

**YUKTI - National Innovation Repository**

|  |  |
| --- | --- |
| **Idea / Proof of Concept (PoC)** | Yes/No |
| **Innova**ti**on / Prototype** | Yes/No |

**\*Title (20 Words Max): CyberSafe:An Intelligent FrameWork For Automated Phishing Detection Using Machine Learning**

**\*Developed as part of**

|  |  |
| --- | --- |
|  | Yes |
| No |
| No |

**\*Choose the Financial Year, during the Idea-PoC/Innovation Developed**

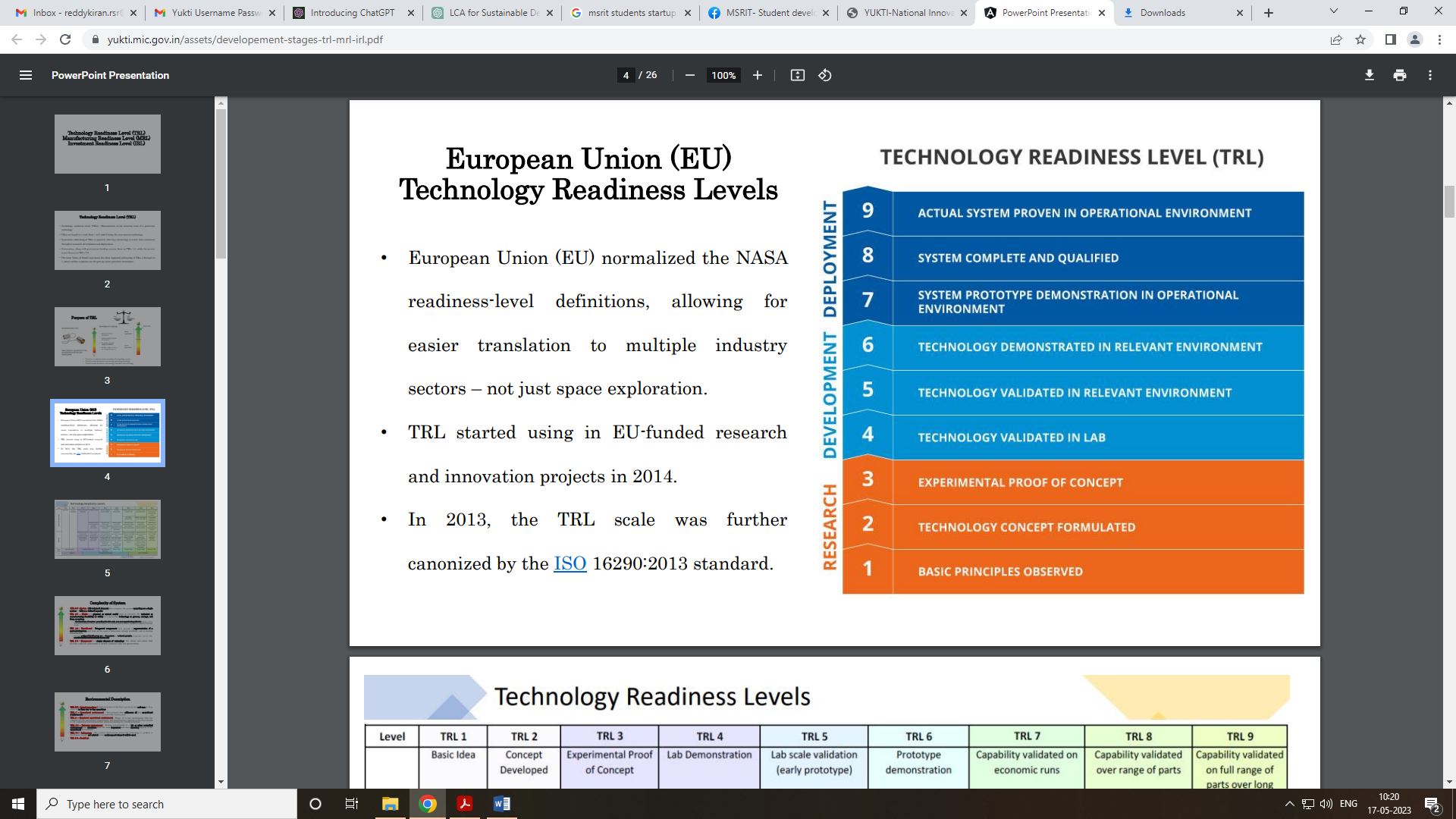
**\*Sector / Domain**

|  |  |
| --- | --- |
| Agriculture & Rural Development. | **No** |
| Clean & Potable water. | No |
| Consumer Goods and Retail | No |
| Defence & Security | No |
| Education | No |
| Fashion and Textiles | No |
| Finance Life Sciences | No |
| Food Processing/Nutrition/Biotech | No |
| Healthcare & Biomedical devices. | No |
| ICT, cyber-physical systems, Blockchain, Cognitive computing, Cloud computing, AI & ML. | Yes |
| Infrastructure | No |
| IoT based technologies (e.g. Security & Surveillance systems etc) | Yes |
| Manufacturing | No |
| Mining, Metals, Materials | No |
| Other Emerging areas Innovation for Startrup | No |
| Renewable and affordable Energy. | No |
| Robotics and Drones. | No |
| Smart Cities | No |
| Smart Education | No |
| Smart Textiles | No |
| Smart Vehicles/ Electric vehicle/ Electric vehicle motor and battery technology. | No |
| Software - Mobile App Development | No |
| Software - Web App Development | Yes |
| Sports & Fitness | No |
| Sustainable Enviroment | No |
| Travel & Tourism | No |
| Waste Management/Waste to Wealth Creation | No |

**\*Innovation Type:**

|  |  |
| --- | --- |
| **Product** | **NO** |
| **Process** | **No** |
| **Service** | **Yes** |
| **Market Place** | **No** |
| **Business/Management Innovation** | **No** |

**\* Development Stage - Technology Maturity of the Solution/Innovation in terms of Technology Readiness Level TRL (if applicable) – TRL Level:**



**Define the problem and its relevance to today's market / society / industry need (Max: 100 Words)**

|  |
| --- |
| The problem addressed in our project is the escalating threat of phishing attacks in today's digital landscape, which poses significant risks to individuals, businesses, and society as a whole. With the exponential growth of online activities and the increasing reliance on digital platforms for communication, commerce, and social interactions, phishing has emerged as a pervasive and deceptive form of cybercrime. Our project's relevance lies in developing innovative techniques for accurate phishing URL detection using machine learning algorithms, aiming to enhance cybersecurity measures and protect users' sensitive information from malicious attacks. |

**\*Describe the Solution / Proposed / Developed (Max: 100 Words)**

|  |
| --- |
| solution involves leveraging advanced machine learning algorithms and feature engineering techniques to develop a robust phishing URL detection system. By extracting informative features from URLs, such as structure, domain age, SSL certificate presence, and traffic ranking, we enhance the system's ability to differentiate between phishing and legitimate URLs accurately. The implementation of ensemble learning techniques further improves detection accuracy and resilience against evolving phishing tactics. Real-time detection capabilities ensure immediate protection, while ethical data handling practices maintain user trust. Overall, our proposed solution offers an innovative approach to combating phishing threats in today's digital environment |

**\*Explain the uniqueness and distinctive features of the (product / process / service) solution (Max: 100 Words)**

|  |
| --- |
| solution stands out for its adaptive algorithms that continuously learn and adapt to evolving phishing tactics, ensuring proactive defense. The incorporation of ensemble learning enhances detection accuracy and resilience against adversarial attacks, marking a notable advancement. Real-time detection capabilities provide immediate protection, while ethical data handling practices prioritize user privacy and trust. The system's ability to maintain a high level of accuracy, balance between precision and recall, and efficiency in execution distinguishes it as a cutting-edge solution in combating phishing threats effectively in today's dynamic digital landscape. |

**\*How your proposed / developed (product / process / service) solution is different from similar kind of product by the competitors if any (Max: 100 Words)**

|  |
| --- |
| solution differs from competitors' products through its adaptive algorithms, real-time detection capabilities, and ethical data handling practices. Unlike traditional methods, our system continuously learns and adapts to evolving phishing tactics, ensuring proactive defense. The implementation of ensemble learning enhances detection accuracy and resilience against adversarial attacks, providing a competitive edge. Furthermore, our focus on user privacy and transparency, along with compliance with data protection regulations, sets us apart by prioritizing trust and ethical data handling. These unique features differentiate our solution as a cutting-edge and user-centric approach in combating phishing threats effectively. |

**\*Is there any IP or Patentable Component associated with the Solution?**

**No**

**\*Has the Solution Received any Innovation Grant/Seed fund Support?**

**No**

**\*Are there any Recognitions (National/International) Obtained by the Solution? No**

**\*Upload the Copy of Latest Achievement: (JPG, PNG, PDF max 2 MB)**

**Softcopy of the Achievements. (Copy and Paste here)**

**\*Is the Solution Commercialized either through Technology Transfer or Enterprise Development/Startup? No**

**\*Had the Solution Received any Pre-Incubation/Incubation Support? No**

**Video URL: Images slideshow video or any short video.**

**Upload Photograph: (JPG, PNG, PDF max 2 MB) – Copy and paste Photographs**

**MRL Level Applicability – Yes/No**

MRL 1: Basic manufacturing implications identified

MRL 2: Manufacturing concepts identified

MRL 3: Manufacturing proof of concept developed

MRL 4: Capability to produce the technology in a laboratory environment

MRL 5: Capability to produce prototype components in a production relevant environment

MRL 6: Capability to produce a prototype system or subsystem in a production relevant environment

MRL 7: Capability to produce systems, subsystems or components in a production representative environment.

MRL 8: Pilot line capability demonstrated. Ready to begin low rate production.

MRL 9: Low rate production demonstrated. Capability in place to begin Full Rate Production.

MRL 10: Full rate production demonstrated and lean production practices in place.

**IR Level Applicability – Yes/No**

IRL 1: Basic Research (Need Identification & Peer Review Publications) & Completed First-Pass Business Model Canvas (BMC)

IRL 2: Applied Research (Market Size and Competitive Analysis) & Business Plan – Value Proposition & IP Identification

IRL 3: Validate Problem - Solution Fit (Confirmed Value Proposition & Techno-Economic Analysis) & Minimum Product Cost (Maturity of Core Technology)

IRL 4: Prototype Low-Fidelity Minimum Viable Product (MVP): “Low-fidelity” - A representative of the component or system that has limited ability to provide anything but initial information about the end product.

IRL 5: Validate Product-Market Fit (Integrated Validation of the Minimum Viable Process and Process Engineering). “High-fidelity” - A high-fidelity laboratory environment would involve testing with equipment that can simulate and validate all system specifications within a laboratory setting.

IRL 6: Validate Business/Revenue Model: Integrated Pilot Development– understanding operational nuances

IRL 7: Prototype High Fidelity MVP: Integrated Pilot Continuous Operation

IRL 8: Pre-Commercial Demonstration – Operating Conditions and quality stabilized

IRL 9: Full Commercial Development – A full time process engineering staff continuously verifies that operations are meeting cost, yield and productivity targets.

**\*Had the Solution Received any Pre-Incubation/Incubation Support? Yes/No**

**\*Utility: Highlight the utility/value proposition (key benefits) aspects of the solution/innovation\* (Max: 100 Words)**

|  |
| --- |
| solution offers key benefits in enhancing cybersecurity and protecting users' sensitive information. The adaptive algorithms ensure proactive defense by continuously learning and adapting to evolving phishing tactics. Real-time detection capabilities provide immediate protection against phishing threats, minimizing risks. The implementation of ensemble learning enhances detection accuracy and resilience against adversarial attacks, ensuring reliable performance. Additionally, ethical data handling practices prioritize user privacy and trust, complying with data protection regulations. Overall, our solution's value proposition lies in its effectiveness, efficiency, and user-centric approach, making it a crucial tool in combating phishing threats and safeguarding digital assets. |

**\*Scalability: Highlight the market potential aspects of the Solution/Innovation (Potential Market Size, segmentation and Target users/customers etc.) (Max: 100 Words)**

|  |
| --- |
| solution targets a wide market potential due to the ubiquitous nature of phishing threats across industries and user segments. The potential market size encompasses businesses of all sizes, government agencies, educational institutions, and individual users globally. Segmentation includes sectors such as finance, healthcare, e-commerce, and more. Target users/customers range from IT security professionals and cybersecurity experts to general users concerned about online security. The scalability of our solution lies in its adaptability to diverse environments and its ability to cater to a broad spectrum of users, making it a valuable asset in mitigating phishing risks across various sectors and user demographics. |

**\*Economic Sustainability: Highlight commercialisation/business application aspects of the solution (how it is going to economic profitable and viable) (Max: 100 Words)**

|  |
| --- |
| offers economic sustainability through its commercialization and business application potential. By addressing a critical need in cybersecurity, our system can be marketed to businesses, government agencies, and organizations seeking robust phishing detection solutions. Revenue streams can be derived from licensing fees, subscription models for ongoing protection, and consulting services for implementation and customization. The scalability of our solution ensures a broad customer base, while its effectiveness and reliability contribute to customer retention and positive referrals. These factors combined make our solution economically profitable and viable in the cybersecurity market. |

**\*Environmental Sustainability: Highlight environmental friendliness aspects and related benefit of the solution/innovation  
(Max: 100 Words)**

|  |
| --- |
| While the solution primarily focuses on cybersecurity, it indirectly contributes to environmental sustainability by reducing the environmental impact of cyberattacks. Phishing attacks often lead to data breaches, resulting in significant energy consumption for data recovery, system repairs, and legal processes. By preventing phishing attacks and data breaches, our solution minimizes the associated energy and resource consumption, leading to reduced carbon emissions and environmental strain. Additionally, the implementation of efficient algorithms and real-time detection capabilities optimizes system performance, further reducing energy usage. Thus, our solution promotes environmental friendliness by mitigating the environmental consequences of cyber incidents. |