SLIIT UNI
THE KNOWLEDGE UNIVERSITY

IT4010 – Research Project - 2023

Topic Assessment Form

Project ID : TMP-23-123

1. Topic (12 words max)

Detecting email-based phishing websites using machine learning

2. Research group the project belongs to

Machine Learning and Soft Computing (MLSC)

3. Research area the project belongs to

Machine Learning (ML)

4. If a continuation of a previous project:

Project ID	
Year	

5. Team member details

Student Name	Student ID	Specialization
Leader: J.M.Lindamulage	IT20222840	CS
Member 2: Mandira Pabasari L.	IT19966236	CS
Member 3: Yapa S.P.J.	IT20050108	CS
Member 4: Perera I.S.S.	IT20222468	CS

6. Brief description of the research problem including references (200 – 500 words max) – references not included in word count

Phishing has become one of the most common cyberattacks today. Attackers launch phishing attacks now in a variety of ways, like spoof calls, messages, social networking, and emails, with the intention of obtaining sensitive information from victims [1]. The most common way victims fall for phishing is by clicking on a fraudulent link in an email that was sent by an attacker. This is called email phishing [2]. This link will take victims to websites that appear legitimate but are actually run by the attackers. Attackers construct illegal email accounts using real company details and send the email to victims, impersonating a real person, while making the victim click on the link to the fraud website using social engineering [3]. If a person clicks on the link and visits the site and tries to login or perform any action, then the attackers can get passwords, login credentials, credit card information, and other sensitive information [2]. With the COVID-19 outbreak, phishing activities have also increased [4]. Even though there are many tools and research studies available, phishing is so widespread that no single solution can reduce all the vulnerabilities. Many people fall victim to this, even though these tools are available, due to a lack of knowledge and the inability to purchase such tools.

References

[1] Dr. Moulana Mohammed,K. Koteswara Prasanth, S. Venkata Sai Subhash, "PHISHING DETECTION USING MACHINE LEARNING ALGORITHMS," in *IEEE*, India, 2022.

[2] "An overview of machine learnng algorithms fo detecting phshing atacks on elecronic messaging services.," in *MIPRO*, Croatia, 2022.

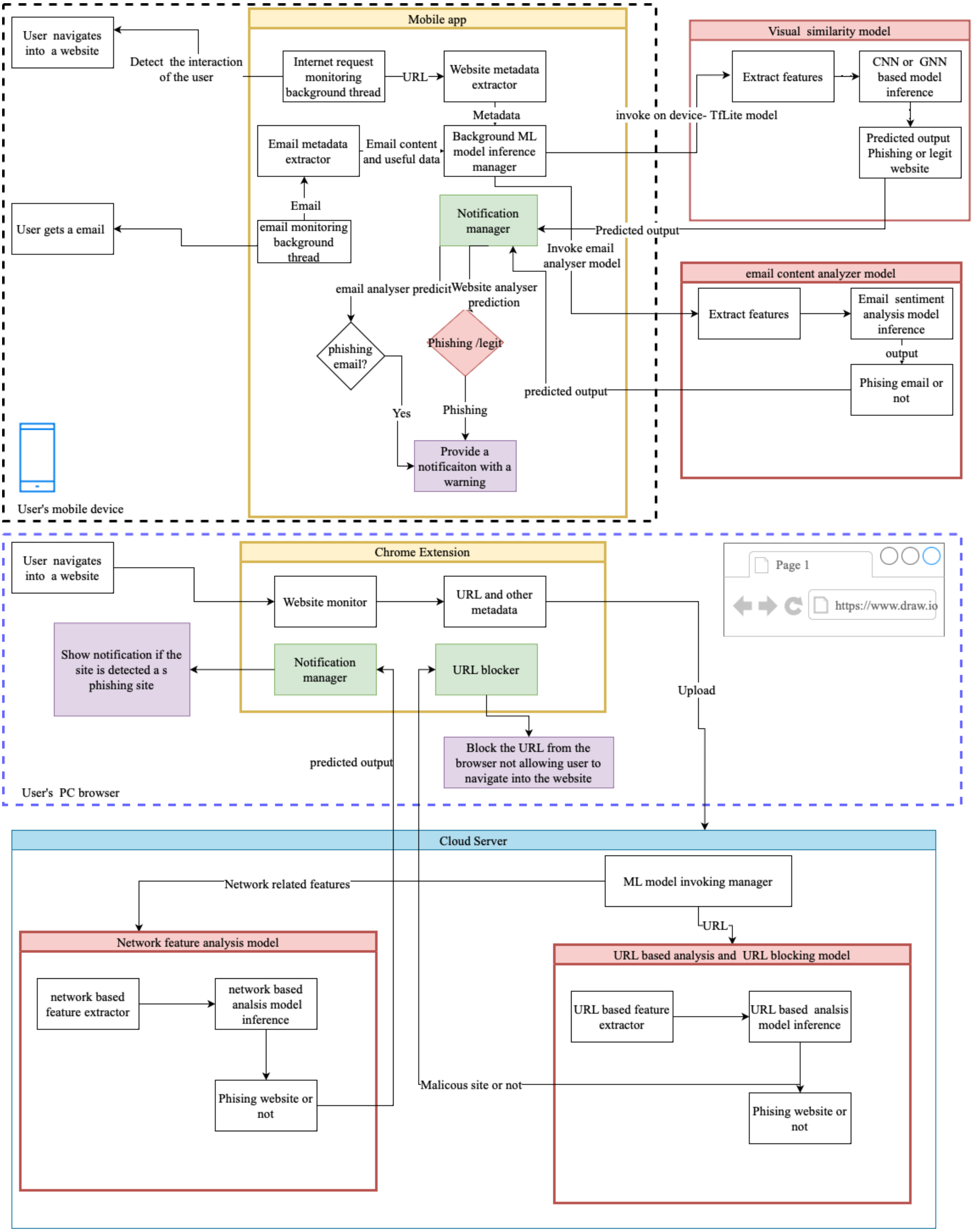
[3] "Phishing Detection using Random Forest, SVM and Neural Network with Backpropagation," in *IEEE*, India, 2020.

[4] SAID SALLOUM 1, TAREK GABER 1,2, SUNIL VADERA 1, AND KHALED SHAALAN 3, "A Systematic Literature Review on Phishing Email Detection Using Natural Language," *IEEE,* vol. 10, pp. 65704-65727, June 14, 2022,.

7. Brief description of the nature of the solution including a conceptual diagram (250 words max)

The solution is to develop a tool that can detect phishing sites and phishing emails. There are a few approaches that are going to be used to identify a phishing site. A content-based approach is based on website content, and it is used to identify the website. In the non-content approach to URLs, host information is used to identify the website. In a visual-based approach, visual elements are used to identify the website. Text analysis can be used in emails that are sent by attackers with urgent requests but contain grammar and spelling errors. Email headers can be analyzed to check if the sender's address is genuine. At last, the network behavior, which can be described as traffic patterns and connections, can be used to determine if the IP address from which the connection was made is phishing or not. Using all the above methods, the final tool will be able to detect phishing websites based on email content, website URL, visual similarity features, and network behavior. The final product will be a mobile application and a web extension that are capable of detecting a phishing site based on email content, website URL, visual similarity features, and network behavior.

(System diagram is in the next page)


Mobile app
User navigates into a website
Detect the interaction of the user
Internet request monitoring background thread
URL
Website metadata extractor
Metadata
Email metadata extractor
Email content and useful data
Background ML model inference manager
invoke on device- TfLite model
Visual similarity model
Extract features
CNN or GNN based model inference
Predicted output Phishing or legit website
Email
User gets a email
email monitoring background thread
Notification manager
Predicted output
Invoke email analyser model
email analyser predicit
Website analyser prediction
phishing email?
Phishing /legit
Yes
Phishing
Provide a notificaiton with a warning
predicted output
email content analyzer model
Extract features
Email sentiment analysis model inference
output
Phising email or not
User's mobile device
Chrome Extension
User navigates into a website
Website monitor
URL and other metadata
Page 1
https://www.draw.io
Show notification if the site is detected a s phishing site
Notification manager
URL blocker
Upload
Block the URL from the browser not allowing user to navigate into the website
predicted output
User's PC browser
Cloud Server
Network related features
ML model invoking manager
URL
Network feature analysis model
network based feature extractor
network based analsis model inference
Phising website or not
Malicous site or not
URL based analysis and URL blocking model
URL based feature extractor
URL based analsis model inference
Phising website or not

8. Brief description of specialized domain expertise, knowledge, and data requirements (300 words max)

Knowledge about how an email-based phishing attack is performed and how attackers gain information is required. After understanding the basic concept of phishing emails, knowledge about image processing and machine learning expertise are required. Furthermore, web scraping, HTML and CSS coding, and Python knowledge are required. Mobile app development using Android or Flutter is required to create the mobile app. Knowledge of how to develop a web extension is required. The data sets for training the model are also required. The data sets from PhishTank, AlexaTop, MillerSmiles, and other datasets from Kaggle need to be downloaded and preprocessed.

9. Objectives and Novelty

Main Objective

To develop a mobile app that runs in the background and a web browser extension that is capable of classifying phishing websites from legitimate websites powered by machine learning and deep learning models to provide the user with warnings regarding any potential risk of being navigated into a phishing website while preserving the privacy of the user, and if the user gets a phishing email, warn the user before the user clicks on any links or is misled by false information.

Member Name	Sub Objective	Tasks	Novelty
J.M.Lindamulage	To develop a phishing website detection model using Convolution Neural Networks (CNN) or Graph Neural Networks (GNN)-based approach using visual similarity features between legit and phishing websites. To optimize inference time and model size of the developed deep learning model using optimization techniques such as model pruning and weight clustering for edge computing, and integrate the optimized model	Observe how features such as text content, background colors, images, etc. can be used as useful features to differentiate phishing sites and identify datasets that contain those features, such as PhishTank. If datasets are not sufficient, collect data by web scraping from domain names included in datasets such as the AlexaTop dataset. Conduct experiments with different CNN architectures, such as EfficientNet and MobileNet, and observe the relationships between features to be able to model this problem as a Graph Neural Network. Develop the models,	A novel deep learning-based solution to classify phishing websites based on the visual similarity features of the website using CNN or GNN. Optimize the developed deep learning model for mobile apps so that the model can be deployed in a constrained environment. Native Android mobile app that runs in the background, monitoring for any potential phishing website capable of running in the

	into an Android mobile application.	compare their performances, and select the best-performing model amongst them. Try to optimize the size and latency caused by the selected model by applying model optimization techniques such as model pruning and weight clustering and integrating the model into the mobile application.	device itself, thus protecting the user's privacy.
Mandira Pabasari L.	To develop a tool to identify phishing websites using network traffic features	Collecting the network traffic features associated with a website, such as the source IP address, destination IP address, protocol used, and other relevant information. Pre-processing the collected data to prepare it for analysis. This may involve cleaning the data, removing any missing or irrelevant information, and transforming the data into a suitable format for the machine learning algorithms.	Achieve real-time analysis and decision making. This model could be designed to perform analysis and make decisions in real-time, which would allow it to provide users with more timely protection against malicious websites.

		Applying machine learning algorithms, such as Logistic Regression (LR), Support Vector Machine (SVM), k-Nearest Neighbor (KNN), or Principal Component Analysis (PCA), to the pre-processed data. Using the trained machine learning model to classify the website as malicious or benign based on the network traffic features. The output of this step would be a decision, indicating whether the website is malicious or not. This decision would be used to provide real-time protection to the user against malicious websites.	
Yapa S.P.J.	To develop a tool to identify a phishing mail based on the content and the header of the mail using Machine learning. To develop deep learning model which can analyze sentiments of the email content to indemnify potential phishing emails.	Explore literature to find out what are the features and patterns which can be considered to classify the sentiment of the sentences. Explore what type of machine learning and deep learning techniques which has been used to recognize sentiments which indicates the email is a phishing email.	Combine natural language processing models with sentiment analysis to develop an ML model that can analyze the sentiments of an email and classify if the email is a phishing email or not.

		Conduct experiments with different features with recognized deep learning models which can classify sentiments. Datasets that use for this are collected from PhishTank and MillerSmiles. Select the best models and develop pipeline to extract text from emails which user reads an email and analyze the content. Develop browser plugin and integrate the developed AI pipeline.	Develop browser plugins that can run in the background, analyze the content of emails, and provide warnings to the user about any potential phishing emails.
Perera I.S.S.	To develop a tool to identify phishing websites using URL and text content using machine learning.	Implement a Python program to extract features from the URL.(feature extraction). using a data set from the Kaggle web site (a phishing dataset for machine learning). Study about address bar features, HTML and Java Script features, and domain features.	Check the phishing , malicious URLs using machine learning techniques and block the URLs using local host file.

		Study classical machine learning techniques like Random Forest, K nearest neighbors, Decision Tree, Linear SVC classifier, One class SVM classifier and wrapper-based features selection, which contains the metadata of URLs, and use the information to determine if a website is legitimate or not.	

10. Supervisor checklist (supervisors should fill sections 10 and 11)

a) Is this research problem valid?

Yes	✓	No	

b) Is the proposed research group correct?

Yes	✓	No	

c) Is the proposed research area correct?

Yes	✓	No	

d) Do the proposed sub-objectives match the students' specialization?

Yes	✓	No	

e) Is the required domain expertise, knowledge, and the data available either through the supervisor or external supervisor?

Yes	✓	No	

f) Is the scope of the solution practical?

Yes	✓	No	

g) Do all sub-objectives have sufficient novelty?

Yes	✓	No	

11. Supervisor details

	Title	First Name	Last Name	Signature
Supervisor	Ms.	Jenny	Krishara	Jenny 09/02/2023
Co-Supervisor	Ms.	Madhuka Nadeeshani	Koralalage	09/02/2023
External Supervisor				
Summary of external supervisor's (if any) experience and expertise				

Summary Sheet

The topic evaluation panel will use the summary sheet to evaluate the suitability of the project

1. Brief description of research problem including references (200 – 300 words max)

Phishing has become one of the most common cyberattacks today. Attackers launch phishing attacks now in a variety of ways, like spoof calls, messages, social networking, and emails, with the intention of obtaining sensitive information from victims [1]. The most common way victims fall for phishing is by clicking on a fraudulent link in an email that was sent by an attacker. This is called email phishing [2]. This link will take victims to websites that appear legitimate but are actually run by the attackers. Attackers construct illegal email accounts using real company details and send the email to victims, impersonating a real person, while making the victim click on the link to the fraud website using social engineering [3]. If a person clicks on the link and visits the site and tries to login or perform any action, then the attackers can get passwords, login credentials, credit card information, and other sensitive information [2]. With the COVID-19 outbreak, phishing activities have also increased [4]. Even though there are many tools and research studies available, phishing is so widespread that no single solution can reduce all the vulnerabilities. Many people fall victim to this, even though these tools are available, due to a lack of knowledge and the inability to purchase such tools.

References

[1] Dr. Moulana Mohammed,K. Koteswara Prasanth, S. Venkata Sai Subhash, "PHISHING DETECTION USING MACHINE LEARNING ALGORITHMS," in *IEEE*, India, 2022.

[2] "An overview of machine learnng algorithms fo detecting phshing atacks on elecronic messaging services.," in *MIPRO*, Croatia, 2022.

[3] "Phishing Detection using Random Forest, SVM and Neural Network with Backpropagation," in *IEEE*, India, 2020.

[4] SAID SALLOUM 1, TAREK GABER 1,2, SUNIL VADERA 1, AND KHALED SHAALAN 3, "A Systematic Literature Review on Phishing Email Detection Using Natural Language," *IEEE,* vol. 10, pp. 65704-65727, June 14, 2022,.

2. Brief description of the nature of the solution (150 words max)

The solution is to develop a tool that can detect phishing sites and phishing emails. There are a few approaches that are going to be used to identify a phishing site. A content-based approach is based on website content, and it is used to identify the website. In the non-content approach to URLs, host information is used to identify the website. In a visual-based approach, visual elements are used to identify the website. Text analysis can be used in emails that are sent by attackers with urgent requests but contain grammar and spelling errors. Email headers can be analyzed to check if the sender's address is genuine. At last, the network behavior, which can be described as traffic patterns and connections, can be used to determine if the IP address from which the connection was made is phishing or not. Using all the above methods, the final tool will be able to detect phishing websites based on email content, website URL, visual similarity features, and network behavior. The final product will be a mobile application and a web extension that are capable of detecting a phishing site based on email content, website URL, visual similarity features, and network behavior.

3. Objectives and novelty

Main Objective To develop a mobile app that runs in the background and a web browser extension that is capable of classifying phishing websites from legitimate websites powered by machine learning and deep learning models to provide the user with warnings regarding any potential risk of being navigated into a phishing website while preserving the privacy of the user, and if the user gets a phishing email, warn the user before the user clicks on any links or is misled by false information.			
Member Name	Sub Objective	Tasks	Novelty
J.M.Lindamulage	To develop a phishing website detection model using Convolution Neural Networks (CNN) or Graph Neural Networks (GNN)-based approach using visual similarity features between legit and phishing websites. To optimize inference time and model size of the developed deep learning model using model optimization techniques such as model pruning and weight clustering for edge computing, and integrate the optimized model into an Android mobile application.	Observe how features such as text content, background colors, images, etc. can be used as useful features to differentiate phishing sites and identify datasets that contain those features, such as PhishTank. If datasets are not sufficient, collect data by web scraping from domain names included in datasets such as the AlexaTop dataset. Conduct experiments with different CNN architectures, such as EfficientNet and MobileNet, and observe the relationships between features to be able to model this problem as a Graph Neural Network. Develop the models, compare their	A novel deep learning-based solution to classify phishing websites based on the visual similarity features of the website using CNN or GNN. Optimize the developed deep learning model for mobile apps so that the model can be deployed in a constrained environment. Native Android mobile app that runs in the background, monitoring for any potential phishing website capable of running in the device itself, thus protecting the user's privacy.

		performances, and select the best-performing model amongst them. Try to optimize the size and latency caused by the selected model by applying model optimization techniques such as model pruning and weight clustering and integrating the model into the mobile application.	
Mandira Pabasari L.	To develop a tool to identify phishing websites using network traffic features	Collecting the network traffic features associated with a website, such as the source IP address, destination IP address, protocol used, and other relevant information. Pre-processing the collected data to prepare it for analysis. This may involve cleaning the data, removing any missing or irrelevant information, and transforming the data into a suitable format for the machine learning algorithms.	Achieve real-time analysis and decision making. This model could be designed to perform analysis and make decisions in real-time, which would allow it to provide users with more timely protection against malicious websites.

		Applying machine learning algorithms, such as Logistic Regression (LR), Support Vector Machine (SVM), k-Nearest Neighbor (KNN), or Principal Component Analysis (PCA), to the pre-processed data. Using the trained machine learning model to classify the website as malicious or benign based on the network traffic features. The output of this step would be a decision, indicating whether the website is malicious or not. This decision would be used to provide real-time protection to the user against malicious websites.	
Yapa S.P.J.	To develop a tool to identify a phishing mail based on the content and the header of the mail using Machine learning. To develop deep learning model which can analyze sentiments of the email content to indemnify potential phishing emails.	Explore literature to find out what are the features and patterns which can be considered to classify the sentiment of the sentences. Explore what type of machine learning and deep learning techniques which has been used to recognize sentiments which indicates the email is a phishing email.	Combine natural language processing models with sentiment analysis to develop an ML model that can analyze the sentiments of an email and classify if the email is a phishing email or not. Develop browser plugins that can run in the background, analyze the content of emails, and provide

		Conduct experiments with different features with recognized deep learning models which can classify sentiments. Datasets that use for this are collected from PhishTank and MillerSmiles. Select the best models and develop pipeline to extract text from emails which user reads an email and analyze the content. Develop browser plugin and integrate the developed AI pipeline.	warnings to the user about any potential phishing emails.
Perera I.S.S.	To develop a tool to identify phishing websites using URL and text content using machine learning.	Implement a Python program to extract features from the URL. (feature extraction). using a data set from the Kaggle web site (a phishing dataset for machine learning). Study about address bar features, HTML and Java Script features, and domain features.	Check the phishing, malicious URLs using machine learning techniques and block the URLs using local host file.

		Study classical machine learning techniques like Random Forest, K nearest neighbors, Decision Tree, Linear SVC classifier, One class SVM classifier and wrapper-based features selection, which contains the metadata of URLs, and use the information to determine if a website is legitimate or not.	

IT4010 – Research Project - 2023

Topic Assessment Form

<u>This part to be filled by the Topic Screening Panel members</u>

Acceptable: Mark/Select as necessary

Topic Assessment Accepted	
Topic Assessment Accepted with minor changes (should be followed up by the supervisor)*	
Topic Assessment to be Resubmitted with major changes*	
Topic Assessment Rejected. Topic must be changed	

* Detailed comments given below

Comments

The Review Panel Details

Member's Name	**Signature**

Important:

1. According to the comments given by the panel, do the necessary modifications and get the approval by the **Supervisor** or the **Same Panel**.
2. If the project topic is rejected, identify a new topic, and request the RP Team for a new topic assessment.
3. The form approved by the panel must be attached to the **Project Charter Form**.