iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** XI **Month of publication:** November 2024

DOI: https://doi.org/10.22214/ijraset.2024.65142

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 12 Issue XI Nov 2024- Available at www.ijraset.com

SDN-Driven Security Framework for DDOS Attack Detection and Mitigation

Asmita Kadam[1], Shruti Anap[2], Saloni Bargal[3], Satvika Marewar[4], Prof. Gayatri Chavan[5]
Computer Engineering, Padmabhooshan Vasantdada Patil Institute of Technology

Abstract: ***The rising complexity and persistence of Distributed Denial of Service (DDoS) attacks, particularly low-rate variants, present significant challenges in detection and mitigation within Software-Defined Networking (SDN) environments. Existing detection systems often flood networks with alerts, burdening security personnel and delaying timely mitigation. Furthermore, many solutions are designed and tested in simulated conditions, limiting their real-world applicability. To address these challenges, we propose an SDN-based security framework enhanced with automated monitoring, detection, and mitigation capabilities, optimized for slow-rate DDoS attacks. Our framework was rigorously evaluated on a physical testbed, achieving mitigation efficiencies between 91.66% and 100% under varied attack conditions, thus proving its robustness in practical settings.***

Additionally, we introduce the SDN-SlowRate-DDoS dataset, designed to assist researchers and industry professionals in developing and testing intrusion detection solutions in more realistic scenarios. To further improve DDoS defense in SDN, we incorporate an ensemble online machine learning model that dynamically adapts to evolving attack patterns, enhancing accuracy across attack types and outperforming traditional models with a detection rate of 99.2% on benchmark datasets. This dual approach leverages both real-world testing and adaptive machine learning, advancing proactive DDoS threat management in SDN environments.

Keywords: SDN security, Slow-rate DDoS, Intrusion detection, Machine learning, intrusion prevention system (IPS), Dataset for DDoS, Network security, Traffic anomaly detection, Denial of Service (DoS), Deep learning, Security frameworks, Attack mitigation, Real-time monitoring, Network traffic analysis.

I. INTRODUCTION

In today's advanced networking landscape, Distributed Denial of Service (DDoS) attacks pose a critical threat to both traditional and Software-Defined Networking (SDN) infrastructures, including next-generation networks like 5G. These attacks disrupt service availability by overwhelming network resources, making effective detection and mitigation essential for network resilience. While conventional Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) generate alerts for such attacks, the sheer volume of alerts can easily exceed the capacity of security teams, hindering timely response. Automated DDoS mitigation solutions, especially those leveraging SDN's flexibility and dynamic programmability, offer a promising avenue for addressing these challenges.

Despite advancements in SDN-based security, there remains a gap between solutions tested in controlled, simulated environments and those robust enough for real-world deployment. Many research efforts rely on synthetic datasets that may not accurately reflect the complexities of real networks, leading to potentially limited effectiveness in production environments. To bridge this gap, there is a pressing need for datasets collected from physical networks and realistic testbeds, allowing researchers to design and evaluate security frameworks that are both practical and effective in live network scenarios.

In response to these challenges, this study presents an automated DDoS mitigation framework built on SDN architecture and evaluated in a real-world experimental environment. The framework integrates a deep learning-based IDS with an adaptive IPS, designed to detect and mitigate slow-rate DDoS attacks, a particularly insidious form of DDoS that can evade traditional detection mechanisms. Utilizing equipment from the European Smart Networks for Industry (SN4I) facility, we demonstrate the framework's efficacy, achieving a mitigation success rate of 91.66% to 100% across varying attack conditions. Additionally, we introduce the SDN-SlowRate-DDoS dataset, a novel resource containing both raw traffic data and SDN controller-based flow statistics from the SN4I testbed. This dataset is invaluable for advancing SDN security research, enabling the development of realistic and adaptive intrusion detection solutions.

©IJRASET: All Rights are Reserved

II. LITURATURE SURVEY

1) *Physical Assessment of an SDN-Based Security Framework for DDoS Attack Mitigation: Introducing the SDN-Slow Rate-DDoS Dataset by Yungaicela-Naula et al.*

This paper by Yungaicela-Naula and colleagues focuses on evaluating a security framework within Software-Defined Networking (SDN) for defending against Distributed Denial of Service (DDoS) attacks. By testing on physical SDN equipment, the study emphasizes real-world application and impact. A notable contribution of this work is the introduction of the SDN-SlowRate-DDoS dataset, which includes real network traffic data specifically capturing low-rate DDoS events. This dataset aims to assist researchers in developing and testing Intrusion Detection Systems (IDS) under realistic conditions, filling a gap in available datasets that often lack representation of such nuanced attack types.

The authors' security framework includes a monitoring switch capable of capturing network-wide traffic data, which aids in identifying anomalies and potential threats. However, they also identify scalability challenges associated with this architecture and propose future enhancements involving P4-enabled switches to optimize traffic monitoring before it reaches the IDS. This addition could significantly boost the framework's scalability and effectiveness. The study concludes by suggesting reinforcement learning-based models as a future direction to further improve attack mitigation. This work stands out for its comprehensive approach to SDN-based DDoS detection and mitigation, offering a foundation for future advancements in scalable security solutions.

2) *Enhancing DDoS Attack Detection and Mitigation in SDN Using an Ensemble Online Machine Learning Model by Alashhab et al.*

In this study, Alashhab and co-authors explore a machine learning-based approach to enhancing DDoS attack detection and mitigation within SDN frameworks. The authors propose an ensemble model that leverages online machine learning (OML) techniques to effectively identify and mitigate both high-rate and low-rate DDoS attacks. The model is designed for adaptability, allowing it to respond to evolving traffic patterns and diverse attack types, a key advantage over traditional detection methods that may struggle with novel or unpredictable traffic.

The ensemble model includes both an OML-based Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS), enabling the framework to proactively detect and address DDoS incidents in real time. During testing, the OML-based IDS achieved high detection rates, with accuracy levels exceeding 99%, highlighting its reliability in identifying a wide range of DDoS attacks. By integrating with the IPS, the framework enhances comprehensive defense capabilities, effectively safeguarding SDN networks. The paper also discusses the modularity of the design, which supports ongoing upgrades and makes the system compatible with various SDN controllers, underscoring its versatility and scalability. This work contributes to SDN security by demonstrating the potential of adaptive, machine-learning-driven frameworks for real-time DDoS mitigation across diverse network environments.

3) *Early Detection of DoS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA)" by S. Roselin Mary, M. Maheshwari, and M. Thamaraiselvan*

Vehicular Ad Hoc Networks (VANETs) are integral to the modern transportation infrastructure, enabling communication between vehicles (V2V) and between vehicles and infrastructure (V2I) to improve safety, traffic management, and emergency response. However, like other network systems, VANETs are vulnerable to various cyber-attacks, particularly Denial of Service (DoS) attacks, which can disrupt vehicle communications, leading to delays and potential accidents.

This paper proposes the Attacked Packet Detection Algorithm (APDA**)** to address the challenge of detecting DoS attacks in VANETs. The core idea behind APDA is to focus on the detection of malicious or anomalous packets that might signify the occurrence of a DoS attack, without introducing significant overhead or delay in the processing of network traffic. The algorithm works by analyzing packet-level data, identifying patterns that deviate from normal communication, and flagging potential attack traffic.

A key strength of APDA is its ability to minimize processing delays, which is crucial for maintaining the low-latency communication needed in VANETs. The authors claim that APDA can enhance network security by effectively filtering out malicious packets, allowing legitimate communication to continue uninterrupted. Their approach shows promise in improving the resilience of VANETs against DoS attacks, ensuring that critical safety data is transmitted reliably even in the presence of potential cyber threats.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

4) *Mitigation and Detection Strategy of DoS Attack on Wireless Sensor Network Using Blocking Approach and Intrusion Detection System" by Faisal Mochamad Teguh Kurniawan, Setiadi Yazid, Abdelrhman Mohammed, Iman Abuel Maaly Abdelrahman*

Wireless Sensor Networks (WSNs) are employed in a variety of mission-critical applications, including environmental monitoring, military surveillance, healthcare, and IoT systems. Due to the resource-constrained nature of the sensor nodes—limited in terms of processing power, memory, and energy—WSNs are particularly susceptible to security threats, with Denial of Service (DoS) attacks being one of the most significant risks.

This paper presents an integrated **blocking approach** coupled with an **Intrusion Detection System (IDS)** to address DoS attacks on WSNs. The blocking approach aims to prevent unauthorized access to the network and mitigate the effects of malicious traffic, while the IDS is responsible for monitoring network activity, identifying abnormal patterns, and detecting DoS attempts. By combining these two methods, the system can block harmful traffic early, reducing the likelihood of successful attacks.

The authors argue that their proposed strategy enhances the overall security of WSNs by not only detecting DoS attacks but also preventing them from causing significant disruptions. This combination of proactive and reactive security measures is essential for protecting WSNs in highly sensitive applications where continuous operation is critical. Their approach is particularly relevant to IoT applications, where WSNs form the backbone of data collection and communication.

5) *Event-Triggered Switching-Type Event-Triggered Switching-Type Fault Detection and Isolation for Fuzzy Control Systems under DoS Attacks" by Xiang-Gui Guo, Xiao Fan, Jian-Liang Wang, and Ju H. Park*

The focus of this paper is on fault detection and isolation (FDI) in networked control systems (NCSs), particularly those using fuzzy control systems under the threat of Denial of Service (DoS) attacks. Networked control systems are increasingly used in industrial automation, robotics, and smart systems, where the integration of fuzzy logic controllers (FLCs) is common due to their ability to handle uncertainty and nonlinearity in the system dynamics.

However, NCSs are vulnerable to DoS attacks, which can disrupt communication between the system components, potentially leading to incorrect system behavior or failure.

To address this challenge, the authors propose a Memory Adaptive Event-Triggered (MAET) approach to fault detection and isolation in fuzzy control systems. The MAET approach dynamically adjusts the triggering threshold for fault detection based on the most recent data, minimizing unnecessary communication and reducing the risk of DoS attacks exploiting the system's communication resources. The approach also incorporates a switching state-feedback controller, which adapts to changes in system dynamics to maintain stability and ensure the system operates effectively even under attack.

The paper demonstrates that this method offers a robust fault detection and isolation mechanism for nonlinear systems, allowing for continued operation and stability of the fuzzy control system even when faced with DoS attacks. This work is particularly important for the reliability and safety of control systems in sectors like automation, manufacturing, and critical infrastructure, where system failure can have severe consequences.

6) *Thwarting DoS Attacks: A Framework for Detection Based on Collective Anomalies and Clustering" by Mohiuddin Ahmed*

The paper addresses the growing threat of Denial of Service (DoS) attacks, which have become a significant challenge for organizations trying to protect their digital infrastructure, particularly in environments with sensitive intellectual property. The approach focuses on collective anomaly detection and clustering techniques to identify and mitigate DoS attacks. Collective anomaly detection looks for unusual patterns that may be indicative of coordinated attack activities, while clustering groups similar data points to identify abnormal traffic patterns in a network.

This methodology is particularly important in the context of the Internet of Things (IoT), where the rapid increase in connected devices has amplified the frequency and complexity of cyber-attacks. The paper explores how combining anomaly detection with clustering techniques can improve the accuracy of detecting DoS attacks and reduce the number of false positives typically seen with traditional detection methods. The proposed framework also aims to increase the resilience of target systems against volumetric attacks, where a high volume of traffic floods the system and causes service disruption. By using this framework, organizations can enhance their ability to safeguard critical services against DoS attacks, ensuring continuous availability and the protection of intellectual assets.

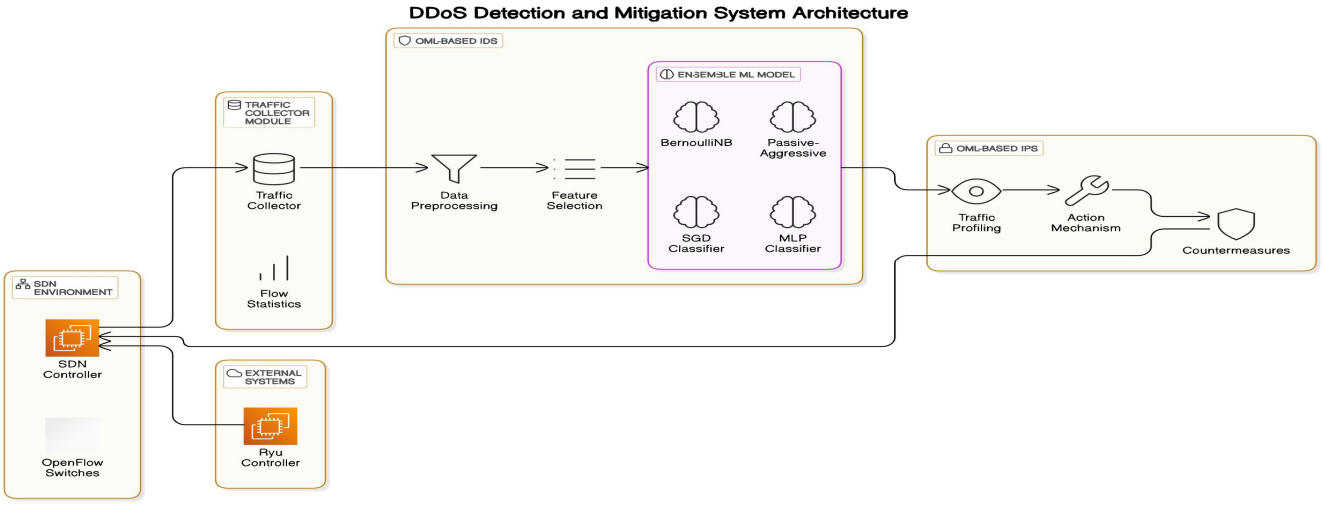
7) Implementation Implementation of SDN-based IDS to Protect Virtualization Servers Against HTTP DoS Attacks" by Saifudin Usman and Idris Winarno

This paper highlights the vulnerabilities faced by virtualization environments in modern cloud computing infrastructures, especially in the context of HTTP-based Denial of Service (DoS) attacks. Virtualization allows for efficient resource utilization and flexible resource allocation, but it also introduces unique security challenges, as these environments are increasingly targeted by DoS attacks. The authors propose an SDN-based Intrusion Detection System (IDS) to detect and mitigate HTTP DoS attacks in virtualized server environments.

The proposed SDN-based IDS utilizes the advantages of Software-Defined Networking (SDN), which enables centralized control and dynamic configuration of network resources. By using SDN, the IDS can effectively monitor network traffic and identify patterns that indicate an impending HTTP-based DoS attack, such as unusual traffic spikes or repetitive request patterns from specific sources. The paper emphasizes the flexibility and scalability of SDN, allowing the IDS to adapt quickly to changing traffic conditions in virtualized environments.

Additionally, the study demonstrates that the SDN-based IDS can not only detect HTTP DoS attacks but can also trigger countermeasures to block malicious traffic, ensuring that legitimate traffic continues to flow without disruption. This approach improves the security posture of virtualized servers, which are often targeted due to their open nature and the critical applications they host. The integration of SDN with IDS technology provides a robust, real-time solution for defending against network-based attacks in cloud-based infrastructures.

III. SYSTEM ARCHITECTURE



A. System Architecture for DDoS Detection and Mitigation in SDN

This modular system architecture is specifically crafted for detecting and mitigating DDoS attacks within Software-Defined Networking (SDN) environments. It employs an ensemble-based Online Machine Learning (OML) method and consists of three key components:

1) Traffic Collector Module: This module, integrated with the SDN controller, captures and mirrors traffic data from OpenFlow switches. By periodically requesting flow entries, it ensures continuous access to packet information needed for analysis. Secure communication channels are maintained to protect against data exposure and enhance security.

2) OML-Based Intrusion Detection System (IDS): Using an ensemble of machine learning models, the IDS examines network traffic in real-time to identify whether it is benign or potentially harmful. The system includes diverse classifiers such as BernoulliNB, Passive-Aggressive, SGD, and MLP, selected for their compatibility and efficiency in handling different data types. The model is updated dynamically to keep up with new DDoS attack trends.

3) OML-Based Intrusion Prevention System (IPS): This module leverages alerts from the IDS to enforce flow rules that mitigate detected threats. With its adaptive learning capability, the IPS responds swiftly to both familiar and emerging attack tactics by applying real-time, tailored mitigation actions.

B. System Workflow

1) The overall process of this system includes:

- Data Collection: The Traffic Collector gathers and transmits flow statistics to the IDS.
- Analysis and Detection: The IDS preprocesses the collected data, selects relevant features, and uses its ensemble model to identify abnormal activity.
- Mitigation: When a threat is detected, the IDS alerts the IPS, which then takes appropriate action, such as modifying flow rules on network devices to block or reroute malicious traffic.

2) This modular framework allows each component to be independently optimized and seamlessly integrated with various SDN controllers via REST APIs. The system's adaptability to shifting attack patterns ensures robust, real-time DDoS mitigation within SDN environments, providing both flexibility and reliability.

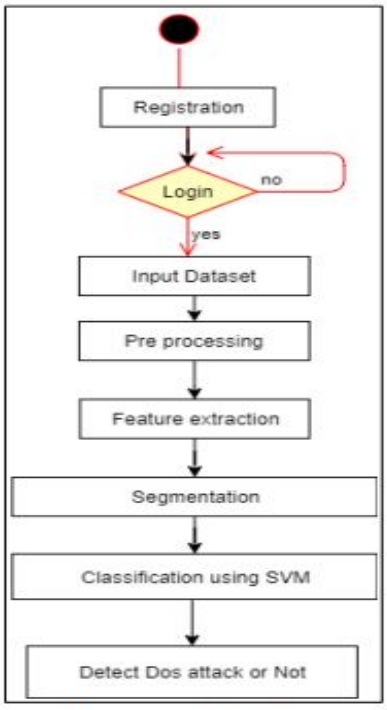


Figure 4.6: Activity Diagram

- User Registration: Users or administrators register their credentials to access the detection system, ensuring that only authorized individuals can proceed.
- User Login: After registration, users log in to access system functions. Failed login attempts prompt retries, allowing only legitimate users to continue.
- Dataset Input: Once authenticated, the user inputs a network traffic dataset, which serves as the foundation for detecting both normal and potentially malicious traffic.
- Data Preprocessing: The dataset undergoes cleaning, normalization, and transformation to enhance data quality, ensuring accuracy in subsequent analysis.
- Feature Extraction: Key attributes like packet frequency and flow rate are extracted, focusing on data relevant for detecting DoS patterns.
- Data Segmentation: The dataset is divided into manageable segments to improve processing efficiency and capture changes in network behaviour.
- Classification using SVM: The segmented data is classified with an SVM model to distinguish between normal and malicious traffic patterns.
- DoS Attack Detection: The system detects potential DoS attacks based on the classification results and can alert administrators or initiate response actions.
- This structured workflow enhances DoS attack detection and response, enabling real-time threat mitigation in the network security framework.

IV. CONCLUSIONS

This study created a good security system to find and stop DDoS attacks in Software Defined Networking (SDN) setups. We tested how well the framework can handle both high and low levels of usage with actual devices. The SDN-Slow-DDoS dataset helps create better intrusion detection systems (IDS) in the future. Our system has monitoring switches that track network connections to help detect complex attack patterns accurately and efficiently, which in turn reduces the workload on the monitoring module caused by traffic. This shows how important scalability and accuracy are in our framework. Furthermore, we will investigate how adaptive learning methods can enhance DDoS protection, specifically by supporting learning-focused strategies. Testing in actual SDN settings and expanding the framework to work in hybrid and cloud-based SDN networks are key areas for future development. This detailed guide offers a scalable solution for managing real-time DDoS attacks in growing network infrastructures. Access to critical resources supported this research. We want to thank Professor Gayatri Chavan for her helpful support, advice, and input during the project. His knowledge and drive are essential for this project to succeed.

V. ACKNOWLEDGMENT

The authors would like to express their heartfelt gratitude to Padmabhooshan Vasantdada Patil Institute of Technology for providing a supportive environment and access to essential resources that greatly facilitated this research. Special thanks go to Prof. Gayatri Chavan for her invaluable guidance, mentorship, and insightful feedback throughout the project. Her expertise and encouragement were fundamental to the successful completion of this work.

REFERENCES

[1] Perez-Diaz, E. Jacob, and C, were heading to the park, to play, Jacob preferred the swings, while C preferred the slide. They both enjoyed their time at the park. Martinez-Cagnazzo discusses a security framework based on SDN to protect against DDoS attacks in their article "Introduction to the SDN-Slow-DDoS dataset" published in IEEE Access, Vol. Volume 11, pages 46829-46839, published in 2023.

[2] A. Alashhab, M. S. Zahid, B. Isyaku, A. A. Elnour, W. Nagmeldin, A. Abdelmaboud, T.A. A. Abdullah and U. are partners. In the journal IEEE Access, D. Maiwada discusses how online machine learning models can improve detecting and stopping DDoS attacks in SDN. 11, ibid., pages 12345–12356 in the year 2023.

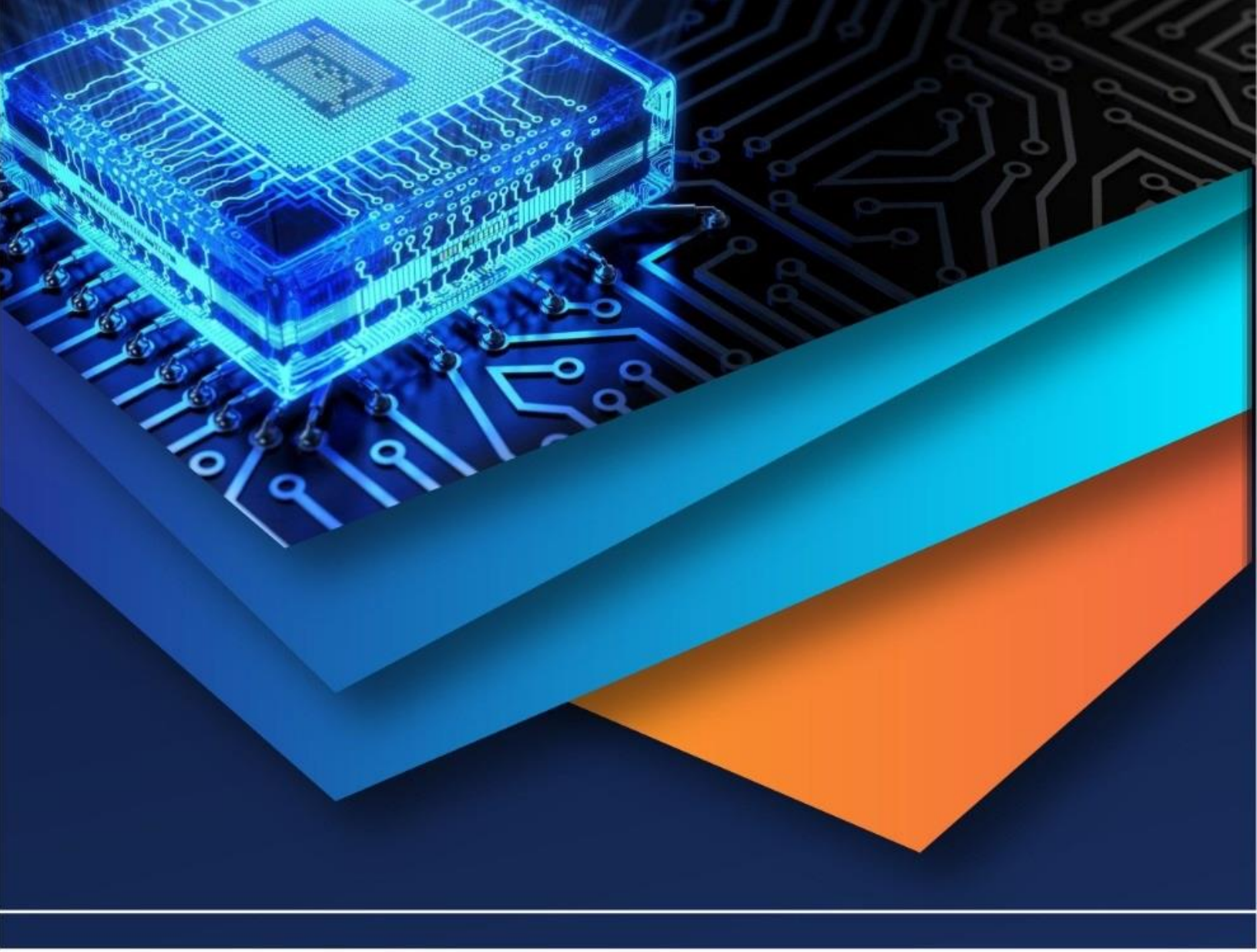
[3] Foreign Affairs Minister T. S. Kurniawan Yazid, A. Mohammed and I.A. M. Abdelrahman wrote about ways to prevent and identify DoS attacks on wireless sensor networks by using blocking methods and intrusion detection in an article published in IEEE Sensors Magazine.

[4] Guo, X., and Fan, J.-L. Wang, J. H. Park wrote about how errors can change in fuzzy control when there is a DoS attack in the IEEE Transactions on Fuzzy Systems

[5] Ahmed wrote an article titled "DoS attack prevention: integration and integration based" in IEEE Access.

[6] Usman and me. Winarno's research explores using SDN-based IDS to protect virtualized servers from HTTP DoS attacks as discussed in the IEEE Transactions on Network and Service Management.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)