International Journal of Trendy Research in Engineering and Technology
Volume 9 Proceedings of NCIES-25
ISSN No. 2582-0958

# Intrusion Detection and Prevention for Web Apps Using SNORT and Proxy Server

[1]Prajna U R,[2]Mohamed Adeeb Farzan,[2]Ranjith Kumar,[2]Manish J Rai,[2]Rohit Kulkarni

[1]*Assistant Professor,* [2]Students,*Department of ISE Sahyadri College of Engineering and Management,*Mangalore, Karnataka, India
prajnau.is@sahyadri.edu.in,adeebsaqib431@gmail.com,ranjithkumarshetty2003@gmail.
commrai263407@gmail.com,ohitkulkarni232002@gmail.com

**ABSTRACT**

The project "Intrusion Detection and Prevention for Web Apps Using SNORT and Proxy Server" is to enhance the security of web applications hosted on Google Cloud Platform (AWS). AWS provides a reliable and scalable foundation, enabling seamless deployment and integration of sophisticated security mechanisms. This solution employs a multi-layered security architecture, combining the NGINX proxy server with SNORT, an open-source intrusion detection and prevention system, to protect against evolving cyber threats.

The NGINX proxy server acts as a gateway. It manages and logs all the incoming traffic. It routes the requests to SNORT for real-time analysis so that all the malicious traffic is caught before it hits the application server. SNORT checks against the database of predefined rules and attack signatures for network packets in order to detect threats like SQL injection, XSS, and DoS attacks. The malicious requests are blocked and logged, and the legitimate ones are forwarded to the web application for processing. Logs are of extreme importance during post-incident analysis to improve security measures.

The project emphasizes a proactive approach to cybersecurity by integrating advanced tools with AWS's cloud capabilities. Features such as automatic scaling, centralized logging, and high availability enhance the application's performance and resilience. It ensures that the application is well protected against known threats as well as emerging ones that support secure user interactions and uninterrupted service delivery.

In addition to the prevention of threats, the system gives insight into patterns and trends in attacks, allowing continuous improve-ment in security policies. Due to the scalability provided by AWS, the solution can efficiently handle different traffic volumes without compromising security. This deployment addresses the present security challenges and sets up a strong foundation for further improvements in cloud-based application protection.

The integration of NGINX, SNORT, and AWS is an example of modern technologies that work in conjunction with each other to provide a safe, scalable, and reliable environment for web applications. This project represents an effective technique for securing digital assets while mitigating risks and delivering a safe and trustworthy user experience in today's threat-laden cyber landscape.

**Keywords**—Intrusion Detection and Prevention for Web Apps Using SNORT and Proxy Server

## I. INTRODUCTION

Web application security forms an integral part of today's digital infrastructure, as web servers are the most important objects for cyberattacks that would lead to exploiting vul-nerabilities for unauthorised access. Data breaches, financial loss, service disruption, and damage to reputation are possi-ble in such attacks. Our project addresses these challenges by securing web applications hosted on the Google Cloud Platform (AWS) using a combination of SNORT, an open-source intrusion detection and prevention system, and NGINX, a high-performance proxy server. This architecture provides a reliable and scalable architecture that ensures the protection and availability of web services.

Web applications have gradually become an important part of people's lives through online banking, shopping, and social networking. This is why web applications are highly targeted by hackers to extract sensitive data or to create service outages. In most cases, firewalls and antivirus software cannot defend against complex attacks like SQL injections, cross-site scripting (XSS), and denial-of-service (DoS). To counter these, our project utilizes the real-time packet inspection capabilities of SNORT and the traffic management capabilities of NGINX to provide multi-layered protection. Since these tools are deployed in the robust environment of AWS, our system only lets legitimate requests into the application while malicious activities are logged and blocked.

This way, it helps protect the web application against certain risks. It also facilitates scalability, central logging, and high availability. The deployment of a cloud infrastructure based on the latest security models from AWS creates a strong and effective environment that can safeguard data and ensure easy access by users. In this paper, a forward-looking solution to the challenge of evolving cyberattacks can be depicted while laying out a groundwork for future advances in protecting web applications.

The rapid advancement of technology and the increasing reliance on web applications in everyday life have made cybersecurity an essential focus for organizations and individuals alike. Web applications, ranging from online banking platforms and e-commerce websites to social networking services, have become indispensable tools for users worldwide. However, their widespread use has also made them primary targets for malicious actors attempting to exploit vulnerabilities for personal, financial, or political gain. Protecting these applications against cyberattacks is critical to preserving data confidentiality, service integrity, and user trust.

Hackers continuously develop sophisticated techniques to breach security systems, including SQL injections, cross-site scripting (XSS), denial-of-service (DoS) attacks, and zero-day exploits. These can result in severe outcomes such as data leaks, financial loss, legal liabilities, and reputational damage. Traditional security tools such as firewalls and antivirus programs fail to mitigate these advanced threats due to their limited detection capabilities. Therefore, a more powerful and proactive approach to web application security is needed to handle these challenges effectively.

Our project would fulfill this need by implementing an SSL-secured, web-scale application on AWS-Google Cloud Platform and harnessing SNORT and NGINX to protect more from cyber threats. An infrastructure with a scalable feature from AWS is designed and provides the most reliable feature, thus supporting advance mechanisms of security that allow it to support high availability of performance of web applications. SNORT is an open-source intrusion detection and prevention system, which monitors traffic in real-time and looks for malicious activity based on a comprehensive database of predefined rules and attack signatures. NGINX is meanwhile acting as a high-performance proxy server, routing the legitimate traffic to the web application while preventing unauthorized access.

The integration of SNORT and NGINX into the AWS environment creates a multi-layered defense architecture designed to mitigate increasingly complex modern cyber threats. SNORT actively checks packets coming through the network for malicious content, logs questionable activity for analysis, and blocks malicious requests while ensuring smooth application performance, further enhanced by NGINIX by enhancing traffic management and load balancing. This dual-layered system not only makes the web application stronger but also reduces the impact of threats on the availability and user experience of applications.

Centralized logging and monitoring capabilities offered by AWS are also very essential for threat analysis and response. The system allows organizations to analyze patterns of attacks, identify vulnerabilities, and refine security measures over time by maintaining a detailed record of incoming traffic and potential threats. Such an approach ensures continuous improvement in the security posture of the application and resilience against emerging threats.

In today's interconnected world, where web applications are integral to personal, professional, and financial activities, ensuring their security is more important than ever. Our project showcases how combining state-of-the-art tools like SNORT and NGINX with the scalability and reliability of AWS can provide a comprehensive and adaptive solution to modern cybersecurity challenges. This innovative approach not only protects web applications from existing threats but also lays a strong foundation for future advancements in cloud-based security systems, demonstrating the importance of integrating advanced cybersecurity measures with cloud computing technologies.

As the digital landscape continues to expand, the need for securing web applications has become increasingly critical. Millions of users rely on these applications for financial transactions, communication, entertainment, and other services; therefore, their protection from the evolving cyber threats is crucial. Cyberattacks are not only a threat to sensitive user data but also cause disruptions in critical operations, which have huge financial and reputational losses for businesses. This is the driving requirement behind our project, which essentially deals with integrating advanced mechanisms of intrusion detection and prevention into modern cloud environments that have a pressing need to ensure robust web application security.

Our foundation project will be based on the scalable and resilient architecture of Google Cloud Platform (AWS), hosting a secure web application. By using AWS robust cloud services, we guarantee high availability, low latency, and seamless scalability for dynamic web traffic. SNORT and NGINX infrastructure will be placed on this reliable platform to create a fortified environment capable of fending off even the most sophisticated cyberattacks.

At the core of our security framework is SNORT, one of the widely recognized open-source intrusion detection and prevention systems (IDS/IPS). This serves as a first line of defense. SNORT analyses real-time incoming network traffic for possible malicious activity, detecting patterns with known attack vectors like malware, SQL injections, or unauthorized access attempts, utilizing a very extensive rule set. Any malicious activity detected is immediately blocked, and detailed logs are generated for further analysis. These logs are very important in understanding the nature of the attack, identifying vulnerabilities, and improving future defenses.

Complementing SNORT, NGINX functions as a high-performance reverse proxy server, ensuring that only legitimate traffic reaches the application server. By effectively managing traffic, filtering out malicious requests, and balancing loads, NGINX enhances the overall performance and security of the application. The combination of SNORT's detection capabili-

ties and NGINX's traffic management ensures that the system remains robust, even under heavy traffic or targeted attacks.

One of the most significant challenges in cybersecurity is staying ahead of emerging threats. Hackers are continuously developing new methods to exploit system vulnerabilities, making static security solutions inadequate. Our project addresses this challenge by adopting a dynamic approach, where SNORT's rule sets can be updated regularly to counteract newly identified threats. This adaptability, coupled with AWS's centralized logging and monitoring features, enables proactive threat management and rapid response to incidents.

This project also highlights the importance of a multi-layered defense strategy. Integrating multiple tools and using AWS's cloud capabilities allows us to create a system that not only blocks malicious traffic but also provides valuable insights into attack trends, which allows for continuous improvement of the security framework so that the application is better prepared to face future challenges.

This project, therefore, again highlights cost-effective security. With its pay-as-you-go approach, AWS presents an environment where organizations with a huge budget can institute complex mechanisms without necessarily undertaking significant front-end investments, thus leveling the playing ground for deploying advanced cybersecurity at small to medium-sized businesses.

## II. LITERATURE SURVEY

In conducting a literature survey, research should focus on current cybersecurity threats and mitigation strategies, including a review of scholarly articles, white papers, and industry reports on web security. Key areas of focus should be the effectiveness of intrusion detection systems (IDS) like SNORT and the role of reverse proxies in enhancing web server security. The survey should also examine case studies to understand the practical challenges and benefits of integrating IDS with proxy servers. This comprehensive analysis will help in developing robust cybersecurity solutions for web applications.

According to Survey on Host and Network Based Intrusion Detection System done by Niva Das et al. [1] Network-based and host-based IDS prevent both insider as well as outsider attacks. There are always changing modes of intrusion detection but Most of the systems use signatures that look for patterns of abuse and either automatically responds to the misuse or intimates system administrator to take proper action. Some intrusion detection systems even sense misappropriation by using behavioral data. forensics. Because some of the automatisms carry an inherent danger, human intervention is always needed that can monitor the state of the system itself.

Amrit Pal Singh et al. [2] suggested that by using IDS, is totally dependent on the requirements and results needed out of it. IDS is very flexible, and can be used for various purposes or can also be used in either HIDS or NIDS mode[2] Also after defining the type of results need to be obtained, its placement can be finalized in case of NIDS. It works totally on what are the priorities of a company or an individual is. We can use IDS to tackle with intruders in standalone or multi-network machines/systems. On the other hand Logs can help us compare or create new set of records/rules for future reference and measuring system efficiency.

As we came across to this research paper we got to know that Kopelo Letou et al. [3] Singh had surveyed the latest up-to-date technology trend on HIDPS and then selected the best intrusions detection techniques and algorithms for building the proposed model expecting high promising security, performance and accuracy. The field of HIDPS is intensive; recent research areas offer hundred percent security on computer systems and Information Systems that can detect and prevent all types of intrusions and malicious activities in real time, creating no false alarms and without any human intervention. This HIDPS chooses the best algorithm individual for Misuse detection is C4.5 Decision tree algorithm and Anomaly detection techniques is Support vector machine algorithm respectively, and intrusions detection test data have to pass through two phases i.e., first misuse detection engine and then anomaly detection engine. Any malicious activities and HIDPS can detect and prevent any internal or external intrusion or attacks in the computer system because of abnormal behaviors.

In the study, the research examines the management of network security using Snort, an open-source intrusion detection system (IDS). The study is focused on securing network infrastructure against hackers and intruders who have been able to target high-profile company networks and web services. The research provides an overview of the many methods developed for improving the security of a network using firewalls, encryption, and virtual private networks and the need for intrusion detection systems to be used in tandem with these techniques. Snort analysis leads to the explanation of how such a system could be implemented within a network to detect any suspicious events and alert administrators to these threats..[4]

The study by Sharma, Mukesh Kumar et al. [5] This paper talks about the performance analysis of a real-time intrusion detection and prevention system using Snort. This includes performance and reports from Snort, network traffic analysis and the alert ratio of various signatures for particular attacks that may occur in the given network. This research proposes to give a comprehensive report on Snort's work as an intrusion detection tool: its ability to identify most web attacks against network safety.

The research paper "Improving the Efficiency of Snort-IDS Rules for Network Probe Attacks" by Phongphan Khamphakdee et al. [6]The methodology adopted in upgrading Snort-IDS rules will be outlined. For the assessment of performance, the researchers used the MIT-DARPA 1999 dataset that contains normal and anomalous traffic. Three procedures are involved: First is the analysis and exploration of previous Snort-IDS rules for improvement; second, analysis by Wireshark software of packet data obtained from the dataset; lastly, implementation of upgraded Snort-IDS rules for detecting probes against the network. The effectiveness of the proposed rules was then compared against the Detection

Scoring Truth, and it is revealed that the proposed rules gained higher accuracy in detecting network probe attacks.

The research paper titled ”Log Visualization of Intrusion and Prevention Reverse Proxy Server Against Web Attacks” by Teddy Mantoro et al. [7] It outlines a methodology using a reverse proxy server integrated with ModSecurity in order to prevent and detect web attacks, especially SQL Injection Attacks (SQLIA). The reverse proxy processes the incoming client requests, applies security rules, and logs suspicious activities. These are then visualized to assist web administrators in monitoring and identifying potential attacks efficiently.

In ”Snort - Lightweight Intrusion Detection for Networks” by Martin Roesch et al. [8], In doing this, the methodology focused on capturing network traffic between the target and attack hosts. The captured data would be analyzed to identify unique signatures that would be condensed into specific Snort rules for the implementation of these in the Snort intrusion detection system. These rules enabled immediate real-time identification and responses against potential threats. Its robust capability towards intrusion detection was validated with numerous experiments and continuous monitoring of these rules.

In the research paper titled ”Network Intrusion Detection using SNORT” by Kurundkar G.D et al. [9] The methodology includes the use of Snort, an open-source network intrusion detection and prevention system, to monitor and analyze network traffic. The system is based on a rule-driven language combining signature, protocol, and anomaly-based inspection methods. The authors implemented Snort in both passive and inline modes to allow for real-time detection and response to potential security threats. The components of Snort include the packet decoder, preprocessors, detection engine, logging and alerting system, and output modules. Configuring these components was set up to effectively identify and mitigate intrusions by analyzing network packets and applying predefined rules.

In the research paper ”Research on Intelligent Intrusion Prevention System Based on Snort,” authored by Hui Li and Dihua Liu [10] the methodology involves using an SVM to improve the Snort intrusion detection system. Authors implement an intelligent intrusion prevention system by combining Snort with a firewall, employing the pattern matching capabilities of Snort for known attacks, and SVM for classifying and detecting new or unknown intrusions. The system preprocesses network data, trains the SVM using this data, and applies learned patterns to classify network traffic, providing real-time responses to identified threats. With the ability of SVMs to work with high-dimensional data, it suits intrusion detection, where the goal of the system is the improvement of detection accuracy along with a reduction in error rates.

In the research paper ”Performance Analysis of Snort-based Intrusion Detection System,” author Akash Garg et al.[11] Investigate efficiency of Snort-based IDS in the detection of the most diverse network attacks. During the research, the use of the IDEVAL dataset enabled simulating network traffic against Snort, an open-source and signature-based IDS. Thus, methodology included detailed examination using Snort rules on different known attack patterns in order to detect intrusions. The authors also incorporated anomaly-based detection techniques to make the system better able to detect new attacks. Therefore, misuse detection along with anomaly detection techniques have been combined in this approach, which was aimed to improve the detection rate by reducing false positives and gives an all-around performance of the IDS in real-world scenarios.

O.B. Lawal et al. [12] They employed a detailed methodology in their study ”Analysis and Evaluation of Network-Based Intrusion Detection and Prevention System in an Enterprise Network Using Snort Freeware.” For this purpose, they used Snort, which is the famous open-source intrusion detection and prevention system. In such a process, the intruder’s suspicious activities could be monitored by setting up Snort on an enterprise network to capture and analyze data packets. They defined multiple attack signatures and rules inside Snort in order to detect common intrusion types. The captured data was further analyzed to examine the Snort’s efficacy in recognizing and preventing attacks on the basis of network activity. They further considered the performance of the system, for example, to handle large amounts of traffic and whether it could properly distinguish legitimate from malicious activity.

In the research paper ”Intrusion Detection Prevention System using SNORT,” the authors Aaliya Tasneem et al. [13] They describe their methodology as follows: They implemented the IDPS using Snort as an open-source tool most widely used for network security. This approach included setting up Snort in various modes that include sniffer mode, packet logger mode, and NIDS mode. The Snort rules have been configured to detect malicious activities and prevent them through real-time analysis of network packets. This practical implementation highlights the importance of using signature-based and anomaly-based detection methods to enhance network security.

## III. METHODOLOGY

The methodology of our project, ”Intrusion Detection and Prevention for Web Apps Using SNORT and Proxy Server,” is centered around building a multilayered security system that integrates SNORT and NGINX within a scalable and robust AWS cloud infrastructure.

### *1) User Interaction*

The system starts with user interaction. Here, the users will access the website deployed on AWS. These interactions generate network traffic that is in terms of requests and responses between the user’s device and the website. This can vary from simple HTTP or HTTPS requests to complex application-specific requests. Although most of the user traffic will be legitimate, there is always a chance of malicious packets trying to exploit some vulnerabilities, so monitoring and securing these interactions before they reach the application layer is essential.

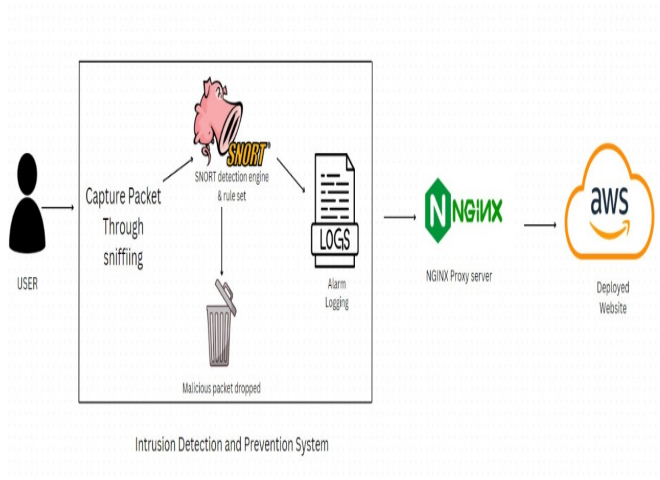



Fig. 1: Architecture Diagram for Intrusion Detection & Prevention for Web Apps Using SNORT & Proxy Server

*2) Packet Sniffing*

The first step towards securing the system is packet sniffing, which involves capturing in real-time all data packets traveling through the network. This process allows the system to analyze the content, source, destination, and behavior of each packet. Intercepting all network communications, packet sniffing thus ensures early identification of potential threats. This mechanism is critical for detecting anomalies such as unauthorized access attempts, suspicious data payloads, or abnormal traffic patterns that may indicate an ongoing attack.

*3) SNORT Detection Engine*

Once packets are captured, they are passed through the SNORT detection engine, which is actually the heart of the IDPS. SNORT uses a rule-based powerful engine to evaluate packets against known attack patterns or suspicious behavior. For example, it can detect threats such as SQL injection and cross-site scripting, block port scans, or DOS attempts. Any packet that can be matched to any defined malicious signatures is dropped as soon as possible to do no further harm, but an alert is logged, and legitimate packets pass the analysis to be allowed to continue. Given that SNORT adapts the rule set for new emerging threats, it is crucial in real-time network security.

*4) Log Management*

Every malicious packet detected by SNORT is logged to maintain a record of security incidents. These logs contain critical details such as the time of detection, the packet's origin and destination, and the rule or signature that flagged it as malicious. Such detailed logging is essential for forensic analysis, enabling system administrators to trace the source of attacks, understand their nature, and fine-tune the system's defenses. Log management also provides historical insights into the threats encountered by the system, assisting in developing stronger and proactive security measures.

*5) NGINX Proxy Server*

After filtering out malicious packets, the legitimate traffic is forwarded to an NGINX proxy server. NGINX improves system performance and security through its reverse proxying, distributing incoming traffic across backend servers and terminating SSL, which saves backend servers from the processing overhead of encryption and decryption of HTTPS traffic. Moreover, NGINX increases user experience by providing cache, which delivers frequently requested data faster. The system with NGINX also ensures smooth traffic flow, balanced server loads, and added protection against web-based attacks.

*6) AWS Deployed Website*

The final level of the system is the AWS-hosted website wherein legitimate and filtered traffic is further processed. This ensures that by using AWS, a deployment environment for web applications is more scalable and secure, making it possible for the website to have high availability and responsiveness even amidst traffic surges. There are more features of infrastructure with auto-scaling global content delivery, and built-in security tools like AWS Shield that support the system itself. The users will be able to access the website in a seamless and secure environment, supported by a backend that effectively combines detection, prevention, and performance optimization mechanisms.

## IV. Result and Discussion

This project successfully demonstrates the development of an integrated system that combines NGINX and Snort to detect and prevent web-based intrusions, such as HTTP flooding, ICMP requests, and DoS attacks. The use of NGINX as a proxy server ensures efficient traffic management, while Snort, a powerful intrusion detection system, monitors incoming requests for malicious activities. Together, these tools improve web application security and protect against potential attacks.

Figure 1 demonstrates HTTP requests logged by Snort in the monitoring activity. The system successfully catches every detail of the HTTP request. It gives detailed information on source IP, destination IP, and the type of traffic. Analyzing that information will help the system realize any patterns that signify possible malicious activities, as well as repeated access through one source.

Similarly, Figure 2 depicts ICMP requests logged by Snort. Most reconnaissance attacks use ICMP requests to check the availability of servers. Snort will be able to detect and log such requests, which helps to identify potential attempts to scan or probe the system. Such traffic can be proactively blocked.

Besides the monitoring provided by Snort, Figure 3 indicates NGINX proxy server logs that can provide an overall view of all incoming and outgoing web traffic. Logs are crucial to understand the behavior of traffic as it will enable the administrator to identify unusual requests or abnormal patterns, which should be investigated further.

To test the system's capability to detect and prevent attacks, Figure 8.4 focuses on intrusion detection for a simulated DoS

(Denial of Service) attack. During the test, Snort successfully detected and logged multiple abnormal requests, thus showing its reliability in identifying malicious attempts to overwhelm the server. The system can then trigger preventive actions by detecting these activities early on.

Lastly, Figure 8.5 displays the deployed website hosted on AWS. Under the cover of the integrated NGINX and Snort system, the website runs fluently while keeping malicious traffic away from legitimate users' access. This successful deployment highlights the practical implementation of the system in a real-world cloud environment.

In conclusion, the project demonstrates the effectiveness of integrating Snort and NGINX for intrusion detection and prevention. The system monitors HTTP and ICMP requests, logs proxy server data, identifies DoS attacks, and ensures enhanced security for web applications. The results validate the system's capability to provide early warnings and enable timely interventions, making it a reliable solution for protecting web servers from malicious threats.

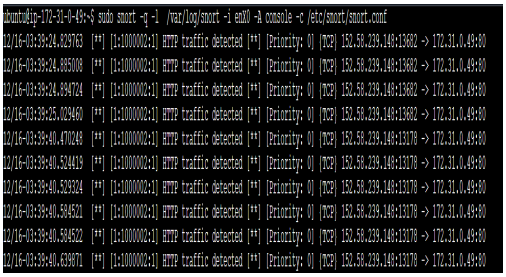



Fig. 2: HTTP Traffic Detection using SNORT

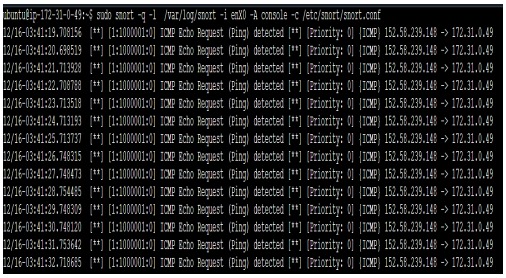



Fig. 3: ICMP Traffic Detection using SNORT

Fig. 4: NGINX Proxy Server logs

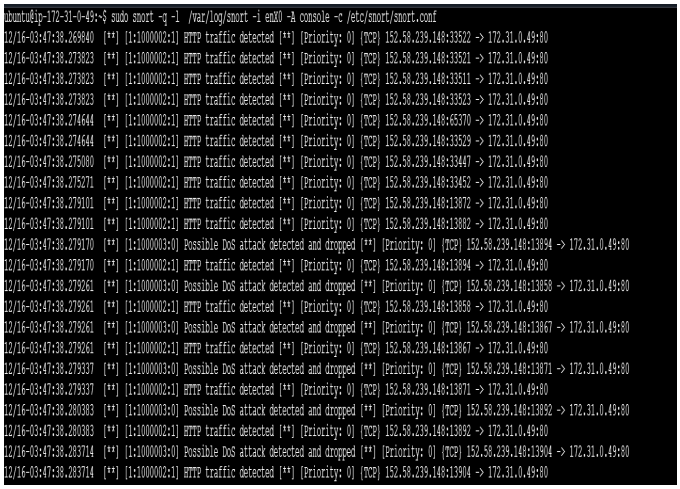



Fig. 5: Intrusion detection for DOS Attack

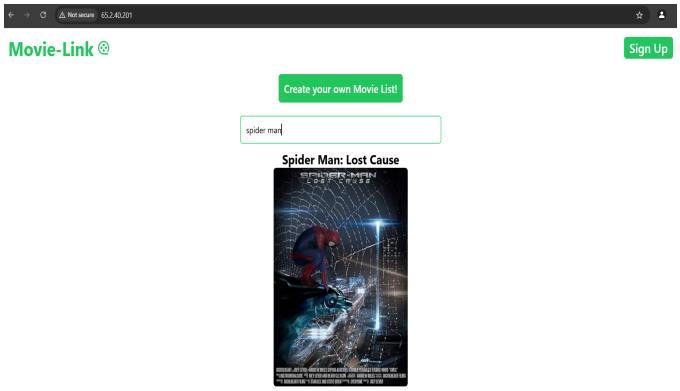



Fig. 6: Deployed Website on AWS

## V. CONCLUSION

The project ”Intrusion Detection and Prevention for Web Apps Using SNORT and Proxy Server” has successfully demonstrated an effective and scalable approach to securing web applications in a cloud-based environment. By integrating SNORT, the open-source intrusion detection and prevention system, with the NGINX proxy server, and by using the robust infrastructure of AWS, the system provides a multi-layered security architecture that is capable of defending against a wide range of cyber threats. This combination ensures real-time detection and mitigation of malicious activities while enhancing the overall performance, availability, and reliability of the web application.

Through precise packet analysis in SNORT and efficient traffic m anagement i n N GINX, t he s ystem p revents unauthorized access to the application while letting legitimate requests proceed normally. Centralized logging and monitoring capabilities of AWS further add to the strength of the security framework as they allow the detailed analysis of attack patterns and trends to refine t he d etection r ules a nd i dentify potential vulnerabilities.

The scalability and adaptability of the system are significant achievements, allowing it to handle fluctuating traffic loads and evolving threat landscapes without compromising security or performance. The proactive nature of this deployment ensures that the web application remains protected against both current and emerging cyber threats. Additionally, the insights gained from this project contribute to the broader understanding of how cutting-edge security mechanisms can be effectively integrated into modern cloud environments.

This project addresses the growing complexity of cyber-attacks by combining advanced security tools with cloud-based solutions. The practical, cost-effective, and scalable methodology for building secure web applications will set an excellent foundation for future enhancement. In general, the successful deployment of this system ensures the protection of the web application and provides a model for safeguarding similar digital services in cloud environments, reinforcing the importance of proactive and adaptive cybersecurity strategies.

## VI. ACKNOWLEDGMENT

We would like to thank Ms. Prajna U R, Assistant Professor, Department of ISE, Sahyadri College of Engineering and Management, for her constant support and guidance throughout our project. Her help and suggestions made this work possible and successful.

## REFERENCES

[1] Niva Das and Tanmoy Sarkar. Survey on host and network based intrusion detection system. International Journal of Advanced Networking and Applications, 6(2):2266, 2014.

[2] Amrit Pal Singh and Manik Deep Singh. Analysis of host-based and networkbased intrusion detection system. International Journal of Computer Network and Infor- mation Security, 6(8):41–47, 2014.

[3] Kopelo Letou, Dhruwajita Devi, and Y Jayanta Singh. Host-based intrusion detection and prevention system (hidps). International Journal of Computer Applications, 69(26):28–33, 2013.

[4] Lawal, B. O. and Julius Olatunji Okesola. “Managing Network Security with Snort Open Source Intrusion Detection Tools.” (2014).

[5] Sharma, Mukesh Kumar et al. “Performance Analysis of Real Time Intrusion Detection and Prevention System using Snort.” International journal of engineering research and technology 1 (2012): n. pag.

[6] N. Khamphakdee, N. Benjamas and S. Saiyod, ”Improving Intrusion Detection System based on Snort rules for network probe attack detection,” 2014 2nd International Conference on Information and Communication Technology (ICoICT), Bandung, Indonesia, 2014,

[7] T. Mantoro, N. b. A. Aziz, N. D. b. M. Yusoff and N. A. b. A. Talib, ”Log Visualization of Intrusion and Prevention Reverse Proxy Server against Web Attacks,” 2013 International Conference on Informatics and Creative Multimedia, Kuala Lumpur, Malaysia, 2013.

[8] Roesch, Martin. “Snort - Lightweight Intrusion Detection for Networks.”(1999).

[9] Kurundkar, G. D., N. A. Naik, and S. D. Khamitkar. ”Network intrusion detection using Snort.” International Journal of Engineering Research and Applications 2.2 (2012): 1288-1296.

[10] Hui Li and Dihua Liu, ”Research on intelligent intrusion prevention system based on Snort,” 2010 International Conference on Computer, Mechatronics, Control and Electronic Engineering, Changchun, China

[11] A. Garg and P. Maheshwari, ”Performance analysis of Snort-based Intrusion Detection System,” 2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2016.

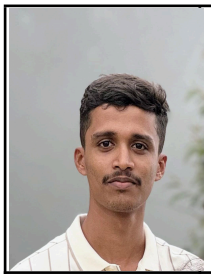
[12] Lawal, Babatunde Ibitola, A Longe, O. (2013). Analysis and Evaluation of Network-Based Intrusion Detection and Prevention System in an Enterprise Network Using Snort Freeware. 6. 169.

[13] Tasneem, A., Kumar, A., Sharma, S. (2018). Intrusion Detection Prevention System using SNORT321. International Journal of Computer Applications, 181(32), 21-24.

PROFILE DETAILS

Guide:
**Mrs. Prajna U R** is serving as an Assistant Professor in the Department of Information Science and Engineering (ISE) with 7 years of teaching experience. She holds an M.Tech degree in Computer Applications in Industrial Drives from VTU, Belagavi. Her areas of interest include the Internet of Things (IoT), Artificial Intelligence & Machine Learning (AI/ML), Cybersecurity, and Renewable Energy

TEAM MEMBERS



Ranjith Kumar
4SF21IS075
ISE 8th B
Sahyadri College of Engineering and Management
Mangaluru
ranjithhkumarshetty2003@gmail.com
8660023548

Mohamed Adeeb Farzan
4SF21IS048
ISE 8th B
Sahyadri College of Engineering and Management
Mangaluru
adeebsaqib431@gmail.com
7349416148

Manish J Rai
4SF21IS043
ISE 8th B
Sahyadri College of Engineering and Management
Mangaluru
mrai263407@gmail.com
7338091893

Rohit Kulkarni
4SF21IS077
ISE 8th B
Sahyadri College of Engineering and Management
Mangaluru
rohitkulkarni232002@gmail.com
8660119800