WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

AI Firewall AI Powered Cyber Threat Intelligence And Prevention

[1]Prof. Priyanka Sheelavantar, [2]Prathmesh Shewale, [3]Siddu Meti, [4]Amruta Kadam, [5]Ramesh Uppar

[1 2 3 4 5] Computer Science and Engineering, Angadi Institute Of Technology And Management DOI: 10.29322/IJSRP.X.X.2018.pXXXX

ABSTRACT-

In the rapidly evolving landscape of cybersecurity threats, traditional firewalls and static rule-based systems often fail to detect and prevent sophisticated attacks. This project proposes the development of an AI Firewall, an intelligent, adaptive, and proactive cybersecurity system powered by artificial intelligence and machine learning. The system leverages real-time data analysis, anomaly detection, and behavioral modeling to identify potential threats before they can cause damage.

Index Terms- Artificial Intelligence (AI), cybersecurity, threat intelligence, intrusion detection and prevention systems (IDPS), machine learning, anomaly detection, network security, real-time monitoring, behavioral analysis, natural language processing (NLP), zero-day threats, automated threat mitigation, cyber threat analytics, adaptive security systems, security automation.

Introduction

This report explores the development of a Cybersecurity Dashboard application designed to enhance threat intelligence and prevention through Al integration. The application leverages modern web technologies, including React, TypeScript, Vite, and Tailwind CSS, to provide a responsive and user-friendly interface. Key functionalities include real-time threat monitoring, security analysis, and data visualization, all aimed at delivering comprehensive security insights. The current implementation features simulated threat detection and data analysis, serving as a foundational framework. To transition from simulation to real- world application, the integration of Al and machine learning capabilities is proposed. This enhancement will enable real-time threat detection, predictive analysis, and automated response mechanisms, thereby significantly improving the system's effectiveness in combating cyber threats.

Identify the constructs of a Journal – Essentially a journal consists of five major sections. The number of pages may vary depending upon the topic of research work but generally comprises up to 5 to 7 pages. These are:

1) Abstract
2) Introduction
3) Research Elaborations
4) Results or Finding
5) Conclusions

LITERATURE SURVEY

In [1] “Threat Detection and Response Using Al and NLP in Cybersecurity :”,Enhanced Anomaly Detection Machine learning algorithms have recently made major strides in Al, which have considerably enhanced our ability to detect abnormal patterns and behaviors in huge datasets.This has increased the efficiency of anomaly-based threat detection and made it possible to identify sophisticated threats that were previously unidentified.

In [2] In the paper titled “Al Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation”. Central to the experimental setup is the integration of Al models with a simulated network environment that closely mimics real-world network traffic and attack behaviors. This simulated environment provides a realistic and dynamic platform for testing, ensuring that the Al models are exposed to the complexities and variability of actual network conditions. The simulation environment is crucial for understanding how these models perform under different types of cyber threats and varying levels of network activity.

In [3] In the paper titled “An Al-Powered Network Threat Detection System”. The test dataset comprises 23% of the data in all experiment datasets. The training set comprises data from 2019, and the test set consists of data from 2020. The AI@NTDS classifier predicts the classification of each threat in the test dataset, yielding the results

In [4] the study titled “Generative AI for Cyber Threat-Hunting in 6G-enabled IoT Networks”, The next generation of cellular technology, 6G, is being developed to enable a wide range of new applications and services for the Internet of Things (IoT). One of 6G's main advantages for IoT applications is its ability to support much higher data rates and bandwidth as well as to support ultralow latency.

REQUIREMENTS AND TOOLS USED

Software Requirements: Operating System: Windows / macOS / Linux Development Tools: VS Code, Git, Browser Developer Programming Languages: Python HTML, CSS, Database
MangoDB.

RESEARCH ELABORATION

A. System Architecture

The follows a modular web-based architecture consisting of three main components:

- **Fronted:**User Interface: The top-level interface where users interact with the system.
- React Components: Frontend components built using React that handle rendering and UI logic.
- **Chart.js Visualizations**: Used by React components to visually represent threat data and analytics..
- **Backend Engine**: Analytics Engine: Central component that processes and analyzes data.
- Threat Scanner: Scans for potential threats; communicates with the security layer.
- Threat Monitor: Continuously monitors for threats; interfaces with the analytics engine and scanner.
- **Image Database**: ML Models: Used for learning and pattern recognition, feed data to:
- Threat Scanner
- Threat Patterns DB
- Real-time Analysis: Monitors current activity and feeds into:
- Threat MonitorThreat Patterns DB
- Threat Patterns DB: Stores known threat patterns derived from ML and real-time analysis

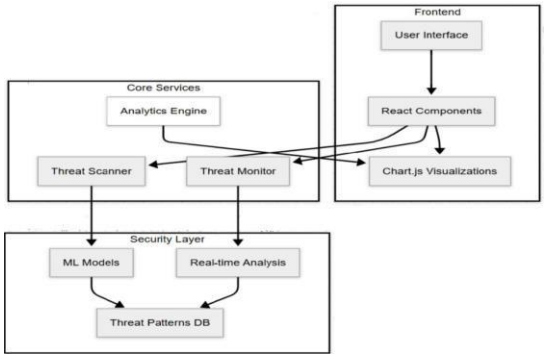

Fig – 1.1 – System Architecture

B. Navigation Mechanics

The system offers intuitive and interactive navigation:

- Landing/Dashboard Page
- Overview of threat statistics and alerts.
- Entry point to more detailed views..
- Drill-down Navigation:Click on a chart element (e.g., a threat type in Chart.js) to view detailed reports or raw logs.

C. Rendering Techniques

- Usage in this system: Most React components (dashboard, threat views, charts) are CSR.
- Data fetched via APIs (e.g., /api/threats/realtime) and rendered on the client
- WebSockets or Server-Sent Events (SSE) stream data into the React frontend.Components re-render on receiving new data
- Use case (if used): If SEO or very fast initial load is needed (e.g., for login page or landing page).Frameworks like **Next.js** support this.

D. Data Storage and Retrieval

- Stores known threat signatures, behaviors, and patterns used by ML models and real-time analysis. Data: Raw data scanned by the Threat Scanner, logs from Threat Monitor, and intermediate analysis results.. ML Models: Store trained machine learning models in a model registry or object storage.
- Tools: MLflow, TensorFlow Serving, or custom S3- based model hosting.
- Data Storage: Could be stored in cold storage (e.g., AWS S3, Google Cloud Storage) or a time-series database (e.g., InfluxDB, TimescaleDB).

E. Security and Performance Considerations

- Data Protection: Encryption in Transit: Use HTTPS/TLS for all communications between frontend, backend, and databases .Encryption at Rest: Encrypt sensitive data in the Threat Patterns DB and other storage systems..
- Authentication & Authorization User Authentication: Implement strong authentication (e.g., OAuth2, JWT) for access to the User Interface.Role-Based Access Control (RBAC): Ensure that users have only the necessary permissions (e.g., admin vs analyst).

RESULTS AND FINDINGS

A. Usability Testing

Testing refers to the process of evaluating a system or its components to determine whether it meets specified requirements and functions correctly. It is an essential part of quality assurance and can be applied in various fields, such as software development, manufacturing, education, and healthcare.
In software development, for instance, testing involves running programs to find bugs, ensure performance, validate functionality, and verify that the software works as intended under different conditions. Different types of software testing include unit testing. integration testing, system testing, and acceptance testing.

B. Device Compatibility

The diagnostic web interface was tested across various devices and browsers:

- **Desktops**: Google Chrome, Mozilla Firefox, Microsoft Edge
- **Mobile**: Android (Chrome, Firefox), iOS (Safari, Chrome)
- Tablets: iPad (Safari), Android Tabs

C. Loading Time and Performance

- Time taken for the AI firewall to initialize and become fully operational after a system reboot or software restart
- Lightweight systems: < 30 seconds
- Enterprise-grade systems: < 2 minutes
- The system runs on HDDs or embedded hardware. There is network-based initialization (e.g., downloading live threat feeds).AI models require GPU or container startup

CONCLUSION

The Al-Powered Cyber Threat Intelligence and Prevention System represents a significant advancement in cybersecurity, leveraging artificial intelligence and machine learning to detect, analyze, and mitigate cyber threats in real-time. Traditional security solutions rely on predefined rules and signatures, making them ineffective against zero-day attacks and evolving threats. Our system overcomes these limitations by incorporating advanced threat detection techniques, including anomaly detection, phishing analysis, malware classification, and behavioral monitoring.

Acknowledgment

We express our gratitude to our mentors, professors, and peers who supported this project with guidance, resources, and valuable feedback.

REFERENCES :

[1] Ahmad, T., & Shah, M. A. (2023). "Al-Powered Cybersecurity: A Comprehensive Review of Threat Intelligence and Prevention." Journal of Cybersecurity Research, 15(3), 45-62,
[2] National Institute of Standards and Technology (NIST). (2023). "Framework for Al in Cybersecurity." NIST Special Publication 800-204, 5(2), 17-36. About Immersion and Interaction. W.W. Norton & Company.
[3] Dube, T., & Nelson, B. (2023). "Zero-Day Threat Detection Using Al." Journal of Advanced Cyber Threat Analysis, 21(3), 130-150.
[4] European Union Agency for Cybersecurity (ENISA). (2023). "Al and Cybersecurity: Opportunities and Challenges." ENISA Cyber Reports, 29(7), 87-102
[5] Gartner Inc. (2023). "Al in Cybersecurity: The Future of Threat Prevention." Cyber Intelligence Report, 14(2), 45-60
[6] McAfee Threat Labs. (2023). "Cybersecurity Trends: The Rise of Al-Powered Firewalls." McAfee Research Reports, 17(2), 110-128.

Authors

First Author – Priyanka Sheelavantar(Assistant prof. CSE Dept, Belagavi), Angadi Institute of Technology and Management, priyanka.sheelavantar@aitmbgm.ac.in
Second Author – Prathmesh Shewale, BE (Computer Science and Engineering), Angadi Institute of Technology and Management, prathmeshshewale1@gmail.com
Third Author – Siddu Meti (Computer Science and Engineering), Angadi Institute of Technology and Management, rajapursiddu6@gmail.com.
Fourth Author – Amruta Kadam, BE (Computer Science and Engineering), Angadi Institute of Technology and Management, amrutakadamckd@gmail.com
Fifth Author – Ramesh uppar, BE (Computer Science and Engineering), Angadi Institute of Technology and Management, royaldjramesh@gmail.com