International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 01 | January - 2024 SJIF Rating: 8.176 ISSN: 2582-3930

Threat Detection System

Kanchan Misal[1], Vaishnavi Pansare[2], Yashsvi Ingulkar[3], Pratiksha Hule[4],

Prof. Mrs.H.N.Bhandare[5]

[1,2,3,4,5]*Computer Engineering Department, Rajashree Shahu college of engineering polytechnic*

Abstract - This research paper is about to control the engine valves of an one cylinder 4-stroke engine with a computer controlled electromagnetic actuator. There are many possibilities in electromagnetic devices. We chose a push solenoid to actuate the engine valve. For controlling the solenoid, we chose a user interface with control options. The user interface communicates serially with a microprocessor. The microprocessor monitors and reports the engine's performance and control the opening/closing of the engine valves. The ultimate goal is improved efficiency, decrease pollutants, and produce maximum power throughout the RPM range with a camless engine.

***Key Words*:** Behavior Analysis, Signature- Based Detection, Intrusion Prevention, Log Analysis.

1. INTRODUCTION

The final layout of the typeset paper will not match this template layout. With more and more educational institutions using online platforms for distance learning, online cheating has become a major concern. Academic dishonesty has become more common due to the availability of access to material and the difficulties of keeping an eye on each student's activity in virtual classes. An advanced intrusion detection system (IDS) designed specifically to identify and stop online cheating is essential to addressing this expanding problem. This study presents an intelligent and proactive intrusion detection system (IDS) that uses state-of-the-art technologies, such as behavioral analysis, to identify patterns suggestive of online cheating on educational platforms.

This IDS promises to protect the legitimacy of academic evaluations in light of the growing significance of online learning and the requirement for equitable and open evaluation procedures. This paper's latter sections will examine the system's architecture, methods, and assessment metrics, emphasizing how effective it is in curbing online cheating and fostering an academic integrity culture in the digital age.Establishing an academic integrity culture in virtual learning environments is facilitated by the implementation of an IDS for online cheating. It gives teachers the resources they need to spot cheating and deal with it quickly, preserving the legitimacy of online learning and the reliability of evaluation procedures.

2. Body of Paper

I. MODULE DESCRIPTION

1) Registration Page: Creating a user registration interface is a standard step in the registration page module intrusion detection system. Administrators and other authorized users can register new users or devices on the network with the help of this module. The Registration Page Module's salient features include:

a) User Input Form: Create a form to gather necessary data, like a username and password, as well as maybe more information based on the needs of the system.

b) Validation Mechanism: Make sure the data entered is correct and complies with security requirements by putting validation tests into place. This covers email format validation and password strength checks.

c) Access restrictions: Include access restrictions to limit registration to individuals who are authorized. aids in keeping unauthorized users out of the system.

d)Unique Identifiers: Give each registered user or device a unique identifier (such as a user ID). This facilitates the tracking and administration of the system's entities.

e) Logging: Put in place logging systems to keep track of registration-related actions. For auditing purposes, this entails recording information such as the timestamp, the user who completed the registration, and any other pertinent details.

f)Notification System: If you'd like, you can incorporate a notification system to let administrators or other pertinent parties know when someone registers again.

g) User Database Integration: To securely store and retrieve user information, connect the registration module to the user database of the system.

h) Security Measures: To guard against frequent flaws like SQL injection and cross-site scripting, use secure coding techniques.

2) Login Page: For approved users, the login page module acts as their first point of access. Usually, it consists of the following:

a) User authentication, which verifies that only authorized users are able to access stored records by comparing user credentials such as password and username with recorded records.

b) Logging: Keeps track of login events, recording information such as the user, time, and location for analysis and audit trails in the event that unusual activity is detected.

c) Two-factor authentication (2FA), often known as captcha, improves security by adding extra verification steps to thwart automated or unauthorized logins.

d) Password Policies: To improve the overall security posture, strong password requirements are enforced.

e) Error Handling: Assists users in securely troubleshooting login issues by displaying relevant error messages while concealing critical information.

3) Exam page: A college-level intrusion detection system's Exam Page module may monitor and analyze exam-related activity to spot any unauthorized or suspect activity. The purpose of this module is to guarantee the security and integrity of online tests. It could have characteristics like:

b)User behavior monitoring is keeping an eye on students' online activities during tests to spot any unusual activity or departure from the norm.

c) Integrity checks involve confirming the accuracy of exam-related data and making sure that the exam's content hasn't been tampered with or altered without authorization.

d) Real-time Alerts: Sending administrators or pertinent staff members immediate messages or alerts in the event that abnormalities or possible security breaches are discovered while an exam is being administered.

4) ScreenShot Display Page: The "Screen Shot Display Page" module for a college-level intrusion detection system can entail building a user interface where administrators or security staff can examine screenshots taken during questionable actions. This page may have characteristics like:

a)Show a list or grid of screenshots that have been taken.

b)Provide a timestamp for every screenshot to facilitate a chronological analysis.

C)Provide details about the person or system that is engaged in the questionable behavior in order to identify the user.

d)Alert Integration: Provide rapid access to pertinent screenshots by linking them to the related alerts if the intrusion system creates any.

5) Database Page: Intrusion Detection System, the database page module would likely involve managing information related to network activity, user behavior, and potential security threats. Here's a basic description:

Database Page Module:

a) User Profile Management:

Store and manage user profiles, including login credentials, roles, and permissions. Record user-specific details such as department, course, and access levels. Network Activity Logging:

b) Capture and store detailed logs of network activities, including IP addresses, timestamps, and protocols. Record data transfer rates, the source, and destination of network traffic.

c) Alerts and Incidents: Store records of detected security incidents and alerts triggered by the IDS. Include details like severity, timestamp, and affected systems.

d) Configuration Settings: Keep configurations for the IDS, including rulesets, sensitivity levels, and exclusions. Store historical configurations for audit purposes.

5) Database Page: Intrusion Detection System, information on network activity, user behavior, and possible security risks would probably be managed by the database page module. Here's a little explanation:

Module for Database Pages:

User Profile Administration

(a): Maintain and store user profiles, together with roles, permissions, and login information.Note information unique to each user, such as department, course, and degree of access.

Network Activity Recording:

b) Record and preserve comprehensive records of network operations, encompassing IP addresses, timestamps, and protocols. Keep track of network traffic's source, destination, and data transfer rates.

c)Alerts and Incidents: Keep track of security incidents and alerts that the IDS detects. Add information about the impacted systems, timestamp, and severity.

d) Configuration Settings: Maintain the IDS's rulesets, sensitivity settings, and exclusion lists.

II. SYSTEM REQUIREMENTS

1. Software Requirement :

- Operating system : Windows X/P7.
- Language : JAVA/JAVASCRIPT.
- Front End : JSP.
- Back End: MySQL database.
- Web sever : Apache tomcat.
- IDE : Eclipse.

2. Hardware Requirement :

- Processor : Core i3
- RAM : 8GB DDR4
- SSD : 256GB

III. METHODOLOGY

Our proposed system aims at providing highly efficient and robust threat detection system. The self analysis method continuously monitors and provides details of user activities for detecting unauthorized entities. As internal system calls (SC) are used to detect the threat attacks, this can be implemented using data mining and forensic techniques. It would help to identify and provide detailed information about a user and its SC patterns. But if restricted activity is found then it needs to be alarmed/informed and reported to the right authorities Advantages:

1. Early Threat identification: In order to lessen the effect of security incidents, early identification and prompt response are made possible by IDSS's ability to recognize and notify administrators about possible security threats in real-time.
2. Network Visibility: Intrusion Detection System (IDS) gives administrators information about network activity and any security holes. Organizations are better equipped to comprehend their network traffic and take well-informed judgments to fortify security thanks to this increased visibility
3. Enhanced Security Posture: By adding an extra line of protection, an IDS installation improves an organization's overall security posture.
4. User Anomaly Detection: Utilizing abnormalities in user behavior, some intrusion detection systems (IDS) can help uncover insider threats or unapproved access. This is essential for safeguarding sensitive data and preventing data breaches.
5. Damage Minimization: By taking proactive steps to control and mitigate security breaches, early detection helps organizations minimize the potential harm to their systems, data, and network infrastructure as a whole.

IV. FUTURE SCOPE

This System can be used to detect the suspicious activity where host machine comprises the confidential files. Attackers can attack on host machine that attacks would be detected by the system and updated files can be recovered by system.

3. CONCLUSIONS

The online version of the volume will be available in LNCS Online. Members of institutes subscribing to the Lecture Notes in Computer Science series have access to all the pdfs of all the online publications. Non-subscribers can only read as far as the abstracts. If they try to go beyond this point, they are automatically asked, whether they would like to order the pdf, and are given instructions as to how to do so.

ACKNOWLEDGEMENT

The heading should be treated as a 3rd level heading and should not be assigned a number.

REFERENCES

[1]. Anupam Mittal; Urvashi Garg Design And Analysis Of Insider Threat Detection And Prediction System Using Machine Learning Techniques July 2023
[2]. Faiaz Rahman; Rafee Zunaied Tanna; Umme Habiba; Cyber Threat Detection Using Machine Learning Algorithms on Heterogeneous MiniVHS-22 Dataset December 2022
[3]. Jyoti Verma; Abhinav Bhandari; Gurpreet Singh Network Intrusion Detection System Employing Big Data and Intelligent Learning Methods December 2022
[4]. Gould, L; Richeson, W; and Erickson, F., 1991,"Performance Evaluation of a Camless Engine Using Valve Actuation with Programmable Timing," SAE Paper No. 910450. Jitti Annie Abraham; V. R. Bindu Intrusion Detection and Prevention in Networks Using Machine Learning and Deep Learning Approaches: A Review October 2021
[5]. Usman Shuaibu Musa; Sudeshna Chakraborty; uhammad M. Abdullahi; Tarun Maini A Review on Intrusion Detection System using Machine Learning Techniques April 2021
[6]. Derek Lin; Anying Li; Ryan Foltz BEAM: An Anomaly-Based Threat Detection System for Enterprise Multi-Domain Data December 2020
[7]. B. Ya. Sovetov; T. M. Tatarnikova; V. V. Cehanovsky Detection System for Threats of the Presence of Hazardous Substance in the Environment November 2019
[8]. Obinna Igbe; Tarek Saadawi Insider Threat Detection using an Artificial Immune system Algorithm August 2019
[9]. Rohit More; Anand Unakal; Vinod Kulkarni; R. H Goudar Real time threat detection system in cloud using big data analytics - January 2018