MiAtbot

[Larrissa, Yeo Xiao Tong], [Lim Michelle Marie Aliling], [Nathan, Leow Chen Tao], [Zhi Qing, Tan], [Carment, Tham Yu Xuan], [Villarico Gabriel Babiera]  
*Infocomm Technology Cluster*  
*Singapore Institute of Technology*Singapore  
{2201935, 2202364, 2200594, 2201805, 2201318, 2200479}@sit.singaporetech.edu.sg

# ***Abstract*—The goal of this project is to improve incident response skills by developing a chatbot driven by artificial intelligence. By providing organized, real-time guidance that is in line with industry standards and enhanced with the most recent threat intelligence, the chatbot overcomes the drawbacks of static playbooks. The goal of the chatbot is to help security professionals navigate complicated threat scenarios more effectively and adaptably by offering interactive and intuitive support.**

# Introduction

Artificial intelligence (AI)-driven chatbots have revolutionized how we use technology by providing real-time, intuitive help in a variety of fields. These chatbots, which are made to mimic human dialogue, swiftly walk users through difficult tasks, offer personalized advice, and respond to inquiries.

Maintaining efficient incident response plans becomes more difficult for corporations as cyber threats become more complex. In order to provide analysts with situational, actionable guidance, traditional methodologies sometimes rely on static playbooks that are not flexible enough to react to changing threat scenarios. In order to fill these gaps, we have created an AI-powered chatbot named MiAtbot that provides users with real-time, structured guidance that is based on industry standards, enhanced with the most recent threat data from MITRE ATT&CK Framework, and customized to meet their individual needs.

# Background Research

## *Literature Review*

1. *Overview of Incident Response and Key Frameworks:* With the increasing number of cyber dangers emerging as technology advances, cybersecurity has become a critical concern for organisations. While organisations invest extensively on cybersecurity defences, a structured Incident Response (IR) approach is critical for limiting the effect of unavoidable breaches. IR is a disciplined technique for swiftly recognising, mitigating, and minimizing events in order to minimise damage, restore damaged systems, and decrease operational and financial impact. With the constant development in complex cyber threats, IR provides a framework for not only responding successfully but also learning from each occurrence, therefore increasing defences over time.

Some key frameworks that organizations typically use to conduct their incident response operations are:

* 1. ***NIST Cybersecurity Framework (CSF)*** is widely adopted for its comprehensive approach, focusing on five core functions: **Identify, Protect, Detect, Respond, and Recover**. This framework helps organizations assess their current risk posture and establish policies and procedures to handle incidents while promoting continuous improvement.
  2. ***MITRE ATT&CK Framework*** provides a detailed matrix of adversarial tactics and techniques, grounded in real-world observations of cyberattacks. It helps organizations understand and model attacker behaviors, enabling more precise detection and analysis in IR processes and supporting proactive defense measures.
  3. ***SANS Incident Handling Process*** offers a straightforward six-phase approach: **Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned**. Recognized for its practicality, it emphasizes preparation and post-incident learning, making it accessible and highly applicable for teams across various organizational sizes.
  4. ***ISO/IEC 27035***, part of the ISO/IEC 27000 family, provides guidelines specifically for information security incident management. It outlines procedures for detection, response, and recovery, integrating seamlessly with broader information security management practices, making it ideal for organizations aligned with international standards.
  5. ***COBIT (Control Objectives for Information and Related Technologies)***, though primarily focused on IT governance, offers robust risk management and incident response guidance within an IT governance framework. COBIT enables organizations to align their IR processes with broader business goals, ensuring that incident management efforts contribute to organisational resilience and compliance.

1. *Role of AI in Cybersecurity Incident Response:* Recent research has highlighted the revolutionary significance of AI in improving cybersecurity and incident response strategies. It emphasises AI's capacity to greatly increase threat detection, reaction time, and operational accuracy in cybersecurity frameworks, while also reducing security professionals' intense workloads. Specifically, AI improves critical domains like vulnerability assessment, intrusion detection and prevention, and digital forensic analysis. However, despite its usefulness, AI has limitations and may bring new risks. As a result, they support further research and development to tackle these issues, arguing that these developments are necessary to fully realise AI's promise in thwarting more complex cyberthreats. [1]
2. *Transformer Models and Their Applications in Cybersecurity:* Transformer models have significantly influenced the field of cybersecurity, particularly through their applications in threat detection, data analysis, and incident response. The integration of these models enhances the capability to process and analyze vast amounts of cybersecurity data, which is crucial in the context of increasing digital transformation and associated risks. For instance, Ranade et al. introduced CyBERT, a domain-specific BERT model that improves the contextual understanding of cybersecurity threats, thereby aiding in the extraction of actionable insights from threat intelligence [2]. This model exemplifies how transformer architectures can be tailored to meet the specific needs of cybersecurity professionals.

Moreover, the use of transformer models in machine learning has been shown to enhance threat detection mechanisms. Sarker et al. discuss how machine learning, including transformer-based approaches, can be leveraged for various cybersecurity applications, such as IoT security and network defense [3]. This is particularly relevant as organizations increasingly adopt digital technologies, which necessitate robust cybersecurity measures to mitigate evolving threats [4]. Furthermore, the application of transformers in automating the analysis of cybersecurity incidents can streamline response efforts, making it easier for organizations to manage and mitigate risks effectively [5].

1. *Challenges in Adapting GPT Models for Incident Response:* The evolution of incident response capabilities has become increasingly critical as organizations face more complex and dynamic threats. Traditional incident response frameworks often exhibit inherent rigidity that limits their effectiveness in dynamic threat environments. Plotnick et al. [6] identified the “threat-rigidity syndrome” in crisis response organizations, where increased control mechanisms and restricted information flow leads to reduced adaptability exactly when flexibility is most crucial. Their study demonstrates how principles from High Reliability Organisations (HRO) and Crew Resource Management can maintain necessary flexibility while ensuring response reliability. Further study was done by Ahmad et al. [7] who revealed that there are significant limitations in contemporary incident response practices, specifically the control of technical solutions at the expense of strategic learning. Their research on global financial institutions demonstrated that organizations typically prioritize immediate business continuity over long-term security improvements. This means that they often neglect opportunities for strategic policy development and system adaptability.

In terms of the evolution beyond generic response models, the inefficiency of generic best practices in addressing modern threats has been well-documented. A double-loop learning model, proposed by Shedden et al. [8], emphasizes the following:

1. Continuous evaluation and adaptation of response procedures
2. Integration of informal learning processes
3. Regular reassessment of fundamental assumptions

Additionally, analysis of standardized frameworks such as the National Incident Management System (NIMS) by Sunshine [9] identified structural limitations when confronting emerging threats. These findings highlight the importance for more flexible response architectures and improved integration of real-time threat intelligence within existing frameworks.

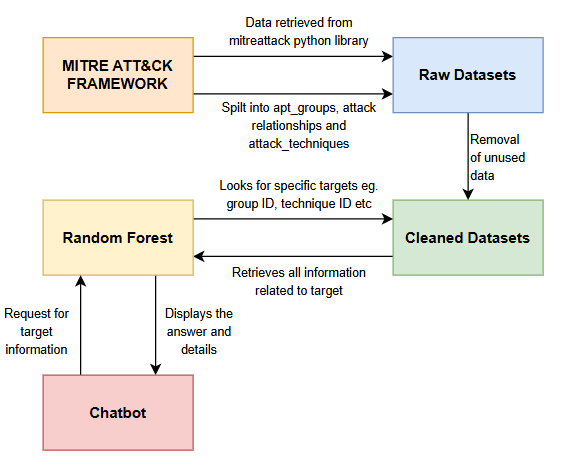
Current developments in Artificial Intelligence present both opportunities and challenges for Incident Response enhancement. Maezo et al [10] explored AI integration within Computer Security Incident Response Teams (CSIRTs), noting an improvement on the threat detection capabilities and response speeds while acknowledging the significant integration challenges within existing protocols.

The development of specialized AI models such as TrafficIncidentResponseGPT [11], demonstrates the potential for context-aware response generation. The research highlights several key considerations including, real-time adaptation mechanisms for evolving situations and the implementation constraints related to transparency and public trust. Another recent study examines Large Language Model applications in specialized domains [12] parallel incident response challenges, particularly in model hallucinations – where LLMs generate plausible but factually falsehood information. In a high-stakes environment, these hallucinations pose significant risk to operational safety and effectiveness which could result in misguided response strategies during critical incidents, incorrect resource allocation decisions and erosion of trust in AI-augmented response systems.

The evolution of incident response research emphasizes the need for adaptive, context-aware approaches that can leverage emerging technologies while maintaining operational reliability and public trust. This requires careful consideration of both the potential benefits and limitations of AI integration, especially in high-stakes decision-making scenarios.

# System diagram

The following system diagram in Fig 1, depicts the flow of the project.



*Fig. 1. System Diagram*

The project uses the MitreAttack Python library as the main source of information. Specific data can be retrieved by stating the keys which will be mentioned in Section IV. The data that is obtained directly from the library is called raw datasets and would require cleaning to remove any unused data or information.

After cleaning, the data is now called Cleaned Datasets. Using the clean datasets, random forest is then utilised to predict the outcome based on what the user has input inside the chatbot by getting all the information that is linked with the user request.

# Dataset used

To retrieve the dataset we will use in this project, We will use the mitreattack-python library. The mitreattack-python library is a Python-based tool created to communicate with the MITRE ATT&CKTM framework, a thorough knowledge base of adversary tactics, techniques, and procedures (TTPs) employed in cyberattacks [13]. This library offers an intuitive interface to automate the data processing, mapping, and querying processes of the ATT&CK framework. Researchers and cybersecurity experts can use it to incorporate ATT&CK data into unique tools and methods, including automated incident response, threat detection, and security monitoring.

By using mitreattack-python, we can access the information about the enterprise domain in the MITRE ATT&CKTM framework using the keys as shown in Table 1 and extract it as a CSV file after converting the raw STIX data into Pandas DataFrames respectively.

*TABLE 1. The key used via the Mitreattack-python library*

| **Key** | **Description** | **Extract the Dataset** |
| --- | --- | --- |
| Groups | Retrieve information about the APT groups | apt\_groups.csv |
| Relationships | Retrieve information about the relationships between techniques, groups and other entities | attack\_relationships.csv |
| Techniques | Retrieve information about the techniques | attack\_techniques.csv |

# Data pre-processing

After extracting the dataset using the mitreattack-python library, the next crucial step is data preprocessing, which includes data cleaning to ensure the information is accurate, consistent and ready for analysis as shown in *Appendix A*.

In our dataset, we have identified the key columns relevant to our analysis, handled missing values, normalized text fields and removed unnecessary columns as shown in Table 2 - 3.

*TABLE 2. Common Key Columns in All the Datasets*

| **Columns** | **Description** |
| --- | --- |
| ID | A unique identifier for the entity used in the analysis |
| name | The name of the entity, such as the technique name, group name, or tactic name |
| description | Provide details about the entity's purpose, behavior, or characteristics. |

*TABLE 3. Common Unnecessary Columns in All the Datasets*

| **Columns** | **Description** |
| --- | --- |
| STIX ID | An internal identifier used in the STIX format, which is not relevant for this specific analysis |
| created | The timestamp indicating when the entity was initially created |
| last modified | The timestamp of the most recent update to the entity |

To ensure that the data analysis is accurate and simple. We have combined relevant columns from multiple datasets into a single consolidated CSV file by filtering and merging them based on the common data values as shown in Table 4

*TABLE 4. Overall Combined Dataset Used for Data Analysis*

| **Dataset** | **Description** |
| --- | --- |
| aptgroup\_relationship.csv | Information that stated which techniques are used by which APT group |

# Data Analysis

Machine Learning (ML) was utilized to perform data analysis. ML focuses on using data and algorithms to help AI mimic human learning processes while progressively increasing its accuracy. There are various types of models such as regression, classification, clustering, and anomaly detection.

Random Forest is a machine learning technique that builds a large number of decision trees during training and is used for classification, regression, and other applications. Being an ensemble learning technique, it creates more reliable and accurate predictions by combining the predictions of several models (decision trees) as shown in Appendix B. Using this algorithm we are trying to predict the following:

1. What techniques are there in Mitre Attack?
2. What sub-techniques can be linked to a main technique?
3. What are some groups that utilise the attacks?
4. What platforms are exploited by the technique?

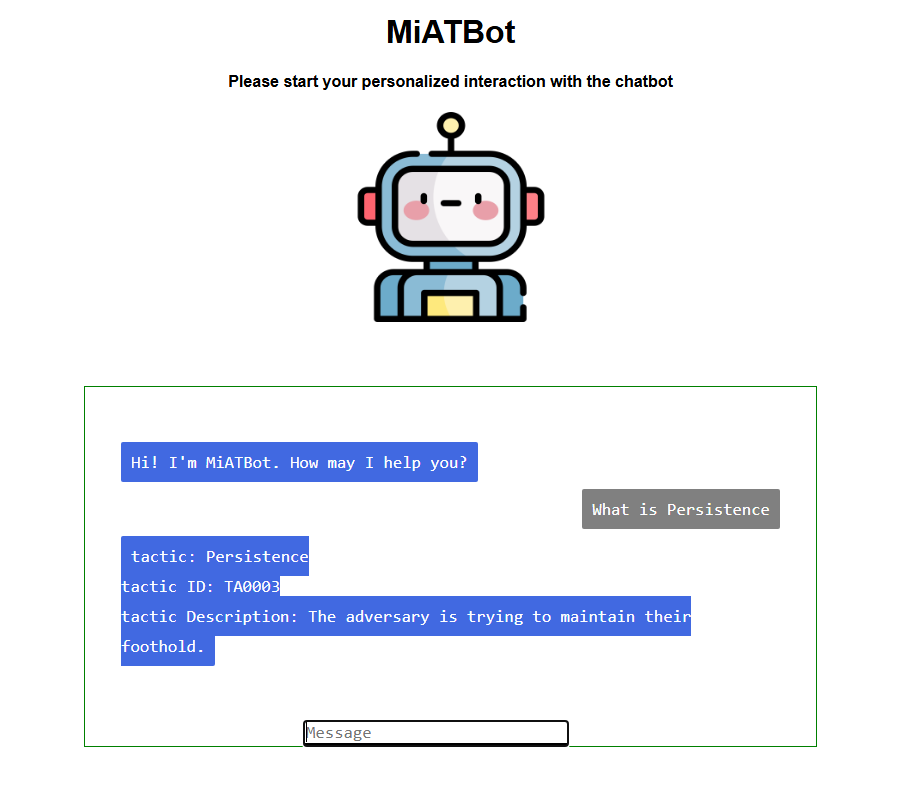
The data in these attributes mainly fall under categorical data. As random forest does not utilize a linear relationship between input features and the target variable, it is able to capture complex patterns and interactions in categorical data.

Decision trees are the building blocks of random forest and they work well with categorical data through the splitting of data into subsets based on feature values. This inherently removes the need to transform the data hence making the trees directly applicable to categorical features. By combining multiple of these trees, random forest reduces the likelihood of overfitting which might occur when individual trees fit too closely to the training data.

Last but not least, random forest uses bootstrap aggregation, which reduces variance and improves generalization. This is crucial for datasets with categorical features that might otherwise lead to overfitting in individual trees.

# Result and Insight

Based on the dataset results mentioned in Section VI, we were able to process the dataset through a front-end web application. We used Flask App to host the web application and utilised a python library package called chatbotAI which is a builder platform that furnishes both bot intelligence and chat handler.



*Fig. 2. Chatbot Interface*

Developing a chatbot that uses MITRE ATT&CK framework provides insights for enhancing cybersecurity operations by acting as a virtual assistant to cybersecurity professionals. The chatbot improves real-time incident response by providing quick access to information on tactics, techniques and procedures (TTPs) whilst offering decision support by suggesting mitigation strategies specific to the detected threats. It prioritizes critical incidents correlated to active adversary campaigns which helps professionals be more efficient.

The chatbot serves as a central knowledge-based, streamlining access to the huge MITRE dataset which helps reduce manual effort and enhance productivity. The chatbot is integrated with machine learning to allow continuous improvement, allowing it to adapt to emerging threat scenarios.

Moreover, the chatbot simplifies complex data by providing readable solutions and/or descriptions to user query inputs such as “What is Malicious Files?” or “What is Persistence?”, thus making the MITRE framework more comprehensible for cybersecurity professionals as shown in Appendix C.

# Conclusion

In conclusion, the team successfully developed a chatbot designed to provide organised, real-time guidance which surmounts the drawbacks of static playbooks. With the integration of machine learning models such as Random Forest which was used to reduce the probability of overfitting, variances and improved generalization for the datasets, it ensured that the chatbot operated on a robust foundation of accurately reliable information. The team also ensured that the datasets have been cleaned and processed to allow for more precise and context-aware responses for the chatbot which, in turn, efficiently assist users in navigating complex scenarios without the need to spend hours on the MITRE ATT&CK framework and being overloaded with information.

## *Tasks Allocation*

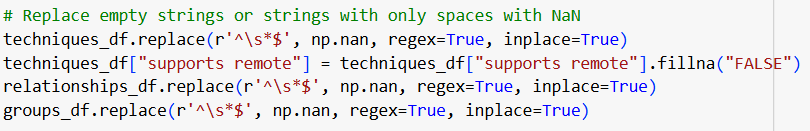
| **Members** | **Task** |
| --- | --- |
| Zhi Qing | Literature Review  Data Finding  Data gathering from MITRE ATT&CKTM framework  Data pre-processing  Report and documentation |
| Gabriel | Literature Review  Data gathering from MITRE ATT&CKTM framework  Data pre-processing  Report and documentation. |
| Nathan | Literature Review  Data Finding  Data Model Coding  Data Analysis  Report and documentation |
| Carment | Literature Review  Data Model Coding  Data Analysis  Report and documentation |
| Larrissa | Literature Review  Chatbot Development via Web app Flask  Report and documentation |
| Michelle | Literature Review  Chatbot Development via Web app  Flask  Report and documentation |

##### References

1. S. K. Hassan and A. Ibrahim, “The role of Artificial Intelligence in Cyber Security and Incident Response: Syed Khurram Hassan, Asif Ibrahim,” International Journal for Electronic Crime Investigation, vol. 7, no. 2, 2023. doi:10.54692/ijeci.2023.0702154
2. P. Ranade, A. Piplai, A. Joshi and T. Finin, "CyBERT: Contextualized Embeddings for the Cybersecurity Domain," 2021 IEEE International Conference on Big Data (Big Data), Orlando, FL, USA, 2021, pp. 3334-3342, doi: 10.1109/BigData52589.2021.9671824.
3. Sarker, I.H., Kayes, A.S.M., Badsha, S. et al. Cybersecurity data science: an overview from machine learning perspective. J Big Data 7, 41 (2020). Doi: 10.1186/s40537-020-00318-5
4. Li, Z., Li, Z., & Ren, Y. (2023). The Impact of Industrial Internet and the Digital Economy on the Management and Development of Manufacturing Information Systems Triggering Digitization as IoT and Artificial Intelligence. Journal of Information Systems Engineering and Management, 8(4), 23796. doi: doi.org/10.55267/iadt.07.14038
5. K. Sandhu, “Advancing Cybersecurity for Digital Transformation: Opportunities and Challenges,” in Advances in Information Security, Privacy, and Ethics, Hershey, PA: IGI Global, 2021, pp. 1–17. dot: dot.org/10.4018/978-1-7998-6975-7.ch001
6. L. Plotnick, M. Turoff and G. Van Den Eede, "Reexamining Threat Rigidity: Implications for Design," 2009 42nd Hawaii International Conference on System Sciences, Waikoloa, HI, USA, 2009, pp. 1-10. doi: 10.1109/HICSS.2009.365
7. A. Ahmad, J. Hadgkiss, and A. B. Ruighaver, "Incident response teams – Challenges in supporting the organisational security function," Comput. Secur., vol. 31, no. 5, pp. 643-652, 2012. doi: 10.1016/j.cose.2012.04.001
8. P. Shedden, A. Ahmad, and A. B. Ruighaver, "Organisational learning and incident response: Promoting effective learning through the incident response process," in Proc. 8th Australian Inf. Secur. Manage. Conf., 2010, pp. 131-142. doi: 10.4225/75/57b6771734788
9. J. Sunshine, "The response structure: Managing emergent threats in the digital age," J. Nat. Secur. Law Policy, vol. 15, no. 1, pp. 56-78, 2017.
10. R. G. Maezo and A. E. Rey, "Boosted CSIRT with AI powered open source framework," 2023 JNIC Cybersecurity Conference (JNIC), Vigo, Spain, 2023, pp. 1-8, doi: 10.23919/JNIC58574.2023.10205787.
11. A. Grigorev et al., "TrafficIncidentResponseGPT: AI-driven incident response for urban traffic management," arXiv preprint arXiv:2404.18550, 2023.
12. R. Smith et al., "Large language models in construction: Applications and limitations," Autom. Constr., vol. 148, p. 104567, 2023. Doi: 10.1016/j.dibe.2023.100300
13. “Mitreattack-python library — mitreattack-python 2.0.0 documentation,” Readthedocs.io. [Online]. Available: https://mitreattack-python.readthedocs.io/en/latest/.

##### Appendix

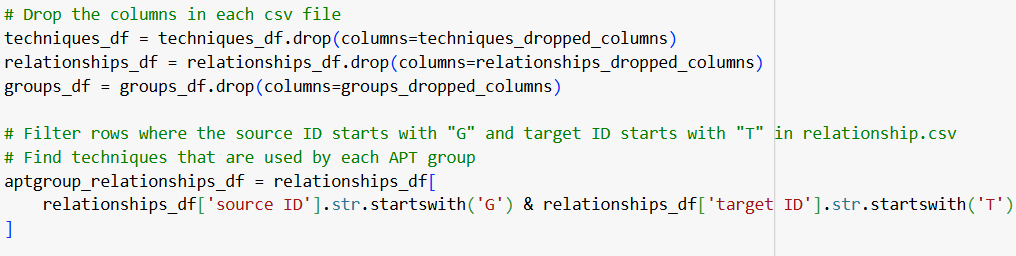
## *Data Pre-processing*



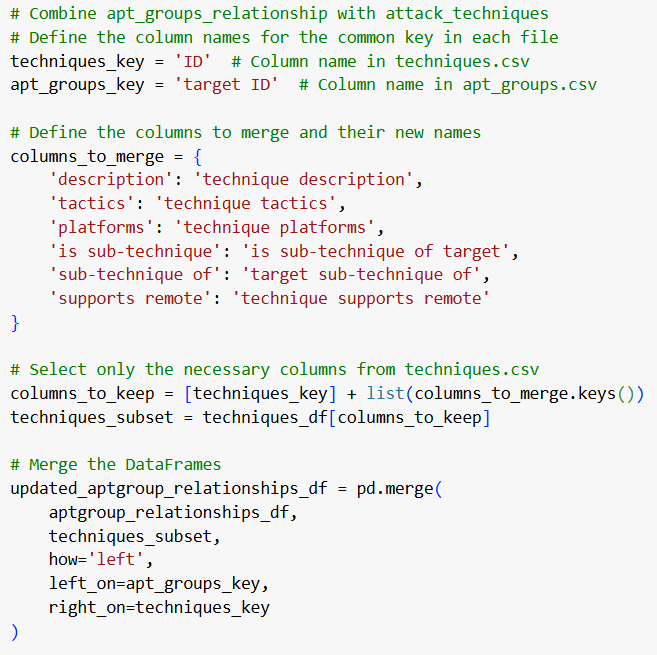
*Fig. 3. Fill empty spaces with Nan values*

**

*Fig. 4. Remove unnecessary columns in the dataset*

**

*Fig. 5. Find techniques that each APT group uses*

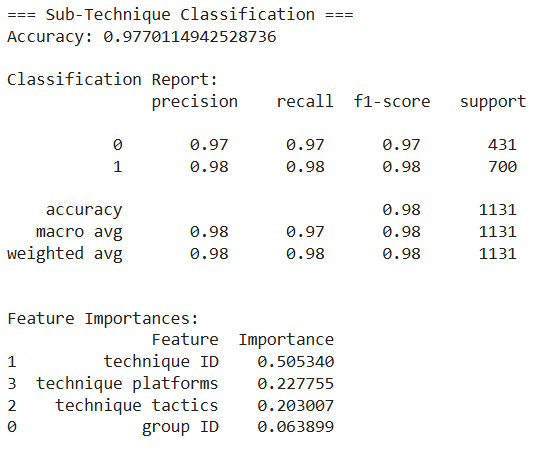
**

*Fig. 6. Combine columns from multiple datasets to form one single dataset for analysis*

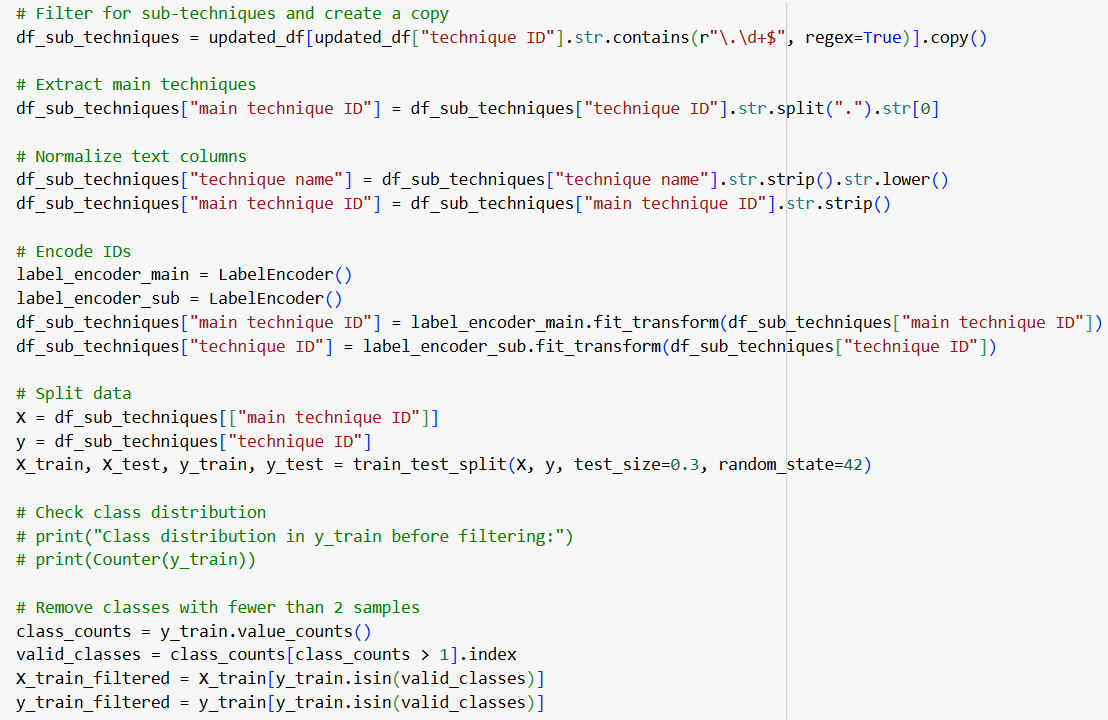
## *Random Forest*



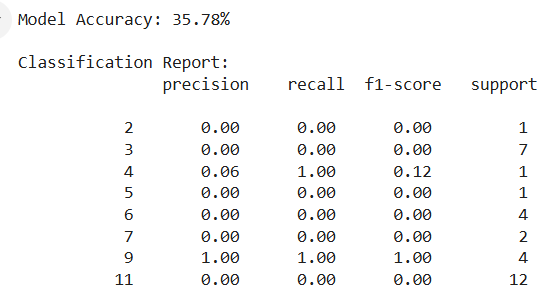
*Fig. 7. Sub-Technique Classification*

**

*Fig. 8. Prediction of “Sub-Technique Classification”*

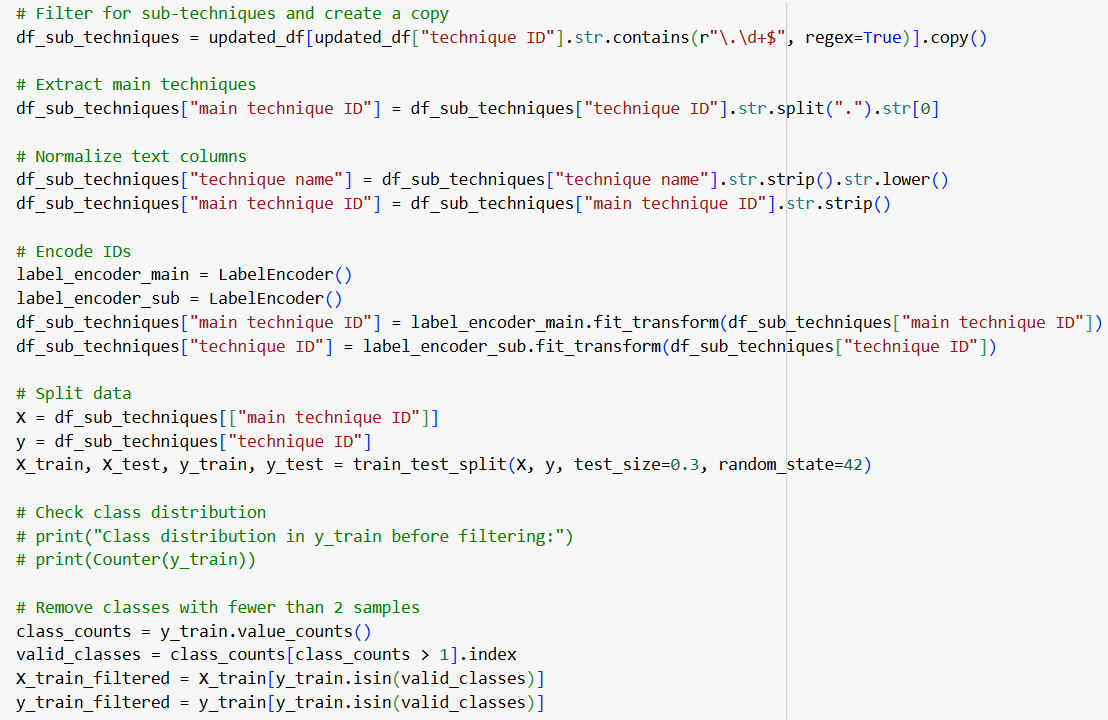


*Fig. 9. Sub-Technique to Main Technique Classification*

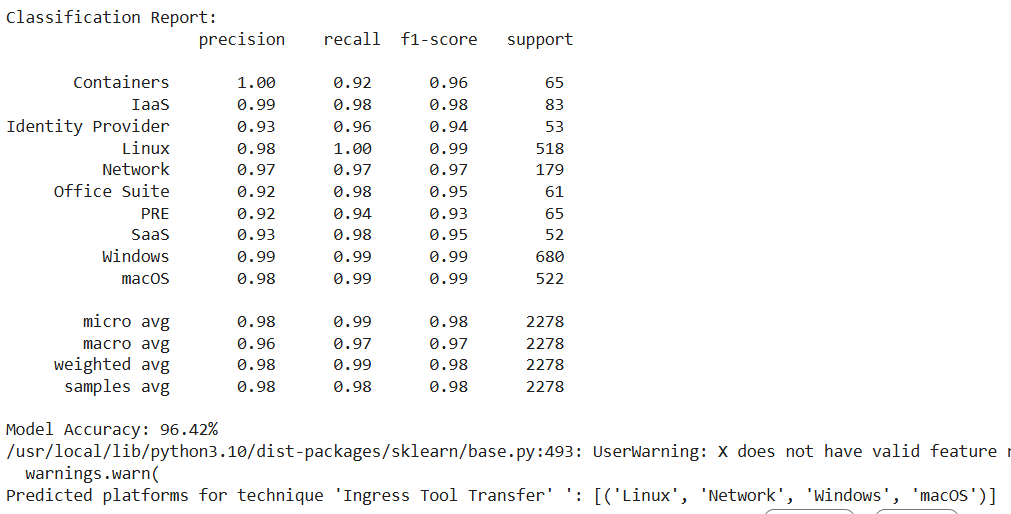
**

**

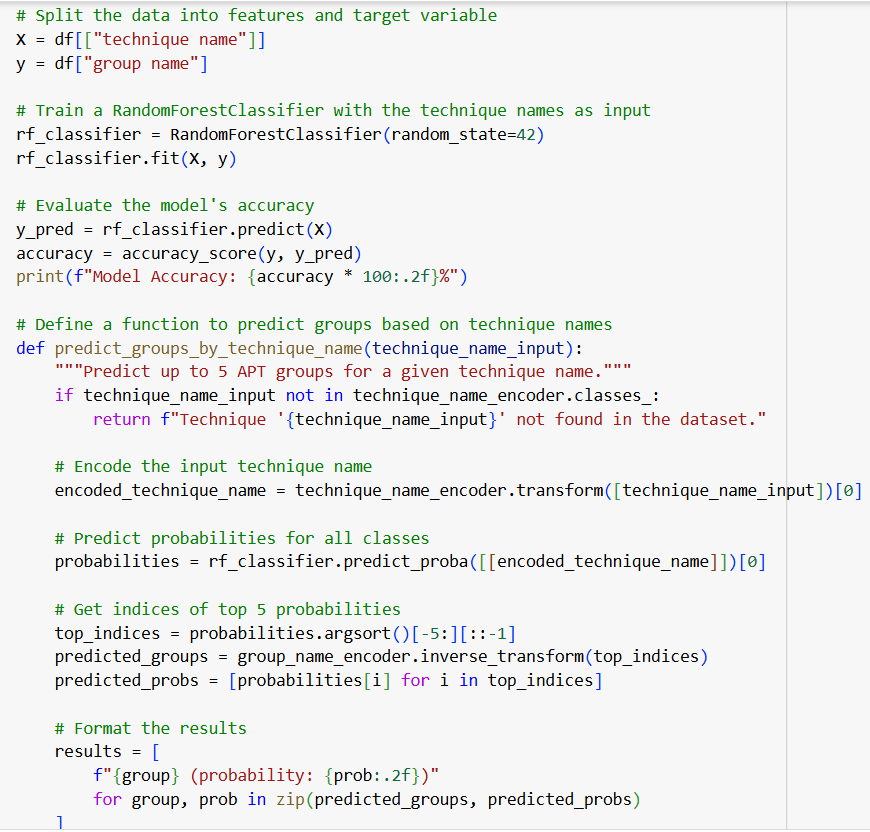
*Fig. 10. Prediction of “Sub-Technique to Main Technique Classification”*



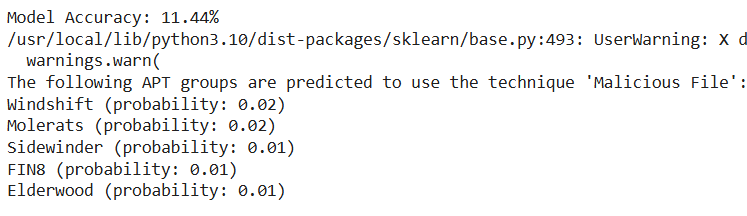
*Fig. 11. Platforms Exploited By Techniques*

**

*Fig. 12. Prediction of “Platforms Exploited By Techniques”*

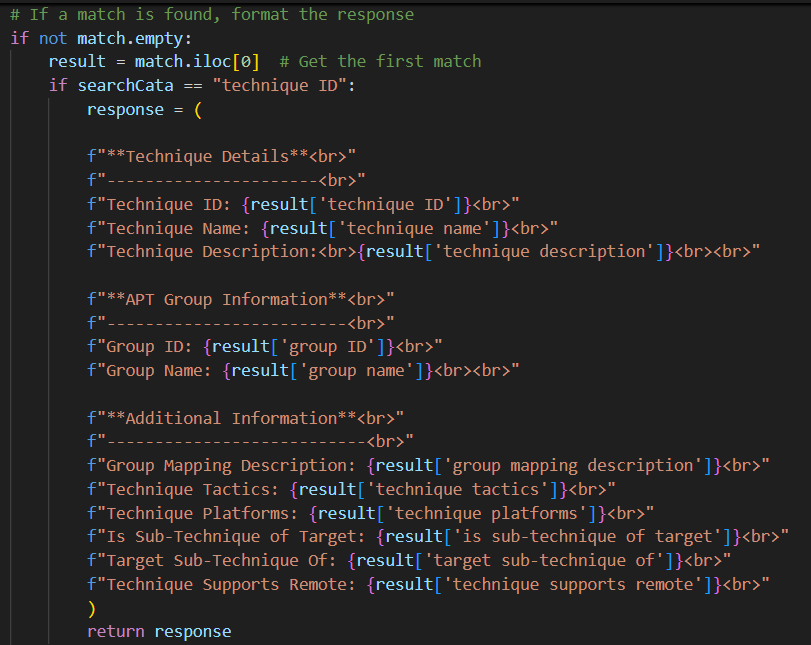


*Fig. 13. Which APT Group Use Which Tech*

**

*Fig. 14. Prediction of “Which APT Group Use Which Tech”*

## *Flask*



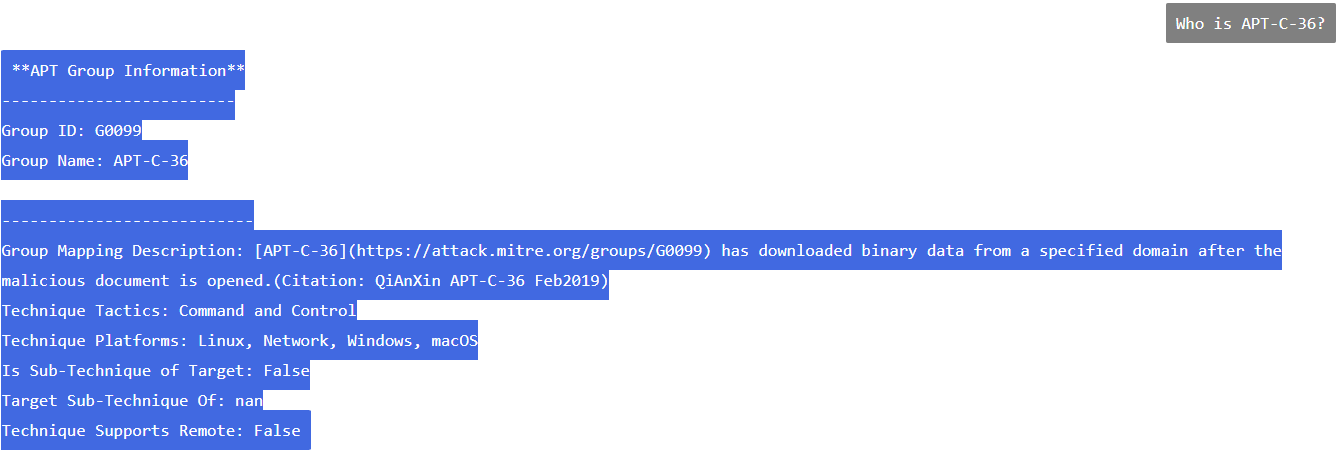
*Fig. 15. Search Algorithm in Chatbot*



*Fig. 16. Technique ID queries in Chatbot*



*Fig. 17. Technique name queries in Chatbot*



*Fig. 18. Group name queries in Chatbot*