WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Cyber Threat Detection Using Machine Learning

Om Jagtap[1], Atharva Rajmane[2], Vaibhav Jagtap [3]

[1] Entc Engineer omjagtap1105@gmail.com
[2] Entc Engineer atharvarajmane.1709@gmail.com
[3] Entc Engineer vaibhav2632@gmail.com

ABSTRACT

Cybersecurity remains a dynamic field essential for protecting digital assets and sensitive information in our interconnected world. As cyber threats grow in complexity and frequency, the demand for effective threat detection mechanisms becomes increasingly critical. Support Vector Machine (SVM) algorithms have gained traction in cybersecurity due to their capacity to categorize data, rendering them wellsuited for identifying malicious activities and cyber threats. This research paper delves into the application of SVM algorithms in the realm of cybersecurity threat detection, aiming to construct a robust and efficient system capable of accurately identifying and classifying potential threats.

I. INTRODUCTION

The Internet of Things is the connection of physically moving "things" contained in electronic devices, devices' electricity, and other hardware over the Internet. Each device is uniquely identified worldwide by a Radio Frequency Identifier (RFID). These smart objects can be monitored and controlled remotely by communicating with other connected devices. IBM said the number of internet-connected devices is expected to grow to 50 billion, leading to a network of connected smart devices and big data that can share the air. IoT technology can be used to create smart cities, education, e-shopping, e-banking, managing our health, managing our businesses, entertaining

It can be used for attacks that are open to in-depth analysis that security experts need for certain types of attacks, such as: On the other hand, social media information analysis can help uncover new types of cyber threats and security threats, including data theft, hacking, and hacking. Threat analysis is the practice of analyzing the entire security ecosystem to identify potential threats. It may damage the network. If a threat is detected, mitigating measures must be taken to eliminate the threat before existing vulnerabilities can be implemented.

II. PROBLEM STATEMENT

Social media use does not replace the need for security professionals to perform indepth analysis of specific attacks, such as checking for network inconsistencies, viruses, and hacks. On the other hand, social media information analysis can help uncover new types of cyber threats and security threats, including data theft, hacking, and hacking. Threat analysis is the practice of analyzing the entire security ecosystem to identify threats. It may damage the network. If a threat is detected, mitigating measures must be taken to eliminate the threat before existing vulnerabilities can be implemented.

III. MODULE

Administrator

Within this module, administrators are required to log in using a valid username and password to access various functionalities. Upon successful login, administrators gain the ability to view user details and permissions, explore ecommerce sites and their associated permissions, examine products and reviews, assess early market products, scrutinize keyword search terms, delve into product search comparisons, and review product ranking based on customer feedback.. User Management and Authorization: Administrators, within this module, possess the capability to view and authorize users. which is used to evaluate expectation of log by using latest estimate of parameters and Maximization. This involves accessing

a comprehensive list of all users, where detailed information such as the user's name, email, address, and specific permissions granted by the administrator can be reviewed. Chart Visualization: The module allows administrators to visualize charts related to product search results, general search outcomes, and product review rankings. E-Commerce User Operations: This section caters to 'n' users who are required to undergo a registration process before engaging with the platform. User information is securely stored in the database postregistration.

End Users

There are n users in this module. Users must register before doing this. When users register, their information is stored in a database. After the registration process is completed, you must log in using your authorized username and password. After successfully logging in, the user will perform certain tasks such as account management, searching for products by keywords and purchases, viewing and looking up your business search.

IV. SOFTWARE REQUIREMENT

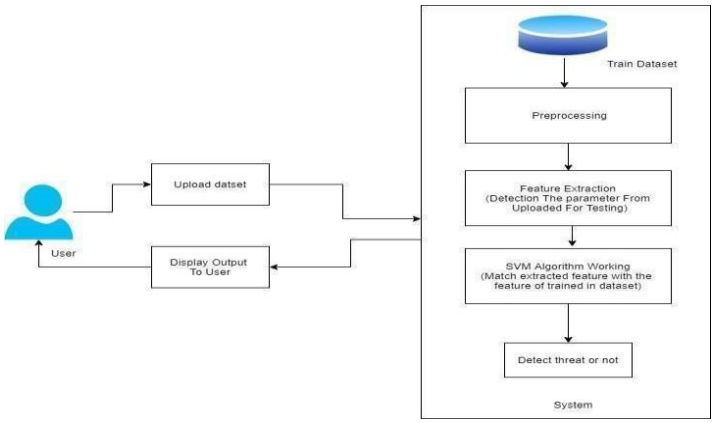
Python, established by Guido van Rossum in 1991, stands out as an interpreted, high-level, generalpurpose programming language. Crafted with a design ethos prioritizing code readability via strategic use of white space, Python's language structure and implementation objectives are tailored to facilitate the creation of clear and concise proposals, accommodating projects of varying scales.

Distinguished as dynamically typed and equipped with garbage collection, Python supports diverse operations, including object orientation and transaction functions, earning it the moniker of a "batterypowered" language, owing to its robust library.

Initially conceived in the 1980s as a successor to the ABC language, Python 2.0 was unveiled in 2000, introducing features like list comprehension and enumeration garbage collection. Python 3.0, released in 2008, represents a significant yet incomplete revision, sharing several features with Python 2 but requiring code modifications for compatibility. The deprecation of Python 2 in 2020, initially slated for 2015, marked the end of an era, with Python 2.7.18 serving as its final release. With no security patches or further improvements planned, support shifted exclusively to Python 3.6.x and later versions. A graphical user interface named Anaconda Navigator complements the command line interface (CLI) for user-friendly interaction with the distribution

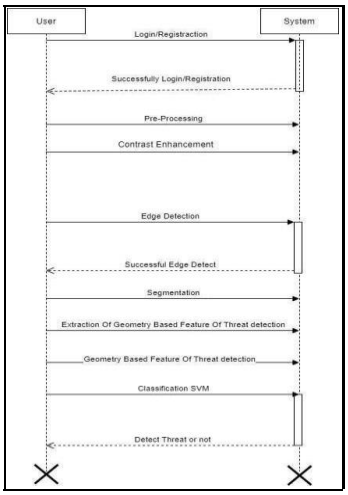
V. METHODOLOGY

SYSTEM ARCHITECTURE

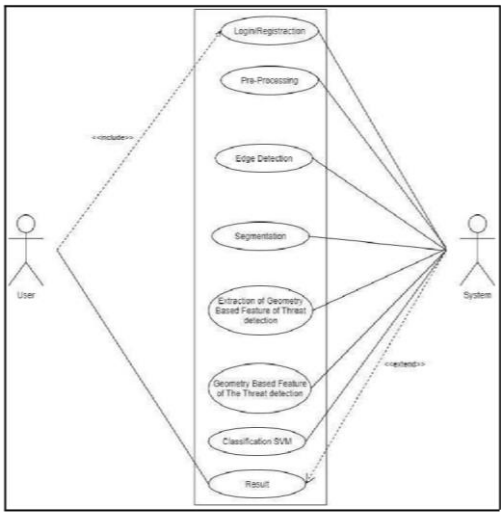


UML DIAGRAMS

The Unified Modeling Language (UML) serves as a language for articulating software blueprints, enabling the visualization, specification, design, and documentation of features within softwareintensive systems. UML is adaptable to various processes, being process-agnostic, but is most effectively employed in data-driven, architecture-centric, iterative, and incremental methodologies. The spectrum of UML diagrams encompasses a diverse tools, contributing to range of visualization

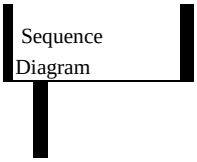


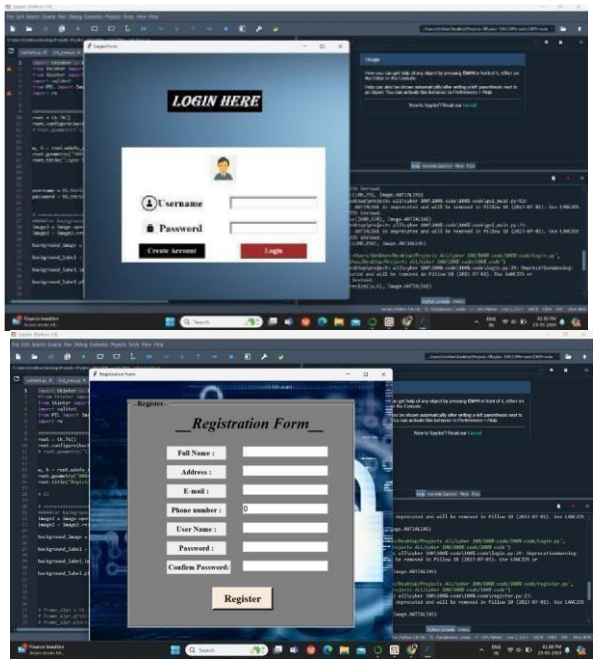
1) Use the example diagram



2) Use the example diagram

2) Sequence diagram





VI. Discussion

1) Creating Login and Register page using GUI Algorithm. Login and Register page is important so that only authorized users can access the data.

2)Creating a page at backend describing testing and training feature. Training set is aboutb70-80% of data whereas Testing set is of about 20-30%.

3)After giving data as input, it is going to show the output(threat) on the basis of threat which have been taught to machine or software using machine learning.

VII. CONCLUSION:

In conclusion, a cyber threat detector based on machine learning offers a robust and intelligent defense mechanism against a wide range of cyber threats. Its ability to learn, adapt, and provide realtime insights empowers organizations to stay one step ahead of potential security risks. The implementation of such technology represents a proactive and strategic approach to cybersecurity, ultimately safeguarding sensitive data and critical systems from malicious actors.

VIII. REFERENCES

1. C. R. Srinivasan, B. Rajesh, P. Saikalyan, K. Premsagar, and E. S. Yadav, “A review on the different types of Internet of Things (IoT),” J. Adv. Res. Dyn. Control Syst., vol. 11, no. 1, pp. 154–158, 2019.

2. Khan, L., Awad, M. and Thuraisingham, B. “A New Intrusion Detection System using Support Vector Machines and Hierarchical Clustering”, The VLDB Journal: ACM/Springer-Verlag, 16(1), page 507-521, 2007.

3. Lazarevic, A., et al., “Data Mining for Computer Security Applications”, Tutorial Proc. IEEE Data Mining Conference, 2003.

4. Abedin, M., Nessa, S., Khan, L., Thuraisingham, B.,“Detection and Resolution of Anomalies in Firewall Policy Rules”, In Proc. 20th IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec 2006), SpringerVerlag, July 2006, Sophia Antipolis, France, page 15- 29.

5. S. Hofmeyr, S. Forrest, and A. Somayaji, ``Intrusion Detection Using Sequences of System Calls", *Journal of Computer Security* Vol. 6, pp. 151-180 (1998).

6. Thuraisingham B., “Database and Applications Security”, CRC Press, 2005.

7. R. Agrawal and R. Srikant, "Privacy-Preserving Data Mining", *Proc. of the ACM SIGMOD Conference on Management of Data*, Dallas, May 2000.

8. M. Atallah, M., E. Bertino, E., A. K. Elmagarmid, A.K., M. Ibrahim, and V. S. Verykios, ``Disclosure Limitation of Sensitive Rules", In *Proceedings of 1999 IEEE Knowledge and Data Engineering Exchange Workshop (KDEX'99)* pp. 45-52, November 1999, Chicago, IL.

9. Dakshi Agrawal and Charu C. Aggarwal, ``On the design and quantification of privacy preserving data mining algorithms", in *Proceedings of the twentieth ACM SIGMOD_SIGACTSIGART symposium on principles of Database Systems on Principles of database systems*, 2001.

10. S. Rath, D. Jones, J. Hale, S. Shenoi, ``A Tool for Inference Detection and Knowledge Discovery in Databases", in *Proceedings of the 9th IFIP WG11.3 Workshop on Database Security*.