International Journal of Business Quantitative Economics and Applied Management Research
Volume-7, Issue-1, 2021 ISSN No: 2349-5677

SOFTWARE DEFINED NETWORKING IN IOT: SCOPING STUDY IN CONTEST TO THE SECURITY FACTORS CONNECTED TO THESE SYSTEMS

Tharunika Sridhar
Azure for Operators
Microsoft, Texas, USA
sridhar.tharunika@gmail.com

Abstract

The research will critically evaluate and analyze the security capabilities of ML and DL models in SDN, especially in heterogeneous IoT networks. Traditional measurements of cybersecurity are no longer adequate for protecting IoT systems due to their increasing size and complexity. This research explores how ML and DL models can be used to enhance the security of IoT networks through the integration of SDN flexibility with AI-based cybersecurity solutions. The best performing ML models for traffic pattern classification and known anomalies in medium-scale networks are SVM, KNN, and Isolation Forest. DL models, especially Deep Neural Networks, learn complex features and adapt to changing threats in large dynamic networks. Although there are many advantages that can be attributed to these models, they still face some problems and challenges. One of the challenges is that it is too resource-intensive for any model; the problem of scalability is tough, and it is extremely prone to overfitting. The study has concluded that this combination model of ML-DL is of significant improvement compared to related anomaly detection as well as real-time mitigation. It is a model making the IoT network more secure and adaptive for complex threats. Future developments in such models will target them to be more adaptive, resource-friendly, and resistant to overfitting to ensure them to be more stable and deployable in SDN-based IoT security frameworks.

IndexTerms—SDN network, SDN cyber risks, IoT cyber risks, ML cyber protection, DL cyber protection, cyber protection standard IoT

I. INTRODUCTION

Internet-connected devices that interact autonomously without human interaction developed the Internet of Things. Kevin Ashton introduced it 17 years ago, and the second digital revolution relies on it [1]. IoT applications encompass home and building automation, smart industries, smart cities, smart health, intelligent traffic management, health monitoring, emergency and surveillance services, retail, and supply chain management [2]. Researching its technology improves it. Previously, 83 billion IoT devices were expected by 2024.

International Journal of Business Quantitative Economics and Applied Management Research
Volume-7, Issue-1, 2021 ISSN No: 2349-5677

The vendor's proprietary interface configures these devices' complicated routing topologies, making real-time adjustments impossible. Programmability is limited by devices, necessitating several rules to optimize network services. IoT and its applications required a new network design for QoS. Traditional networking was limited, thus SDN was established. A programmable network separated network control logic from data transmission components [3].
Software-defined networking (SDN) uses software-based controllers or APIs to manage traffic with the hardware infrastructure. This architecture differs from typical networks, which use switches and routers to control traffic. SDN controller software builds and manages virtual networks and hardware [4]. Forwarding devices were freed from control and focused on guiding traffic flows according to control logic judgments. This has improved network administration, flexibility, and innovation. SDN autonomous reconfiguration is expected to enable several new technologies, including IoT [5]. General SDN architecture is given below in Figure 1.
The SDN architecture as described by [6] can be divided into three layers: the infrastructure layer or data plane, which will handle data forwarding and monitoring; the control layer, also known as the control plane, that programs and manages the data plane using southbound interfaces like OpenFlow; and the application layer, where network applications enable features such as security and manageability through guidance to the control layer using northbound interfaces. This framework allows for a centrally designed and programmable network.
This growth shows SD-IoT applications' continued innovation and future potential. However, as a resource-constrained device, the 'things' might be a prime target for contemporary attack vectors like DoS, Fuzzing, DDoS, OS Fingerprinting, and Port Scanning. Attacks on SD-IoT devices are increasing. A security provider reported 100 million IoT attacks in the first half of 2019.

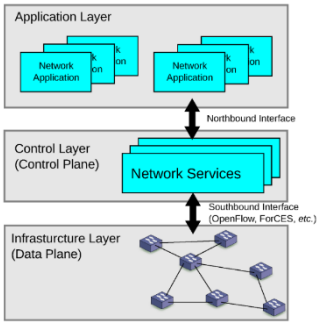

Figure 1: Architecture of Software defined network [6]

Attacks on SD-IoT applications and servers could destroy the application environment and prevent genuine users from enjoying the service. Scalability, integrity, intrusion detection, and prevention make SD-IoT security solutions difficult to implement [7].
In order to detect, investigate, and mitigate security threats in their real contexts, researchers have suggested many security solutions for SDN planes. Celesova et al. presented a potential solution to reduce the impact of DoS and DDoS attacks in SDN systems by using machine learning technologies [8]. Recent studies on SDN cyber security have examined several cutting-

edge methods. These include employing deep learning and machine learning to detect and mitigate DDoS and DoS assault s [9].

At this point, this research seeks to conduct an analysis and evidence-based evaluation of the security capabilities of these two models and their potential for developing more flexible and secure SDN models in the future. Specifically, SDNs function as controllers in heterogeneous IoT networks, which are particularly vulnerable to cyber attack threats in the absence of robust and multi-layered cybersecurity measures. This research endeavours to enhance the secure IoT networking environment through the integration of SDN flexibility and the establishment of standardized AI based cyber risk protection solutions.

II. RELATED WORK

We start by critically reviewing the available scholarly papers written about cybersecurity issues in SDN and IoT systems and the role of preventive technologies, particularly deep learning and ML models. From the analyses presented based on papers regarding SDN, ML, and security frameworks of IoT, it is quite evident that there are impressive developments taking place while focusing on improving the usefulness and security of IoT networks. For example, in SDN, network configurations can be dynamic and flexible. ML algorithms such as the Random Forest and Support Vector Machines (SVM) are always being used for intrusion detection and mitigation within IoT networks. Coordination of IoT systems in this direction is through safety and, therefore, by blockchains of SDN.

This is an area that has been widely discussed and covered over recent years by edge, fog, and cloud computing technologies. Notably, such integrations have been studied by researchers like [1] and [7] while discovering the possibility of SDN-ML solutions in solving IoT network security. These articles have, as its critical requirement, considered a machine learning approach toward detecting abnormal behaviors and attacks. Such approaches appear to be particularly more important for anomaly detection systems, as discussed by [11]. [7], for example discussed the use of SVM for the detection of DDoS attacks on the SDN controller based on time attack patterns and installing flows in switches to mitigate the impact of the attack reduced the effects of the attack on the Ryu controller by 36% in a simulated tree network topology – A machine learning method.

Currently, the SDN with ML-integrated protocols in IoT models are not standardized yet; this is the limiting factor in terms of interoperability and widespread acceptance. Formulation of a global standard to harmonize and align data formats, communication methods, and security measures would be part of future work, according to [12] and [8]. More research works are required to be carried out to check if the SDN-ML solutions may be adaptable for various IoT applications, even industrial and health-scenario setups. This would include developing adaptive models of machine learning that may learn to adapt to the changing real-time variability of network conditions and the behavior of IoT devices, as proposed by [11] and [7].

The third issue is the legitimacy of IoT devices. To prevent spoofing and other identity theft threats, the current methodologies have further verification. In this research area, [13] and [14] proposed hybrid methodologies where authentication of IoT devices are combined with SDN

and blockchain techniques. The fourth challenge is scalability because the current SDN-ML frameworks are not designed to handle the large amount of traffic produced in an environment containing numerous IoT devices used for edge and mobile computing. Scalable and low-latency technologies for high volumes of data are key recommendations for future research as proposed by [15] and [10].

The last fundamental problem is ensuring compatibility with legacy IoT systems. Most of the solutions designed recently using SDN and ML bring significant interoperability issues when relating them to existing infrastructure. Hybrid systems in which characteristics of both traditional and next-generation networks are integrated can significantly improve the flexibility of the entire IoT security framework, as highlighted by [16] and [8]. These mentioned limitations can be removed or improved to heighten the efficiency and reliability of SDN-ML-based security frameworks in IoT networks.

III. LIMITATION

All the reviewed studies on SDN and ML applications for IoT security show promising advancements but also point to various research gaps in standardization, flexibility, authenticity, scalability, and compatibility. These gaps will be critical in enhancing the usability, security, and reliability of IoT networks.

With the exponential growth of IoT networks, it is a highly critical challenge in terms of security because of the growing vulnerabilities of connected devices. In SDN, traditional cybersecurity measures mostly fail to provide adequate solutions because IoT systems are dynamic and generally more complex than its predecessors. Thus, the research seeks to conduct an evidence-based analytical and exploratory study on integrating ML and DL models for cybersecurity in architectures based on SDN [16]. This promise has more to do with improved internet safety, compatibility, and scalability, allowing the construction of IoT networks that are more secure, adaptable, and effective at managing the scope and complexity of modern IoT applications

IV. METHODS AND TOOLS

This research is planned and developed by means of secondary resources where it assesses AI-based cybersecurity solutions for enhancement of the SDN model and security of IoT networks. The secondary resources are collected from recognized research journals, like IEEE, Elsevier, Science Direct, Semantic Scholar and other institute recognized journals. Time period of study is chosen up to till 2021. The study adopts exploratory and evidence-based analytical framework to justify the research objectives and establish the proposed goals. The present study integrates the collected resources and evaluates AI's ability, particularly the ML and Deep Learning based systems in enhancing the flexibility and scalability of SDN, security against cyber attacks, and issues such as standardization, interoperability, and integration with legacy IoT systems. Against this massive research background, we will provide evidence-based insights and

recommendations to design stronger, scalable, and secure models for SDN to protect IoT networks from future cyber security risks.

V. RESULTS AND DISCUSSION

This study is divided in segments, where the first segment provides an overview on the cyber attack vulnerabilities present in IoT networks, scope of ML and DL based cyber protection system and advantages of SDN based model to improve network security against frequent cyber attacks. Succeeding segments discuss on the individual ML and DL models analysis and assessment, their scope with SDN and lastly a comparative assessment of both the AI based cyber security models of IoT associating their advantages and scope with SDN networks in terms of building a standard, safe and reliable network model.

A.Overview of Cyber threats in IoT networks, scope of ML and DL based models and advantages of integrating SDN in IoT networks

Agreeing to the findings of [17], we consider cyber threats as prevalent and common in various layers and functional segments of IoT.

Geo Location and Physical Security	Communication Technology & Topology	Centralized or Distributed Network	Network Segmentation	Network Virtualization
- Device Capture	- Eavesdropping	- Malware Attacks	- DoS Attacks	- Unauthorized Access to the Network
- Timing Attacks & Hardware Exploitation	- Node Cloning/Replication	- Storage Attacks	- Device Compromise	- Unauthorized Access to Devices (over IP)
- Node Cloning	- ID Spoofing and Masquerading Attack	- Unauthorized Data Sharing	- Unauthorized Access to the Network	- DoS Attacks
- Node Tampering	- **DoS Attacks**: - Collision Attack - Channel Congestion Attack - CSMA Exploitation - PANId Conflicts	- Disclosure of Private/Sensitive Data		- DDoS Attacks (IoT Botnets)
- Semi-invasive & Invasive Intrusion	- MITM (Man-in-the-Middle) Attacks	- Threats to User Privacy		
	- **Routing Attacks**: - Selective Forwarding - Sybil Attack - Wormhole Attack - Blackhole Attack	- Data Manipulation		
		- DoS Attacks (Hardware Compromise/Malfunction)		

Figure 2: Cyber Threats prevalent and commonly present in IoT [18]

It is currently recognized that unsecured IoT devices IoT segments susceptible to cyber attack include geographic placement and the physical security of devices. Depending on infrastructure criticality and data sensitiveness, vulnerabilities occur within the systems. Communication protocol and network topology are affected because frequency hopping or spread spectrum may mitigate against wireless channel jamming. Centralized versus distributed network control, network segmentation, and security measures with virtualization are some of the integral aspects in countering IoT-specific attacks. These measures are shaped according to the type and scale of threats that generally characterize the different layers of the architecture of IoT [18].

Table below shows the layer wise cyber threat vulnerabilities present in IoT network.

TABLE I. LAYERWISE CYBER THREAT VULNERABILITIES PRESENT IN IOT NETWORK

IoT Layer	Cyber Attack	Description
Perception Layer	**Botnets**	Devices get infected by malware (e.g., Mirai), turning them into bots. These bots attack a target server when controlled by a botmaster.
	Sleep Deprivation Attack	Targets battery-powered sensor nodes and devices, forcing them to stay awake, depleting their energy and causing performance issues.
	Node Tampering and Jamming	**Node Tampering**: Attackers alter sensitive data (e.g., routing tables, cryptographic keys). **Jamming**: Interfering with radio frequencies to disrupt wireless sensors.
	Eavesdropping	Attackers intercept and listen to private communications or data transmissions, threatening data confidentiality.
Network Layer	**Man-in-the-Middle (MiTM)**	The attacker intercepts communication between two devices, posing as one of the devices to access or manipulate data.
	Denial of Service (DoS)	Attackers flood IoT devices with numerous pointless requests, overwhelming the system and preventing legitimate access.

IoT Layer	Cyber Attack	Description
	Routing Attacks	Malicious nodes interfere with routing functionality, either blocking it or launching DoS attacks to disrupt network traffic.
Middleware Layer	**Middleware Attacks**	Attacks target the middleware components, which handle communication between devices. Common attacks include cloud-based attacks and breaches of authentication/signature packaging.

Machine learning-based models have arisen as a countermeasure against cyber attacks in the Internet of Things (IoT) ecosystem, and the integration of deep learning and machine learning methodologies constitutes a noteworthy advancement that necessitates meticulous evaluation. Research findings demonstrate that machine learning and deep learning approaches are key catalysts for automation in knowledge work, therefore influencing economic impact. Recent technology breakthroughs are significantly altering our planet. By 2025, we anticipate an estimated yearly economic impact of $5.2–$6.7 trillion from the automation of intellectual labor [19].

The table below shows, we provide the scope of ML and DL based cyber security protection system in IoT network model and advantages of SDN integration.

TABLE II. ML AND DL BASED CYBER SECURITY PROTECTION SYSTEM IN IOT NETWORK MODEL

Security Feature	Use of ML/DL	Limitations	Scope	Advantages of Integrating SDN & AI
Intrusion Detection and Prevention (IDPS)	ML algorithms analyze network traffic, logs, and device data to detect known attacks or suspicious activity.	Limited by false positives/negatives and inability to detect zero-day attacks.	Essential for detecting unauthorized access, malicious activities, and network anomalies.	SDN enhances centralized control, allowing better traffic management and quicker detection and mitigation.
Anomaly Detection	ML models learn device and network behavior	Needs a large dataset for training; struggles with	Effective for dynamic and real-time	AI integration allows for real-time anomaly

Security Feature	Use of ML/DL	Limitations	Scope	Advantages of Integrating SDN & AI
	to identify deviations that signal security breaches.	detecting novel or evolving threats.	network environments, particularly IoT.	detection, enhancing flexibility in a rapidly changing network.
Threat Intelligence and Prediction	ML models analyze big security data to predict potential attack pathways and vulnerabilities.	Prediction accuracy depends on the quality of training data; risks of overfitting or underfitting.	Helps in preemptively identifying emerging threats, improving proactive security strategies.	SDN enables dynamic updates to network policies based on AI-driven insights, improving proactive defense.
Firmware and Software Vulnerability Analysis	ML analyzes firmware/software for vulnerabilities, identifying weaknesses before deployment.	Limited to known vulnerabilities; may miss newly discovered flaws.	Enhances IoT device security by addressing vulnerabilities in firmware and software.	AI-based systems in SDN help ensure the secure deployment of patches across a wide network.
Behavior-based Authentication	ML models develop behavioral profiles for IoT devices and users, triggering alerts for suspicious activity.	Can be circumvented by attackers mimicking legitimate behavior or using stolen credentials.	Useful in securing sensitive IoT applications by enforcing additional authentication based on device behavior.	SDN offers centralized management, providing scalable authentication mechanisms for diverse IoT devices.
Data Privacy and Encryption	ML supports encryption techniques, like homomorphic encryption, and data anonymization to protect privacy.	Computationally intensive; may not be suitable for low-power IoT devices.	Ensures that sensitive IoT data remains secure even when processed or transmitted.	AI in SDN can help manage encrypted data flows, improving both performance and security in IoT

Security Feature	Use of ML/DL	Limitations	Scope	Advantages of Integrating SDN & AI
				environments.
SDN and AI Integration for Network Management	AI optimizes SDN controllers for better traffic flow and intrusion management in real-time.	Complex integration process; requires high-performance hardware and infrastructure.	Improves overall network security by providing centralized control and dynamic traffic management.	SDN provides the flexibility needed for AI models to adapt to real-time threats, optimizing IoT network security.
Network Function Virtualization (NFV)	NFV works with ML to deploy on-demand security functions, like firewalls and IDS, based on network traffic.	Complexity in scaling virtualized network functions for large IoT environments.	Scalable and adaptable, providing virtualized security components that can be deployed as needed.	SDN's centralized nature allows rapid deployment and management of virtualized security functions.

B. Assessment of ML Model in Cyber Security of IoT Network and its scope with SDN model

From the insights of the review of literature that we've presented, dynamic and efficient strategy for addressing escalating security Issues in the IoT can be resolved by adding machine learning with the SDN in the IoT security frameworks. This is a dynamic approach that takes on an increasingly efficient form for fighting escalated security concerns in the IoT ecosystem. A strategy using the ML technique is one that combines Network Function Virtualization (NFV) with SDN for enhanced enforcement and orchestration. Note that NFV and SDN are two complementary networking technology where SDN control the traffic routing and NFV virtualizes the network functioning. The system has closed-loop threat detection, monitoring, and prevention capabilities.

Thus, we consider that Machine learning (ML) significantly plays a central role in enhancing the efficiency of VNF-SDN toward anomaly detection and classification. To analyse and assess in details, we examine the performance of the ML integrated VNF-SDN model presented by [20]. The integration of ML with the SDN-NFV model helps to keep track of traffic, detect anomalies, and mitigate threats. The methods used by supervised, unsupervised, and reinforcement

learning ensure that accurate detection of anomalies occurs in case of network behavior, either as it is normal or anomalous, by using features from traffic stream, data transformation for analysis, and model training between these two. The end result is a system handling overload conditions and providing optimized security management without interference from humans.
Given below is the architecture of SDN-NFV network controller that acts as the initial anomaly detection and identifier as designed in the model. The architecture shows the ML integration stage in the model:

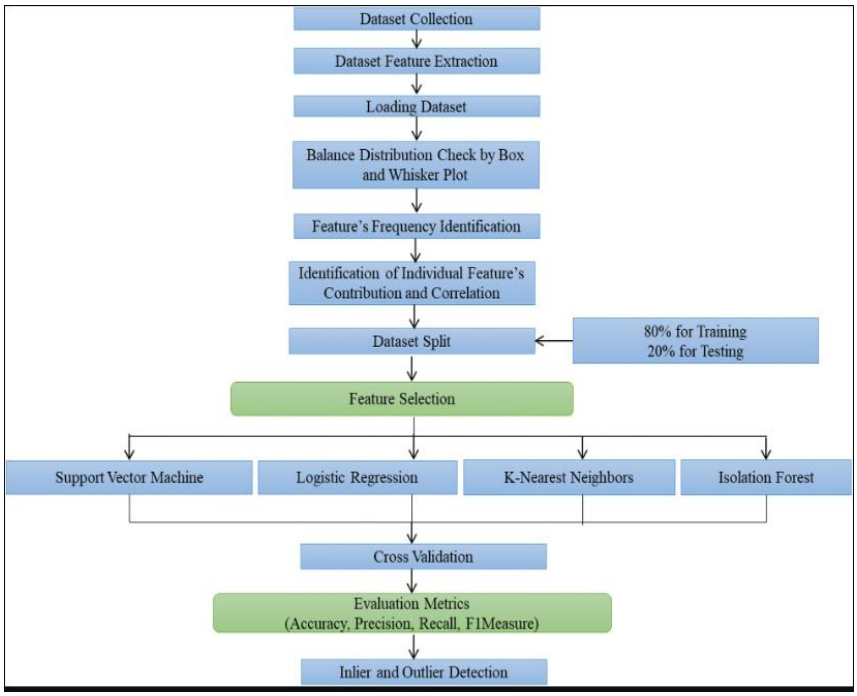

Figure 3: SDN-NFV network traffic controlling model architecture integrated with ML classifier [20]

The diagram below shows the ML classifier functionality in cyber attack anomaly detection. In the model, the authors have confirmed the ML integrated SDN model to be capable to detect anomalous behavior, utilizing traffic patterns real-time for ensuring security, as well as efficiency of the virtualized network environment. Above all, attacks become sophisticated with time like HTTP Flood, UDP Flood, Smurf Flood, or SiDDoS Flood.

International Journal of Business Quantitative Economics and Applied Management Research
Volume-7, Issue-1, 2021 ISSN No: 2349-5677

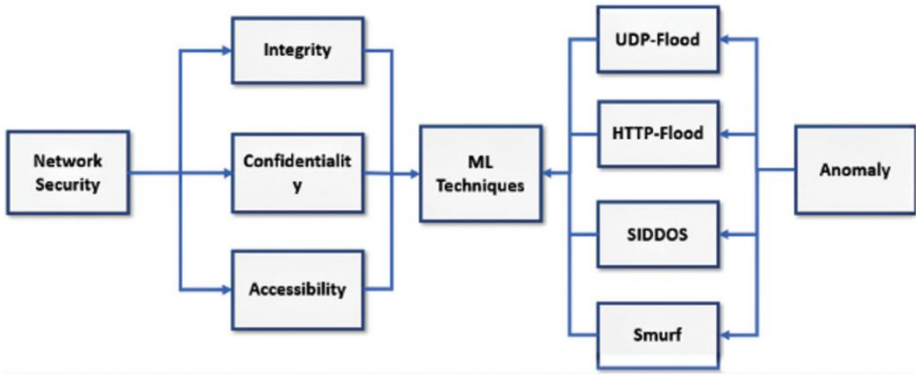

Figure 4: ML classifier of SDN-NFV network traffic control model used for cyber attack classifier [20]

From the outcome of anomaly detection and classification performance of the SDN model enhanced with ML classifier, we present the scope of ML in SDN network anomaly identification as:

Feature	Scope in SDN based Network Model
Traffic Monitoring	Capturing and preprocessing traffic at multiple levels to detect anomalies in the NFV component.
Anomaly Detection	Identifying traffic irregularities using classifiers such as SVM, KNN, Logistic Regression, and Isolation Forest.
Classification	Categorizing network traffic into normal or anomalous classes to identify specific attack types.
Data Transformation	Preparing multiclass data using encoding techniques for efficient processing by ML models.
Model Training	Employing cross-validation and feature selection to optimize ML classifiers for accurate detection.
Real-Time Decision Making	Analyzing VNF-level and network-level traffic to mitigate overload conditions and maintain stability.
Mitigation Strategies	Reacting to anomalies by adjusting traffic flow or invoking network-wide measures for comprehensive mitigation.

C. Assessment of DL Model in Cyber Security of IoT Network and its scope with SDN model

DL greatly enhances the detection of cyber threats in SDN-based networks by automatically learning complex patterns and features from raw data. In this comparative assessment of SDN enhancements and improvement in its efficacy in terms of security, we examine the functioning of a DNN model as proposed by [21].

The model is designed with multi-layered structure, processes traffic data for real-time anomaly detection, thus ensuring higher accuracy and efficient threat management. DL can deal with complex and constantly developing attack patterns like DoS, R2L, U2R, and Probe attacks as opposed to traditional methods of machine learning since DL finds abstract and hierarchical representations of features. Through this SDN controller integration with DNN, it monitors at the granular level for the traffic going through a system and adapts according to threats by changing the flow rules using OpenFlow protocol. This will lead towards strong intrusion detection and mitigation techniques while making it even safer and more stable in terms of the SDN environment.

Examining the functionality and performance of deep learning anomaly detection component in the SDN model, we provide the table of DL features and scope in the SDN network:

Deep Learning Feature	Scope in SDN-Based Network Model
Feature Extraction	Automatically discovers hierarchical and abstract features from raw traffic data (e.g., duration, src_bytes).
Anomaly Detection	Identifies abnormal patterns using selected features to differentiate between normal and malicious traffic.
Traffic Classification	Classifies traffic into normal or anomalous categories with high precision, recall, and F1-score.
Real-Time Monitoring	Monitors and analyzes real-time network statistics provided by OpenFlow switches.
Adaptability	Learns and adapts to new attack patterns with a minimal set of input features for generalization.
Scalability	Effectively handles large-scale traffic data in SDN environments, ensuring low latency in detection.

International Journal of Business Quantitative Economics and Applied Management Research
Volume-7, Issue-1, 2021 ISSN No: 2349-5677

Deep Learning Feature	Scope in SDN-Based Network Model
Intrusion Mitigation	Dynamically modifies flow rules and propagates security policies to OpenFlow switches to neutralize threats.
Performance Optimization	Utilizes hyperparameters like learning rate and epochs to maximize accuracy and minimize loss during training.

The SDN architecture where DL based anomaly detection component is integrated in this examined model is given below:

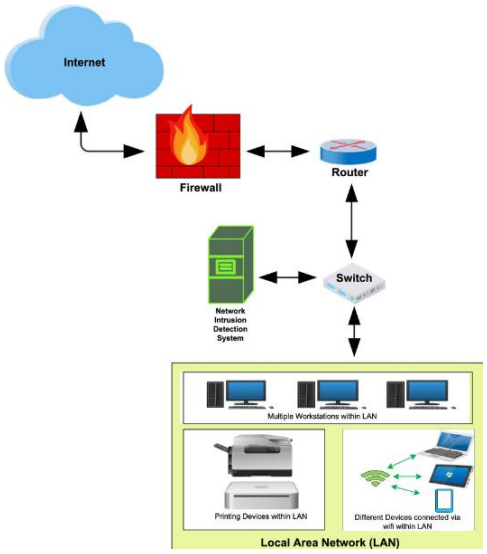

Figure 5: The SDN Network Architecture where DL anomaly detection component in integrated [22]

D. Comparative Assessment of ML and DL cyber protection models and their scope with SDN model

To our understanding through the study outcome, we feel that Machine Learning (ML) [20] and Deep Learning (DL) [21] models are most important in the context of SDN integrated with NFV for improving security through the detection of anomalies. However, both models have unique capabilities; ML is used majorly for classifying traffic pattern, while DL allows for an automatic learning of complex features to capture more sophisticated attacks. An evaluation of ML and DL model in SDN networks is provided herein, which includes their advantages and disadvantages as well as its future potential.

The most popular ML models used for anomaly detection in SDN networks include SVM, KNN, and Isolation Forest. These models classify network traffic as normal or anomalous according to the extracted features. It performs well when the attack patterns are known; in such cases, it will detect quickly and perform efficient security management in medium-scale networks. The advantages of ML models are the simplicity of models, rapid detection of known anomalies, and ease of deployment. However, they are not effective in handling new or complex attack types and require careful feature selection and preprocessing, which is very resource-intensive.

DL models, especially DNNs, automatically learn hierarchical patterns from raw traffic data. They can then detect DoS, R2L, and U2R attacks, which tend to be more complex and mutating. DL models can automatically handle large-scale networks while adapting to new attack patterns without human intervention. Their strong advantage is scalability and adaptability, generalizing to previously unforeseen threats. However, DL models are very resource-intensive and training is slow. And they tend to overfit more readily, especially where the training data are incomplete.

ML models bloom well with monitoring and traffic classification in less complex SDNs with well-defined attack patterns. They quickly detect anomalies; adjustment of flow can alleviate overloaded conditions. They will have difficulties more in more dynamic and highly complex environments with changing attack patterns. DL models, however, are great in large complex networks, automatically discovering features from raw data and adapting to new threats. They have the ability to scale and learn continuously, which is ideal for networks that have to face sophisticated, ever-evolving cyber threats.

For ML, increasing adaptability to new attacks and automatically generating features would improve performance. For DL, lowering the computational requirements and increasing generalization to avoid overfitting are the areas to improve. Both models could improve with more efficient training and better resource management to enhance real-time deployment in SDN networks.

VI. CONCLUSION

In this research, based on the outcome and performance assessments of the two models, we can infer that integration of ML and DL models in the SDN-NFV framework enhances the security of the networks by a large margin due to the significant improvement in anomaly detection and mitigation. ML is efficient in small, static networks with defined patterns of attacks; however, DL is good for larger dynamic networks with changing threats. The systems in SDN-NFV can benefit from the advantages of both the models for robust and real-time detection and response. The future improvements of this model include scaling up and real-time detection with further integration into the IoT security framework. These models will subsequently help fortify network security through some improvement in risk areas, such as data integrity and overfitting, and reducing false positives while supporting proactive security policies.

REFERENCES

1. R. Ande, B. Adebisi, M. Hammoudeh, and J. Saleem, "Internet of Things: Evolution and technologies from a security perspective," *Sustainable Cities and Society*, vol. 54, p. 101728, Mar. 2020, doi: https://doi.org/10.1016/j.scs.2019.101728 Available: https://www.sciencedirect.com/science/article/abs/pii/S2210670719303725?via%3Dihub
2. J. Chung *et al.*, "Advance reservation access control using software-defined networking and tokens," *Future Generation Computer Systems*, vol. 79, pp. 225–234, Feb. 2018, doi: https://doi.org/10.1016/j.future.2017.03.010
3. T. Semong *et al.*, "Intelligent Load Balancing Techniques in Software Defined Networks: A Survey," *Electronics*, vol. 9, no. 7, p. 1091, Jul. 2020, doi: https://doi.org/10.3390/electronics9071091
4. K. Benzekki, A. El Fergougui, and A. Elbelrhiti Elalaoui, "Software-defined networking (SDN): a survey," *Security and Communication Networks*, vol. 9, no. 18, pp. 5803–5833, Dec. 2016, doi: https://doi.org/10.1002/sec.1737
5. M. He, A. Martínez Alba, A. Basta, A. Blenk, and W. Kellerer, "Flexibility in softwarized networks: Classifications and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1518-1538, 2019,
6. W. Braun and M. Menth, "Software-Defined Networking Using OpenFlow: Protocols, Applications and Architectural Design Choices," *Future Internet*, vol. 6, no. 2, pp. 302–336, May 2014, doi: https://doi.org/10.3390/fi6020302
7. S. Y. Mehr and B. Ramamurthy, "An SVM Based DDoS Attack Detection Method for Ryu SDN Controller," *Proceedings of the 15th International Conference on emerging Networking Experiments and Technologies*, Dec. 2019, doi: https://doi.org/10.1145/3360468.3368183
8. S. Lee *et al.*, "A comprehensive security assessment framework for software-defined networks," *Computers & Security*, vol. 91, p. 101720, Apr. 2020, doi: https://doi.org/10.1016/j.cose.2020.101720
9. Al-Hayajneh, Bhuiyan, and McAndrew, "Improving Internet of Things (IoT) Security with Software-Defined Networking (SDN)," *Computers*, vol. 9, no. 1, p. 8, Feb. 2020, doi: https://doi.org/10.3390/computers9010008
10. K. M. S. A. Azad, N. Hossain, M. J. Islam, A. Rahman, and S. Kabi, "Preventive Determination and Avoidance of DDoS Attack with SDN over the IoT Networks," *2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI)*, Rajshahi, Bangladesh, 8-9 July 2020, pp. 1-6,
11. S. S. Bhunia and M. Gurusamy, "Dynamic attack detection and mitigation in IoT using SDN," *IEEE Xplore*, 2017. doi: https://doi.org/10.1109/ATNAC.2017.8215418
12. A. Bicaku, M. Tauber, and J. Delsing, "Security standard compliance and continuous verification for Industrial Internet of Things," *International Journal of Distributed Sensor Networks*, vol. 16, no. 6, p. 155014772092273, Jun. 2020, doi: https://doi.org/10.1177/1550147720922731

13. 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, doi: https://doi.org/10.3390/s21144884
14. A. Derhab et al., "Blockchain and Random Subspace Learning-Based IDS for SDN-Enabled Industrial IoT Security," *Sensors*, vol. 19, no. 14, p. 3119, Jul. 2019, doi: https://doi.org/10.3390/s19143119
15. A. Huertas Celdrán, K. K. Karmakar, F. Gómez Mármol, and V. Varadharajan, "Detecting and mitigating cyberattacks using software defined networks for integrated clinical environments," *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, pp. 2719–2734, Feb. 2021,
16. Mariya Ouaissa, A. Rhattoy, and M. Lahmer, "Group access authentication of machine to machine communications in LTE networks," *ACM Digital Library*, pp. 1–5, Mar. 2017, doi: https://doi.org/10.1145/3018896.301894
17. A. Qureshi, M. A. Qureshi, H. A. Haider, and R. Khawaja, "A review on machine learning techniques for secure IoT networks," *IEEE Xplore*, Nov. 01, 2020. doi: https://doi.org/10.1109/INMIC50486.2020.9318092. Available: https://ieeexplore.ieee.org/document/9318092
18. I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of Threats to the Internet of Things," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1636–1675, 2019, doi: https://doi.org/10.1109/comst.2018.2874978. Available: https://ieeexplore.ieee.org/document/8489954
19. M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deep Learning for IoT Big Data and Streaming Analytics: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2923–2960, 2018, doi: https://doi.org/10.1109/comst.2018.2844341
20. S. Shahzadi *et al.*, "Machine Learning Empowered Security Management and Quality of Service Provision in SDN-NFV Environment," *Computers, Materials & Continua*, vol. 66, no. 3, pp. 2723–2749, 2021, doi: https://doi.org/10.32604/cmc.2021.014594
21. 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," *2016 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, Oct. 2016, doi: https://doi.org/10.1109/wincom.2016.7777224. Available: http://eprints.whiterose.ac.uk/106836/8/Tuan%20Tang_WINCOM16.pdf
22. Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, pp. 1–29, Oct. 2020, doi: https://doi.org/10.1002/ett.4150. Available: https://onlinelibrary.wiley.com/doi/full/10.1002/ett.4150