“ B.R.I.C.S Firewall - Behavioral Response and Intrusion Classification System”

Synopsis submitted to

Shri Ramdeobaba College of Engineering & Management, Nagpur

in partial fulfillment of requirement for the award of

degree of

Bachelor of Engineering

In

COMPUTER SCIENCE AND ENGINEERING

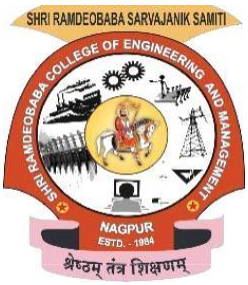
(CYBERSECURITY)

By

Mr. Eeshan Wadodkar
Mr. Ayush Kambde
Mr. Kalash Jaiswal
Mr. Vedank Naidu
Mr. Vedant Madhwe

Guide

Dr. Rashmi Welekar



Computer Science and Engineering

Shri Ramdeobaba College of Engineering & Management, Nagpur

440013

Project Title: “B.R.I.C.S Firewall”

Project Definition:

Developing a machine learning-driven Behavioral Response and Intrusion Classification System to enhance network security by accurately detecting and categorizing emerging threats, facilitating timely and effective response mechanisms.

The B.R.I.C.S Firewall project addresses the critical need for enhancing network security in today's digital landscape. By developing a sophisticated Behavioral Response and Intrusion Classification System, the project aims to fortify cybersecurity measures, ensuring the protection of sensitive information, organizational integrity, and national security interests. This initiative responds to the escalating cyber threats posed by increasingly sophisticated adversaries, leveraging machine learning and behavioral analysis to detect and categorize emerging threats in real-time.

Project Objectives:

- **Phase 1: Research and Analysis**

  Analyze user requirements and prevailing cybersecurity trends.
  Engage with cybersecurity professionals and law enforcement agencies to understand expectations.
  Identify emerging threats and evolving attack vectors.

- **Phase 2: Design and Prototyping**

  Design a robust system architecture capable of adaptive response to dynamic cyber threats.
  Develop prototypes for key components to validate design assumptions and refine functionalities.

- **Phase 3: Development and Implementation**

  Implement machine learning algorithms and behavioral analysis techniques.
  Develop the core functionalities of the B.R.I.C.S Firewall, including intrusion detection and classification modules.
  Integrate components into a cohesive cybersecurity solution.

- **Phase 4: Evaluation and Optimization**

Conduct rigorous testing in simulated and real-world environments.
Evaluate system performance, detection accuracy, and false positive rates.
Identify vulnerabilities and areas for optimization.
Iterate on system design and algorithms to enhance effectiveness and reliability.

- **Phase 5: Documentation and Training**

  Prepare comprehensive documentation detailing system architecture, algorithms, and operational procedures.
  Develop training materials to educate users on system operation, maintenance, and best practices.

- **Phase 6: Deployment and Support**

  Deploy the B.R.I.C.S Firewall in operational environments.
  Provide ongoing technical support and maintenance services.
  Address user queries, troubleshoot issues, and optimize system performance.

Methodology:

The methodology adopted for the B.R.I.C.S Firewall project encompasses a systematic approach, comprising research, design, development, evaluation, and deployment phases. Key aspects of the methodology include:

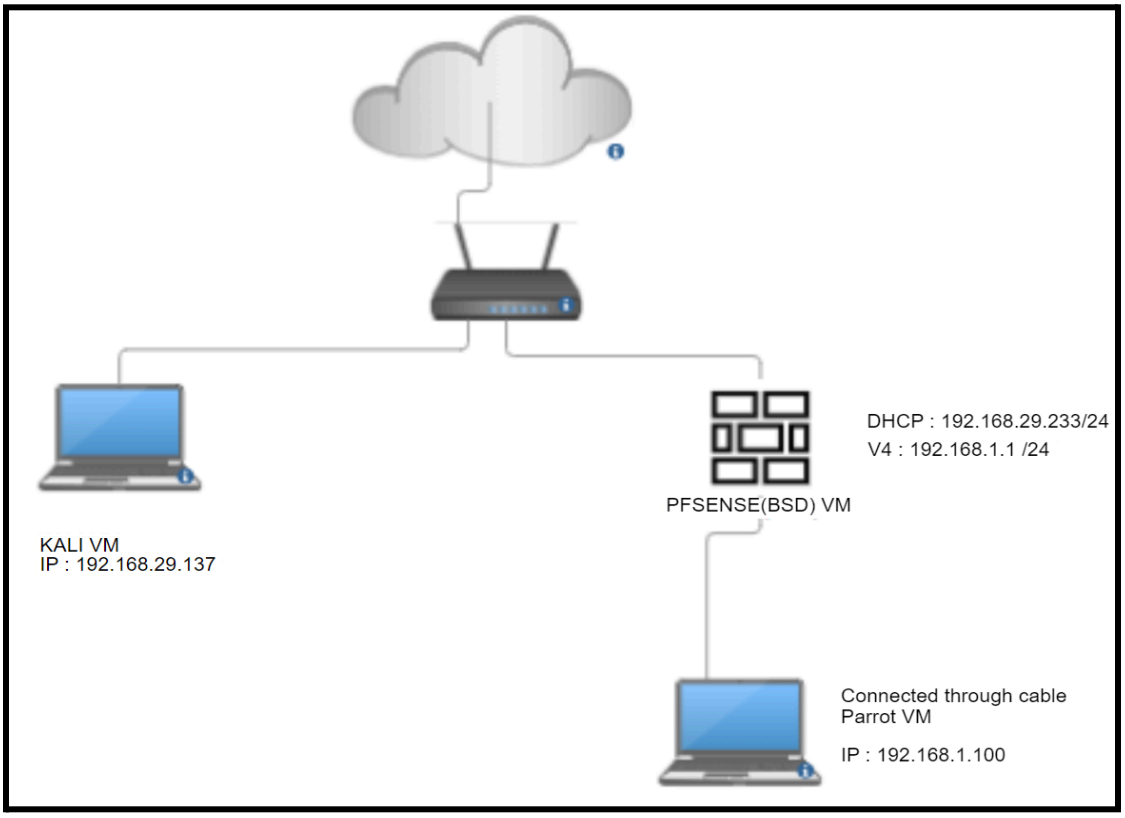
Research: Conducting comprehensive research on cybersecurity trends, user requirements, and emerging technologies to inform system design and development.
Design: Designing a flexible and scalable system architecture capable of accommodating evolving cybersecurity threats and user needs.
Development: Implementing machine learning algorithms, behavioral analysis techniques, and other advanced technologies to realize the functionality of the B.R.I.C.S Firewall.
Evaluation: Evaluating the performance of the system through rigorous testing in controlled environments and real-world scenarios, identifying areas for optimization and improvement.
Deployment: Deploying the B.R.I.C.S Firewall in operational environments, providing user training, and offering ongoing support and maintenance services to ensure system reliability and effectiveness.
Deliverables:

Fully Functional B.R.I.C.S Firewall Software: The primary deliverable of the project is a fully functional Behavioral Response and Intrusion Classification System capable of detecting and categorizing cyber threats effectively.

Comprehensive Documentation: Detailed documentation encompassing system architecture, algorithms, operational procedures, and user manuals to facilitate system understanding and utilization.

Training Materials: Educational materials including training modules, tutorials, and workshops to equip users with the knowledge and skills required to operate and maintain the B.R.I.C.S Firewall.

Deployment and Support Services: Deployment of the B.R.I.C.S Firewall in operational environments, along with ongoing technical support and maintenance services to address user queries and ensure system reliability and performance.



Expected Outcome

Project Scope:

The project scope encompasses the development of a comprehensive cybersecurity solution designed to:

Detects and responds to cyber threats based on behavioral patterns and intrusion classification.
Implement machine learning algorithms for accurate threat detection with minimal false positives.
Provide ongoing technical support and maintenance services to ensure system reliability and effectiveness in an operational environment.

Technology:

1. PfSense
2. Parrot OS
3. Kali Linux
4. FreeBSD
5. Rsyslogs
6. DDOS detection ml model

Deliverables :

Following are the expected outcomes of our project :

1. A web Firewall to gather
2. Similar attack pattern analysis
3. Early detection.
4. efficient evidence collection.

Roll no.	NAME	Guide
33	Ayush Kambde	Dr. Rashmi Welekar
35	Eeshan Wadodkar	
39	Kalash Jaiswal	
64	Vedank Naidu	
65	Vedant Madhwe	

approved by:
Dr. Rashmi Welekar
RCOEM, Nagpur