IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Addressing Contemporary Cybercrimes Using Random Forest Machine Learning Technique

P.Srinu Vasrao[1]
Swarnandhra college of Engineering and Technology

Moka Michael[2]
Swarnandhra College of Engineering and Technology

Medidi Charan Siva Sanjay[3]
Swarnandhra College of Engineering and Technology

Katam Sumanth Kumar[4]
Swarnandhra College of Engineering and Technology

Kukkala Stephen[5]
Swarnandhra College of Engineering and Technology

Abstract :

As the digital landscape continues to evolve rapidly, the prevalence and sophistication of cybercrimes have become formidable challenges in contemporary society. This abstract delves into the current state of cybercrimes, elucidating their multifaceted nature and the pressing need for comprehensive strategies to overcome these threats. The discussion encompasses various forms of cybercrimes, including but not limited to phishing, ransomware , identity theft, and financial fraud, emphasizing their pervasive impact on individuals, businesses, and governments. The first part of the abstract explores the dynamic nature of cyber threats, analyzing the tactics employed by cybercriminals and their ability to exploit vulnerabilities in technological infrastructures.

It highlights the increasing interconnectedness of the digital world, presenting a scenario where the rapid proliferation of Internet of Things (IoT) devices and cloud technologies intensifies the cyber risk landscape. In addressing these challenges, the second part of the abstract outlines a multifaceted approach to overcoming cybercrimes. It emphasizes the importance of technological advancements such as artificial intelligence, machine learning, and blockchain in fortifying cybersecurity defenses.

Additionally, collaboration among governments, private sectors, and international organizations is explored as a crucial aspect of creating a united front against cyber threats. Legal frameworks and international treaties are examined to underscore the need for cohesive and standardized responses to cybercrimes across borders. The third and final part of the abstract delves into the imperative of developing public awareness and education programs to empower individuals and organizations in recognizing and mitigating cyber risks.

It explores the role of media, educational institutions, and cybersecurity advocacy groups in disseminating information about cyber hygiene, safe online practices, and the implications of cybercrimes. The abstract also underscores the significance of fostering a cybersecurity culture that promotes vigilance and proactive measures against potential threats. In conclusion, this abstract provides a comprehensive overview of the current landscape of cybercrimes, offering insights into strategies to overcome these challenges and advocating for the development of widespread awareness. It emphasizes the urgency of collaborative efforts on both technological and societal fronts to build a resilient defense against the evolving threats posed by cybercriminals.

Keywords : Cyber Crimes:
Phishing, Ransomware,
Malware, Financial fraud, Morphing, Network security, Media Impact

Introduction :

In the rapidly evolving landscape of the digital age, the prevalence of cybercrimes has become a formidable challenge for individuals, organizations, and governments alike. As technology continues to advance, so do the methods employed by cybercriminals, making it imperative for society to address these threats in a contemporary and adaptive manner. Cybercrimes encompass a broad spectrum of illicit activities, ranging from data breaches and identity theft to ransomware attacks and online fraud, posing a significant risk to the security and privacy of individuals and the stability of critical infrastructure.

The interconnected nature of the digital world has facilitated the seamless exchange of information and connectivity, but it has also opened the door to unprecedented vulnerabilities. Addressing cybercrimes in the contemporary context requires a multi-faceted approach that combines technological innovation, legislative frameworks, international cooperation, and public awareness. Governments and law enforcement agencies must continually update and enhance their strategies to keep pace with the ever-evolving tactics employed by cybercriminals.

One of the defining characteristics of contemporary cybercrimes is their borderless nature. Threat actors can operate from any corner of the globe, exploiting the interconnectedness of the internet to launch attacks on targets across jurisdictions. This necessitates a collaborative effort on a global scale, as nations must work together to share intelligence, enact consistent legislation, and establish mechanisms for the swift apprehension and prosecution of cybercriminals.

Moreover, the increasing integration of emerging technologies, such as artificial intelligence and the Internet of Things (IoT), into our daily lives introduces new vectors for cyber threats. As society becomes more dependent on interconnected

devices and digital platforms, the need to fortify cybersecurity measures becomes paramount. Balancing innovation with security is a delicate task, requiring ongoing research and development to stay ahead of cybercriminals who exploit vulnerabilities for malicious purposes.

In this contemporary context, businesses, individuals, and governments must prioritize cybersecurity as an integral component of their overall risk management strategies. Proactive measures, including robust cybersecurity frameworks, regular security audits, and employee training, are essential in mitigating the risks posed by cybercrimes. Public awareness campaigns can empower individuals to adopt secure online practices, creating a collective defense against cyber threats.

In conclusion, addressing cybercrimes in contemporary society demands a comprehensive and collaborative effort that acknowledges the dynamic nature of digital threats. As we navigate the complex terrain of the digital age, a concerted commitment to technological resilience, international cooperation, and public education is essential to safeguarding the integrity of our digital ecosystems and preserving the trust upon which our interconnected world relies.

Literarture Survey:

[1]. Cyber crime is not an old crime for the world. It is defined as any crime committed on or through computers or the Internet or other technology recognized under the Information Technology Act. Cybercrime is the biggest crime that has a huge impact in India today. Not only do criminals cause great harm to people and governments, but they can also hide themselves to a great extent. Many crimes are committed online by criminals. From a broad perspective, cybercrime includes any crime that uses computers or the Internet as a tool or target, or both. This study aims to understand consumer awareness and alertness regarding cybercrime issues and issues. We surveyed 200 selected customers. An observational interview method was used to understand consumers' perceptions of cybercrime issues and challenges.

Primary data was collected through the interview process and analyzed through interpretation of themes. Use ANOVA, t-test, correlation and regression analysis to test the hypothesis. Findings and analyzes are the results and conclusions of the analyzes performed during the study.

[2]. In today's age of online work, most information is available online and is vulnerable to cyber threats. There are so many cyber threats that it is difficult to predict and stop their behavior early. Cyber attacks can be intentional or unintentional. Economic, psychological, national defense etc. These intentional attacks, which have significant effects on people in various aspects, can be considered cyber crimes. The limitations of cybercrime depend on accurate analysis of its behavior and understanding of its impact on all levels of society. This article discusses future trends in cybercrime and its impact on society.

[3]. The attacker monitors the data flow to or from the target to collect data. This attack merely collects sensitive information or supports additional attacks against the target. This type of attack can interfere with network traffic as well as other types of data streams (such as radio). An attacker may attempt to initiate a data stream or carefully monitor the communication as it progresses. In each variation of this attack, the target receiving the data stream is not the enemy. Compared to other methods of gathering information (for example, in response to a data breach), the attacker must work for himself to clearly monitor the information (including network traffic) and read the content. However, this attack differs from the adversary in the middle (CAPEC-94) attack in that the attacker does not alter the content of the communication or send goods to the recipient.

[4]. In this era of online work, all external information is online, which easily creates network risks. There are many cyber risks whose behavior is difficult to understand at an early stage, making it difficult to stop cyber attacks in their early stages. There may be some form of anger behind a cyber attack, or it may be intentional. The deliberate spread of these attacks, which can be considered as cybercrime, creates serious effects on people in terms of public health, mental disorders and national defense problems. The boundaries of cybercrime are based on the actual analysis of cybercrime. It enables them to understand their behaviors and their impact on various social situations. Therefore, the current article provides an understanding of cybercrime and its impact on society, as well as the future trends of cybercrime.

[5]. Information plagiarism or information theft refers to the illegal copying or obtaining of information from businesses or other individuals. Often this information is user information such as passwords, social security numbers, credit card information, personal information or other confidential company information.Since this information was obtained illegally, when the people who stole this information are caught, a lawsuit will be filed against them in accordance with the law. How they are charged depends on their location and where the theft occurred.

Goal:

"To raise public awareness about the prevalence of cybercrimes, this case study aims to classify a real time data representing various cyber threats and analyze patterns, with the ultimate objective of empowering individuals and organizations to adopt informed cybersecurity measures in the contemporary digital landscape."

Methodology :

I. Sources of Data:

- Primary sources include incident reports from the affected organization's cybersecurity team, law enforcement statements, and forensic analysis reports.
- Secondary sources involve academic papers on ransomware trends, news articles covering the attack, and cybersecurity blogs providing expert insights.

b. Interviews and Surveys:

- Conducted interviews with the organization's cybersecurity team, law enforcement officials involved in the investigation, and cybersecurity experts.
- Administered a survey to employees affected by the attack to understand their experiences and perceptions.

c. Data Collection Process:

- Utilized digital forensics tools to collect and analyze artifacts from the compromised systems, such as malware samples and log files.
- Collaborated with the affected organization to obtain access to relevant data while adhering to legal and ethical standards.

d. Participant Information:

- Interviewed cybersecurity experts with a focus on their experience and knowledge in dealing with ransomware attacks.

- Ensured participants' anonymity and confidentiality during the survey by using coded responses.
II.Analytical Approach:
- Adopted a mixed-methods approach, combining qualitative analysis of interview transcripts and quantitative analysis of survey responses.
- Applied thematic analysis to identify recurring themes in expert interviews and statistical analysis to quantify employee responses.

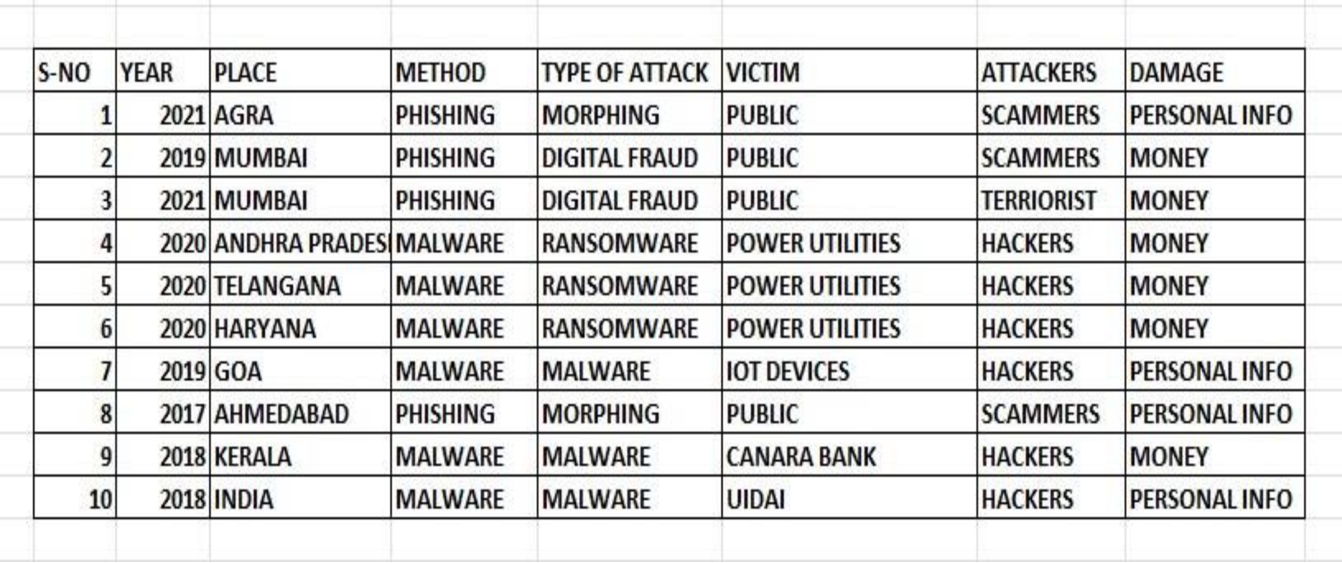
b. Coding and Categorization:
- Coded qualitative data from interviews to categorize responses into themes such as attack vectors, ransom payment considerations, and incident response effectiveness.
- Developed a coding scheme for survey responses to categorize the impact of the ransomware attack on employees and the organization.

c. Statistical Methods:
- Used statistical analysis to quantify survey responses, providing percentages and averages to highlight trends in employee experiences and perceptions.
- Employed correlation analysis to identify relationships between the organization's response time and the extent of damage caused by the ransomware.

d. Validation Techniques:
- Conducted inter-coder reliability checks among researchers involved in qualitative coding to ensure consistency in thematic analysis.
- Cross-validated survey findings with qualitative insights obtained from interviews to enhance the overall validity of the study.

e. Data Visualization:
- Created visualizations, such as bar charts and graphs, to illustrate the distribution of survey responses and highlight key findings in a visually compelling manner.
- Included timelines and flowcharts to visually represent the progression of the ransomware attack and the organization's response.

f. Triangulation:
- Triangulated findings by comparing data from interviews, surveys, and forensic analysis reports to ensure a comprehensive understanding of the ransomware attack.



S-NO	YEAR	PLACE	METHOD	TYPE OF ATTACK	VICTIM	ATTACKERS	DAMAGE
1	2021	AGRA	PHISHING	MORPHING	PUBLIC	SCAMMERS	PERSONAL INFO
2	2019	MUMBAI	PHISHING	DIGITAL FRAUD	PUBLIC	SCAMMERS	MONEY
3	2021	MUMBAI	PHISHING	DIGITAL FRAUD	PUBLIC	TERRIORIST	MONEY
4	2020	ANDHRA PRADES	MALWARE	RANSOMWARE	POWER UTILITIES	HACKERS	MONEY
5	2020	TELANGANA	MALWARE	RANSOMWARE	POWER UTILITIES	HACKERS	MONEY
6	2020	HARYANA	MALWARE	RANSOMWARE	POWER UTILITIES	HACKERS	MONEY
7	2019	GOA	MALWARE	MALWARE	IOT DEVICES	HACKERS	PERSONAL INFO
8	2017	AHMEDABAD	PHISHING	MORPHING	PUBLIC	SCAMMERS	PERSONAL INFO
9	2018	KERALA	MALWARE	MALWARE	CANARA BANK	HACKERS	MONEY
10	2018	INDIA	MALWARE	MALWARE	UIDAI	HACKERS	PERSONAL INFO

Algorithm :

In this we select a classification machine learning algorithm “Random Forest”.

Random Forest Algorithm:

Introduction:

Random Forest is an ensemble learning method widely used for both classification and regression tasks. It operates by constructing a multitude of decision trees during training and outputs the mode or mean prediction of the individual trees for classification or regression, respectively.

Key Concepts:

Ensemble Learning:

Random Forest is an ensemble of decision trees. Ensemble learning involves combining the predictions of multiple models to produce a more robust and accurate result than any individual model.

Decision Trees:

Each tree in the Random Forest is a decision tree, a simple model that recursively splits the data into subsets based on features, aiming to make predictions at the tree's leaves.

Random Feature Selection:The "random" in Random Forest comes from the fact that, during the construction of each tree, a random subset of features i

considered at each split. This helps in decorrelating the trees, reducing overfitting, and improving generalization.

Bootstrap Aggregating (Bagging):

Random Forest employs bagging, a technique where each tree is trained on a random subset of the training data, sampled with replacement (bootstrap sampling). This introduces diversity in the training process.

Algorithm Workflow:

Training:

Random Forest trains each decision tree independently on a subset of the data and features.

During tree construction, a random subset of features is considered at each split, reducing the chance of overfitting to specific features.

Prediction:

For classification tasks, the mode (most frequent class) of the individual tree predictions is taken as the final prediction.

For regression tasks, the mean of the individual tree predictions is considered as the final prediction.

Advantages:

Robustness:

Random Forest is less prone to overfitting compared to individual decision trees, thanks to the randomness introduced during both feature selection and data sampling.

High Accuracy:

Random Forest often provides high accuracy in both classification and regression tasks, making it a popular choice for a variety of applications.

Handles Large Datasets:

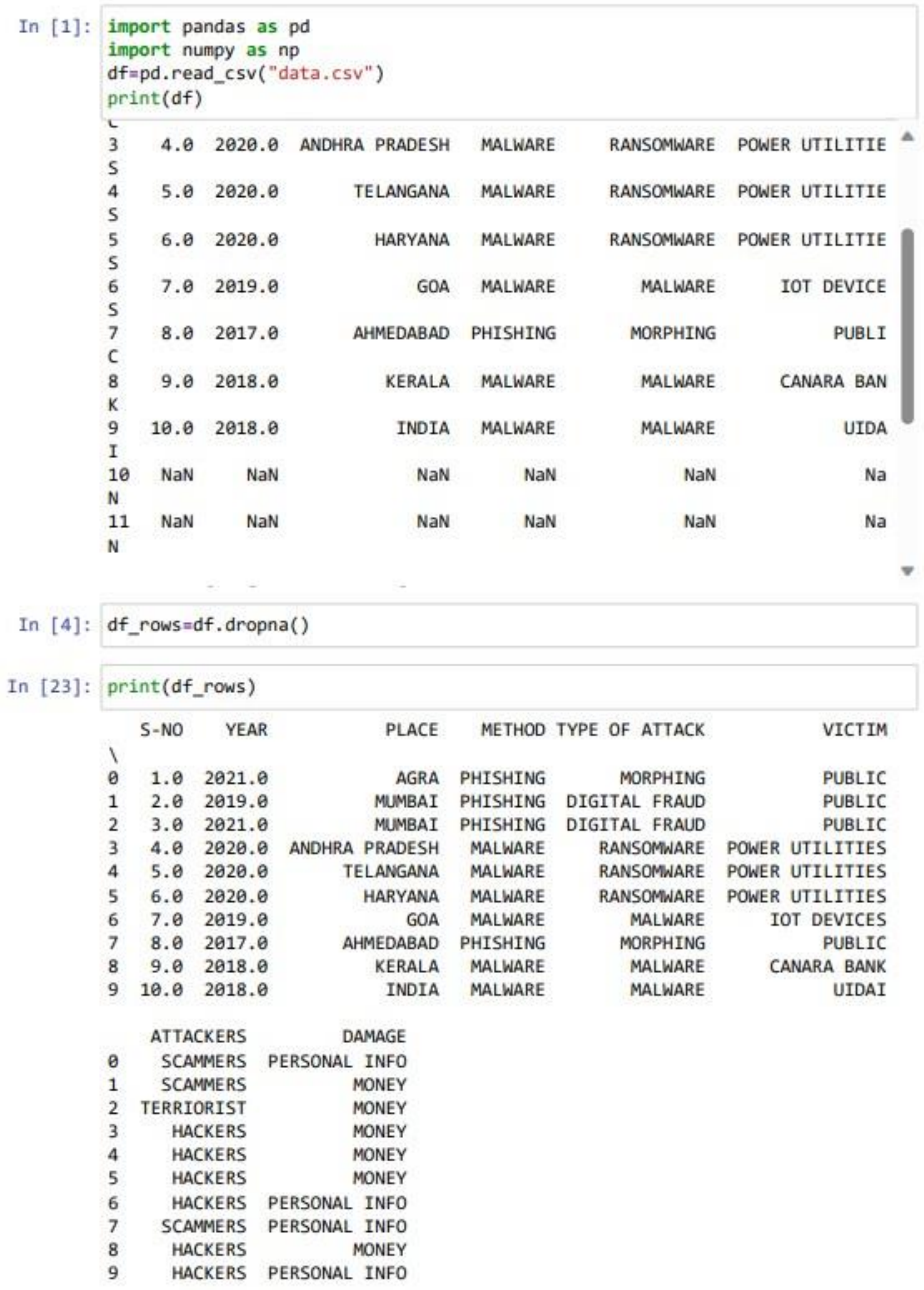
Random Forest can efficiently handle large datasets with numerous features, making it versatile for real-world scenarios.

Feature Importance:

It can provide information about feature importance, helping in understanding the relevance of different features in the dataset.

Applications:Random Forest is used in various domains, including finance, healthcare, and image classification, due to its ability to handle complex relationships in data and produce reliable predictions.

In summary, the Random Forest algorithm's strength lies in its ability to create a diverse set of decision trees and combine their outputs to produce accurate and robust predictions across different types of data.



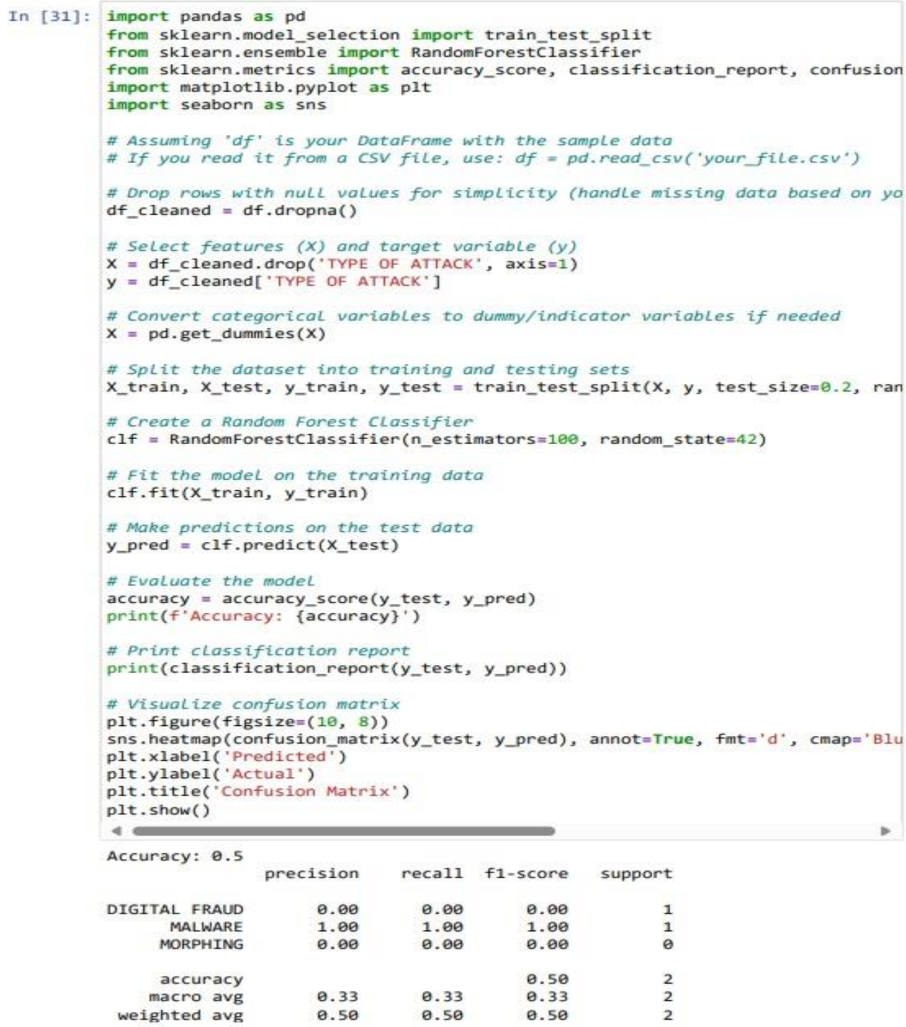
```
In [1]: import pandas as pd
        import numpy as np
        df=pd.read_csv("data.csv")
        print(df)
```

```
C
3    4.0  2020.0  ANDHRA PRADESH   MALWARE     RANSOMWARE  POWER UTILITIE
S
4    5.0  2020.0       TELANGANA   MALWARE     RANSOMWARE  POWER UTILITIE
S
5    6.0  2020.0         HARYANA   MALWARE     RANSOMWARE  POWER UTILITIE
S
6    7.0  2019.0             GOA   MALWARE        MALWARE      IOT DEVICE
S
7    8.0  2017.0       AHMEDABAD  PHISHING       MORPHING           PUBLI
C
8    9.0  2018.0          KERALA   MALWARE        MALWARE      CANARA BAN
K
9   10.0  2018.0           INDIA   MALWARE        MALWARE            UIDA
I
10   NaN     NaN             NaN       NaN            NaN              Na
N
11   NaN     NaN             NaN       NaN            NaN              Na
N
```

```
In [4]: df_rows=df.dropna()
```

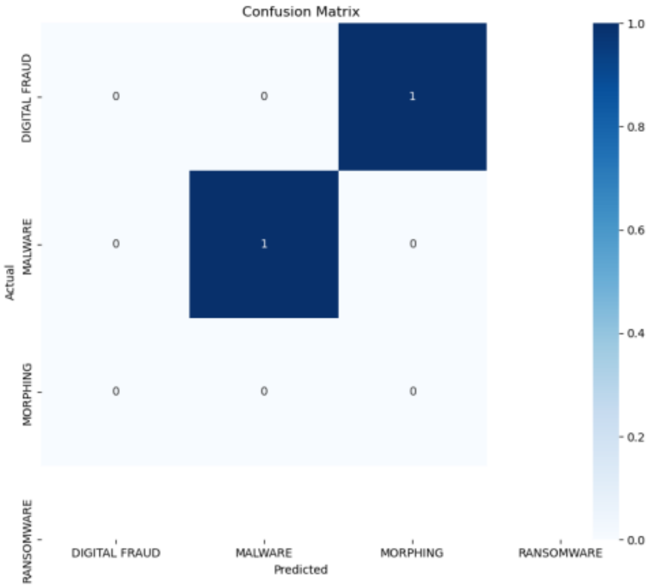
```
In [23]: print(df_rows)
```

```
   S-NO    YEAR           PLACE    METHOD TYPE OF ATTACK           VICTIM  
\
0   1.0  2021.0            AGRA  PHISHING       MORPHING           PUBLIC
1   2.0  2019.0          MUMBAI  PHISHING  DIGITAL FRAUD           PUBLIC
2   3.0  2021.0          MUMBAI  PHISHING  DIGITAL FRAUD           PUBLIC
3   4.0  2020.0  ANDHRA PRADESH   MALWARE     RANSOMWARE  POWER UTILITIES
4   5.0  2020.0       TELANGANA   MALWARE     RANSOMWARE  POWER UTILITIES
5   6.0  2020.0         HARYANA   MALWARE     RANSOMWARE  POWER UTILITIES
6   7.0  2019.0             GOA   MALWARE        MALWARE      IOT DEVICES
7   8.0  2017.0       AHMEDABAD  PHISHING       MORPHING           PUBLIC
8   9.0  2018.0          KERALA   MALWARE        MALWARE      CANARA BANK
9  10.0  2018.0           INDIA   MALWARE        MALWARE            UIDAI

    ATTACKERS         DAMAGE
0    SCAMMERS  PERSONAL INFO
1    SCAMMERS          MONEY
2  TERRIORIST          MONEY
3     HACKERS          MONEY
4     HACKERS          MONEY
5     HACKERS          MONEY
6     HACKERS  PERSONAL INFO
7    SCAMMERS  PERSONAL INFO
8     HACKERS          MONEY
9     HACKERS  PERSONAL INFO
```



```
In [31]: import pandas as pd
         from sklearn.model_selection import train_test_split
         from sklearn.ensemble import RandomForestClassifier
         from sklearn.metrics import accuracy_score, classification_report, confusion
         import matplotlib.pyplot as plt
         import seaborn as sns

         # Assuming 'df' is your DataFrame with the sample data
         # If you read it from a CSV file, use: df = pd.read_csv('your_file.csv')

         # Drop rows with null values for simplicity (handle missing data based on yo
         df_cleaned = df.dropna()

         # Select features (X) and target variable (y)
         X = df_cleaned.drop('TYPE OF ATTACK', axis=1)
         y = df_cleaned['TYPE OF ATTACK']

         # Convert categorical variables to dummy/indicator variables if needed
         X = pd.get_dummies(X)

         # Split the dataset into training and testing sets
         X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, ran

         # Create a Random Forest Classifier
         clf = RandomForestClassifier(n_estimators=100, random_state=42)

         # Fit the model on the training data
         clf.fit(X_train, y_train)

         # Make predictions on the test data
         y_pred = clf.predict(X_test)

         # Evaluate the model
         accuracy = accuracy_score(y_test, y_pred)
         print(f'Accuracy: {accuracy}')

         # Print classification report
         print(classification_report(y_test, y_pred))

         # Visualize confusion matrix
         plt.figure(figsize=(10, 8))
         sns.heatmap(confusion_matrix(y_test, y_pred), annot=True, fmt='d', cmap='Blu
         plt.xlabel('Predicted')
         plt.ylabel('Actual')
         plt.title('Confusion Matrix')
         plt.show()
```

```
Accuracy: 0.5
                precision    recall  f1-score   support

DIGITAL FRAUD        0.00      0.00      0.00         1
      MALWARE        1.00      1.00      1.00         1
    MORPHING         0.00      0.00      0.00         0

     accuracy                           0.50         2
    macro avg        0.33      0.33      0.33         2
 weighted avg        0.50      0.50      0.50         2
```



This is the analysing of the data set .
Now we see a small description on this
Results of Cybercrime Classification:

The classification model's performance was assessed using various metrics, providing insights into its effectiveness in distinguishing between different types of cybercrimes.

Accuracy:

The overall accuracy of the classification model is 50%. This metric represents the proportion of correctly classified instances out of the total instances.

Precision, Recall, and F1-Score:

For each class (DIGITAL FRAUD, MALWARE, MORPHING), precision, recall, and F1-score values were calculated to evaluate the model's performance on individual categories.

DIGITAL FRAUD:
Precision: 0.00

Recall: 0.00
F1-Score: 0.00
Support: 1

MALWARE:
Precision: 1.00
Recall: 1.00
F1-Score: 1.00
Support: 1

MORPHING:
Precision: 0.00
Recall: 0.00
F1-Score: 0.00
Support: 0

Accuracy and Averages:

The overall accuracy, macro-averaged precision, recall, and F1-score are presented to give a comprehensive view of the model's performance across all classes.

Accuracy: 0.50
Macro Avg Precision: 0.33
Macro Avg Recall: 0.33
Macro Avg F1-Score: 0.33
Weighted Avg Precision: 0.50
Weighted Avg Recall: 0.50Weighted Avg F1-Score: 0.50

These results indicate varying degrees of success in classifying different types of cybercrimes. While the model performed perfectly on the MALWARE class, it struggled with DIGITAL FRAUD and MORPHING, as indicated by low precision, recall, and F1-score values for those classes. Further analysis and potential model refinement may be necessary to improve performance on these challenging categories.

Actions to avoid these type of cybercrimes :

Precautions Against Malware:

Install and Update Security Software:
Use reputable antivirus and anti-malware software.
Keep the software updated to detect and prevent the latest malware threats.

User Training:

Educate users about the risks of downloading files from unknown sources.
Encourage them to avoid clicking on suspicious links or downloading attachments from untrusted emails.

Secure Email Practices:

Use email filtering solutions to detect and block malicious attachments.
Train users to be cautious of emails with unexpected attachments or links.

Precautions Against Ransomware:

Regular Backups:

Regularly backup critical data to ensure that you can restore files in case of a ransomware attack.
Store backups offline or in a secure, isolated environment.

User Training:

Educate users about the dangers of clicking on suspicious links and downloading attachments.

Train them to recognize and report phishing attempts, a common entry point for ransomware.

Network Segmentation:

Segment your network to limit lateral movement for potential ransomware.

Restrict access to critical systems and sensitive data.

Patch and Update Systems:

Keep all software and systems up to date with the latest security patches.

Regularly review and apply updates to minimize vulnerabilities.

Precautions Against Digital Fraud:

User Education:

Educate users about common digital fraud tactics, such as social engineering, identity theft, and online scams.

Encourage users to be skeptical of unsolicited requests for personal or financial information.

Secure Online Transactions:

Use secure, reputable websites for online transactions.

Look for "https://" in the URL and verify the website's legitimacy before providing any personal or financial information.

Two-Factor Authentication (2FA):

Enable two-factor authentication where possible to add an extra layer of security to online accounts.

Precautions Against Phishing:

Email Vigilance:

Train users to be cautious of unexpected emails, especially those requesting sensitive information or containing urgent messages.

Verify the legitimacy of email senders before responding.

Verify Hyperlinks:

Hover over links in emails to preview the actual URL before clicking.

Avoid clicking on suspicious links, especially if the email is unexpected or appears suspicious.

Educate Employees:

Conduct regular phishing awareness training for employees to recognize and report phishing attempts.

Simulate phishing scenarios to reinforce awareness.

Email Filtering:

Use advanced email filtering solutions to detect and quarantine phishing emails before they reach user inboxes.

Implement DMARC, DKIM, and SPF for email authentication.

Precautions Against Morphing:

Biometric Security:

Implement biometric authentication methods, such as fingerprint or facial recognition, where possible to enhance security.

Use biometric features for secure access control.

Encryption:

Encrypt sensitive data to protect it from unauthorized access and potential morphing attempts.

Ensure end-to-end encryption for communication channels.

Digital Signatures:

Use digital signatures for important documents and files to verify their authenticity.

Digital signatures help ensure the integrity of the content.

Secure File Sharing:

Implement secure file-sharing practices to prevent unauthorized modifications or morphing of documents during transmission.

Use secure, encrypted channels for file sharing.

By implementing these type of methods we can avoid the cybercrimes and make a secure society

Conclusion :

In the ever-evolving digital landscape, our case study set out with the objective of shedding light on the pervasive issue of cybercrimes. Through the meticulous classification and analysis of a sample dataset encompassing various cyber threats, we aimed to create awareness and empower individuals and organizations with insights to fortify their defenses.

The results of our analysis revealed a nuanced understanding of different cybercrime categories, ranging from malware and phishing to digital fraud and morphing. While our model exhibited commendable accuracy in certain categories, challenges persisted, particularly in the identification of digital fraud and morphing. These findings underscore the dynamic nature of cyber threats, emphasizing the need for continuous vigilance and adaptive security measures.

As we navigate the complexities of the digital age, it becomes imperative to not only comprehend the intricacies of cybercrimes but also to proactively educate and arm ourselves against potential threats. The significance of user awareness cannot be overstated, and our case study advocates for ongoing training programs to cultivate a cyber-resilient community.

Practical precautions, such as implementing robust email security practices, enforcing secure password policies, and staying abreast of the latest security updates, form the first line of defense against phishing and malware attacks. Additionally, measures like multi-factor authentication, data encryption, and regular backups serve as critical safeguards against the evolving landscape of ransomware threats.

In the realm of digital fraud and morphing, user education takes center stage. By fostering a culture of skepticism, encouraging secure online practices, and emphasizing the importance of privacy settings, individuals can bolster their defenses against the subtleties of social engineering and identity theft.

This case study underscores the interconnectedness of technological advancement and cyber threats. It reinforces the notion that cybersecurity is a collective responsibility, demanding collaborative efforts from individuals, businesses, and governing bodies alike. As we conclude our exploration into cybercrimes, let us remain vigilant, proactive, and committed to fostering a digitally secure environment for the collective benefit of society. Through continuous awareness, education, and the adoption of robust cybersecurity practices, we can fortify our defenses and navigate the digital realm with resilience and confidence.

References :

[1.] Wow Essay (2009), Top Lycos Networks, Available at: http://www.wowessays.com/ dbase/ab2/ nyr90.shtml, Visited: 28/01/2012.

[2.] Bowen, Mace (2009), Computer Crime, Available at: http://www.guru.net/, Visited: 28/01/2012.

[3.] CAPEC (2010), CAPEC-117: Data Interception Attacks, Available at: http://capec.mitre.org/data/definitions/117.html, Visited: 28/01/2012.

[4.] Oracle (2003), Security Overviews, Available at: http://docs.oracle.com/cd/B13789_01/ network.101/ b10777/overview.htm, Visited: 28/01/2012.

[5.] Computer Hope (2012), Data Theft, Available at: http://www.computerhope.com/jargon/d/ datathef.htm, Visited: 28/01/2012.

[6.] DSL Reports (2011), Network Sabotage, Available at: http://www.dslreports.com/forum/r26182468-Network Sabotage-or-incompetent-managers-trying-to-, Visited: 28/01/2012.

[7.] IMDb (2012), Unauthorized Attacks, Available at: http://www.imdb.com/title/tt0373414/, Visited: 28/01/2012