IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024

Intrusion Detection System

Aishwarya Londhe[1], Sahil Gawathe[2], Prathamesh Pandey[3], Gajanan Date[4], Sameer Meshram[5]
Faculty, Department of Computer Engineering[1]
Students, Department of Computer Engineering[2,3,4,5]
KC College of Engineering, Thane, India

Abstract: *Our project introduces an Integrated Intrusion Detection System (IDS) designed to bolster network and system security through a multi-faceted approach. This comprehensive IDS seamlessly combined Machine Learning, Anomaly Detection, File Scanning, and DDoS Prevention mechanisms to offer robust defense against diverse cyber threats. At the heart of the system lies the Machine Learning component, which continuously adapts to the evolving threat landscape. By analyzing network traffic and system behavior, it identifies both known and emerging threats in real-time, reducing reliance on traditional signature-based detection methods and allowing organizations to proactively stay ahead of cybercriminals. Anomaly Detection constantly monitors network and system activity, comparing it against established baselines. Any deviations from these baselines trigger alerts, facilitating swift responses to unusual activities that may indicate security breaches. File Scanning is another vital component ensuring data integrity and preventing malware infiltration or data exfiltration. It conducts thorough file analysis, checking for suspicious code, behavior, or unauthorized access, and offers continuous monitoring to detect anomalies in real-time. Additionally, our IDS includes Distributed Denial of Service (DDoS) Prevention mechanisms. By detecting and mitigating DDoS attacks, the system ensures the continuous availability of network resources and services even under intense traffic loads. This integrated approach to intrusion detection and prevention leverages Machine Learning, Honeypots, Anomaly Detection, File Scanning, and DDoS Prevention, empowering organizations to safeguard critical assets, maintain data integrity, and ensure network security in today's dynamic and perilous digital landscape. Our IDS solution serves as a valuable addition to the cybersecurity toolkit for organizations seeking comprehensive security against a wide range of threats.*

Keywords: Intrusion Detection System

I. INTRODUCTION

In today's interconnected world, safeguarding the security of our digital networks and systems is paramount. The continuous evolution of cyber threats demands a flexible defense strategy. Our project introduces an Integrated Intrusion Detection System (IDS) that seamlessly integrates Machine Learning, Honeypot technology, Anomaly Detection, File Scanning, and DDoS Mitigation to deliver a robust and multi-layered security solution. Cyber threats can result in severe consequences, ranging from data breaches to financial losses. Our IDS utilizes Machine Learning to dynamically adapt to these threats, strategically capturing intruders using Honeypots, perpetually monitoring network activity through Anomaly Detection, and upholding data integrity with File Scanning. Furthermore, it proactively prevents DDoS attacks, ensuring uninterrupted service availability. A notable feature of our IDS is the storage of attack patterns utilized by intruders who have been enticed into our Honeypots. This repository of historical attack data empowers organizations to strengthen their security stance and forestall future attacks with greater accuracy. Additionally, our system diligently identifies malware, viruses, and Trojans, offering a comprehensive approach to intrusion detection and prevention. Our project presents a holistic solution to the ever-evolving cybersecurity landscape. It enables organizations to safeguard their assets, preserve data integrity, and defend against a wide array of threats while leveraging captured attack patterns to fortify their defenses. In a digital environment where innovation and threats coexist, our IDS emerges as a steadfast guardian of the digital realm.

DOI: 10.48175/IJARSCT-17606

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024

II. LITERATURE SURVEY

A survey of multiple papers on Intrusion Detection Systems (IDS) reveals a diverse array of techniques, challenges, and advancements within the field. Khraisat et al. (2019) offer insights into anomaly detection systems, emphasizing their application in IDS. Abbasgholi et al. (2021) explore Machine Learning methodologies like Random Forest and Convolutional Neural Networks (CNN) for early intrusion detection in industrial LAN networks, particularly leveraging Honeypots. Halimaa et al (2019) concentrate on machine learning-based adaptive defense mechanisms and pattern recognition within IDS. Musa et al. (2020) highlight the significance of detecting zero-day and novel threats using Machine Learning techniques in IDS. Ozkan-Okay et al. (2023) provide a thorough overview of existing IDSs, covering detection techniques, emerging attack types, protective measures, and recent scientific studies in the field. Samet et al. (2022) conducted a survey encompassing IDS techniques and tools, discussing various types of IDSs, detection methods, and challenges, and offering a comparative analysis of different IDS tools. Together, these studies significantly contribute to the understanding and advancement of IDS, addressing the constantly evolving cybersecurity landscape with a range of approaches and insights.

III. PROPOSED METHOD

Our proposed strategy for the Intrusion Detection System (IDS) entails a comprehensive approach aimed at detecting and addressing cyber threats effectively. Utilizing machine learning-based anomaly detection, role-based access control, encryption protocols, DDoS prevention measures, malware detection mechanisms, and strategically positioned honeypots, our IDS aims to offer robust defense capabilities. Through machine learning algorithms, we scrutinize network traffic patterns to detect any irregularities signaling potential intrusions, while role-based access control restricts unauthorized entry to critical resources. Encryption ensures data confidentiality and integrity, while DDoS prevention methods thwart large-scale attacks. Malware detection mechanisms pinpoint and isolate malicious software, and honeypots entice intruders, enabling us to gather valuable threat intelligence. By amalgamating these strategies, our IDS is poised to safeguard our network infrastructure against emerging cyber threats, ensuring operational security and continuity.

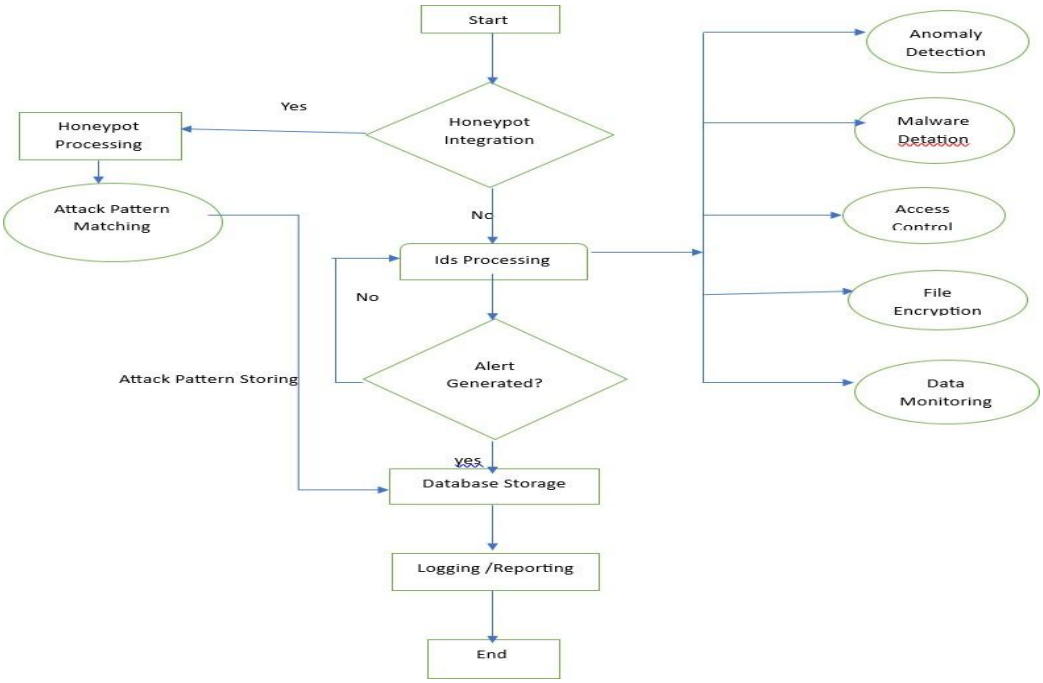


Fig 1 Flow Chart

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024

IV. IMPLEMENTATION

System Requirements:

Software Requirement:

- **Operating System:** Windows/Linux/Mac
- **Programming Language:** Python
- **Libraries/Frameworks:** Kivy

Desktop/Laptop Specifications:

- **Processor:** Intel Core i5 and above
- **RAM:** 8GB recommended
- **Storage:**10GB
- **Database** - MYSQL

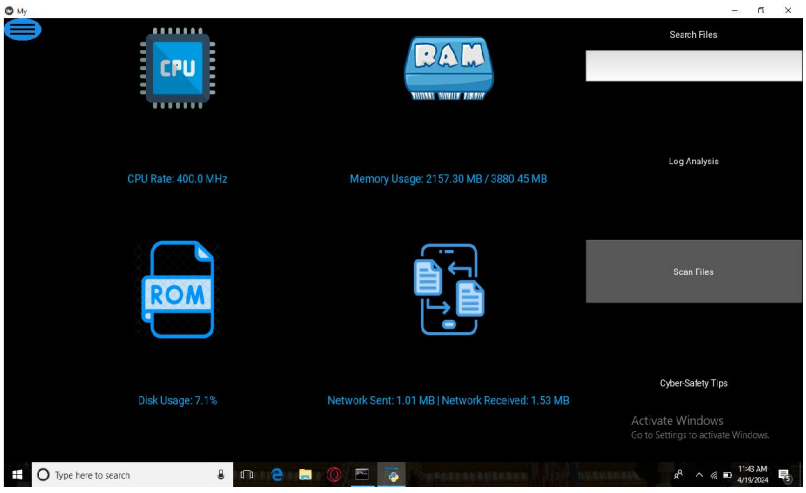


Fig 1 Home screen

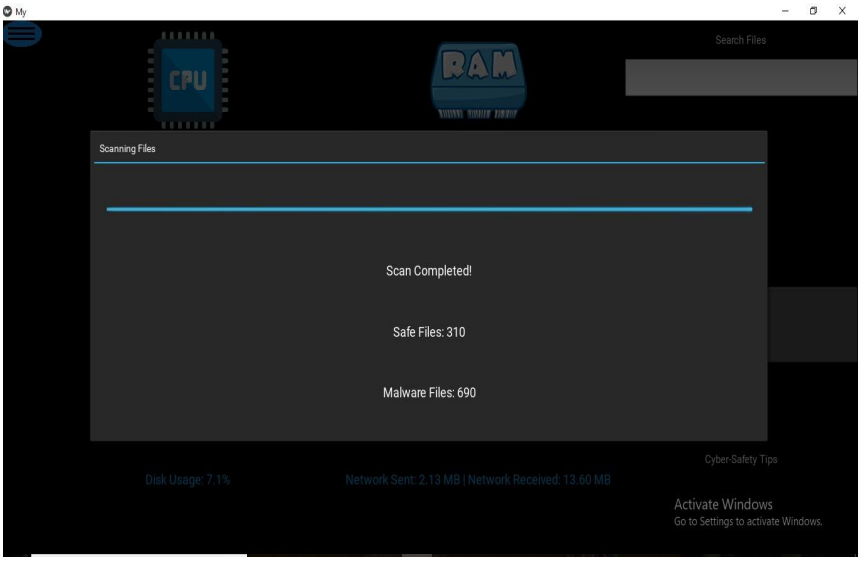


Fig 2 Scan File

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024

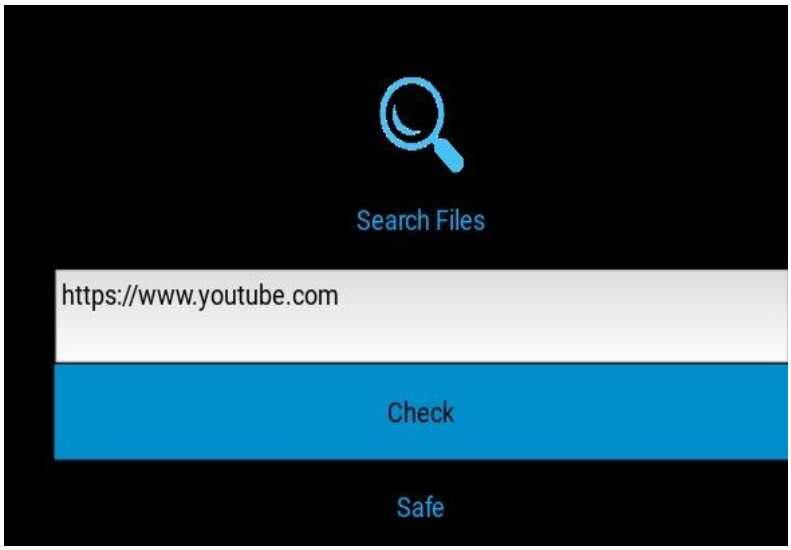
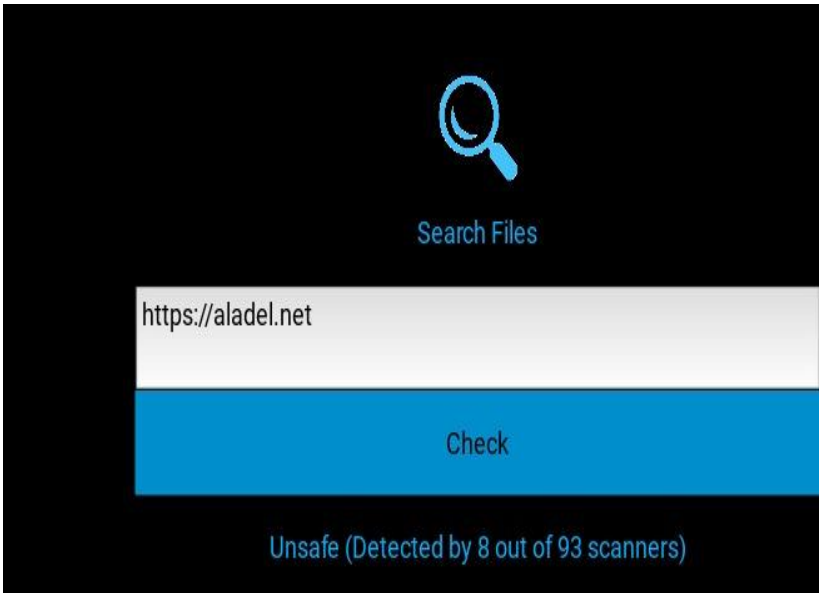


Fig 3 Search File



V. FUTURE SCOPE

The project scope for our Comprehensive Intrusion Detection System (IDS) encompasses several crucial elements. It involves designing and structuring the IDS, and delineating its fundamental components, such as Machine Learning, Anomaly Detection, File Scanning, DDoS Mitigation, and Attack Pattern Storage. This entails exploring how each element operates independently and collaboratively to furnish a robust defense against a myriad of cyber threats. The scope also encompasses data collection, establishing baselines, and generating alerts. Additionally, it extends to storing and analyzing historical attack patterns, facilitating future attack prevention, and bolstering malware detection capabilities.

The project delves into the advantages of deploying the IDS and delineates potential applications across diverse sectors, including enterprise networks and data centers. It offers insights into implementation considerations, and scalability guidelines, and addresses ongoing maintenance and regulatory compliance concerns. Finally, a concise cost analysis is provided to assess financial considerations. This comprehensive yet succinct scope delineates the primary areas of focus in the project.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024

VI. CONCLUSION

Our IDS project marks a significant leap forward in network security. Through a holistic approach that integrates machine learning-driven anomaly detection, role-based access control, encryption, DDoS prevention, and malware detection, we've established a resilient security framework. The project's triumph underscores our dedication to preemptive threat mitigation and adaptability amidst evolving cyber risks. Our IDS is primed to counter both known and unknown threats, with its incorporation of honeypots enabling us to capture emerging dangers. We've tackled challenges with inventive remedies, accruing invaluable insights for future endeavors. To sum up, our IDS stands as a formidable bulwark in the ever-changing cybersecurity arena, shielding digital assets and networks with unwavering commitment and expertise.

REFERENCES

[1]. Anderson, B., & Lee, J. (2018). Intrusion Detection Systems with Machine Learning: A Review.Journal of Network and Computer Applications, 60, 19-31.

[2]. Cisco. (n.d.). Implementing Role-Based Access Control. Retrieved from https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_rbac/configuration/xe-16-12/s ec-user-rbac-xe-16-12-book/sec-rbac-xe-16-12-book.pdf

[3]. Kaspersky. (2020).APT Trends ReportQ1 2020. Retrieved from https://securelist.com/apt-trends-report-q1-2020/96264/

[4]. Krebs, B. (2018). DDoS Attacks Skyrocket. Retrieved from https://krebsonsecurity.com/2018/12/ddos-attacks-skyrocket/

[5]. Microsoft. (n.d.). Encrypt Files and Folders. Retrieved from https://support.microsoft.com/en-us/windows/encrypt-files-and-folders-5a6bf6f7-199b-4b 2a-a854-29c2d83b6e30

[6]. Panda Security.(2019). Types of Malware and How to Detect Them. Retrieved from https://www.pandasecurity.com/mediacenter/malware/types-malware-detect/

[7]. RFC Editor.(2017). Guidelines for Writing an IANA Considerations Section in RFCs.Retrieved from https://www.rfc-editor.org/rfc/rfc8126.txt

[8]. Stallings, W. (2017). NetworkSecurity Essentials: Applications and Standards (6th ed.). Pearson.

[9]. The Web Application Security Consortium. (n.d.). Web Appliation Firewall Evaluation Criteria. Retrieved