International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 13; Issue: 7; July- 2024

CYBER SECURITY ATTACK DETECTION USING MACHINE LEARNING

Mary Anitha T
Associate Professor
Department of MCA
The Oxford College of Science
mary.anitha.charlton@gmail.com

Sathwika H
PG Student
Department of MCA
The Oxford College of Science
hsathwika818@gmail.com

ABSTRACT

Cyber crimes are spreading everywhere by exploiting vulnerabilities in computing environments. Ethical hackers focus more on assessing vulnerabilities and recommending mitigation's. Developing effective technology in the field of cyber security has become an urgent need. Many of the techniques used in IDS today cannot cope with the power and complexity of cybersex attacks on computer networks. Machine learning for cyber security has become a hot topic recently due to its effectiveness in cyber security problems. Developments in personal computers and new communication technologies have greatly influenced and led to changes compared to the past. Although the use of innovations may cause problems, they provide great benefits to people, organizations and governments.

INTRODUCTION

There has been a competition between cybersex criminals and defenders since the 1970s, when the first computer virus appeared. Protecting against and keeping up with cyber security threats has become increasingly difficult. To overcome these security issues, researchers are currently working on the urgent need to find new security mechanisms. Algorithms can detect new and unknown criminal behaviour.

Today's modern security technologies include firewalls, antivirus software, intrusion prevention systems (IPS), SEIM solutions and threat management Traditional solutions rely on static management of devices based on network security rules and lack of automation (using artificial intelligence). AI-based systems are more effective than traditional threat systems at detecting events, errors, and responding to cybersex attacks. They also have a lower error rate than traditional systemsin detecting and responding to attacks.

PROJECT DESCRIPTION

Cyber crimes are spreading everywhere by exploiting vulnerabilities in computing environments. Ethical hackers focus more on assessing vulnerabilities and recommending mitigation's. Developing effective technology in the field of cyber security has become an urgent need. Many of the techniques used in IDS today cannot cope with the power and complexity of cybersex attacks on computer networks. Machine learning for cyber security has become a hot topic recently due to its effectiveness in cyber security problems. Developments in personal computers and new communication technologies have greatly influenced

and led to changes compared to the past. Although the use of innovations may cause problems, they provide great benefits to people, organizations and governments.

For example, protection of important information, security of information storage platforms, accessibility of information, etc. Based on these issues, torture based on digital fear is one of the most important problems of our age

EXISTING SYSTEM

Many of the techniques used in IDS today cannot cope with the power and complexity of cyber attacks on computer networks. Machine learning for cyber security has become a hot topic recently due to its effectiveness in cyber security problems.IDS does not record these attacks until they travel deeper into the network, making your system vulnerable to attacks before the attack is detected. This is a big problem because encryption is becoming increasingly important to keep our data safe. One of the main problems with IDS is that it constantly alerts you to vulnerabilities. In many cases, the vulnerability is more widespread than the actual threat. If the negatives are not addressed, the real fight is over or ignored. When an IDS detects suspicious activity, it typically reports the breach to the security information and event management (SIEM) system, which ultimately determines whether the actual threat originating from the traffic is good or bad. However, the longer it takes to discern the threat, the greater the damage.

PROPOSED SYSTEM

There are three main types of network analytic for accessing analytic systems. The purpose of vulnerability-based detection is to detect attacks. Anomaly detection monitors normal network and physical activity and identifies abnormalities in the network and behavior. Finally, to improve detection results, hybrid-based detection strategies combine both positive and negative strategies . Attackers can successfully exploit these vulnerabilities in traditional defenses. Therefore, it is becoming difficult to protect users from new and evolving threats.

TOOLS AND TECHNOLOGIES USED

This article describes a traditional machine learning method. The most commonly used machine learning methods, their duration, advantages and disadvantages, and publication years. When it comes to IDS, SVM is considered the most popular and effective method of machine learning. Based on the labels of the edges on both sides of the hyperplane, SVM splits and splits the two datasets. ..

Multidimensional hyperplanes use kernels to partition multidimensional data. In other words, the plane should be used – the maximum or maxima of the data points. A hyperplane is a dividing plane. SVM is used to classify multidimensional data, so a hyperplane is a straight line with two inputs and a 2D plane with three or more inputs.Used for regression analysis.

USERS

Administrators

Part: Dependable for by and large framework administration and configuration.

Duties: Setting up and designing the discovery framework, overseeing client accounts and consents, managing framework execution and health.

Security Analysts

Part: Effectively screen and explore cautions produced by the system.

Duties: Looking into identified irregularities or potential assaults, conducting assist examination, confirming untrue positives, and taking suitable activities to moderate affirmed threats.

Framework Integrators

Part: Included in coordination the location framework with existing cybersecurity infrastructure.

Duties: Guaranteeing consistent communication and information trade between distinctive security frameworks and the location system.

Conclusion Clients

Part: Depending on the sending situation, conclusion clients might associated by implication with the framework by accepting security notices or updates.

FUNCTIONAL REQUIREMENTS

Information Collection and Preprocessing

Necessity: The framework should collect information from different sources such as organize activity logs, framework logs, and application logs.

Basis: Guarantee that the framework has get to to significant information for analysis.

Peculiarity Detection

Prerequisite: The framework should utilize machine learning calculations to distinguish peculiarities in the collected data.

Method of reasoning: Distinguish abnormal designs or behaviors that may show potential cybersecurity threats.

Assault Design Recognition

Necessity: The framework might distinguish known assault designs and marks utilizing machine learning models.

Method of reasoning: Recognize particular assault methods and marks to precisely classify threats.

Real-time Checking and Alerting

Necessity: The framework might screen information streams in real-time and create alarms upon identifying suspicious activities.

Method of reasoning: Empower incite reaction to potential dangers to minimize impact.

5**.Caution Administration and Reporting**

Necessity: The framework might give a dashboard for security examiners to see alarms, examine episodes, and oversee responses.

Method of reasoning: Back effective occurrence reaction and administration workflows.

SYSTEM PERSPECTIVE

Framework Setting Diagram

Portrayal: Give a high-level chart that outlines the connections between the cybersecurity assault discovery framework and outside substances,

such as clients, other frameworks, and information sources.

Reason: Clarify the boundaries and intuitive of the framework inside the organization's ecosystem.

Interfaces

Outside Interfacing: Indicate interfacing with outside frameworks, such as SIEM (Security Data and OccasionAdministration)
frameworks, risk insights nourishes, and client administration systems.

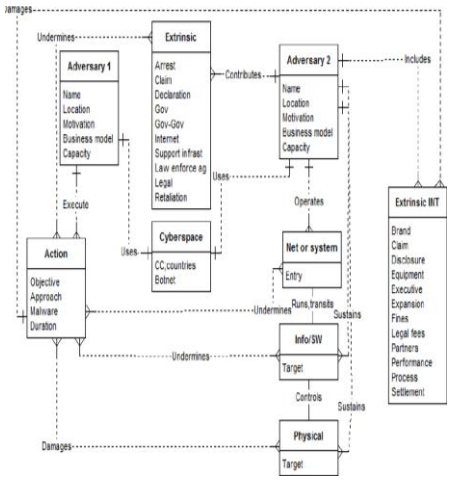
Illustration: "The framework might coordinated with existing SIEM frameworks by means of Relaxing APIs for the trade of security occasion data."

ER DIAGRAM

A substance relationship chart (ERD), moreover known as a substance relationship

demonstration, is a graphical representation of a data framework that delineates the connections

among individuals, objects, places, concepts or occasions inside that framework. An ERD is a point, should to any investigating or trade prepare re-engineering be required afterwards.

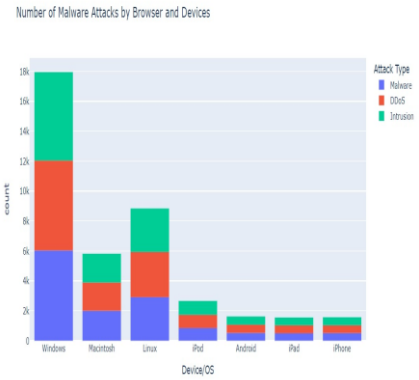


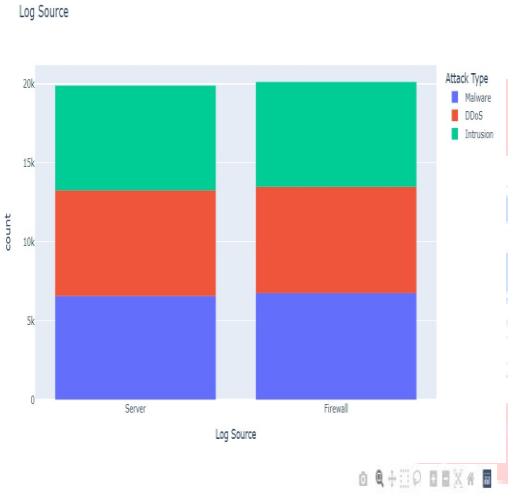
TESTING

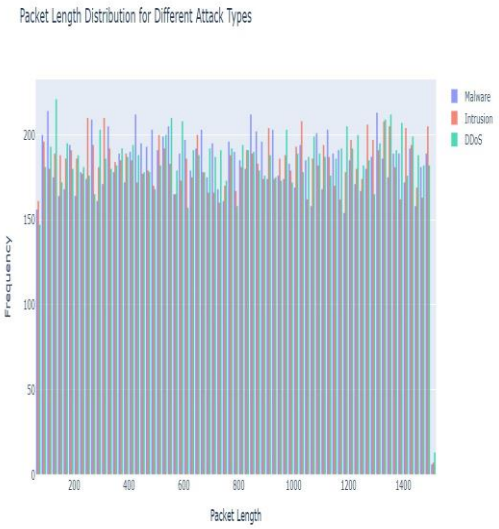
The Program Testing Life Cycle (STLC) is an efficient approach to testing a program application to guarantee that it meets the prerequisites and is free of abandons. It is a handle that takes after an arrangement of steps or stages, and each stage has particular targets and deliverable s. The STLC is utilized to guarantee that the program is of high quality, solid, and meets the needs of the end-users. The fundamental objective of the STLC is to distinguish and report any abandons or issues in the program application as early as conceivable in the improvement handle.

Test Case Description	Preconditions	Test Steps	Expected Result	Actual Result
Data Ingestion from Log Files	System is configured to access log files	1. Start the data ingestion module 2. Provide path to log files 3. Monitor data ingestion process	Log files are successfully read and data is ingested into the system	Passed/Failed
Preprocessing of Ingested Data	Data ingestion is completed	1. Start the data preprocessing module 2. Apply data cleaning and normalization steps	Data is cleaned and normalized, ready for feature extraction	Passed/Failed
Feature Extraction	Preprocessing is completed	1. Start feature extraction module 2. Apply feature extraction algorithms	Relevant features are extracted and ready for model training	Passed/Failed
Model Training with Historical Data	Feature extraction is completed	1. Select training dataset 2. Choose machine learning algorithm 3. Train the model	Model is successfully trained with the historical data	Passed/Failed
Model Validation	Model training is completed	1. Select validation dataset 2. Validate the trained model	Model validation metrics (accuracy, precision, recall) meet the predefined thresholds	Passed/Failed

RESULT:
SCREENSHOTS







CONCLUSION

At the present time, assessments of help vector machine, ANN, CNN, Random Forest and significant literacy estimations reliant upon current CICIDS2017datasetwere presented relatively. Results show that the significant learning estimation performed generally stylish results over SVM, ANN, RF and CNN. We'll use harbor age compass attempts just as other attack types with AI and significant learning computations, a ache Hadoop and shimmer advancements together shield on this datasets latterly on. Every one of these estimation assists us with feting the digital assault in network. It occurs in the manner that when we suppose about long back a long time there might be similar innumerable assaults passed so when these assaults are perceived also the highlights at which esteems these assaults are going on will be put down in some datasets. So by exercising these datasets we will anticipate if digital assault is finished.

FUTURE ENHANCEMENTS

Advanced trouble Discovery:

Behavioral Analysis-ml models will evolve to dissect stoner and reality

actions(UEBA) more deeply, detecting anomalies that may indicate bigwig pitfalls or sophisticated attacks.

Contextual mindfulness ML algorithms will incorporate contextual information from colorful sources(e.g., stoner gestate

, network business, operation logs) to enhance discovery delicacy and reduce false cons.

Inimical Machine Learning Defense:

ML models will incorporate defenses against inimical attacks, which essay to deceive or manipulate ML systems. ways similar as inimical training and robust ML models will be developed to alleviate these pitfalls.

Resolvable AI(XAI) in Cyber security:

There will be a focus on making ML models more interpret-able and resolvable, enabling cyber security judges to understand the logic behind a model's decision and trust its labors.

REFERENCE

- K. Graves, Ceh: The Official Certified Ethical Hacker Study Guide: Exam 312-50. John Wiley & Sons, Inc., 2007.R. Christopher, "Port Scanning Techniques and Defenses", SANS Institute, 2001. M. Barbara, R. DaÅ .
- KaraokeŸan, "Review of tools used in information security systems", 1st International Digital Symposium on Forensic Medicine and Security (ISDFS13), 2013, Page 231 - 239. Kashmir V. â Predicting system.

\