing network data for known attack signatures or detecting previously unseen attack patterns. This proactive approach helps identify and block malicious activities before they can cause significant harm, minimizing the impact of cyber-attacks. Furthermore, these technologies enable dynamic and adaptive security measures in SDN-based IoT environments. AI, ML, and DL algorithms can adjust security policies and configurations based on the evolving threat landscape by leveraging real-time data analysis and decision-making capabilities. This adaptability is crucial in countering sophisticated attacks that may change their behavior or employ novel evasion techniques [17]. Moreover, AI, ML, and DL techniques enhance network traffic classification and ensure data privacy. By analyzing packet headers, payload contents, and flow characteristics, these technologies can classify network traffic into

different categories, such as IoT devices, applications, or anomalies. This granular traffic analysis enables the enforcement of fine-grained access control policies and enhances data privacy protection by identifying and preventing unauthorized data access or transmission [18].

In summary, integrating AI, ML, and DL techniques in SDN-based IoT environments offers promising avenues for improving security and mitigating cyber threats. These technologies enable efficient anomaly detection, intrusion detection and prevention, adaptive security measures, and enhanced traffic classification. By leveraging the power of AI, ML, and DL, organizations can bolster the security and resilience of their SDN-based IoT deployments, ensuring the protection of sensitive data, mitigating risks, and maintaining the integrity of interconnected networks in the face of evolving cyber threats.

V. Related Works Review

The literature review section offers a thorough overview and critical evaluation of the knowledge already available on the subject at hand. This literature review aims to identify key themes, trends, and gaps in the current body of knowledge by examining a wide range of peer-reviewed articles, conference papers, and other relevant sources. By synthesizing and evaluating the existing literature, this section lays the foundation for the subsequent discussion and analysis, offering valuable insights and setting the context for this study's research objectives and contributions.

Dey *et al.* in [19] utilized ML, gain ratio, and Random Forest (RF) techniques to analyze the performance of SDN-based systems for intrusion detection while modifying the feature set. However, the training phase was carried out with an accuracy of 81.9% when the NSL-KDD dataset was employed.

Nguyen *et al.* in [20] presented SeArch as an intelligent and cooperative Network-Based Intrusion Detection System (NIDS) architecture for SDN-based cloud IoT networks that utilized ML/DL methods in order to detect threats within an SDN environment. The authors used three well-known network datasets: CAIDA, KDD Cup 1999, and UNSW-NB15. The obtained results from their introduced approach showed that around 95.5% of anomalies were detected by the SeArch solution.

Alzahrani *et al.* in [21] incorporated traditional and cutting-edge Decision Trees (DT), RF, and XGBoost methods for tree-based ML that were implemented in an SDN controller for traffic monitoring and intrusion detection. The NSL-KDD dataset was considered, and 5 of the 41 characteristics were selected for the tests, yielding a 95.95% accuracy for the developed model.

The Deep Neural Networks (DNN) technique was employed by Tang *et al.* in [22] for identifying flow-based anomalies in an SDN environment. In the developed DL models, six features were chosen from a total of 41 for the tests using the NSL-KDD dataset. The DNN was used to get an accuracy of 75.75%, which was below the average level for AI models that employed DL techniques.

Hannache *et al.* [23] introduced a Neural Network-based Flow of Traffic Classifier (TFC-NN) for real-time detection of DDoS in an SDN environment. Live migration was turned on after a DDoS attack was identified to defend the network. This study served as the main tool for locating and thwarting DDoS attacks, with a 96.13% accuracy rate when using a unique dataset. Hande *et al.* in [24] suggested Convolutional Neural Network (CNN) models-based detection of network intrusions for SDN. The KDD99 dataset was used to train a model that the SDN controller used. This model took into consideration six features. The suggested model's effectiveness was still being assessed.

DL technique for flow-based anomaly identification in SDN was presented by Tang *et al.* in [25]. The authors used DNN and GRU-RNN (Gated Recurrent Neural Network) to identify network threats. To evaluate the DL models, the dataset from NSL-KDD was used. The performance results showed that the introduced models' accuracy were 80.7% and 90%, respectively.

Wani *et al.* in [26] used a DL classifier to implement anomaly-based SDN intrusion detection for the IoT. Activity tracking, activities analyzer, and classifier—three elements of the proposed intrusion detection system—captured traffic data, identified features, minimized features, and detected anomalies using DL approaches. Their developed model's accuracy with the CSE-CIC-IDS2018 dataset was 96.05%.

Li *et al.* in [27] presented a two stages intrusion detection technique for an IoT context based on SDN. A weighted RF was used to classify the network flow traffic after it had been collected from the SDN controller and analyzed using the Bat algorithms with binary differentiated mutations and swarm division to select the best characteristics. Their proposed method was tested using the KDD99 dataset, and the accuracy was 96.03%.

Another intrusion detection system with two stages for SDN-based IoT networks was presented by Tian *et al.* in [28]. The firefly algorithm enhanced their research approach, and the wrapper feature selection was performed by the group algorithms for learning C4.5 DT, Multi-Layer Perceptron (MLP), as well as instance-based learning. Based on the general rule that the minority should obey the majority, the last feature subset was chosen. The weighted voting approach was used to estimate the traffic classification. However, NSL-KDD and UNSW-NB15 datasets were employed. According to the experimental results, their suggested multiclass classification approach had an accuracy of 99.00% and 88.46%, respectively.

Ye *et al.* in [29] presented Support Vector Machine (SVM) algorithms for classifying SDN-based DDoS attack defense. When a custom dataset was employed to train their SVM model, the experimental findings showed that their proposed approaches achieved an average accuracy rating of 97%.

Hadem *et al.* in [30] utilized the SVM technique with selective records for IP Traceback. The author introduced an SDN-based IDS That had an accuracy rating of detecting 95.98% when the entire features of the NSL-KDD dataset were employed and achieved an accuracy of 87.74% when sub-features from the NSL-KDD dataset was utilized during the model training.

Kumar *et al.* in [31] proposed a cyberattack detection system for Internet of Medical Things (IoMT) networks based on ensemble learning and fog-cloud architecture. The ensemble design integrated the DT, Naive Bayes, and RF models created by the individual models. The dataset used was ToN-IoT, and the developed model achieved an accuracy of 96.35%.

Atefi *et al.* in [32] proposed IDS depending on the DNN for the DL framework, Binary Algorithm (BA) in terms of Binary Genetic Algorithmic (BGA), Binary Gravitational Searching Algorithm (BGSA), and Binary Bat Algorithm (BBA) as optimizer to increase detection rates. The accuracy of the authors' model, which used the CICIDS2017 dataset, was 99.002%.

Chaganti *et al.* in [17] employed an IDS powered by SDN in IoT networks. The authors employed Long Short-Term Memory (LSTM) to recognize network threats in their introduced approach. The authors trained their model using SDN-IoT and SDN-NF-TJ datasets with an accuracy of 97.1%.

Sabeel *et al.* in [33] proposed ML models for binary classifiers of unidentified DoS/DDoS assaults using DNN and LSTM with dataset CICIDS2017. The performance analysis for the conducted experiments showed that True positive rates for LSTM and DNN were 99.9% and 99.8%, respectively.

Kshirsagar *et al.* in [34] proposed a new technique for reducing the feature selection that was used to classify web attacks. The ensemble approach was founded on data gain, correlation gains ratios, chi-square, and relief. Additionally, the system utilized a J48 classifier with a condensed feature subset for categorizing web attacks. The tested system's trained model had an accuracy score of 99.6191% when evaluated using the CICIDS2017 web-attack dataset.

Said *et al.* in [35] developed a new method using the One-class Support Vector Machines (OC-SVM) and LSTM autoencoder to identify assaults based on anomalies in an unbalanced dataset. The accuracy of 90.5% offered within the InSDN set of data used by the authors gave them considerable confidence in their ability to protect SDN networks against malicious traffic.

Elsayed *et al.* in [36] proposed a CNN method using L2 regularization with a dropout technique to combat the overfitting problem when employing the InSDN dataset. The trained model achieved an accuracy of 93.01%.

Table 1 summarizes the key findings and contributions of relevant studies within the field of securing SDN-based IoT environment. The table concisely overviews the included studies, outlining their datasets, methodologies, and main outcomes.

Table 1. Summary table for recent state-of-the-art-researches in the field of securing SDN-based IoT environment

Ref.	Employed Dataset	Utilized Technique	Model Accuracy
[19]	NSL-KDD	Gain ratio and RF techniques	81.9 %
[20]	CAIDA, KDDCup1999, and UNSW-NB15	SeArch solution	95.5 %
[21]	NSL-KDD	ML approaches such as DT, RF	95.95 %
[22]	NSL-KDD	DNN technique	75.75 %
[23]	Custom dataset	A traffic flow classifier using neural networks (TFC-NN)	96.13 %
[24]	KDD99	CNN	-
[25]	NSL-KDD	DNN and GRU-RNN	80.7 % and 90 %
[26]	CSE-CIC-IDS2018	DL techniques for anomaly detection with three components are Activities track, Activity analyzer, and Classifier, which capture traffic, extract features, reduce features	96.05 %.
[27]	KDD99	The bat algorithm applies binary differentiation mutation, swarm division is chosen for analysis, and it follows up with classification using the weighted random forest.	96.03 %.
[28]	NSL-KDD and UNSW-NB15	Instance-based learning, C4.5 DT, and MLP algorithms are suggested multiclass categorization approaches.	99.00 % and 88.46 %

[29]	Custom dataset	SVM classification algorithms	97 %
Ref.	**Employed Dataset**	**Utilized Technique**	**Model Accuracy**
[30]	NSL-KDD	SVM	87.74 %
[31]	ToN-IoT	Fog-cloud architecture and ensemble learning are the foundations of a cyberattack detecting system for IoMT networks. The decision tree, the Naive Bayes, and the RF models are all integrated into the ensemble design.	96.35 %
[32]	CICIDS2017	DNN as DL platform and BBA, BGA, and BGSA as an optimizer	99.002 %
[17]	SDN-IoT, SDN-NF-TJ	Employing an intrusion detection system powered by SDN in IoT networks, an LSTM-based technique	97.1 %
[33]	CICIDS 2017	ML models for binary estimation of unidentified DoS/DDoS assaults (DNN and LSTM)	The true Positive Rate for DNN is 99.8 %, and True Positive Rate for LSTM is 99.9 %
[34]	CICIDS 2017	A new technique for reducing the feature selection used to classify web attacks	99.6191 %
[35]	InSDN	LSTM autoencoder-based hyper method with One-class support vector machine (OC-SVM)-based attack detection	90.5 %
[36]	InSDN	CNN method using L2 regularization and dropout techniques	93.01 %.

VI. RESULTS AND DISCUSSIONS

In the literature review section, a wide range of studies and scholarly works have been examined pertaining to improving the security in SDN-based IoT environment. The review has revealed several key themes and trends within the existing body of research. One prominent theme is the increasing importance of developing an AI-based technique to detect various attacks that threaten IoT security, as evidenced by the growing number of studies exploring its implications in multiple contexts.

Table 1 demonstrates the employment of various datasets in reviewed works, and Fig. 1 visualizes the statistical analysis that includes 26.3% NSL-KDD, 10.5% KDD99, 5.3% CICIDS, 5.3% CAIDA, 5.3% UNSW-NB15, 5.3% ToN-IoT, 10.5% InSDN, 5.3% SDN-NF-TJ, and SDN- IoT, and 10.5% custom datasets.

It is worth noting from Table 1 that most prior efforts employed analytical data models to identify intrusions into networks in SDN and non-IoT scenarios. In most cases, IoT network traffic and threats were not considered when creating the datasets. Most of those studies used datasets that are not part of the IoT, such as NSL-KDD, KDDCup99, as well as UNSW-NB15 are only a few examples of attack detection and classification network training and evaluation datasets. Since these datasets were originally constructed in a traditional network environment, they do not reflect the majority of recent attack trends. Message Queuing Telemetry Transport Protocol (MQTT) and Advanced Messaging Queuing Protocol (AMQP) datasets generated in the presence of IoT network traffic are necessary for testing and assessing IoT network vulnerabilities. Several research, such as CSE-CIC-IDS2018, SDN-NF-TJ, and SDN-IoT, were proposed in the SDN and IoT network environment and used the non-IoT datasets. These datasets offer academics

invaluable tools for analyzing IoT traffic in SDN settings, learning about the peculiarities of IoT interaction, and creating foolproof security protocols. Researchers can use these datasets to improve the assurances of IoT deployments, identify and counteract attacks, and strengthen SDN-based IoT networks.

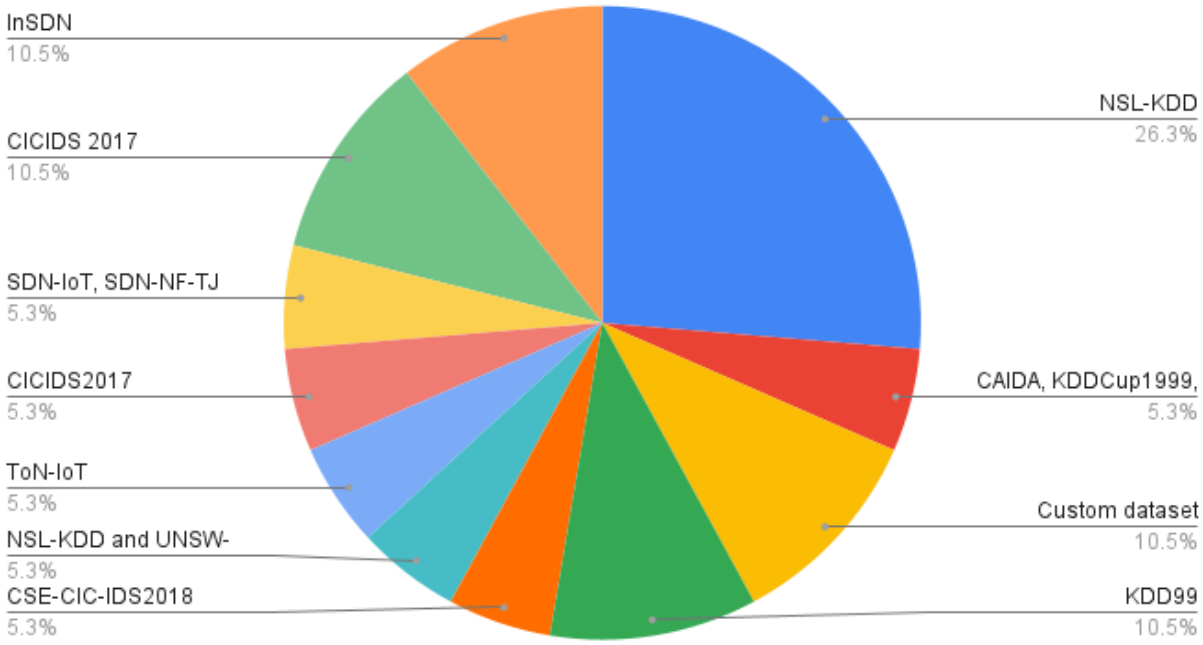

FIG. 1. The percentage of Datasets used from the literature review

In order to resolve the difficulties involved in the practical application of cybersecurity solutions in IoT-SDN networks, more study is necessary. It is essential to handle problems including the necessity for large labeled datasets, technology needs, understanding of models, increasing accuracy, and potential adversarial attackers. DL can play a significant role in assuring the security and reliability of IoT systems within organizations by overcoming these challenges.

Employing public datasets in the context of SDN-based IoT security offers several advantages that contribute to advancing research, promoting collaboration, and facilitating the development of effective security measures. Some of the key benefits include:

- Accessibility and Reproducibility: Public datasets are readily available to researchers, eliminating the need for extensive data collection efforts. Researchers from different institutions or organizations can access and use the same dataset, ensuring the reproducibility of experiments and facilitating the comparison of results. This accessibility promotes transparency and fosters collaboration within the research community.
- Diversity and Real-World Representation: Public datasets often encompass a wide range of IoT traffic captured from diverse sources and environments. This diversity allows researchers to analyze and study different aspects of IoT communication, such as various device types, protocols, and network behaviors. The real-world representation of public datasets helps researchers develop security mechanisms that are robust and adaptable to different deployment scenarios.
- Benchmarking and Comparison: Public datasets provide a benchmark for evaluating the performance of security mechanisms, algorithms, and protocols. Researchers can use the same dataset to compare the effectiveness of different approaches, enabling a standardized evaluation process. This benchmarking helps identify best practices and facilitates the development of more reliable and efficient security measures.
- Validation and Generalization: Public datasets enable researchers to validate their findings and conclusions on a larger scale. Researchers can verify the generalizability of their approaches by testing and validating security mechanisms on diverse datasets collected from different sources. This validation ensures that the proposed security measures are not overly specific to a particular dataset or scenario, but rather have broader applicability.

On the other hand, employing custom datasets in the context of SDN-based IoT security offers several advantages that enhance the effectiveness of security mechanisms and improve overall system resilience. Some of the key benefits include:

- Realistic Representation: Custom datasets allow for the collection and generation of real-world IoT traffic, capturing IoT devices' diverse behavior and communication patterns in an SDN environment. By reflecting the actual characteristics of IoT traffic, custom datasets provide a more accurate representation of the challenges and complexities of securing SDN-based IoT deployments.
- Tailored Evaluation: Custom datasets can be designed to address specific research questions or security concerns. Researchers can focus on particular aspects of IoT traffic, such as device-to-device communication, control messages, or sensor data transmission, enabling a targeted evaluation of security mechanisms. This tailored approach allows a deeper understanding of the security requirements and potential vulnerabilities specific to the SDN-based IoT environment.

- Anomaly Detection and Intrusion Detection: Custom datasets facilitate developing and evaluating anomaly detection and intrusion detection systems tailored to SDN-based IoT environments. By training algorithms on custom datasets that capture normal and anomalous network behavior, researchers can improve the accuracy and reliability of these systems. This enables early detection and response to potential security threats and enhances the overall security posture of SDN-based IoT networks.

VII. CONCLUSION

This paper has comprehensively analyzed cyber-attacks in SDN-based IoT environments, shedding light on the evolving threat landscape and the potential risks associated with this convergence. By exploring various attack vectors, vulnerabilities, and their implications, this study highlights the urgent need for robust security measures to safeguard SDN-based IoT deployments. The findings of this research underscore the importance of understanding the unique characteristics and complexities of SDN-based IoT environments to mitigate cyber threats effectively. By naming and critiquing common attack methods, including denial-of-service, distributed denial-of-service, port scanning, operating system fingerprinting, and fuzzing, this paper emphasizes the critical need for organizations to implement comprehensive security measures at both the device and network levels.

Furthermore, this study highlights the potential impact of cyber-attacks on network performance, data integrity, and user privacy. The risks associated with unauthorized access, data breaches, and manipulation of IoT devices and services are strong reminders of the vulnerabilities within SDN-based IoT environments.

REFERENCES

[1] İ. Kök, F. Y. Okay, Ö. Muyanlı and S. Özdemir, "Explainable Artificial Intelligence (XAI) for Internet of Things: A Survey," in *IEEE Internet of Things Journal*, vol. 10, no. 16, pp. 14764-14779, August, 2023.

[2] S. He, K. Shi, C. Liu, B. Guo, J. Chen and Z. Shi, "Collaborative Sensing in Internet of Things: A Comprehensive Survey," in *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1435-1474, Thirdquarter 2022.

[3] S. Vashi, J. Ram, J. Modi, S. Verma and C. Prakash, "Internet of Things (IoT): A vision, architectural elements, and security issues," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, 2017, pp. 492-496.

[4] M. Kavre, A. Gadekar and Y. Gadhade, "Internet of Things (IoT): A Survey," in *2019 IEEE Pune Section International Conference (PuneCon)*, Pune, India, 2019, pp. 1-6.

[5] K. Singh and D. S. Tomar, "Architecture, Enabling Technologies, Security and Privacy, and Applications of Internet of Things: A Survey," in *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on*, Palladam, India, 2018, pp. 642-646.

[6] A. Khanna and S. Kaur, "Internet of Things (IoT), Applications and Challenges: A Comprehensive Review," in *Wireless Personal Communications*, vol. 114, no. 2., pp. 1687–1762, May, 2020.

[7] A. Abdullah, R. Hamad, M. Abdulrahman, H. Moala, and S. Elkhediri, "CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques," in *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, 2019, pp. 1–6.

[8] M. Elbediwy, B. Pontikakis, J. -P. David and Y. Savaria, "A Hardware Architecture of a Dynamic Ranking Packet Scheduler for Programmable Network Devices," in *IEEE Access*, vol. 11, pp. 61422-61436, 2023.

[9] J. Chen, Y. Wang, M. Ye and Q. Jiang, "A Secure Cloud-Edge Collaborative Fault-Tolerant Storage Scheme and Its Data Writing Optimization," in *IEEE Access*, vol. 11, pp. 66506-66521, 2023.

[10] D. Javeed, T. Gao, and M. T. Khan, "SDN-Enabled Hybrid DL-Driven Framework for the Detection of Emerging Cyber Threats in IoT," in *Electronics*, vol. 10, no. 8, p. 918, Apr. 2021.

[11] H. Ahmadvand, C. Lal, H. Hemmati, M. Sookhak and M. Conti, "Privacy-Preserving and Security in SDN-Based IoT: A Survey," in *IEEE Access*, vol. 11, pp. 44772-44786, 2023.

[12] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," in *IEEE Access*, vol. 7, pp. 82721-82743, 2019.

[13] R. W. Anwar, A. Zainal, T. Abdullah, and S. Iqbal, "Security Threats and Challenges to IoT and its Applications: A Review," in *2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*, 2020, pp. 301–305.

[14] R. A. Elsayed, R. A. Hamada, M. I. Abdalla, and S. A. Elsaid, "Securing IoT and SDN Systems Using Deep-Learning Based Automatic Intrusion Detection," in *Ain Shams Engineering Journal*, vol. 14, no. 10., pp. 102211, October, 2023.

[15] A. K. Sarica and P. Angin, "Explainable Security in SDN-Based IoT Networks," in *Sensors*, vol. 20, no. 24, p. 7326, Dec. 2020.

[16] R. I. Mukhamediev *et al.*, "Review of Artificial Intelligence and Machine Learning Technologies: Classification, Restrictions, Opportunities and Challenges," *Mathematics*, vol. 10, no. 15, p. 2552, Jul. 2022.

[17] R. Chaganti, W. Suliman, V. Ravi, and A. Dua, "Deep Learning Approach for SDN-Enabled Intrusion Detection System in IoT Networks," *Information*, vol. 14, no. 1, p. 41, Jan. 2023.

[18] D. Javeed, T. Gao, M. T. Khan, and I. Ahmad, "A Hybrid Deep Learning-Driven SDN Enabled Mechanism for Secure

Communication in Internet of Things (IoT)," *Sensors*, vol. 21, no. 14, p. 4884, Jul. 2021.

[19] S. K. Dey, Md. Raihan Uddin, and Md. Mahbubur Rahman, "Performance Analysis of SDN-Based Intrusion Detection Model with Feature Selection Approach," in *Proceedings of International Joint Conference on Computational Intelligence*, 2019, pp. 483–494.

[20] T. G. Nguyen, T. V. Phan, B. T. Nguyen, C. So-In, Z. A. Baig and S. Sanguanpong, "SeArch: A Collaborative and Intelligent NIDS Architecture for SDN-Based Cloud IoT Networks," in *IEEE Access*, vol. 7, pp. 107678-107694, 2019.

[21] A. O. Alzahrani and M. J. F. Alenazi, "Designing a Network Intrusion Detection System Based on Machine Learning for Software Defined Networks," in *Future Internet*, vol. 13, no. 5, p. 111, April 2021.

[22] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi and M. Ghogho, "Deep learning approach for Network Intrusion Detection in Software Defined Networking," in *2016 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, 2016, pp. 258-263.

[23] O. Hannache and M. Batouche, "Neural Network-Based Approach for Detection and Mitigation of DDoS Attacks in SDN Environments," in *International Journal of Information Security and Privacy*, vol. 14, pp. 50–71, 2020.

[24] Y. Hande and A. Muddana, "Intrusion Detection System Using Deep Learning for Software Defined Networks (SDN)," in *2019 International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 2019, pp. 1014-1018.

[25] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, M. Ghogho, and F. El Moussa, "DeepIDS: Deep Learning Approach for Intrusion Detection in Software Defined Networking," in *Electronics*, vol. 9, no. 9, p. 1533, Sep. 2020.

[26] A. Wani, R. S, and R. Khaliq, "SDN- based intrusion detection system for IoT using deep learning classifier (IDSIoT- SDL)," in *CAAI Transactions on Intelligence Technology*, vol. 6, no. 3, pp. 281–290, March, 2021.

[27] J. Li, Z. Zhao, R. Li and H. Zhang, "AI-Based Two-Stage Intrusion Detection for Software Defined IoT Networks," in *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2093-2102, April, 2019.

[28] Q. Tian, D. Han, M.-Y. Hsieh, K.-C. Li, and A. Castiglione, "A Two-Stage Intrusion Detection Approach for Software-Defined IoT Networks," in *Soft Computing*, vol. 25, no. 16, pp. 10935–10951, April, 2021.

[29] J. Ye, X. Cheng, J. Zhu, L. Feng, and L. Song, "A DDoS Attack Detection Method Based on SVM in Software Defined Network," in *Security and Communication Networks*, vol. 2018, pp. 1–8, 2018.

[30] P. Hadem, D. K. Saikia, and S. Moulik, "An SDN-Based Intrusion Detection System Using SVM with Selective Logging for IP Traceback," in *Computer Networks*, vol. 191, pp. 108015, May 2021.

[31] P. Kumar, G. P. Gupta, and R. Tripathi, "An Ensemble Learning and Fog-Cloud Architecture-Driven Cyber-Attack Detection Framework for IoMT Networks," in *Computer Communications*, vol. 166, pp. 110–124, January, 2021.

[32] K. Atefi, H. Hashim and T. Khodadadi, "A Hybrid Anomaly Classification with Deep Learning (DL) and Binary Algorithms (BA) as Optimizer in the Intrusion Detection System (IDS)," in *2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA)*, 2020, pp. 29-34.

[33] U. Sabeel, S. S. Heydari, H. Mohanka, Y. Bendhaou, K. Elgazzar and K. El-Khatib, "Evaluation of Deep Learning in Detecting Unknown Network Attacks," in *2019 International Conference on Smart Applications, Communications and Networking (SmartNets)*, 2019, pp. 1-6.

[34] D. Kshirsagar and S. Kumar, "An ensemble feature reduction method for web-attack detection," in *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 23, no. 1, pp. 283–291, January, 2020.

[35] M. Said Elsayed, N.-A. Le-Khac, S. Dev, and A. D. Jurcut, "Network Anomaly Detection Using LSTM Based Autoencoder," in *Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, November, 2020, pp. 37–45.

[36] M. S. Elsayed, H. Z. Jahromi, M. M. Nazir, and A. D. Jurcut, "The Role of CNN for Intrusion Detection Systems: An Improved CNN Learning Approach for SDNs," in *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp. 91–104, 2021.