NEIL GOGTE INSTITUTE OF TECHNOLOGY
PROMOTED BY KMIT

Project School Certificate

Title of the Project: Ransomware Detection

Session Duration: 12Weeks [April 2023 – July 2023]

Mentor: Ms. Suthoju Girija Rani,
Assistant Professor,
Department of CSE, NGIT.

Name of the Student: K. NITHIN

Roll Number: 245321748093

Department: CSE-AIML

Class/Section: CSM-B

K. NITHIN

Signature of Faculty

Signature of Student

I. ABSTRACT

Ransomware attacks pose a great threat to Cloud services and can lock the service with or without damage to system files. Further, zero-day attacks can exploit the vulnerability in the cloud service till the vulnerability is detected by the developer and fixed. The solution must provide an AI-powered alert management system that can automatically detect problem ransomware & zero-day attacks and help reduce the workload of security analysts. The solution must have an analytics section to measure its performance by evaluating false positives.

II. OBJECTIVE

- Ransomware attacks pose a great threat to Cloud services and can lock the service with or without damage to system files. Further, zero-day attacks can exploit the vulnerability in the cloud service till the vulnerability is detected by the developer and fixed. The solution must provide an AI-powered alert management system that can automatically detect problem ransomware & zero-day attacks and help reduce the workload of security analysts. The solution must have an analytics section to measure its performance by evaluating false positives.

- The proposed solution seeks to address these challenges by implementing an AI-powered alert management system. This system will leverage advanced machine learning and artificial intelligence techniques to automatically detect potential ransomware and zero-day attacks in real-time. By proactively identifying these threats, the solution aims to prevent or minimize their impact on Cloud services, ensuring the availability, integrity, and confidentiality of critical data and applications.

- One key aspect of the solution is its focus on reducing the

workload of security analysts. Ransomware and zero-day attacks can generate a vast amount of security alerts, overwhelming security teams and delaying incident response. With the AI-powered alert management system, security analysts can prioritize their efforts by focusing on high-risk incidents while low-risk incidents are handled automatically. This optimized workflow will enable security teams to respond more efficiently to genuine threats, minimizing response times and reducing the likelihood of successful attacks.

III. TECHNICAL DESCRIPTION

1. AI and Machine Learning Models: The core of the system will be based on AI and machine learning models. These models will be trained on historical data containing examples of known ransomware attacks and zero-day exploits. The models will learn patterns and characteristics of such attacks, enabling them to identify similar behaviors in real-time data.

2. Anomaly Detection: The AI-powered alert management system will primarily rely on anomaly detection techniques. It will establish a baseline of normal behavior within the Cloud environment and compare incoming data against this baseline. Any deviation from the norm that matches the patterns learned during training will be flagged as a potential ransomware attack or zero-day exploit.

3. Threat Classification: The system will be equipped to classify detected threats based on their severity and potential impact. It will prioritize critical threats over low-risk incidents, allowing security analysts to focus their attention on the most significant risks.

4. Real-time Alerting: When a potential ransomware attack or a zero-day exploit is detected, the system will generate real-time

alerts. These alerts will contain relevant information about the threat, the affected assets, and its severity. Security teams will be immediately notified to initiate incident response procedures.

5. Automated Response and Mitigation: For known and previously encountered threats, the system will be configured to trigger automated response actions. These actions may include isolating affected assets, blocking suspicious network traffic, or rolling back changes to mitigate the impact of ransomware attacks. The system will raise alerts for manual investigation and response for zero-day exploits.

6. Performance Analytics: The solution will include an analytics section to measure its performance and effectiveness. It will track the number of true positive and false positive alerts generated by the system. The analytics component will continuously evaluate the accuracy and precision of the AI models, fine-tuning them to improve detection capabilities.

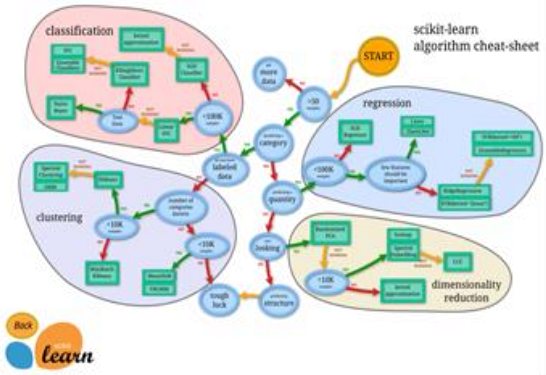
IV. PLATFORM USED

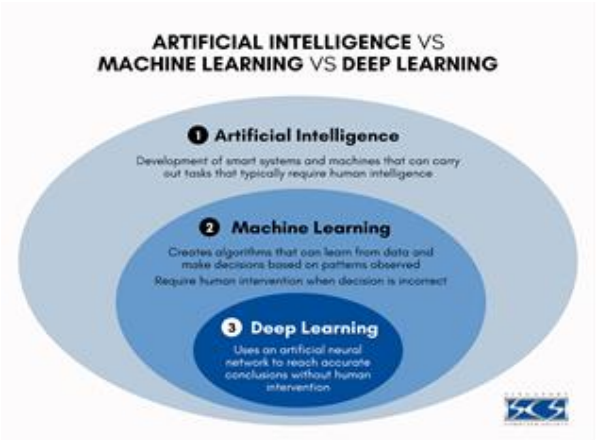
1. Machine Learning and Deep Learning Frameworks: To develop and train AI and machine learning models, popular frameworks such as TensorFlow, PyTorch, or scikit-learn can be used. These frameworks provide a wide range of tools for building and training machine learning models, including neural networks for deep learning tasks.

2. Programming Languages: The project can be implemented using programming languages like Python, which is widely used in the data science and machine learning communities. Python offers a vast ecosystem of libraries and tools for data manipulation, model development, and analytics.

3. Web Application Development: To build the user interface for security analysts and administrators, web development frameworks like Flask or Django (both based on Python) can be

used. These frameworks simplify the process of building interactive web applications





Streamlit

V. SYSTEM CONFIGURATION

1. Machine Learning Environment:

- Programming Language: Use Python as the primary programming language for developing the machine learning models and data processing scripts.
- Machine Learning Frameworks: Employ popular frameworks like TensorFlow or PyTorch for building and training the AI models. Leverage scikit-learn for traditional machine learning tasks.
- High-Performance GPUs: If deep learning models are used, consider utilizing GPUs for faster training and

inference.

2.Web Application:

- Web Framework: Use Flask or Django to build the user interface for security analysts and administrators.

- User Authentication and Access Control: Implement user authentication and access control to ensure secure access to the application.

- Real-Time Alerts: Develop a real-time alerting system to notify security analysts immediately upon detecting potential threats.

3.Virtual Environment

1. Isolation: Virtual environments provide isolation from the system-wide Python installation. When you create a virtual environment, it creates a separate directory with its own Python interpreter and site-packages directory, allowing you to work in isolation.

2. Package Management: With virtual environments, you can install and manage packages independently for each project. This means you can have different versions of packages in different virtual environments, avoiding version conflicts.

3. Easy Setup: Creating a virtual environment is straightforward. You can use Python's built-in venv module or third-party tools like virtualenv to create virtual environments w21qazith just a few commands.

4. Activation/Deactivation: Once you've created a virtual environment, you need to activate it to start using it. Activation sets the appropriate environment variables, so the Python interpreter and packages from the virtual

environment are used. When you're done working in the virtual environment, you can deactivate it to revert to the system-wide Python.

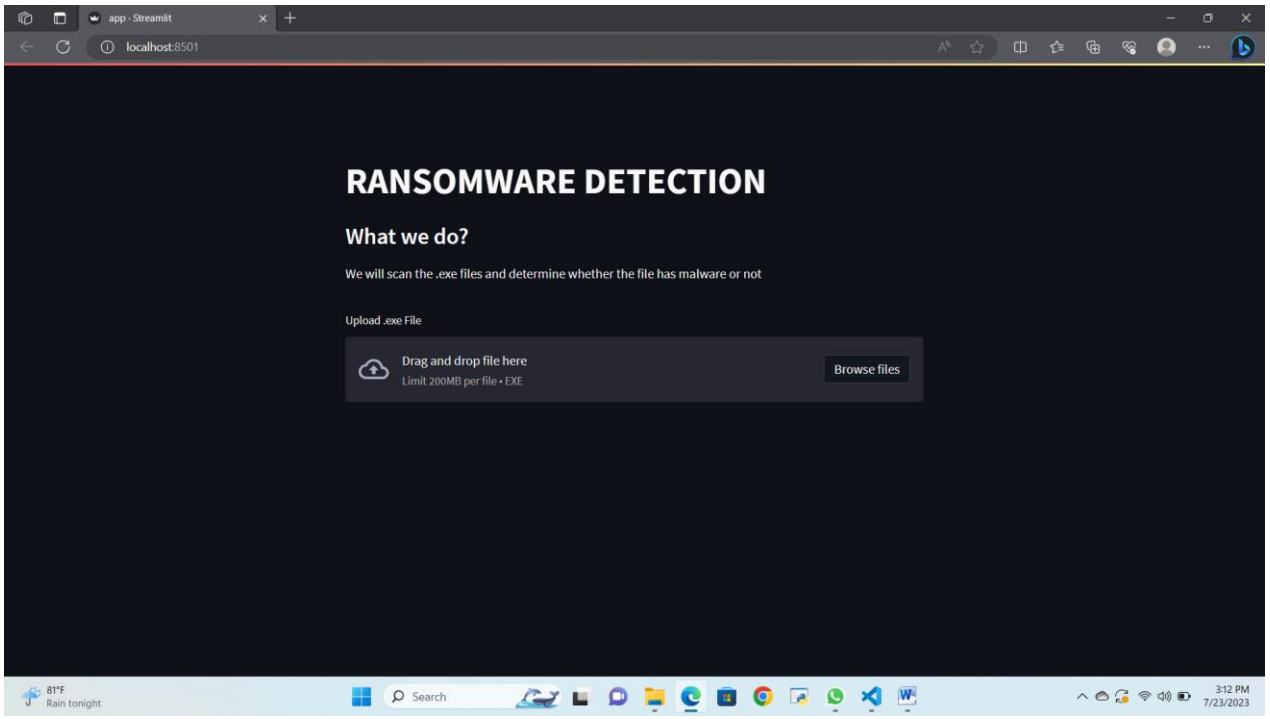
5. Dependency Management: Virtual environments allow you to manage project dependencies effectively. By specifying the required packages and their versions in a requirements.txt file, you can easily recreate the same environment on another machine.

6. Reproducible Environments: Virtual environments ensure that your project remains reproducible, even across different systems. By using a virtual environment, you can avoid compatibility issues when running your code on different computers.

VI. IMPLEMENTATION

I .Front End

- ♦ Streamlit is used to build the user interface for the ML model.
- ♦ Streamlit is an inbuilt python library.
- ♦ FLASK was also used to develop the web Page.
- ♦ The pickle module allows you to save Python objects into a file in a compact binary format and later load them back into memory. This is especially useful when you need to save the state of an object or data structure and retrieve it later, without losing its structure and attributes.

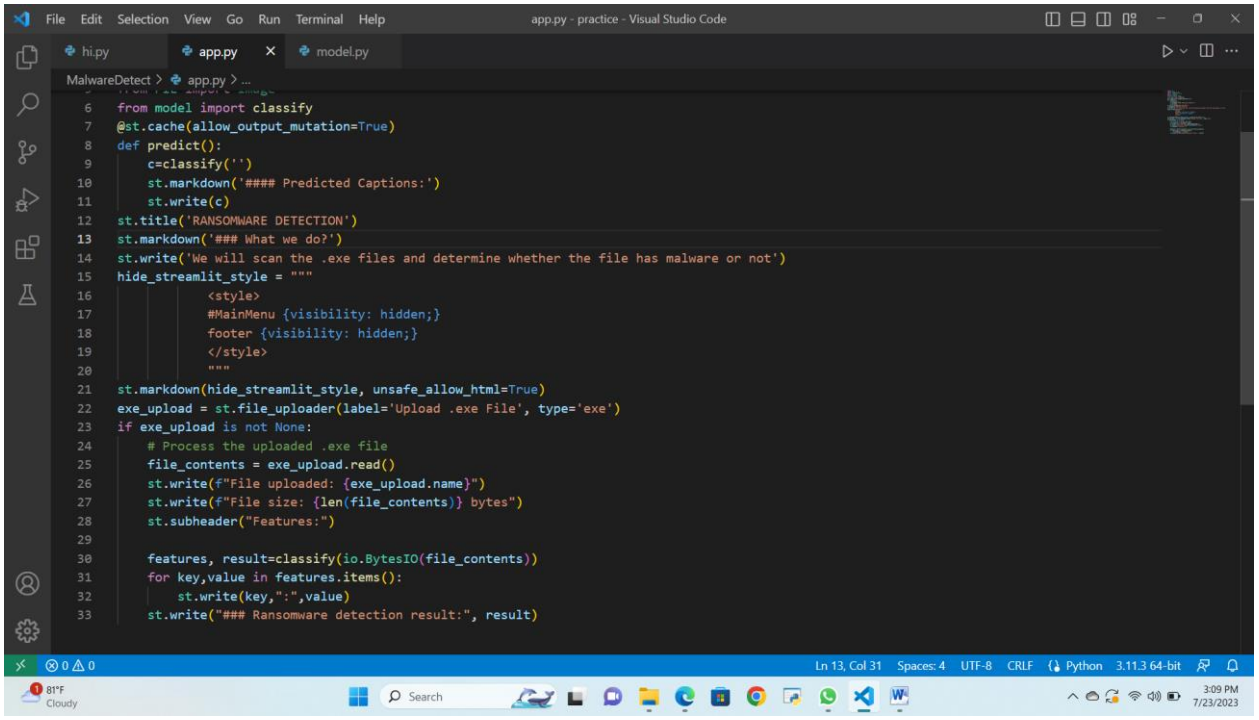


II .Back End

Model.py has the model training and after the prediction, it will pass the result to app.py To display on the screen.

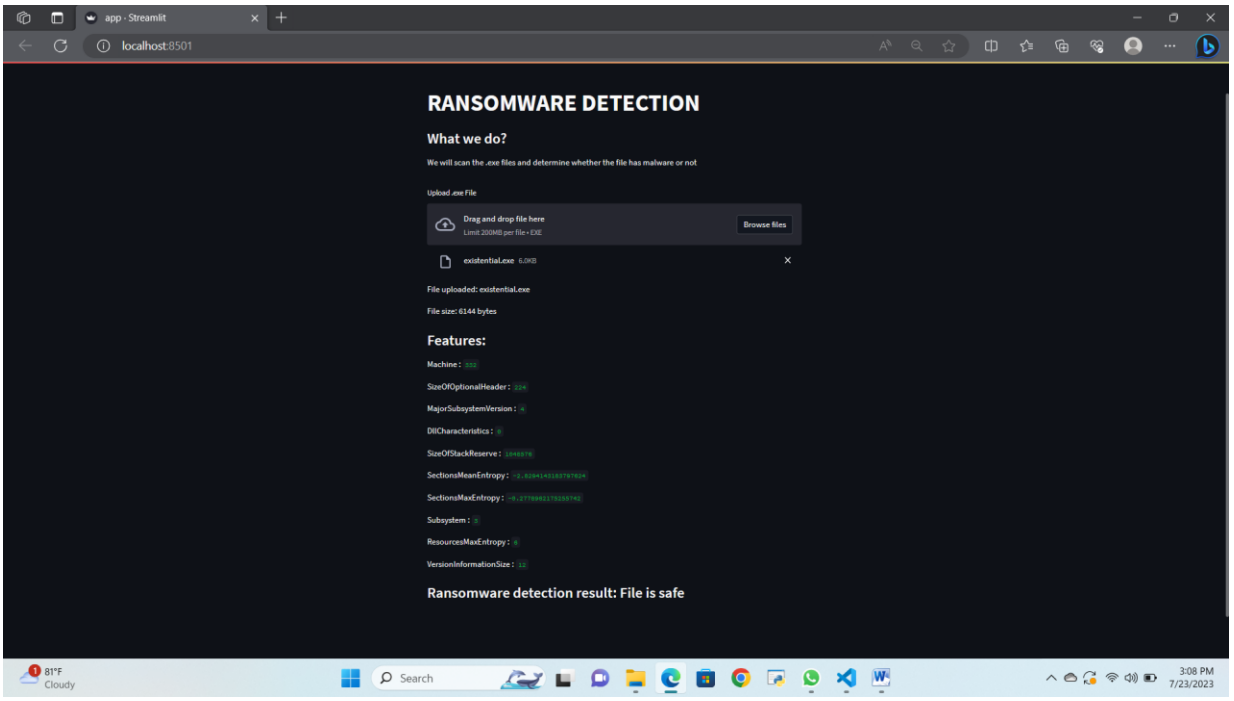
"randomModel.pkl" has the pickle file .The pickle module allows you to save Python objects into a file in a compact binary format and later load them back into memory.

UI WITH STREAMLIT

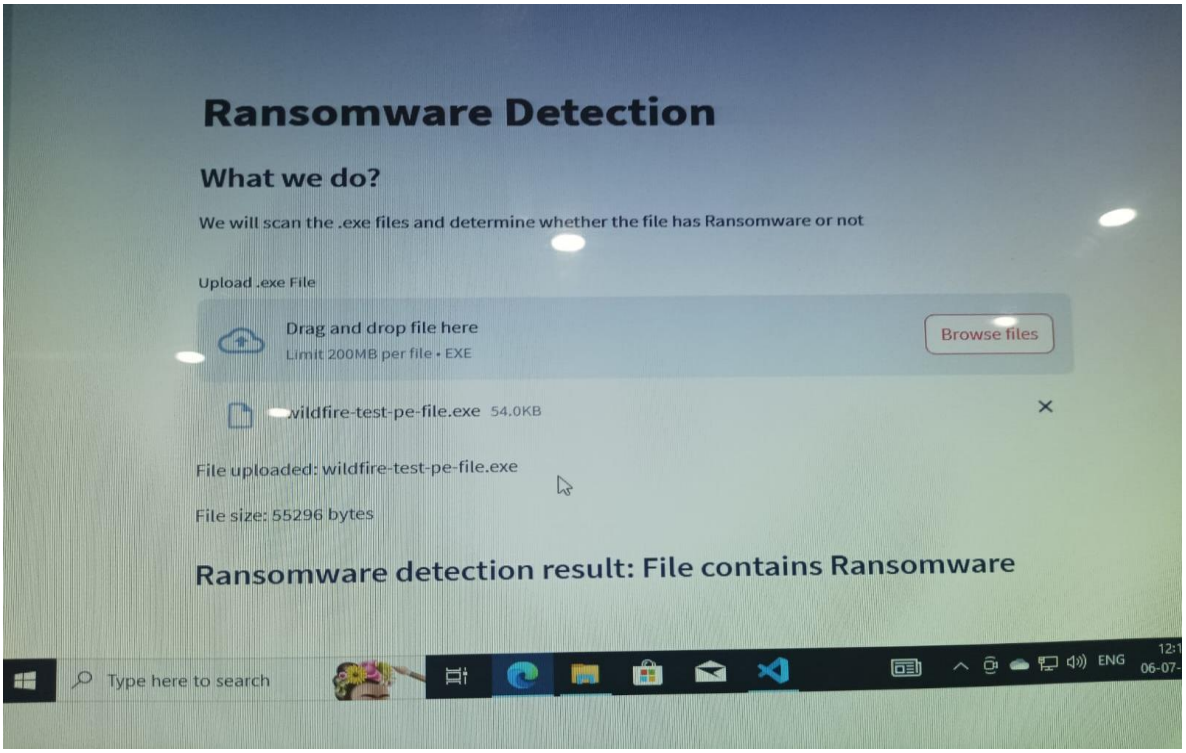


VII .TESTING

When executable file is Safe



When the executable file contain Ransom



VII. CONCLUSION

The Ransomware detection project provides early detection Proactive defense and collaboration , safeguarding organizations from ransomware threats and minimizing Financial and operational damages.

XI. FUTURE SCOPE

The AI-powered alert management system to detect ransomware attacks and zero-day exploits in Cloud services has significant future scope, as cybersecurity and Cloud technologies continue to evolve. Here are some potential future enhancements and expansions for the project:

1. Enhanced AI Models: Continuously improving and fine-tuning the AI models using more advanced machine learning techniques and larger datasets will lead to better detection accuracy and reduced false positives.

2. Zero-Day Exploit Detection: Developing specialized AI models to detect zero-day exploits more effectively by analyzing behavior patterns and abnormal activities in real-time.

3. Threat Intelligence Integration: Integrating threat intelligence feeds and services to enrich the system's knowledge of emerging threats and to proactively detect new attack vectors.

4. Multi-Cloud Support: Expanding the system's capabilities to work across multiple Cloud service providers, allowing organizations to monitor and protect their assets in different Cloud environments.

5. Cloud-Native Security Features: Integrating with Cloud-native security features and APIs to enable automated responses

using Cloud provider-specific tools.

6. User Behavior Analytics: Implementing user behavior analytics to identify suspicious user activities, abnormal login attempts, and potential insider threats.

7. Continuous Learning: Enabling the system to continuously learn from new data and adapt to evolving threat landscapes, ensuring it stays up-to-date with the latest attack patterns.

8. Threat Hunting and Incident Response: Extending the system to support advanced threat hunting capabilities, enabling security analysts to investigate incidents more deeply.

9. Adaptive Response Actions: Implementing adaptive response actions that dynamically adjust based on the severity and nature of the detected threat.

10. Integrating with Security Orchestration, Automation, and Response (SOAR) Platforms: Integrating with SOAR platforms to streamline incident response workflows and automate incident handling.

VIDEO LINK:-

https://drive.google.com/file/d/1YrM44I6d6m0ffsUNvt9CZCY_cWPY-laR/view?usp=drivesdk

X . REFERENCES

[1] Steve Morgan. Cybercrime to cost the world $10.5 trillion annually by 2025. https://cybersecurityventures.com/ cyberwarfare-report-intrusion/. Online; Post : 2020-11-13.

[2] Harjinder Singh Lallie, Lynsay A. Shepherd, Jason R.C. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks

during the pandemic. Computers and Security, 105:102248, 2021.

[3] Av-test. https://www.av-test.org/fr/?r=1. Accessed: 2022-05-30.

[4] Todd Drew. Costa rica declares state of emergency after conti ransomware attack. https://www.secureworld.io/industry-news/ costa-rica-emergency-ransomware. Online; Post : 2022-05-12.

[5] Ross J. Anderson, Chris J. Barton, Rainer Bolme, Richard ¨ Clayton, Carlos Hernandez Gan˜an, Tommaso Grasso, Michael ´ Levi, Tyler W. Moore, and Marie Vasek. Measuring the changing cost of cybercrime. 2019.

[6] Daniele Ucci, Leonardo Aniello, and Roberto Baldoni. Survey of machine learning techniques for malware analysis. Computers and Security, 81:123–147, 2019.

[7] Edward Raff and Charles Nicholas. A Survey of Machine Learning Methods and Challenges for Windows Malware Classification. 2020