# GuardianCyber: An AI-Driven Cybersecurity Solution for Small Businesses

Devansh Khandelwal



*Abstract*

In an era marked by escalating cyber threats, small businesses face heightened vulnerabilities, often lacking the resources to deploy robust cybersecurity measures. This project introduces "GuardianCyber," an innovative AI-driven cybersecurity solution meticulously designed to prevent cyber attacks on small businesses. Recognizing the imperative for user-friendly and cost-effective security, GuardianCyber combines real-time threat detection, data protection, and secure access controls.

Through comprehensive market assessments, we identified a burgeoning need for tailored cybersecurity solutions in the small business sector. The solution addresses the limitations of existing products by prioritizing simplicity, affordability, and effectiveness. Leveraging AI algorithms, GuardianCyber analyzes network activity, encrypts sensitive data, and adapts user access controls in response to evolving threats.

Our business model revolves around a subscription-based pricing strategy, ensuring scalability and accessibility for businesses of varying sizes. The project culminates in the development of a prototype, featuring a user-friendly interface and a robust AI architecture. Basic visualizations, exploratory data analysis, and machine learning modeling validate the efficacy of GuardianCyber.

By aligning with applicable regulations, considering constraints, and benchmarking against existing products, GuardianCyber aims to empower small businesses with a proactive defense against cyber threats. The prototype represents a significant step toward realizing a comprehensive and accessible cybersecurity solution for the evolving needs of small enterprises.

# 1.0 Problem Statement

Small businesses face increasing cybersecurity threats, and existing solutions may be complex, expensive, or inadequate. Developing a user-friendly, AI-driven cybersecurity solution tailored to the unique needs of small businesses is essential. Set the **context**: Help the reader understand general information about the problem or need area, including any necessary definitions, statistics, etc. Use pictures and visual images as much as possible.

**Top 5 Cybersecurity Challenges Facing Small Businesses Today**

* Phishing Attacks
* Ransomware
* Malware
* Insider Threats
* Weak Passwords

# 2.0 Customer Needs Assessment

Looking into what small businesses need for cybersecurity, it's clear they want something affordable and easy to use. Many small businesses lack tech experts, so they need a solution that's not too complicated.

Our study found that small business owners are more aware than ever about the risks of cyber attacks. They want a tool that's simple and won't require a lot of time to learn. Current cybersecurity options are often too complicated or costly for small businesses, leaving them vulnerable.

GuardianCyber aims to fill this gap by offering a user-friendly and budget-friendly cybersecurity solution. The research indicates a clear need in the market for a tool that's just right for small businesses – not too complex, not too expensive, but still strong enough to keep them safe online.

This type of real-time response helps businesses avoid service downtime and lost business while maintaining customer trust.

With AI to help defend against cyberattacks, financial institutions can identify intrusions and anticipate future threats to keep financial records, accounts and transactions secure.

# 3.0 Target Specifications

The envisioned system/service is tailored to empower shopkeepers and small businesses, especially startups, by equipping them with effective techniques to prevent cyber attacks. Recognizing the vulnerability of businesses with limited cybersecurity knowledge, the system focuses on real-time threat detection, providing immediate insights into potential threats like malware attacks.

**Consequences of Cyberattacks on Businesses**

* Financial Losses
* Reputation Damage
* Operational Disruptions

**With the help of this Product we can prevent such kind of Consequences**

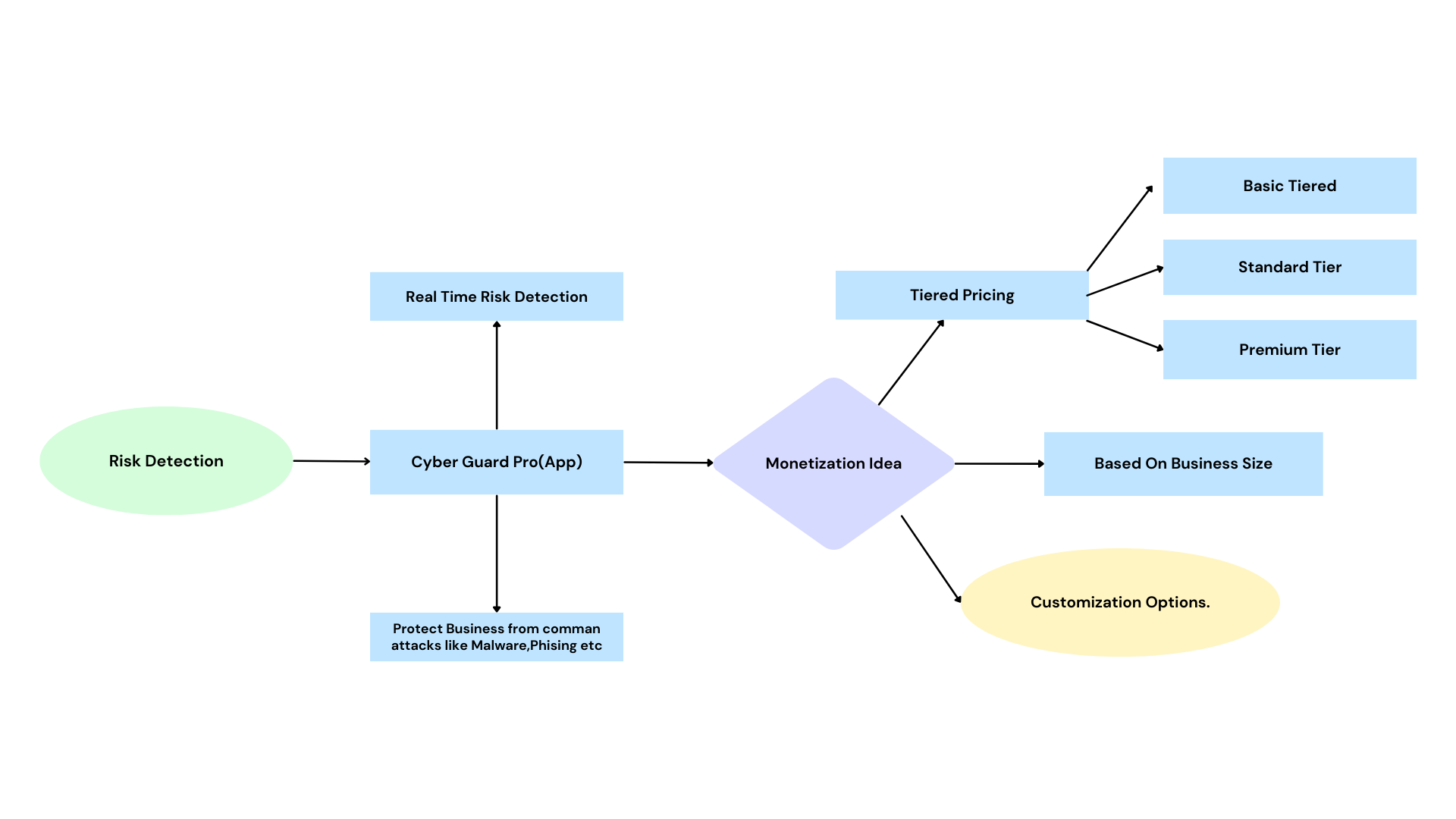
# 4.0 External Search

The sources I have used as reference for analyzing the need of such a system for local

businesses

* [Cybersecurity Challenges Facing Small Businesses Today](https://redfoxsec.com/blog/cybersecurity-challenges-small-businesses/)
* [How AI-Based Cybersecurity Strengthens Business Resilience](https://blogs.nvidia.com/blog/ai-cybersecurity-business-resilience/#:~:text=This%20type%20of%20real%2Dtime,records%2C%20accounts%20and%20transactions%20secure.)
* [Importance for Cyber Security for business](https://www.nu.edu/blog/what-is-cybersecurity/)

## 5.0 Product Design



**6.0 Product Prototype**

Product prototype introduces an AI-driven cybersecurity guardian meticulously crafted for the unique needs of small businesses. This innovative solution combines real-time threat detection, robust data protection, and secure access controls to fortify the digital resilience of small enterprises. With an emphasis on user-friendliness and proactive defense, this cybersecurity guardian aims to provide a comprehensive and accessible shield against the evolving landscape of cyber threats.

Small Business

Network

Network Traffic

Real Time Thread Detection  
 ( AI Algorithm)

Security Events

Data Protection Mechanism

(Encryption, etc.)

Notifications

User Friendly Interface

(Dashboard, Alerts Tutorials)

**Product Prototype**

## 7.0 Product details

**7.1 How it will work :-**

1. **Data Collection**:

We can collect relevant datasets that include examples of cybersecurity threats faced by small businesses. This may include historical data on attacks and incidents.

1. **Data Preprocessing**:

Clean and preprocess the collected data to ensure it's suitable for training your machine learning model.

1. **Choose Machine Learning Algorithms**:

Select machine learning algorithms suitable for the classification of cybersecurity threats. Common algorithms include Decision Trees, Random Forests, or more advanced techniques like Neural Networks.

1. **Feature Selection**:

Identify and select relevant features from your dataset that contribute to the identification of cybersecurity threats.

1. **Training the Model**:

Train your machine learning model using labeled data, where each example is tagged with the type of threat it represents.

1. **Validation and Testing**:

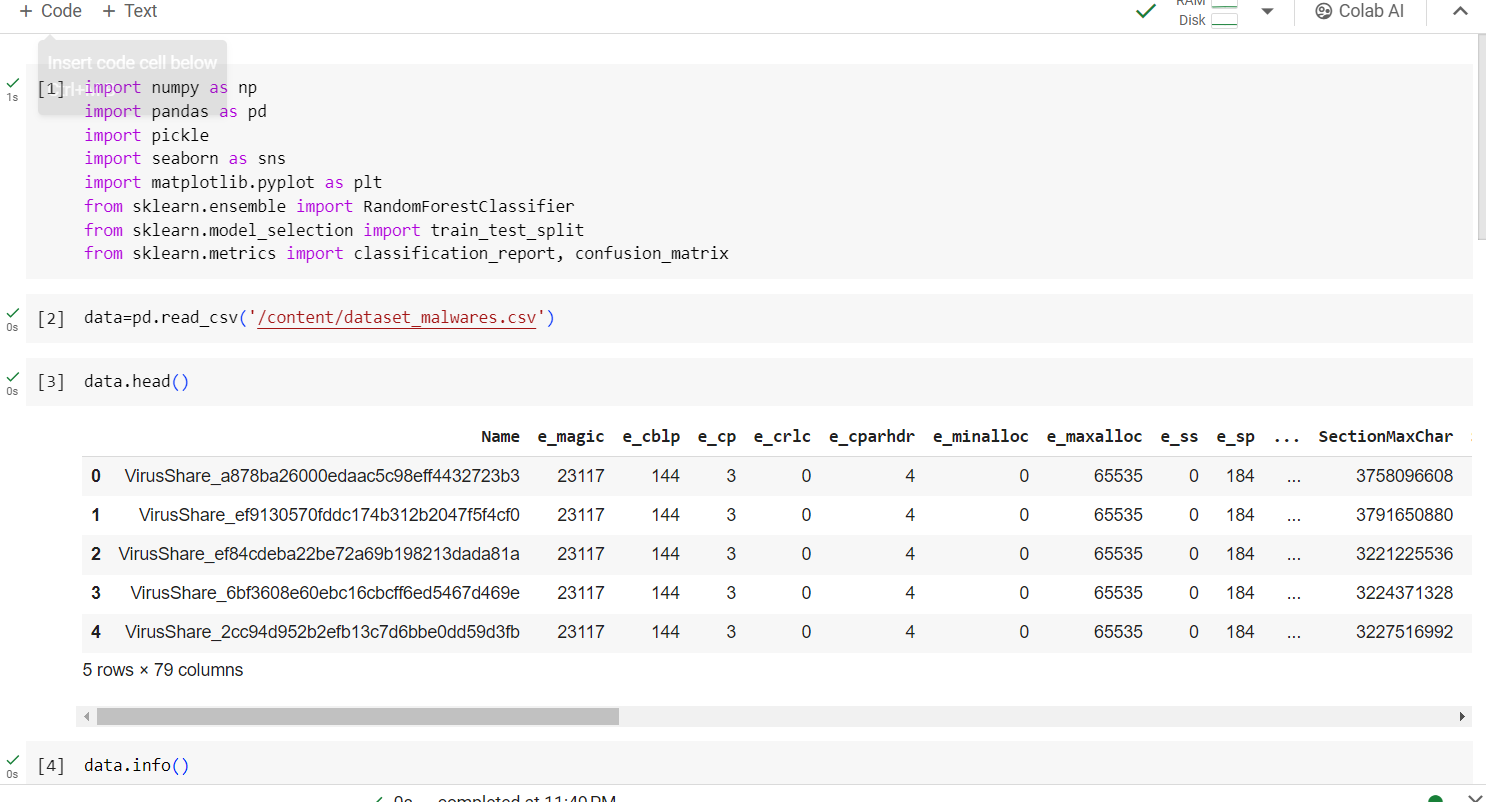
Validate your model using a separate dataset to ensure its accuracy and effectiveness.

Test the model with new, unseen data to evaluate its real-world performance.

1. **Real-Time Threat Detection:**
2. **Alert Mechanism:**
3. **User-Friendly Interface**

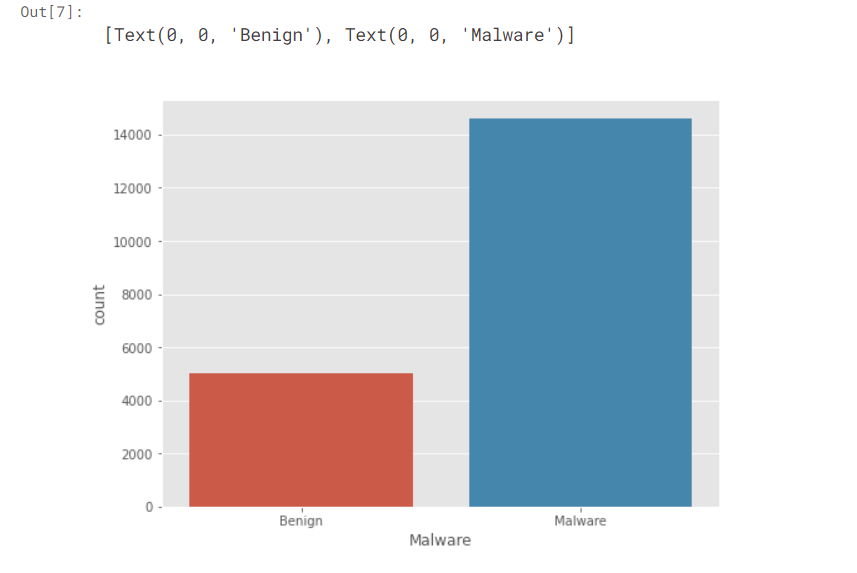
## 8.0 Concept Development

1. Data Collection :- [Malware\_Dectection\_Dataset](https://www.kaggle.com/code/maidaly/malware-detection-with-machine-learning/input)
2. Data Preprocessing

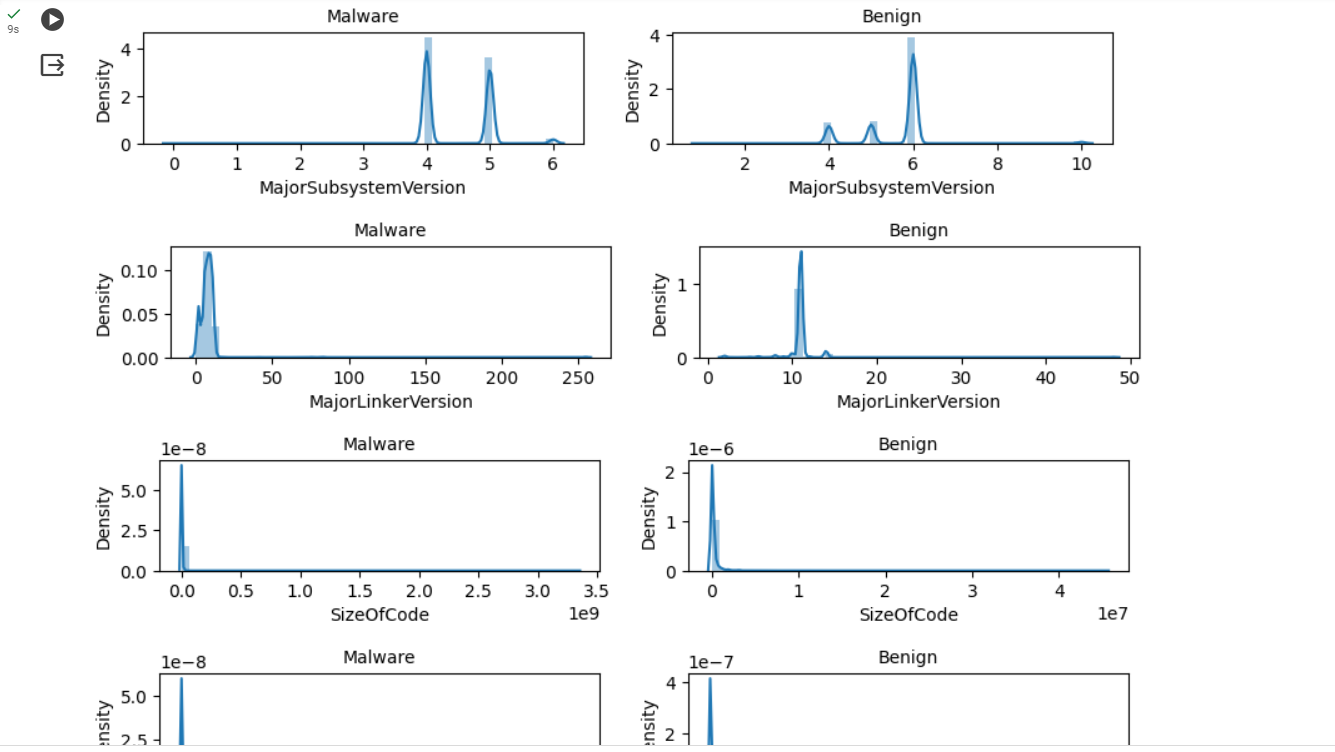


1. Classes Distribution :-





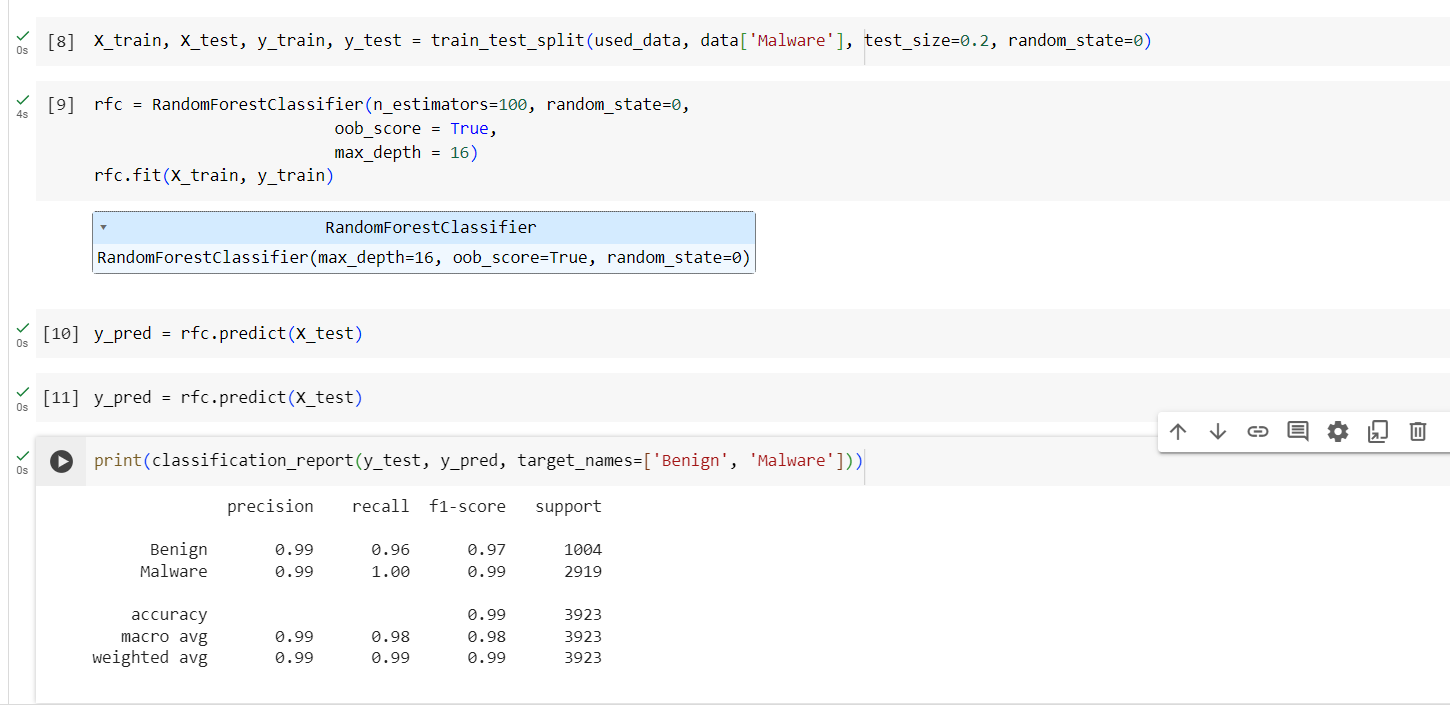




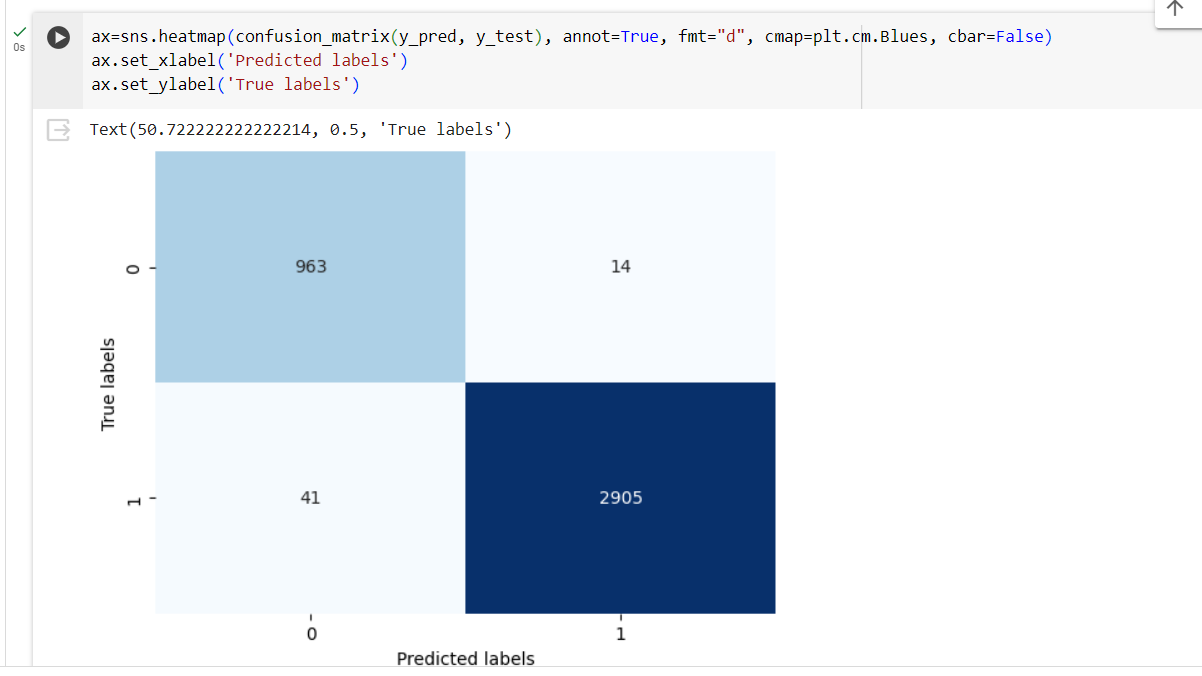
1. Splitting the data :-



1. Building the model :-



1. Confusion matrix



## 9.0 Conclusions

* The randomforest model provide very good results without any preprocessing on the data.
* The reult is good despite the fact that the data is imbalnced. So, I found that we do not need to use any technique to rebalance it.
* Scaling is not nessecry, Random forest model is recursive partitioning model depends on data partition because it works on separation of features values and not make calculations on it.