CYBER SECURITY THREAT DETECTION

[1]Dr.G. Prasuna, [2]Annapareddy Venkata Ramana Naga Jyothi,[3]Upputuri Tarun Kumar,[4]Vari Sailaja,[5]Kagitha Jaswanth Raju

[1]Associate Professor, Dept COMPUTER SCIENCE AND ENGINEERING, St. Ann's College of Engineering and Technology Autonomous, Chirala 523155, India.

[2,3,4,5]U.G. Student, Dept of COMPUTER SCIENCE AND ENGINEERING, St. Ann's College of Engineering and Technology Autonomous, Chirala 523155 India.

ABSTRACT

Cyber security threat detection is a crucial aspect of protecting digital systems and networks from unauthorized access and attacks. With the rapid growth of technology, cyber threats have become increasingly complex and sophisticated. Organizations face challenges in identifying and mitigating these threats in real time. Cyber security threat detection systems aim to monitor network traffic, detect anomalies, and respond to potential attacks. These systems utilize advanced techniques such as machine learning, intrusion detection, and pattern analysis. Real-time monitoring helps prevent data breaches and financial losses. The proposed system can detect malware, phishing attacks, DDoS attacks, and unauthorized access attempts. Automated alerts notify administrators of suspicious activities. Threat detection enhances system reliability and trustworthiness. It reduces the dependency on manual monitoring. Data encryption and secure protocols complement detection mechanisms. Historical attack data helps improve system accuracy. Cloud-based monitoring ensures scalability. AI algorithms improve predictive capabilities. Threat detection protects sensitive information and user privacy. It is applicable to organizations, government agencies, and individuals. The system supports proactive security measures. Cyber security awareness is critical for all users. Overall, cyber threat detection systems play a vital role in maintaining digital safety.

KEYWORDS

Cyber Security Threat Detection Intrusion Detection System (IDS) Malware Detection Network Security

INTRODUCTION

In the digital age, cyber security has become a critical concern for organizations and individuals alike. Cyber attacks are increasing in frequency and complexity, targeting sensitive data and critical infrastructure. Threat detection systems are designed to identify potential security breaches and take preventive action. These systems continuously monitor networks, analyze traffic patterns, and detect abnormal behavior. Cyber threats can include malware, phishing attacks, ransomware, and DDoS attacks. Early detection helps reduce financial loss and reputational damage. Machine learning and artificial intelligence have improved detection accuracy. Threat detection systems can be implemented at network, application, and endpoint levels. Real-time monitoring is essential for quick response. Logging and alerting mechanisms help administrators respond efficiently. Historical attack data can be used to identify trends. Threat intelligence feeds enhance predictive capabilities. Automated systems reduce human error in monitoring. Cloud-based platforms provide scalability and flexibility. Security policies must be integrated into organizational procedures. Employees and users play a key role in security awareness. Detection systems complement firewalls and antivirus solutions. Overall, cyber threat detection ensures a secure computing environment.

LITERATURE SURVEY

Research on cyber security threat detection has evolved rapidly with technological advancements. Early systems relied on signature-based detection, which required known attack patterns. Anomaly-based detection systems emerged to identify unusual behavior. Machine learning algorithms such as decision trees, SVM, and neural networks have been applied to improve detection accuracy. Intrusion Detection Systems (IDS) monitor network traffic to detect potential threats. Studies show that combining signature and anomaly detection enhances system performance. Cloud-based security monitoring has gained popularity for scalability. Research highlights the importance of real-time detection and automated response. Data preprocessing and feature selection improve machine learning outcomes. Ensemble learning methods provide better predictive performance. Security Information and Event Management (SIEM) systems integrate logs and alerts. Threat intelligence feeds are used to detect emerging threats. Studies show DDoS and ransomware are the most common attacks. Network traffic analysis helps detect malware propagation. Deep learning methods improve detection of zero-day attacks. Comparative studies emphasize accuracy, speed, and false-positive reduction. Mobile and IoT security has become a research focus. Research also explores the integration of blockchain for secure logging. Overall, literature supports the use of AI and real-time monitoring in cyber security threat detection.

RELATED WORK

Several studies have been conducted on cyber security threat detection to improve network and system security. Early research focused on signature-based intrusion detection systems (IDS) that could detect only known attacks. Anomaly-based detection approaches were later introduced to identify unusual patterns in network traffic. Machine learning techniques, such as decision trees, support vector machines, and neural networks, have been applied to improve detection accuracy. Research highlights the use of hybrid systems combining signature and anomaly detection for better performance. Deep learning and AI-based models are increasingly used to detect zero-day attacks. Cloud-based threat detection systems have been proposed for scalability and real-time monitoring. Security Information and Event Management (SIEM) tools integrate logs from multiple sources to provide centralized monitoring. Studies emphasize reducing false positives to improve system reliability. Network traffic analysis is widely used to detect malware, phishing, and DDoS attacks. IoT and mobile device security are emerging areas of research. Data preprocessing and feature selection enhance detection efficiency. Ensemble learning methods have been applied to improve predictive performance. Threat intelligence feeds are integrated to detect emerging attacks proactively. Research also focuses on endpoint monitoring and automated response. Blockchain-based secure logging has been explored for tamper-proof records. Studies show AI models outperform traditional IDS in detecting sophisticated attacks. Continuous updates and adaptive learning improve system robustness. Comparative studies emphasize accuracy, speed, and scalability. Overall, literature demonstrates that combining machine learning, AI, and real-time monitoring is the most effective approach to modern cyber threat detection.

EXISTING SYSTEM

Existing cyber security systems rely heavily on manual monitoring and signature-based approaches. Firewalls and antivirus programs provide the first line of defense but cannot detect unknown threats. Traditional Intrusion Detection Systems (IDS) often generate high false-positive rates. Network traffic analysis is limited to predefined attack patterns. Monitoring large-scale networks in real time is challenging. Many existing systems fail to detect zero-day attacks. Malware detection is often reactive rather than proactive. Logging mechanisms may not provide actionable insights. Incident response is delayed due to manual intervention. Security Information and Event Management (SIEM) systems aggregate logs but require constant tuning. Existing cloud security solutions face scalability and latency issues. Some platforms do not support integration with AI-based detection. Mobile and IoT device monitoring is limited. Anomaly detection algorithms in older systems lack efficiency. False alerts reduce administrator confidence. Historical attack data is underutilized. Manual security audits are time-consuming. Overall, existing systems are insufficient for modern, complex threats.

PROPOSED SYSTEM

The proposed cyber security threat detection system aims to provide real-time, automated detection of cyber threats. It combines signature-based and anomaly-based detection methods for improved accuracy. Machine learning algorithms analyze network traffic to identify suspicious patterns. The system detects malware, phishing attempts, ransomware, and DDoS attacks. Automated alerts notify administrators immediately when threats are detected. Historical attack data is used for predictive analysis. Threat intelligence feeds help identify emerging attacks. Cloud-based architecture ensures scalability and performance. Endpoint security monitoring is integrated for comprehensive coverage. AI-driven anomaly detection reduces false positives. The system supports secure logging and auditing. User authentication and access control enhance protection. Admin dashboards provide visualized insights into network activity. Continuous updates ensure protection against new threats. Integration with SIEM systems provides centralized management. Mobile and IoT monitoring is included. The system prioritizes high-risk threats for quick response. Overall, it provides proactive cyber security defense.

SYSTEM ARCHITECTURE

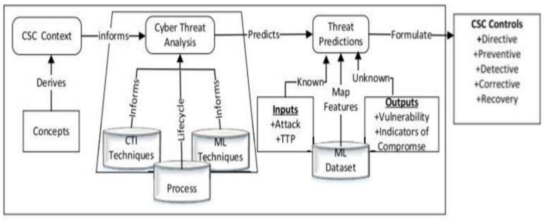

Fig-5 Architecture diagram

Fig.1 System Architecture

METHODOLOGY DESCRIPTION

The development of the proposed system begins with requirement analysis to identify organizational security needs. System architecture design defines modules for network monitoring, data collection, and threat analysis. Data preprocessing cleans and normalizes network traffic data. Feature extraction identifies relevant patterns for detection. Machine learning models are trained using historical attack data. Signature-based detection is integrated to identify known threats. Anomaly-based detection identifies unusual behaviors. Real-time monitoring ensures immediate response. Automated alerting and logging mechanisms are implemented. Threat intelligence feeds enhance detection of emerging threats. Cloud-based deployment ensures scalability and accessibility. Endpoint monitoring covers all connected devices. Security dashboards provide visual insights to administrators. System testing validates accuracy, speed, and reliability. False-positive reduction techniques improve system performance. Continuous updates keep the system current. Incident response protocols are defined. Data encryption ensures secure communication. Overall, the methodology emphasizes proactive, automated cyber threat detection.

RESULTS & DISCUSSION:

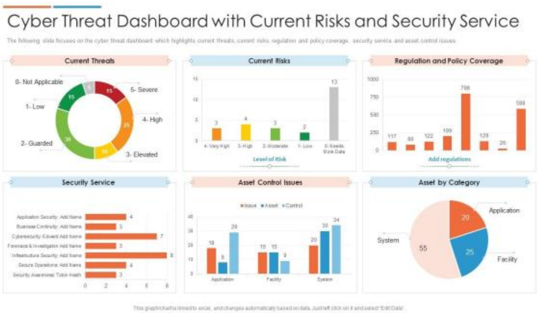

Fig:2 Security Service page

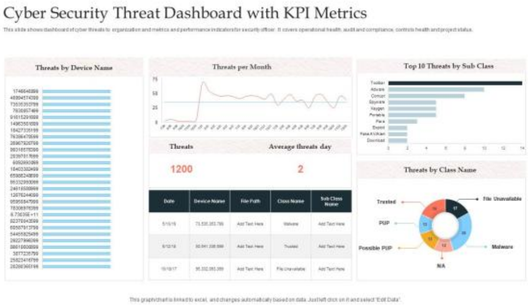

Fig:3KPI Metrics page

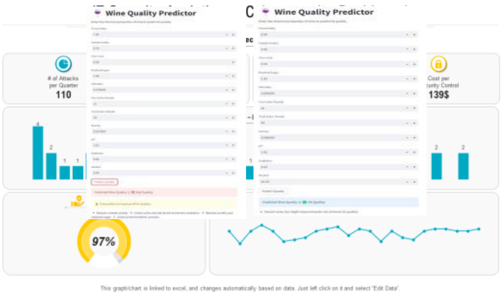

Fig.4 Wine Quality Prediction Results

CONCLUSION & FUTURE

ENHANCEMENT

Cyber security threat detection is essential in today's digital environment. The proposed system improves upon existing solutions by combining signature and anomaly detection. Machine learning algorithms enhance the ability to detect unknown and emerging threats. Real-time monitoring and automated alerts reduce response time. Historical data and threat intelligence provide predictive capabilities. Cloud-based deployment ensures scalability and flexibility. Endpoint monitoring ensures comprehensive coverage. User-friendly dashboards support effective administration. Integration with SIEM systems centralizes management. Automated threat detection reduces reliance on manual monitoring. False-positive reduction improves system reliability. Malware, phishing, ransomware, and DDoS attacks can be detected proactively. The system supports secure logging and auditing. Continuous updates maintain protection against evolving threats. Mobile and IoT device monitoring enhances security coverage. Overall, the system provides a robust and efficient solution for cyber security. Cyber threat detection is critical for protecting data, infrastructure, and user trust. The implementation of AI-based detection ensures modern readiness. This system represents a significant improvement over traditional methods.

REFERENCE

1. Harini, D. P. (2024b). New Efficiency System for Brain Tumor Classification using Machine Learning Algorithm. *Machine Intelligence Research, 18*(01), 836–843.
2. Stallings, W., *Network Security Essentials: Applications and Standards*.
3. Bishop, M., *Computer Security: Art and Science*.
4. IEEE Papers on Intrusion Detection Systems.
5. ACM Digital Library on Cyber Security.
6. Scarfone, K., and Mell, P., *Guide to Intrusion Detection and Prevention Systems*.
7. Symantec Security Reports.
8. CISCO Security Solutions Documentation.
9. Machine Learning Approaches to Cyber Security, Springer.
10. Research on AI-Based Threat Detection, Elsevier.
11. Network Traffic Analysis Techniques, IEEE.
12. Malware Detection Using Deep Learning.
13. Phishing Attack Detection Studies.
14. Security Information and Event Management (SIEM) Research.
15. Cloud Security Architecture Guidelines.

16. IoT Security Threat Detection Papers.

17. DDoS Attack Detection Methods, IEEE.

18. Cyber Security Threat Intelligence Research.

19. Historical Attack Data Analysis Studies.

20. Data Encryption and Secure Communication Techniques.

21. Modern Trends in Cyber Security, ACM Journals.