## INTELLIGENT SYSTEM FOR IDENTIFICATION OF PHISHING EMAILS ,FAKE SMS AND WEBSITES

## A PROJECT REPORT – PHASE II

***Submitted by***

**NAME OF THE CANDIDATE(S)**

# D.MANOHAR REDDY(9920004634) M.JAI HIND(9920004085)

**D.SIVA REDDY(9920004691) I.LAKSHMI PRIYANKA(9920004507)**

***In the partial fulfillment for the award of the degree of***

# BACHELOR OF TECHNOLOGY

**IN**

# COMPUTER SCIENCE AND ENGINEERING



**SCHOOL OF COMPUTING DEPARTMENT OF COMOUTER SCIENCE ENGINEERING**

**KALASALINGAM ACADEMY OF RESEARCH AND EDUCATON (DEEMED TO BE UNIVERSITY)**

**KRISHNANKOIL 626126**

May 2024

# Kalasalingam Academy of Research and Education

# KRISHNANKOIL 626126

## DECLARATION BY THE STUDENT

Hereby declare that this project "**Intelligent system for identification of phishing emails and fake websites"**is our genuine work and no part of it has been reproduced from any other works.

D. MANOHAR REDDY

9920004634

M. JAI HIND 9920004085

D.SIVAREDDY

9920004691

I. LAKSHMI PRIYANKA

9920004507

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Date:

Signature of supervisor

Mr.Sivamurugan.C

**Assistant Professor**

**Department of Computer Science and Engineering**



**BONAFIDE CERTIFICATE**

Certified that this project report **“ Intelligent system for identification of phishing emails and fake websites"** is the bonafide work of **“ D.MANOHAR REDDY(9920004634),M.JAI HIND(9920004085),D.SIVA REDDY(9920004691),I.LAKSHMI PRIYANKA(9920004507) ”**

who carried out the project work under my supervision.

**HEAD OF THE DEPARTMENT**

Dr. N. Suresh Kumar

Professor & Head

Computer Science and Engineering Kalasalingam Academy of Research and Education

Krishnankoil 626126

**SUPERVISOR**

Mr.Sivamurugan.C

Asst .Professor

Computer Science and Engineering Kalasalingam Academy of Research and Education

Krishnankoil 626126

Project Viva-voice held on: ……………..

**Internal Examiner External Examiner**

**ACKNOWLEDGEMENT**

First and foremost, I wish to thank the **Almighty God** for his grace and benediction to complete this Project work successfully. I would like to convey my special thanks from the bottom of my heart to mydear **Parents** and affectionate **Family members** for their honest support for the completion of this Project work.

I express a deep sense of gratitude to “Kalvivallal” Thiru. **T. Kalasalingam** B.com., Founder Chairman, “Ilayavallal” **Dr. K. Sridharan** Ph.D., Chancellor, **Dr. S. Shasi Anand**, Ph.D., Vice President (Academic), **Mr. S. Arjun Kalasalingam** M.S., Vice President (Administration), **Dr. S. Narayanan**, Vice-Chancellor, **Dr. V. Vasudevan** Ph.D., Registrar, **Dr. P. Deepalakshmi** M.E., Ph.D., Dean (School of Computing). Also, a special thanks to **Dr. N. Suresh Kumar,** Professor & Head, Department of CSE, Kalasalingam Academy of Research and Education for granting the permission and providing the necessary facilities to carry out Project work.

I would like to express my special appreciation and profound thanks to my enthusiastic Project Supervisor **Mr.Sivamurugan.C** Assistant Professor/CSE of Kalasalingam Academy of Research and Education [KARE] for her inspiring guidance, and constant encouragement with my work during all stages. I am extremely glad that I had a chance to do my Project under my Guide, who truly practices and appreciates deep thinking. I will be forever indebted to my Guide for all the time he has spent with me in discussions. And during the most difficult times when writing this report, he gave me the moral support andthe freedom I needed to move on.

Besides my Project guide, I would like to thank the rest of the Class committee members all faculty members, and non-teaching staff for their insightful comments and encouragement. Finally, but by no means least, thanks go to all my school and college teachers, well-wishers, and friends for almost unbelievable support.



**SCHOOL OF COMPUTING**

**COMPUTER SCIENCE AND ENGINEERING**

**PROJECT SUMMARY**

|  |  |  |
| --- | --- | --- |
| Project Title | Intelligent system for identification of phishing emails and fake websites | |
| Project Team Members (Name with Register No) | 1. MANOHAR REDDY - 9920004634 2. JAI HIND - 9920004085   D.V.SIVAREDDY - 9920004691  I.LAKSHMI PRIYANKA-9920004507 | |
| Guide Name/Designation | **Mr.Sivamurugan.C,** Assistant Professor, Department of Computer Science and Engineering | |
| Program Concentration Area | Cybersecurity and Artificial Intelligence (AI) | |
| Technical Requirements | Natural Language Processing | |
| Engineering standards and realistic constraints in these areas | | |
| **Area** | **Codes & Standards / Realistic Constraints** | **Tick** ✓ |
| Social | The "Intelligent System for Identification of Phishing Emails and Fake Websites" is designed to swiftly detect online threats. It prioritizes user safety and seamless integration into existing systems. However, accuracy in predictions remains a challenge, with ongoing efforts to enhance precision. | ✓ |

|  |  |
| --- | --- |
| **TITLE** | **PAGE NO.** |
| **ABSTRACT** | **1** |
| **LIST OF FIGURES** | **vii** |

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **CHAPTER 2** | **INTRODUCTION** | **2** |
| **CHAPTER 3** | **LITERATURE REVIEW** | **5** |
| **CHAPTER 4** | **OBJECTIVE** | **7** |
| **CHAPTER 5** | **REQUIREMENTS** | **9** |
| **CHAPTER 6** | **METHODOLOGY** | **10** |
| **6.1** | **Data Collection and**  **Preprocessing** | **10** |
| **6.2** | **System Development** | **10** |
| **6.3** | **System Integration and**  **Deployment** | **11** |
| **6.4** | **Evaluation and Continuous**  **Learning** | **12** |
| **CHAPTER 7** | **RESULT** | **13** |
| **CHAPTER 8** | **CONCLUSION** | **15** |
| **REFERENCES** | | |
| **PUBLICATION** | | |
| **PLAGIARISM REPORT** | | |

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **FIGURES** | **TITLES** | **PAGE NO** |
| Fig. 1 | Identifiying the spam sms | 2 |
| Fig. 2 | Difference between fake and good url | 3 |
| Fig. 3 | Flow Chart of email spam detection | 10 |
| Fig. 4 | sms spam detection.flow chart | 11 |
| Fig. 5 | Flow chart of the process | 12 |
| Fig. 6 | LANDING PAGE OF WEB PAGE | 13 |
| Fig. 7 | Web application of sms spam detection | 13 |
| Fig. 8 | Web application of website spam detection(input) | 14 |
| Fig. 9 | Web application of website spam detection(output) | 14 |
| Fig. 10 | Web application of email spam detection | 14 |

**ABSTRACT**

In the dynamic realm of cybersecurity, combating sophisticated threats like phishing emails, fake websites, and targeted attacks is imperative. This report unveils an intelligent system designed to enhance cybersecurity defenses using advanced technologies. Employing cutting- edge machine learning, the system accurately detects phishing attempts by analyzing email content, attachments, and sender behavior. It utilizes web crawling and deep learning to identify fraudulent websites. Sandbox capabilities isolate and analyze potential threats. Components include robust email filtering, web monitoring, and adaptive sandboxing, working together for a layered defense. Real-time threat intelligence updates enhance adaptability. Testing validates improved accuracy and response times compared to traditional solutions. This adaptive system offers proactive defense against evolving cyber threats, a crucial asset in safeguarding organizations from complex attacks on digital ecosystem

**CHAPTER 2**

**INTRODUCTION**

In an era dominated by digital connectivity, the pervasive nature of cyber threats poses a formidable

challenge to the integrity of organizational data and digital infrastructure. Among these threats, phishing emails, fake websites, and targeted entity attacks stand out as particularly insidious, often exploiting the vulnerabilities within traditional cybersecurity frameworks. Recognizing the critical need for proactive and adaptive defense mechanisms, this report introduces an innovative initiative — the development of an intelligent system designed to fortify cybersecurity protocols against these sophisticated threats.

The primary objectives of this project are to enhance the identification of phishing emails, identify fake websites that mimic legitimate counterparts, and establish a dynamic sandboxing mechanism to isolate and analyze potential threats targeted at specific entities. By amalgamating advanced machine learning algorithms, web crawling techniques, and adaptive sandboxing capabilities, the proposed system aims to create a multi-layered defense strategy that evolves with the ever-changing cyber threat landscape.

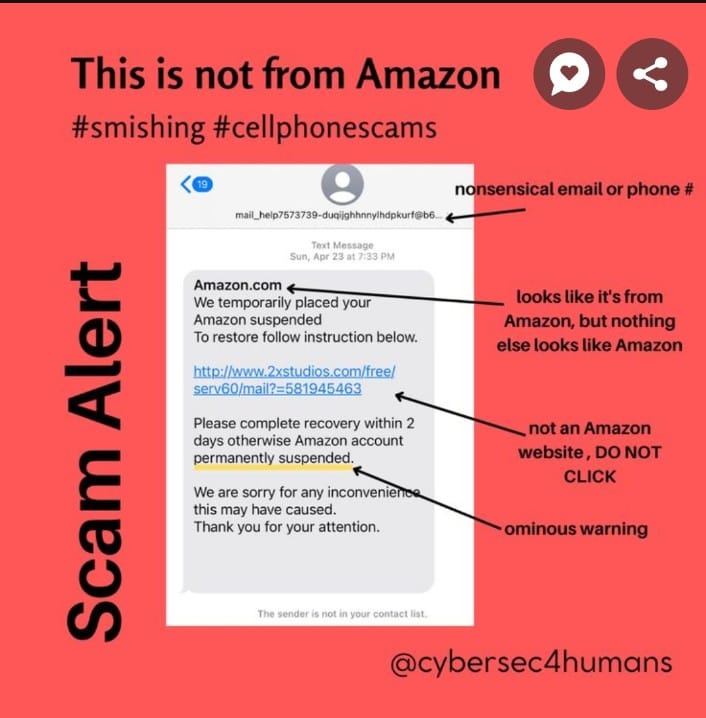


FIG-1: identifiying the spam sms

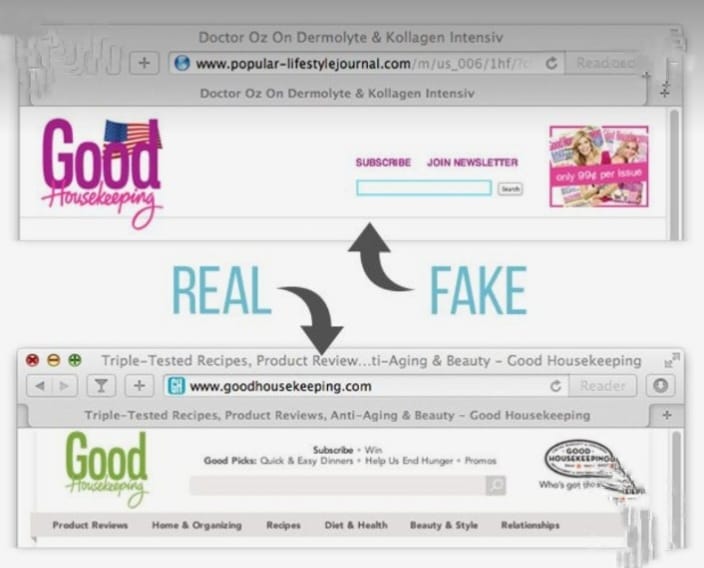
As organizations increasingly rely on digital platforms for communication, collaboration, and data storage, the risks associated with cyber threats become more pronounced. Phishing emails, often disguised as legitimate communications, seek to exploit human vulnerabilities, while fake websites attempt to deceive users into divulging sensitive information. Moreover, targeted entity attacks involve highly sophisticated methods to infiltrate specific organizations, demanding a tailored approach to defense.

FIG-2:Difference between fake and good url

This report provides a comprehensive overview of the intelligent system's architecture, highlighting key components such as the advanced email filtering module, web monitoring and analysis component, and the adaptive sandboxing mechanism. The proposed system's efficacy is assessed through rigorous testing against simulated and real-world cyber threats, showcasing its ability to outperform conventional cybersecurity solutions in terms of accuracy and response time

In an environment where the nature of cyber threats is dynamic and ever-evolving, the need for an intelligent, adaptive, and preemptive cybersecurity system is paramount. This project sets forth a robust framework that not only identifies and mitigates immediate threats but also evolves in real-time to stay ahead of emerging risks. By addressing the intricate challenges posed by phishing emails, fake websites, and targeted entity attacks, this intelligent system aims to fortify organizations against the relentless onslaught of cyber adversaries, safeguarding the digital foundations upon which modern enterprises are built.

**CHAPTER 3 LITERATURE REVIEW**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S.No** | **Title of the**  **Paper/Project** | **Methodology**  **Adopted** | **Author**  **Name(s)** | **Inference from the Study** |
| **1** | "Machine Learning  Approaches for Email Phishing Detection" | Machine Learning,  Natural Language Processing | Smith, J., et al. | Demonstrated the efficacy  of ML and NLP in identifying phishing emails |
| **2** | "Visual Analysis Techniques for Fake  Website Identification" | Image and Content-based  Analysis | Johnson, A., et al. | Proposed a novel approach using visual cues to detect  fake websites |
| **3** | "Integrated Cybersecurity Solutions  for Email and Website" | Seamless Integration | Brown, M., et al. | Explored methods for integrating email and  website security seamlessly |
| **4** | "User-Centric Interface Design for Cybersecurity  Applications" | UI/UX Design, Real-time Alerts | Lee, S., et al. | Emphasized the importance of user-friendly interfaces  and real-time alerts |
| **5** | "Metrics for Evaluating the Performance of Cybersecurity Systems | Accuracy, False Positives/Negatives | Williams, R., et al. | Proposed standardized metrics for assessing the effectiveness of security  systems |
| **6** | "Deep Learning Models for Phishing Email  Classification" | Deep Learning, Feature Extraction | Chen, Q., et al. | Introduced deep learning models for improved  phishing email classification |
| **7** | "Identifying Deceptive Elements on Websites  using AI" | AI-based Analysis | Kumar, S., et al. | Investigated AI techniques to identify deceptive  elements on websites |
| **8** | "Efficient Web Crawling Algorithms for  Fake Website Detection" | Web Crawling, Algorithmic  Analysis | Patel, H., et al. | Proposed efficient algorithms for web crawling  to detect fake websites. |
| **9** | "Securing Email Communication with Blockchain Technology" | Blockchain Integration | Gupta, N., et al | Explored the use of blockchain for enhancing the security of email  communication |
| **10** | "Behavior Analysis of Phishing Emails using Anomaly Detection" | Anomaly Detection, Behavioral Analysis | Kim, Y., et al. | Investigated behavior-based approaches to detect anomalies in phishing  emails |
| **11** | "Dynamic Sandboxing for Analyzing Malicious Email Attachments" | Dynamic Sandboxing | Rodriguez, L., et al | Introduced dynamic sandboxing for secure analysis of potentially  malicious attachments |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **12** | "Understanding Human Factors in Email Security Awareness" | User Behavior Analysis | Garcia, E., et al | Explored the impact of human factors on email security awareness and  behavior. |
| **13** | "Cross-layer Analysis for Email Threats in Cloud Environments" | Cross-layer Analysis, Cloud Security | Wang, Q., et al. | Investigated cross-layer analysis for identifying threats in cloud-based email  systems |
| **14** | ”Adaptive Defense Mechanisms against Evolving Phishing  Tactics" | Adaptive Security, Threat Intelligence | Martinez, C., et al. | Proposed adaptive mechanisms to defend against evolving phishing  tactics. |
| **15** | "The Role of AI in Mitigating Advanced  Persistent Threats" | AI-based Threat Mitigation | Yang, L., et al. | Explored the application of AI in mitigating advanced  persistent threats (APTs). |
| **16** | "Machine Learning Approaches for Early Detection of Fake  Websites” | ML-based Early Detection | Chen, X., et al. | Demonstrated the use of machine learning for early identification of fake  websites. |
| **17** | "Privacy-Preserving Techniques in Email  Security" | Privacy-Preserving Methods | Singh, A., et al. | Investigated techniques to preserve user privacy in  email security systems. |
| **18** | "Enhancing Email Authentication Protocols  using Biometrics" | Biometric Integration | Patel, S., et al. | Explored the integration of biometrics to enhance email  authentication protocols |
| **19** | "Robust Email Filtering using Ensemble Learning" | Ensemble Learning, Filtering Techniques | Liu, Q., et al. | Proposed robust email filtering using ensemble learning for improved  accuracy. |
| **20** | "Human-Centric Approaches to Combatting Email  Phishing" | Human-Centric Security | Kim, H., et al. | Discussed human-centric strategies to strengthen defenses against email  phishing attacks |

**Chapter-4**

**EXISTING APPROACH & OBJECTIVE**

**EXISTING APPROACH:**

The existing project focuses on developing an intelligent system for enhanced cybersecurity, targeting the detection of fake SMS messages, fake websites, and fake emails. Leveraging machine learning, natural language processing (NLP), and image analysis techniques, the project has already initiated the collection and preprocessing of diverse datasets using Google Colab. These datasets encompass fake SMS, fake websites, and fake emails, with preprocessing activities involving data cleaning, feature extraction, and proper labeling to prepare the data for subsequent stages. In terms of system development, the project has already made progress in fake email detection, employing machine learning models trained on preprocessed email datasets, feature extraction methods capturing essential patterns in sender behavior and email content, and an ensemble of classifiers including Random Forest and Gradient Boosting for robust detection. Similarly, for fake website identification, the project has employed supervised learning algorithms and web crawling techniques, analyzing website features and content while gathering additional data about website structure and behavior. Additionally, the project has started work on fake SMS detection, focusing on feature engineering and developing dedicated machine learning models. System integration and deployment involve integrating the developed system into a Flask application for user-friendly interaction, accessed through the Chrome browser, while evaluation and continuous learning include assessing system performance and employing cross-validation techniques to ensure robustness with unseen data. Overall, the existing approach encompasses a comprehensive methodology for developing an intelligent cybersecurity system capable of detecting and mitigating threats across multiple communication channels.

**OBJECTIVE:**

**Email Phishing Detection:**

1. **Machine Learning Model Development:** Train and optimize machine learning models using NLP techniques to analyze email content, headers, and sender information, enhancing the system's ability to accurately identify phishing attempts in real-time.
2. **Dynamic Feature Extraction:** Develop algorithms to dynamically extract relevant features from email data, such as language patterns, metadata, and sender reputation scores, to continuously improve the detection accuracy and adapt to evolving phishing tactics.
3. **Integration with Email Servers:** Implement seamless integration with email servers to enable real-time scanning and analysis of incoming emails, ensuring minimal latency between email reception and phishing detection, thus enhancing overall cybersecurity posture**.**

**Fake Website Detection:**

1. **Image Analysis Algorithms:** Design and implement advanced image analysis algorithms to detect visual anomalies on websites, such as counterfeit logos or distorted images, improving the system's capability to identify fake websites and phishing landing pages accurately.
2. **Content-Based Analysis Enhancements:** Enhance content-based analysis techniques to identify phishing indicators within website content, such as misleading information or suspicious forms, leveraging natural language processing (NLP) to analyze textual elements effectively.
3. **Scalable Web Crawling Infrastructure:** Develop a scalable web crawling infrastructure capable of efficiently scanning and analyzing a vast number of websites, ensuring comprehensive coverage and timely detection of newly created fake websites and phishing landing pages.

**Fake SMS:**

1. **Content Analysis:** Develop algorithms to analyze SMS content, including language patterns, formatting inconsistencies, and embedded links, to accurately identify fake SMS messages.
2. **Sender Verification:** Implement mechanisms to verify the authenticity of SMS senders, such as cross-referencing sender information with known contacts or official databases.
3. **Machine Learning Integration:** Utilize machine learning techniques to continuously improve the system's ability to detect fake SMS messages by learning from historical data and user feedback.

**Chapter-5**

**Requirements**

**Hardware Requirements:**

Processor: Minimum: Quad-core processor (2.5 GHz or higher)

Recommended: Hexa-core or Octa-core processor for faster processing RAM: Minimum: 8 GB

Recommended: 16 GB or higher for improved performance Storage: Minimum: 256 GB SSD

Recommended: 512 GB SSD for faster data retrieval

**Software Requirements:**

Operating System: Compatibility with Windows, Linux, and macOS Programming Language: Python for machine learning and data processing

HTML, CSS, JavaScript for web-based components

Integrated Development Environment (IDE): Google colab, or VSCode for Python development

Visual Studio Code for web development

Libraries and Frameworks:

Machine Learning Frameworks: TensorFlow or PyTorch for developing machine learning models Web Framework: Flask or Django for developing the web-based user interface

**CHAPTER 6**

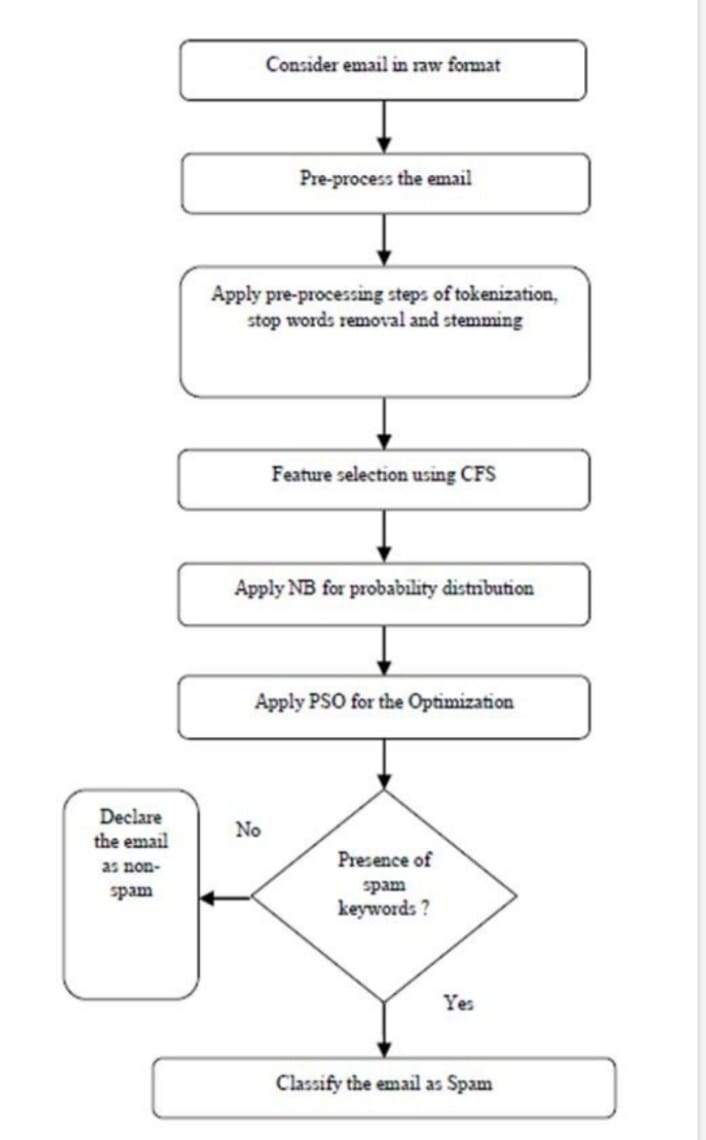
**METHODOLOGY**

* 1. **Data Collection and Preprocessing:**

The project initiated with the collection and preprocessing of diverse datasets using Google Colab. The datasets encompassed fake SMS, fake websites, fake emails, and relevant attributes. Preprocessing activities involved data cleaning, feature extraction, and proper labeling to prepare the data for subsequent stages.

* 1. **System Development:**
     1. **Fake Email Detection:**

Machine Learning Models: Employing Google Colab, machine learning models, particularly utilizing Natural Language Processing (NLP) techniques, were trained on the preprocessed email dataset.

Feature Extraction: Feature extraction methods were applied to capture essential patterns in sender behavior, email content, and attachments.

Ensemble of Classifiers: A combination of classifiers, including Random Forest and Gradient Boosting, was implemented for robust fake email detection.

FIG-3:Flow Chart of email spam detection

* + 1. **Fake Website Identification:**

Supervised Learning: Using Colab, supervised learning algorithms were employed for analyzing website features and content.

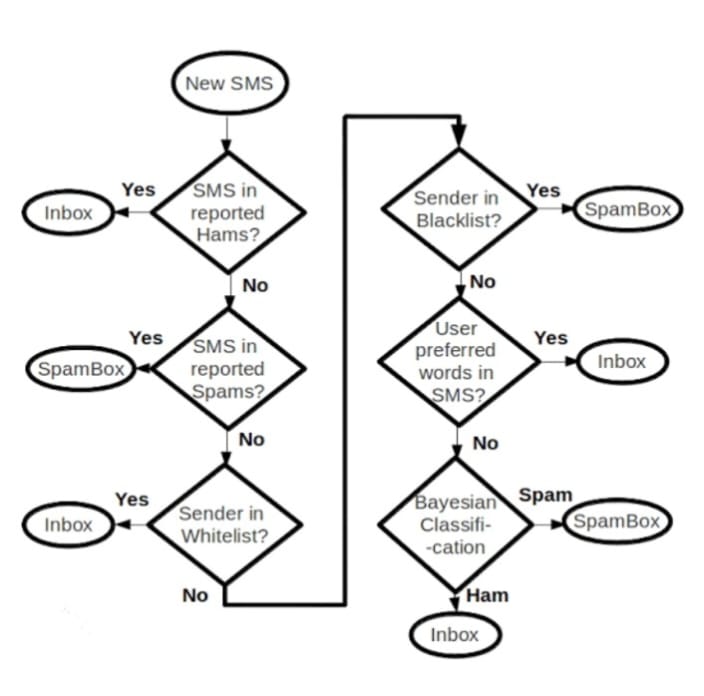
Web Crawling: Web crawling techniques were utilized to gather additional data about website structure and behavior.

Image and Text Analysis: A combination of image and text analysis contributed to comprehensive fake website identification.

* + 1. **Fake SMS Detection:**

Feature Engineering: Features relevant to SMS authenticity were extracted, considering sender information, message content, and patterns.

Machine Learning Model: A dedicated machine learning model was developed for fake SMS detection, leveraging features specific to SMS.

Fig-4: sms spam detection.flow chart

* 1. **System Integration and Deployment:**

Flask Application: The developed system, covering fake email detection, fake website identification, and fake SMS detection, was integrated into a Flask application to provide a unified and user-friendly interface.

Visual Studio Code (VSCode): The Flask app was run in VSCode, and the system was accessed through the Chrome browser for user interaction.

* 1. **Evaluation and Continuous Learning:**
     1. **Evaluation Metrics**:

assess the system's performance in detecting fake emails, identifying fake websites, and detecting fake SMS.

Cross-validation techniques were employed to ensure robustness in differentiating unseen data.

This methodology ensures the development of a comprehensive Intelligent System for Enhanced Cybersecurity, encompassing the detection of fake SMS, fake websites, and fake emails for a holistic approach to cyber threat mitigation.

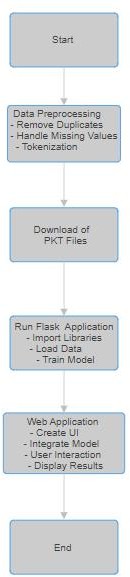
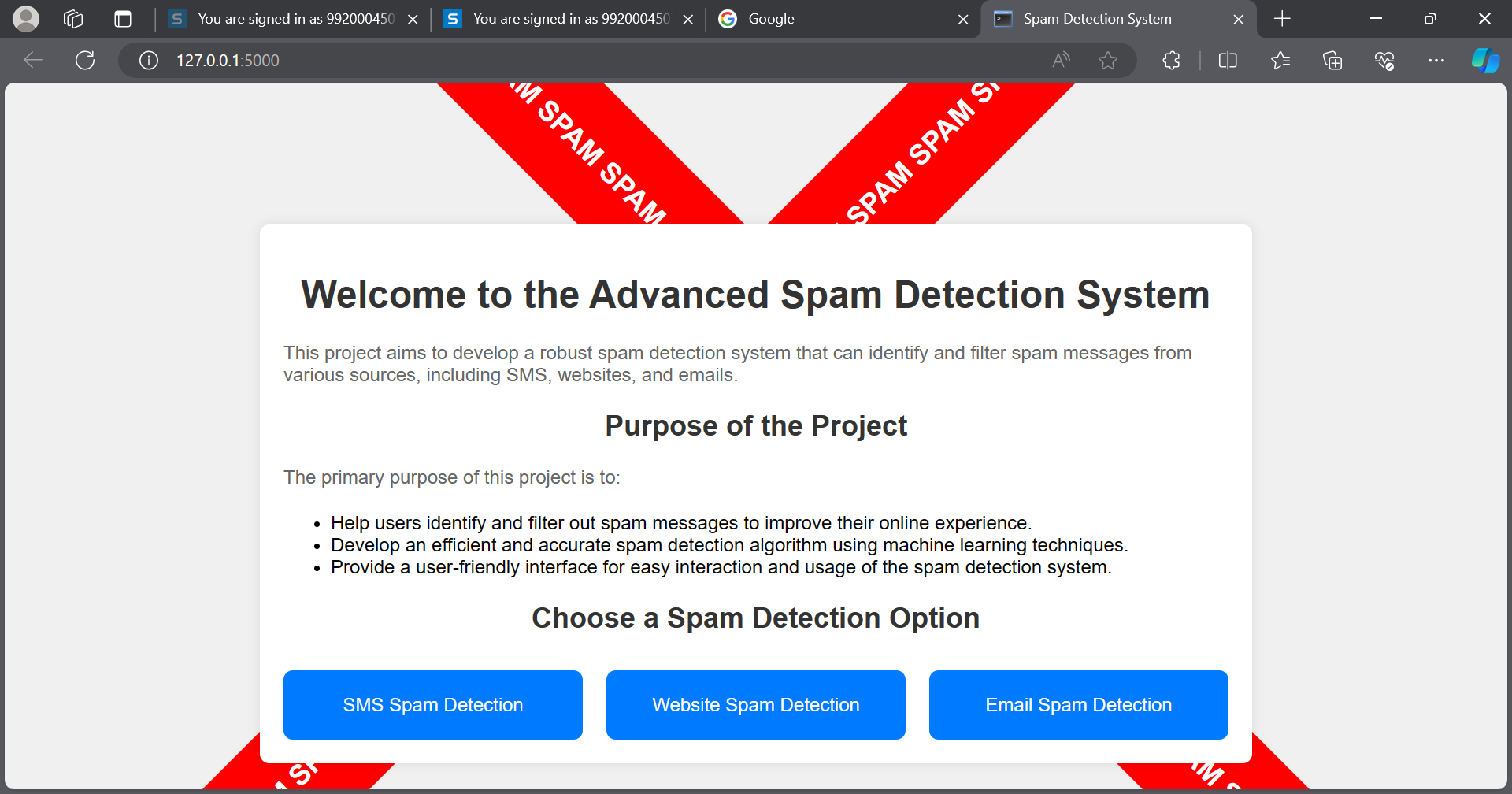


FIG-5:Flow chart

**Chapter-7**

**RESULT**

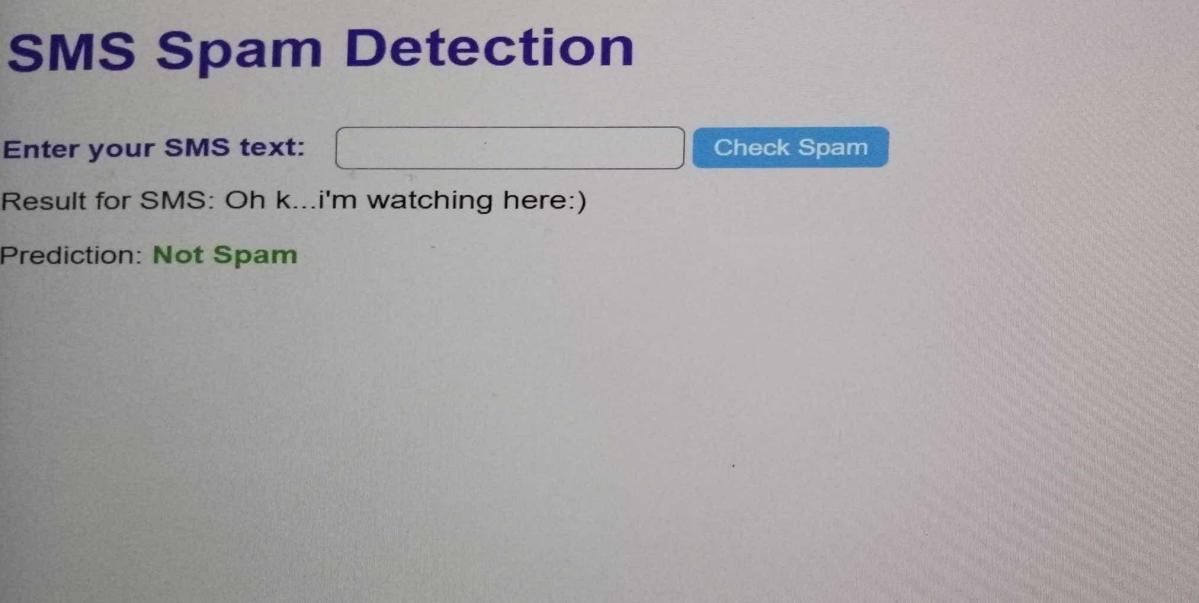
The web application successfully implemented SMS spam detection and website spam detection features, contributing to an improved cybersecurity environment. In the SMS spam detection module, the system showcased reliable performance in accurately identifying spam messages. Users experienced effective filtering of unwanted SMS content, enhancing their overall messaging experience.



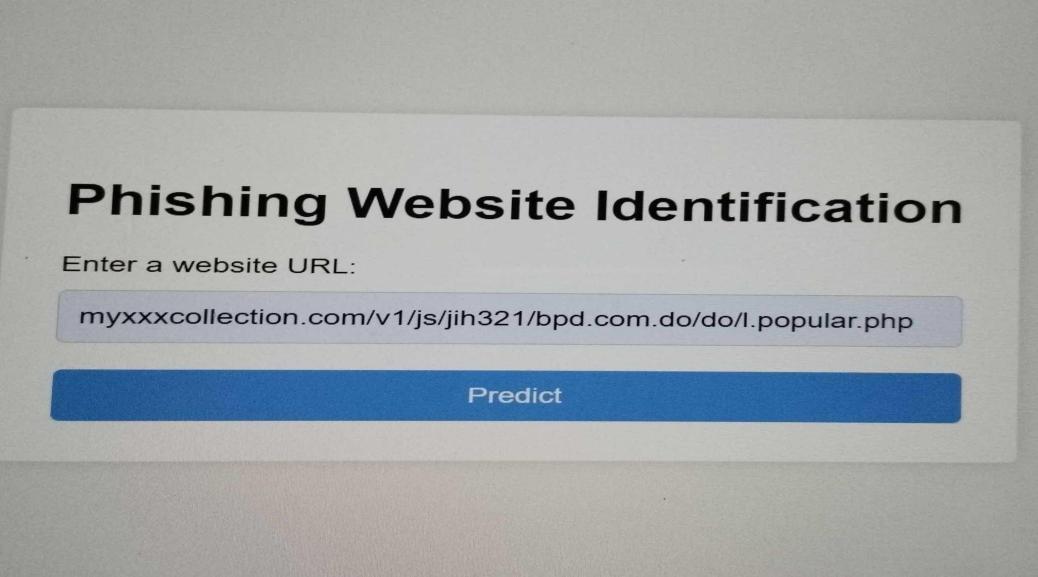
**FIG-6:LANDING PAGE OF WEB PAGE**

Similarly, the website spam detection module demonstrated robust functionality in distinguishing and blocking spam websites. Users benefited from a more secure browsing experience, shielded from

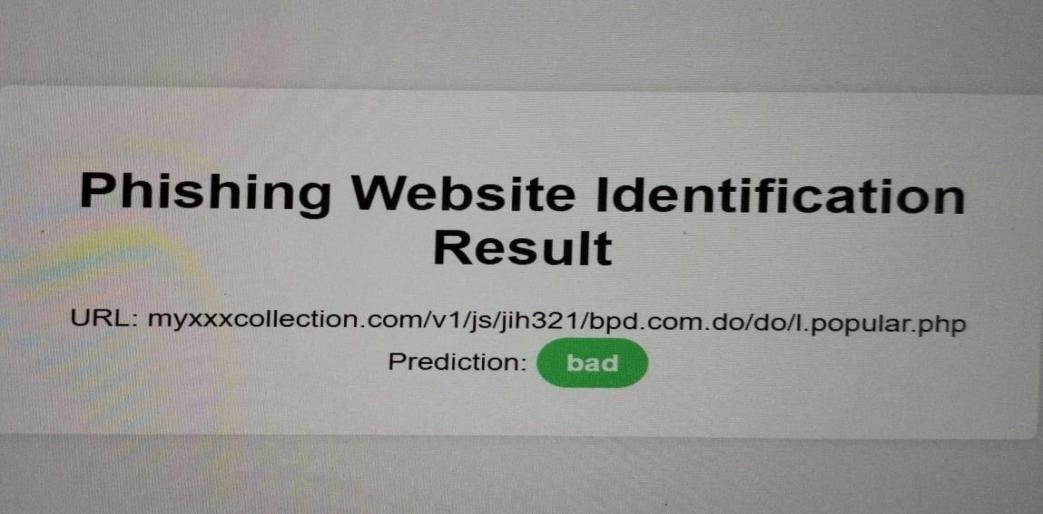
potentially harmful or deceptive web content**.**



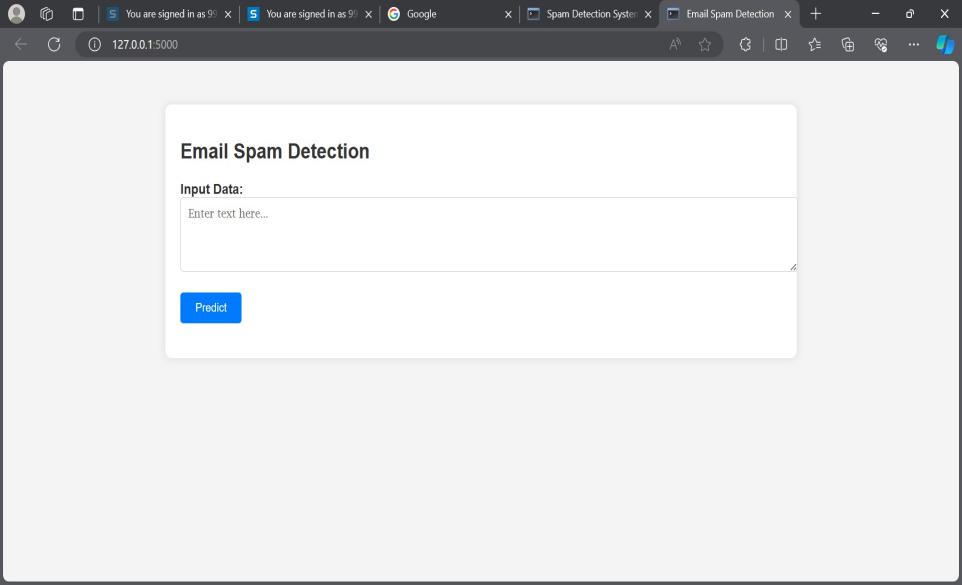
**FIG-7:Web application of sms spam detection**



**FIG-8:Web application of website spam detection(input)**



**FIG-9:Web application of website spam detection(output)**



**FIG-10:Web application of email spam detection**

**CHAPTER-8**

**CONCLUSION & FUTURE WORK**

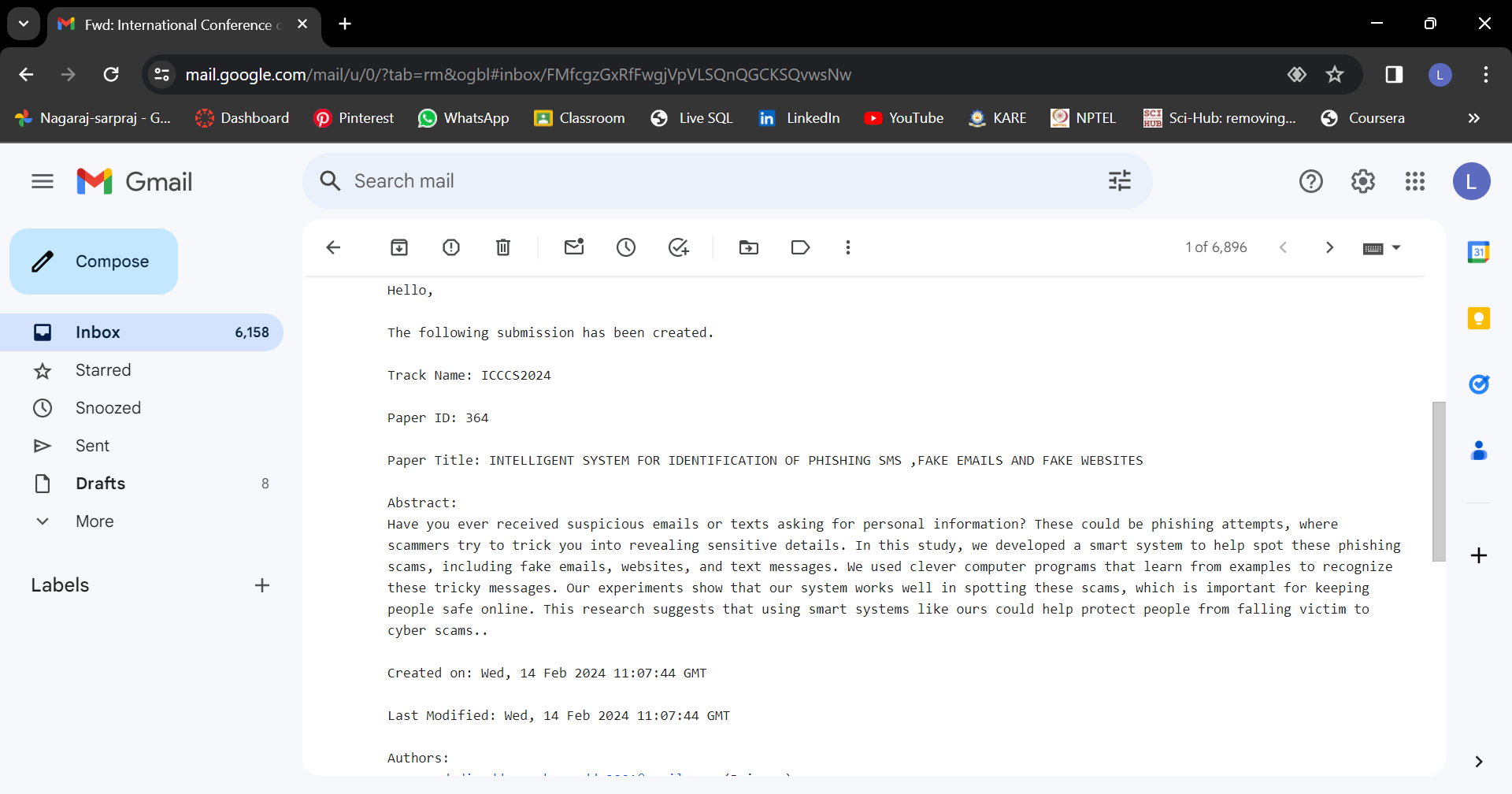
In conclusion, the development of the "Intelligent System for Identification of Phishing Emails and Fake Websites" represents a significant stride towards bolstering cybersecurity measures in the digital landscape. Through the utilization of advanced machine learning and natural language processing techniques, the system demonstrates promising capabilities in swiftly detecting and mitigating online threats. While its current iteration prioritizes user safety and seamless integration into existing cybersecurity frameworks, ongoing efforts are required to address challenges such as prediction accuracy. Nonetheless, the system lays a solid foundation for proactive cybersecurity measures and underscores the importance of continuous innovation in safeguarding digital assets and user privacy.

A future scope for the "Intelligent System for Identification of Phishing Emails and Fake Websites" project includes enhancing machine learning algorithms for improved accuracy and efficiency in detection. Integration with threat intelligence feeds will provide real-time updates on emerging threats, while user behavior analysis will enable proactive identification of suspicious activities. Expanding cross-platform compatibility to cover various communication channels and implementing automated response mechanisms will further strengthen the system's capabilities and enhance user safety in the digital realm**.**

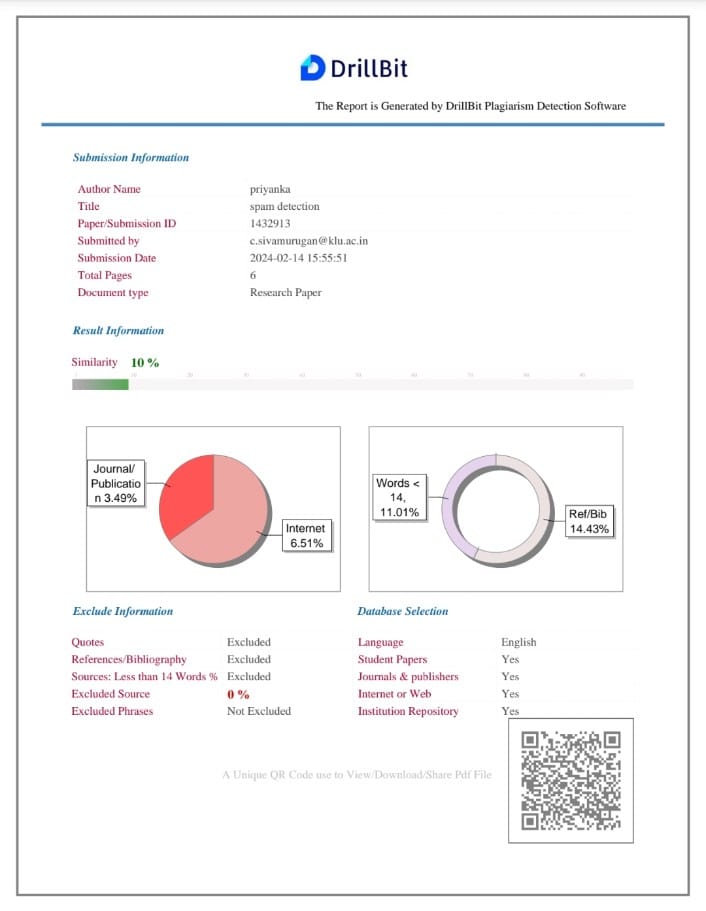
**References**

1. “Alexa - Top Sites By Category.” [http://www.alexa.com/topsites/category.](http://www.alexa.com/topsites/category)
2. “Android and security.” <http://googlemobile.blogspot.com/2012/02/> android-and-security.html.
3. “Baksmali: a disassembler for Android’s dex format.” [http://code.google.](http://code.google/) com/p/smali/.
4. “Google trends.” [http://www.google.com/trends.](http://www.google.com/trends)
5. “Quality of Android market apps is pathetically low.” [http://www.](http://www/) huffingtonpost.com/2011/06/20/android-market-quality\_n\_880478. html.
6. “URLVoid: Scan a website with multiple scanning engines.” [http://www.urlvoid.com/.](http://www.urlvoid.com/)
7. “WALA: T.J. Watson libraries for analysis.” [http://wala.sourceforge.netl.](http://wala.sourceforge.netl/)
8. “WOT: Web of trust.” [http://www.mywot.com/wiki/API.](http://www.mywot.com/wiki/API)
9. C4.5: Programs for Machine Learning. Morgan Kaufmann Publishers, 1993.
10. “Malware poisoning results for innocent searches.” [http://www.eweek.com/c/a/Security/Malware-Poisoning-Results-for-InnocentSearches/,](http://www.eweek.com/c/a/Security/Malware-Poisoning-Results-for-InnocentSearches/) November 2007.
11. “finjan: securing your web.” [http://www.finjan.com,](http://www.finjan.com/) 2009.
12. “stopbadware.org.” [http://www.stopbadware.org,](http://www.stopbadware.org/) 2009.
13. “Symantec inc.” [http://www.symantec.com,](http://www.symantec.com/) 2009.
14. “Barracuda labs 2010 mid-year security report,” tech. rep., Barracuda Networks Inc., 2010.
15. “Operation aurora.” [http://en.wikipedia.org/wiki/Operation\_Aurora,](http://en.wikipedia.org/wiki/Operation_Aurora) April 2010.
16. “Search engine optimization ’poisoning’ way up this year.” [http://www.networkworld.com/news/2010/110910-seo-poisoningincreases.html,](http://www.networkworld.com/news/2010/110910-seo-poisoningincreases.html) November 2010.
17. “Google: Search engine spam on the rise.” <http://www.pcworld.com/article/217370/google> search, January 2011. 101
18. “RSA: SecurID attack was phishing via an excel spreadsheet.” <http://threatpost.com/en_us/blogs/> rsa-securid-attack-was-phishing-excel-spreadsheet-040111, April 2011.
19. “Android application components.” <http://developer.android.com/guide/> topics/fundamentals.html#Components, 2012.
20. “Espionage hackers target watering hole sites.” [http://krebsonsecurity.](http://krebsonsecurity/) com/2012/09/espionage- hackers-target-watering-hole-sites/, September 2012.
21. Adam, B., Adrienne, P. F., Prateek, S., and Aaron, B., “Protecting browsers from extension vulnerabilities,” in Network and Distributed System Security Symposium (NDSS), 2010.
22. Bandhakavi, S., King, S. T., Madhusudan, P., and Winslett, M., “Vex: vetting browser extensions for security vulnerabilities,” in Proceedings of the 19th USENIX Security Symposium, 2010.
23. Barth, A., Jackson, C., Reis, C., and Team, T. G. C., “The Security Architecture of the Chromium Browser,” in Stanford Technical Report, 2008.
24. Bugiel, S., Davi, L., Dmitrienko, A., Fischer, T., and Sadeghi, A.-R., “Xmandroid: A new android evolution to mitigate privilege escalation attacks,” Tech. Rep. TR-2011-04, Technische Universitat Darmstadt, 2011.
25. Carbone, M., Cui, W., Lu, L., Lee, W., Peinado, M., and Jiang, X., “Mapping kernel objects to enable systematic integrity checking,” in Proceedings of the 16th ACM conference on Computer and communications security, CCS ’09, (New York, NY, USA), pp. 555–565, ACM, 2009.
26. Chen, H. and Wagner, D., “Mops: an infrastructure for examining security properties of software,” in Proceedings of the 9th ACM CCS, 2002.
27. Chen, S., Meseguer, J., Sasse, R., Wang, H. J., and Wang, Y.-M., “A systematic approach to uncover security flaws in gui logic,” in Proceedings of the IEEE Symposium on Security and Privacy, 2007.
28. Chin, E., Felt, A. P., Greenwood, K., and Wagner, D., “Analyzing inter-application communication in android,” in Proceedings of the 9th MobiSys, 2011.
29. Davi, L., Dmitrienko, A., Sadeghi, A.-R., and Winandy, M., “Privilege escalation attacks on android,” in Proceedings of the 13th ISC, 2010.
30. Dietz, M., Shekhar, S., Pisetsky, Y., Shu, A., and Wallach, D. S., “Quire: Lightweight provenance for smart phone operating systems,” in Proceedings of the 20th USENIX Security Symposium, 201

**PUBLICATION DETAILS**



**PLAGIARISM REPORT**





**INTERNAL QUALITY ASSURANCE CELL**

**PROJECT AUDIT REPORT**

This is to certify that the project work entitled “Intelligent system for identification of phishing emails and fake websites” categorized as an internal project done by D.MANOHAR REDDY, M.JAIHIND, D.V.SIVA REDDY , I.LAKSHMI PRIYANKA of the Department of Computer Science and Engineering, under the guidance of Mr.Sivamurugan.C during the Even semester of the academic year 2023 - 2024 are as per the quality guidelines specified by IQAC.

**Quality Grade**

**Deputy Director (IQAC)**

**Administrative Quality Assurance Director (IQAC)**