iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67507

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

Digital Twin-based DDoS Attack Detection Using Software Defined Networks

Mr. P. Hari Babu[1], U. Ramya[2], K. Rohith[3], B. Sanjana[4], L. Dushyanth[5]
[1]*Assistant Professor,* [2, 3, 4, 5]*Student, Department of Cyber Security, Raghu Engineering College*

Abstract: ***The concept of Digital Twin (DT) has transformed industries by enabling virtual replicas of physical systems for monitoring and optimization. Integrating DT with Software-Defined Networks (SDN) enhances network flexibility, scalability, and security. This paper presents an SDN-driven digital twin framework for real-time network simulation and cybersecurity enhancement, particularly for Distributed Denial of Service (DDoS) attack mitigation. The system employs Machine Learning (ML) techniques, such as Random Forest, to predict network behavior and dynamically respond to threats. The proposed approach is validated in a simulated environment, demonstrating improved threat detection and adaptive response mechanisms. The study emphasizes how digital twins provide deeper insights into traffic anomalies and attack patterns, thereby optimizing security strategies in an evolving cyber-threat landscape.***

Index Terms: Digital Twins, DDoS Attacks, Software Defined Networks.

I. INTRODUCTION

The Digital Twin (DT) technology has transformed industries by creating virtual models of physical systems, enabling real-time monitoring, simulation, and optimization. It is widely used in industrial automation, aerospace, and smart infrastructure for predictive maintenance and operational efficiency. In the context of 6G networks, DT is expected to support autonomous operations such as self-configuration, self-optimization, and self-management, enhancing network performance and reducing operational costs.

The combination of DT and Software-Defined Networking (SDN) further strengthens network management capabilities. SDN enables centralized traffic control by separating the control and data planes, making networks more flexible and adaptive. When integrated with DT, SDN allows for real-time simulation and management of complex environments, such as smart cities, industrial automation, and cybersecurity systems. This integration also improves network security by enabling intelligent monitoring and rapid response to cyber threats.

A major challenge for Internet Service Providers (ISPs) is ensuring high-speed, reliable connectivity while mitigating security risks, such as Distributed Denial of Service (DDoS) attacks. Traditional DDoS solutions mainly focus on data centers and edge networks, leaving core network components vulnerable. Even if an ISP secures most of its edge devices, attackers can exploit unprotected routers, making current security measures insufficient.

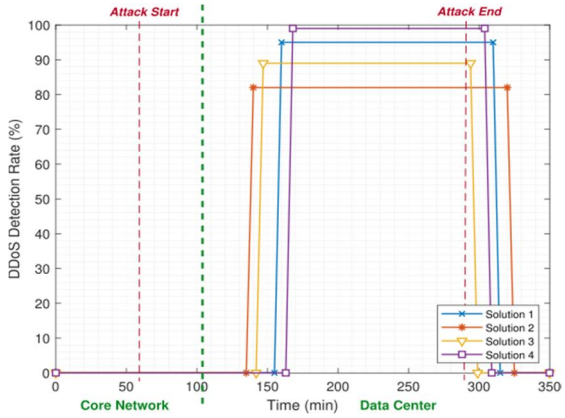


Fig. 1. The detection performance of existing DDoS solutions.

To assess the effectiveness of existing DDoS detection methods, we analyzed four anonymized commercial solutions (Solutions 1–4) with an industry partner. Our study, illustrated in Fig. 1, reveals that these solutions detect DDoS attacks with an average delay of 100 minutes after the attack starts. Such latency is inadequate for protecting network infrastructure and maintaining performance.

To counter Distributed Denial of Service (DDoS) attacks, modern networks primarily use Machine Learning (ML)-based techniques. These methods analyze network traffic patterns to detect and classify malicious activity in real time. Traditional approaches, such as signature-based and rule-based intrusion detection systems, are less effective against evolving attack patterns. In contrast, ML-based techniques improve detection accuracy by using supervised, unsupervised, and deep learning models.

Once an attack is detected, mitigation strategies such as rate limiting, IP blacklisting, traffic filtering, and dynamic routing are applied. Software-Defined Networking (SDN) helps by enabling real-time traffic control and redirection. While ML-based methods improve detection efficiency, they still face challenges like high false positive rates, adaptive attack strategies, and computational overhead. Further advancements are needed to enhance detection accuracy and response mechanisms.

A. Main Challenges of The Autonomous Core Network DDoS Detection

We investigate the challenges from two main aspects in detail as follows:

1) Specific Characteristics of The Core Network: The core network uses high-speed routers with 400 Gbps interfaces, making real-time data processing difficult. ISPs do not focus on DDoS detection in the core network due to these challenges. There are no hardware-based solutions to mitigate DDoS attacks across the entire ISP network. By the time an attack is detected in a data center, critical servers may already be compromised. ISP downtime costs range from $300,000 to $400,000 per hour. Core routers prioritize fast data transmission over security, making DDoS mitigation at this level very challenging.

2) DDoS Attack: A Distributed Denial of Service (DDoS) attack is a severe security threat in which multiple compromised machines coordinate to overwhelm a target server, rendering it inaccessible to legitimate users. The distributed nature of these attacks makes it extremely challenging to trace their origin or implement effective countermeasures. DDoS attacks can take various forms, often disguising themselves within normal network traffic, making detection difficult.

Attackers exploit network vulnerabilities to generate massive service requests, exhausting system resources and disrupting operations. Due to their evolving patterns and ability to adapt, real-time detection and mitigation remain complex tasks. However, detecting and mitigating DDoS attacks is crucial, as they can lead to significant operational and financial consequences for organizations.

B. Related Works

Although there are many previous studies on DDoS detec- tion , these studies generally focus on offline learning methods and data center solutions. We summarized existing DDoS detection approaches in different domains in Table I. J. Boite *et al.* proposed the StateSec is a DDoS detection and mitiga- tion strategy based on stateful Software-Defined Networking (SDN) to protect communication endpoints [2].

Simulation results showed that it is more efficient than sFlow for the control plane occupation. Z. K. Maseer *et al.* compared several ML algorithms, including decision tree (DeT) , naive Bayes (NB), random forest (RF), support vector machine (SVM), expectation-maximization (EM) in the perspective of DDoS detection [3]. Experimental results showed that DeT and RF models achieve better than the others in terms of overall accuracy and runtime. In some studies, an autoencoder, a kind of neural network with multiple layers, is used for feature selection (FS). Then, a classification algorithm is implemented to detect DDoS attacks [4] [6]. T. T. Khoei *et al.* analyzed the performance of three different ensemble-learning techniques: bagging, boosting, and stacking for anomaly detection in smart grid networks. The results confirmed that stacking-based learning techniques outperformed the others.

So far, a few anomaly detection works are using DT in the literature. They focus more on offering the DT system rather than anomaly detection. For example, A. Saad *et al.* suggested an Internet-of-Things (IoTs) based DT for the microgrids to enhance their resiliency against cyber-attacks [9]. They provided mathematical formulation and implementation of the DT. The results showed that their framework successfully mitigates the attacks. Moreover, many works proposed a method to label unlabeled data. One of them offered a modified label propagation method [10]. The results showed that this method improved the fault classification accuracy effectively. None of the above works focused on DDoS detection using online learning and the YANG model, nor did they use DT technology to detect DDoS attacks in the ISP core network

II. PROPOSED SYSTEM

The proposed system integrates Machine Learning (ML) and Digital Twin technology within a Software-Defined Network (SDN) to enhance the detection and mitigation of DDoS attacks. Unlike traditional methods that focus only on real-time detection, this approach predicts future network behavior using the Random Forest algorithm, known for its accuracy in analyzing network traffic patterns.

In this system, APIs are developed for key components such as Car, Garage, and Modbus to simulate real-world network interactions. A Digital Twin environment replicates these interactions, allowing real-time monitoring and predictive analysis of network behavior. The system continuously processes network traffic data and utilizes historical patterns to forecast future anomalies using the Random Forest model.

To simulate a DDoS attack, an attacker API floods the network with excessive requests. When the request rate surpasses a predefined threshold, the system detects the attack and initiates mitigation strategies such as rate limiting, traffic filtering, or SDN-based traffic rerouting. By combining predictive ML modeling with SDN-driven traffic management, this system enhances cybersecurity resilience, enabling proactive threat detection and intelligent response mechanisms for smart infrastructure and IoT-based applications.

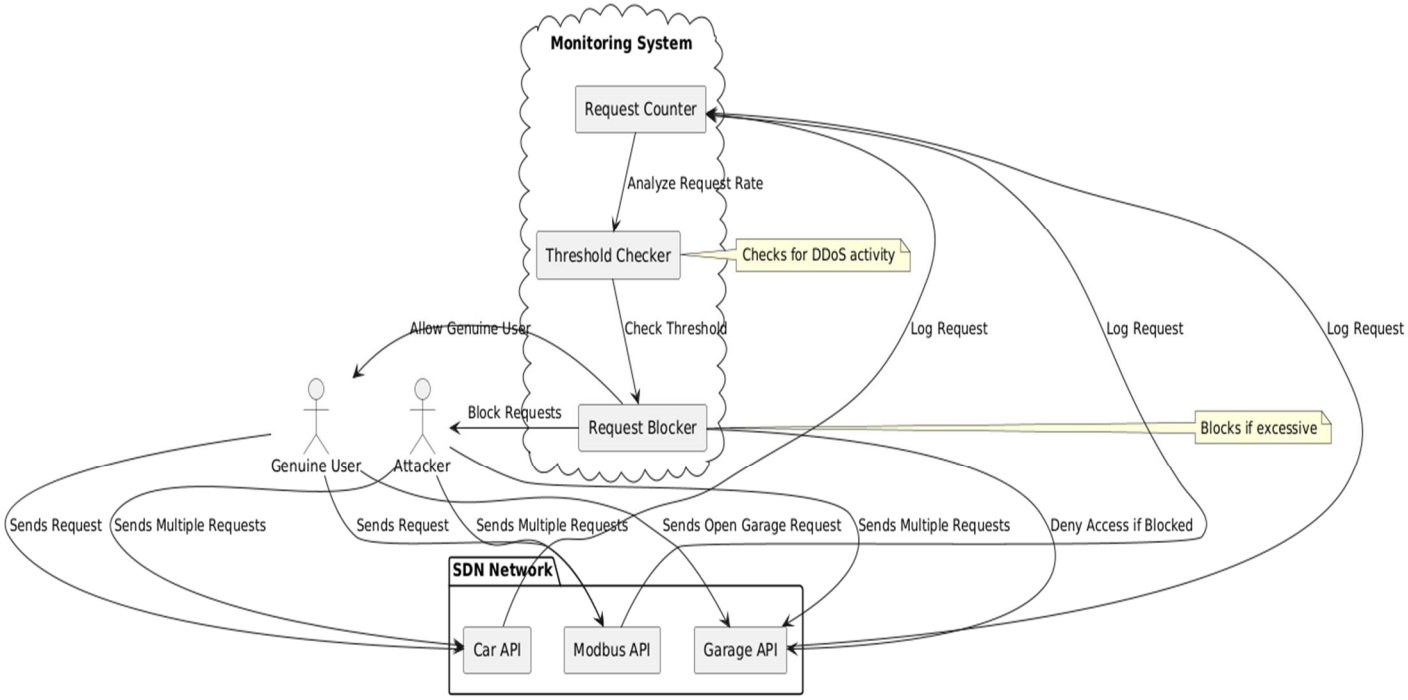


Fig. 2. The proposed system architecture.

III. METHODOLOGY

A. *Data Collection*

To train the Random Forest model for predicting network traffic and detecting DDoS attacks, data collection is essential. This process includes:

1) Simulating network traffic through APIs that replicate real-world interactions between components like Car, Garage, and Modbus.
2) Capturing key network traffic parameters such as request frequency, source IP behavior, packet flow rate, and connection duration.
3) Introducing attack traffic by simulating a DDoS scenario where an attacker API floods the system with excessive requests.
4) Logging both normal and attack traffic patterns to create a labeled dataset for machine learning (ML) training.

B. *Data Preprocessing*

Before feeding data into the Random Forest model, preprocessing ensures data quality and format consistency:

1) Data Cleaning: Eliminating inconsistencies, missing values, and redundant features.
2) Feature Extraction: Selecting critical attributes like packet size, source/destination IP, protocol type, traffic rate, and time intervals to improve classification accuracy.
3) Labeling Data: Classifying traffic as either normal or DDoS attack to build a supervised dataset.
4) Normalization: Scaling numerical values to maintain uniformity in ML model training.

C. Digital Twin Approach

A Digital Twin (DT) is developed to simulate and monitor network traffic in real time, supporting predictive analysis. This includes:

1) Virtualizing system components (Car, Garage, and Modbus) within a Software-Defined Network (SDN) environment.
2) Synchronizing real and virtual environments to ensure accurate traffic behavior representation.
3) Simulating attacks by integrating an attacker API within the digital twin to analyze its impact and test mitigation strategies.
4) Generating future network traffic patterns based on historical data using the Random Forest model, enabling early DDoS attack prediction.

D. System Architecture

The proposed architecture integrates Software-Defined Networking (SDN) with machine learning for real-time threat detection and mitigation:

1) SDN Controller: Dynamically manages network traffic and enforces security policies.
2) Random Forest Model: Identifies abnormal traffic patterns and detects DDoS attacks.
3) Traffic Analyzer: Continuously monitors incoming requests for anomalies.
4) Mitigation Module: Implements security measures such as traffic filtering, rate limiting, and SDN-based routing.
5) Digital Twin Interface: Provides a visual and analytical dashboard for system monitoring.

E. API Development and Integration (Flask)

APIs facilitate seamless interaction between system components:

1) Car API: Sends requests to Garage for access.
2) Garage API: Handles incoming requests and logs traffic patterns.
3) Modbus API: Simulates industrial protocol interactions.
4) Attacker API: Generates excessive traffic to mimic DDoS attacks.
5) Detection API: Uses Random Forest to classify normal vs. malicious traffic.
6) Mitigation API: Implements SDN-driven countermeasures against detected threats.

The APIs are integrated with the SDN controller and digital twin framework, ensuring real-time monitoring and automated response mechanisms for DDoS attacks..

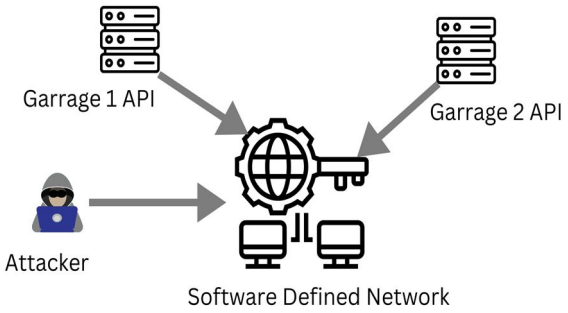


Fig.3.Model_Architecture_01

The diagram represents a Software-Defined Network (SDN) architecture with multiple APIs and a DDoS attack scenario.

1) Software-Defined Network (SDN): The central component that manages and controls network traffic. It connects to different entities, including Garage 1 API, Garage 2 API, and external users.
2) Garage 1 API & Garage 2 API: These are two separate API-based services interacting with the SDN. They could represent different connected devices or smart infrastructure components, such as automated garages in a smart city.
3) Attacker: The malicious entity attempting a DDoS (Distributed Denial of Service) attack .The attacker sends excessive requests to the SDN, trying to overload the network and disrupt legitimate communication.
4) .Arrows Indicating Communication: Both Garage APIs send requests to the SDN, representing normal interactions. The attacker also sends requests, but in large volumes, simulating a DDoS attack.

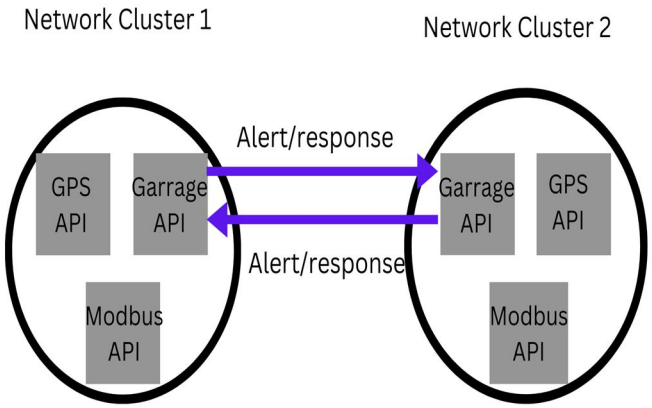


Fig.4.Model_Architecture_02

Network Cluster 1 & Network Cluster 2:

1) Two separate network groups, each containing three APIs:

- GPS API: Handles location-based data.
- Garage API: Manages access and control for a smart garage.
- Modbus API: Simulates an industrial communication protocol for device control.

2) Alert/Response Communication:

- There is bidirectional communication between the two clusters.
- If an issue, such as a DDoS attack or anomaly, is detected in one cluster, an alert is sent to the other.
- The receiving cluster can respond by taking appropriate action, such as activating security measures or rerouting traffic.

IV. CONCLUSION

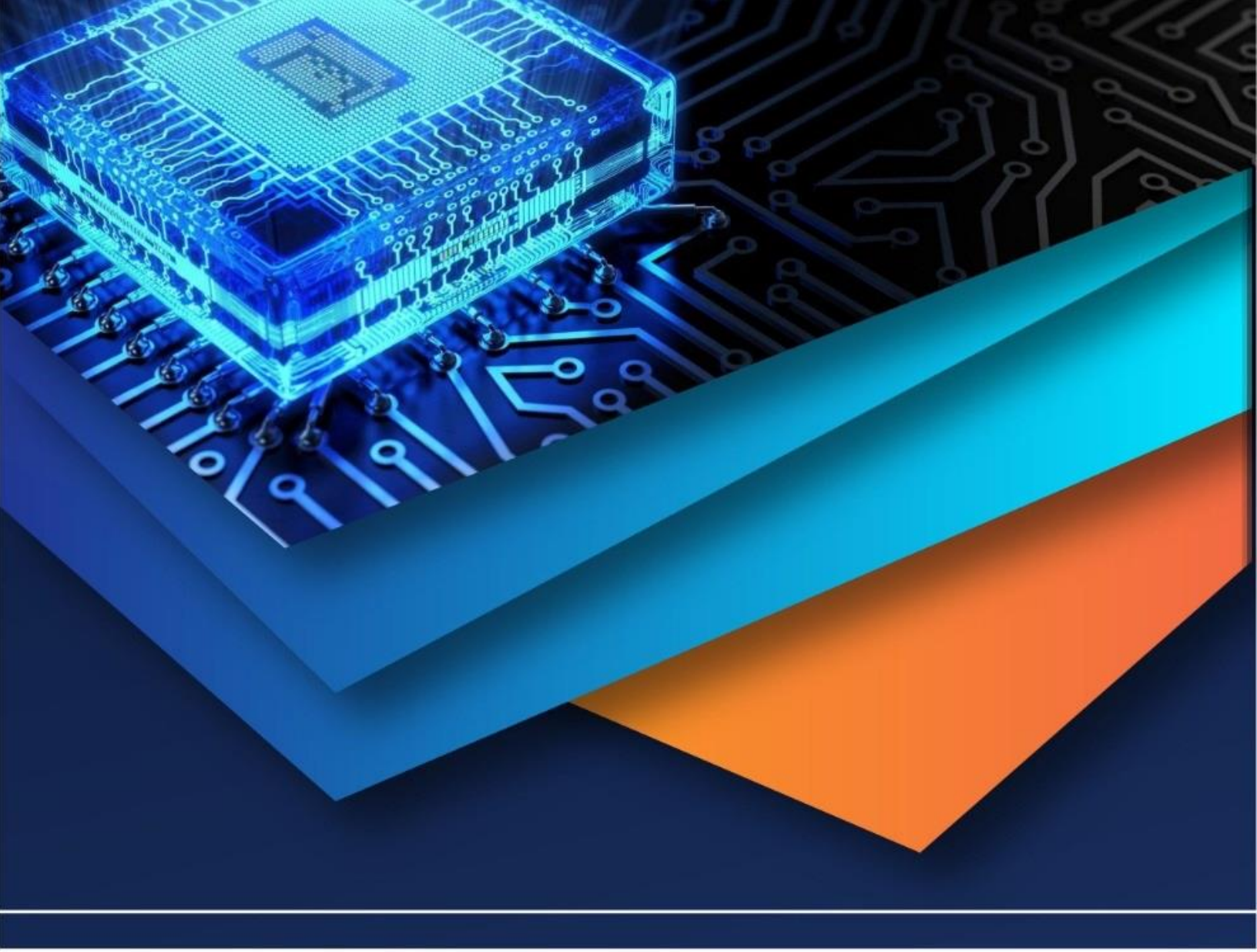
The integration of Digital Twin technology, Software-Defined Networking (SDN), and Machine Learning (ML) provides an effective approach for DDoS detection and mitigation in modern network environments. This study demonstrates how a predictive and automated system can be developed using APIs, Random Forest classification, and SDN-based traffic control to identify and counteract malicious activities. By simulating real-world network components such as Garage, Modbus, and GPS APIs**,** the system creates a dynamic Digital Twin that allows real-time monitoring, analysis, and response to cyber threats. The Random Forest classifier predicts DDoS attacks based on extracted network features, and when an anomaly is detected, an alert-response mechanism is triggered across network clusters. This ensures early detection, collaboration, and coordinated mitigation efforts to prevent system disruptions. Additionally, the SDN controller enhances network security by dynamically adjusting traffic flow and applying rate-limiting or blocking mechanisms when an attack is identified. This approach significantly improves cyber resilience, scalability, and adaptability in smart infrastructure, IoT environments, and critical networked systems**.**

Future enhancements, such as Deep Learning models, blockchain integration, and edge computing, can further strengthen real-time security measures**,** making this system more robust against evolving cyber threats

REFERENCES

[1] Y. Wu, K. Zhang, and Y. Zhang, “Digital Twin Networks: A Survey,” IEEE Internet of Things Journal, vol. 8, no. 18, pp. 13 789–13 804, May 2021.
[2] J. Boite, P.-A. Nardin, F. Rebecchi, M. Bouet, and V. Conan, “Statesec: Stateful monitoring for DDoS protection in software defined networks,” in IEEE Conference on Network Softwarization (NetSoft), Bologna, Italy, July 2017, pp. 1–9.
[3] Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, “Benchmarking of Machine Learning for Anomaly Based Intrusion Detection Systems in the CICIDS2017 Dataset,” IEEE Access, vol. 9,
[4] pp. 22 351–22 370, Feb. 2021.
[5] K. Sadaf and J. Sultana, “Intrusion detection based on autoencoder and isolation forest in fog computing,” IEEE Access, vol. 8, pp. 167 059– 167 068, Sept. 2020.
[6] T. T. Khoei, G. Aissou, W. C. Hu, and N. Kaabouch, “Ensemble Learning Methods for Anomaly Intrusion Detection System in Smart Grid,” in 2021 IEEE International Conference on Electro Information Technology (EIT), July 2021, pp. 129–135.

[7] Y. Wei, J. Jang-Jaccard, F. Sabrina, A. Singh, W. Xu, and S. Camtepe, "Ae-mlp: A hybrid deep learning approach for ddos detection and classification," IEEE Access, vol. 9, pp. 146 810–146 821, Oct. 2021.
[8] T. Alsop. Average cost per hour of enterprise server downtime worldwide in 2019. [Online]. Available: https://www.statista.com/statistics/753938, Accessed Sept. 9, 2021.
[9] B. Claise, J. Clarke, and J. Lindblad, Network Programmability with YANG: The Structure of Network Automation with YANG, NETCONF, RESTCONF, and gNMI. Addison-Wesley Professional, 2019.
[10] A. Saad, S. Faddel, T. Youssef, and O. A. Mohammed, "On the Implementation of IoT-Based Digital Twin for Networked Microgrids Resiliency Against Cyber Attacks," IEEE Transactions on Smart Grid, vol. 11, no. 6, pp. 5138–5150, June 2020.
[11] Y. Xie, "Modified Label Propagation on Manifold With Applications to Fault Classification," IEEE Access, vol. 8, pp. 97 771–97 782, May.
[12] 2020.
[13] C. Zhou, H. Yang, X. Duan, D. Lopez, A. Pastor, Q. Wu, M. Boucadair, and C. Jacquenet. Digital Twin Network: Concepts and Reference Architecture. [Online]. Available: https://datatracker.ietf.org/doc/html/ draft-zhou-nmrg-digitaltwin-network-concepts-06, Accessed Dec. 15, 2021.
[14] M. Bjorklund. The YANG 1.1 Data Modeling Language, RFC 7950. [Online]. Available: https://www.rfc-editor.org/rfc/rfc7950.html, Accessed Aug. 12, 2022.
[15] Microsoft. Azure Digital Twins Documentation. [Online]. Available: https://docs.microsoft.com/en-us/azure/digital-twins, Accessed Sept. 27, 2021.
[16] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani. DDoS Evaluation Dataset (CIC-DDoS2019). [Online]. Available: https://www.unb.ca/cic/datasets/ddos-2019.html, Accessed June 21, 2021.
[17] N. Moustafa. ToN IoT datasets. [Online]. Available: https://ieee-dataport.org/documents/toniot-datasets, A



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY