International Journal of Multidisciplinary Engineering in Current Research - IJMEC
Volume 8, Issue 12, December-2023, http://ijmec.com/, ISSN: 2456-4265

MULTI DESIGN AND IMPLEMENTATION OF MASS VACCINATION USING WEB APPLICATION

Dereddy Krishna Kuamr Reddy, Dr. Narsappa Reddy

[1]B.tech Student, Department Of Electronics and Computer Engineering, J.B Institute of Engineering and Technology

[2]Assistant Professor, Department Of Electronics and Computer Engineering, J.B Institute of Engineering and Technology

Abstract: Mass vaccination clinics are complex systems that combine professionals who do not typically work together. Coordinating vaccine preparation and patient intake is critically important to maintain patient flow equilibrium, requiring continuous communication and shared decision-making to reduce vaccine waste. Objectives: To develop a mobile application (app) that can address the information needs of vaccination clinic stakeholders for end-of-day doses decision-making in mass immunization settings; and to understand usability and clinical implementation among multi-disciplinary users. Methods: Contextual inquiry guided 71.5 hours of observations to inform design characteristics. Rapid iterative testing and evaluation were performed to validate and improve the design. Usability and integration were evaluated through observations, interviews, and the system usability scale. Results: Designing the app required consolidating contextual factors to support information and workload needs. Twenty-four participants used the app at four clinics who reported its effectiveness in reducing stress and improving communication efficiency and satisfaction. They also discussed positive workflow changes and design recommendations to improve its usefulness. The average system usability score was 87 (n = 22). Discussion: There is significant potential for mobile apps to improve workflow efficiencies for information sharing and decision-making in vaccination clinics when designed for established cultures and usability, thereby providing frontline workers with greater time to focus on patient care and immunization needs. However, designing and implementing digital systems for dynamic settings is challenging when healthcare teams constantly adapt to evolving complexities. System-level barriers to adoption require further investigation. Future research should explore the implementation of the app within global contexts.

Keywords: Decision support systems, human factors, mass vaccination clinics, mobile applications, usability testing

I. INTRODUCTION

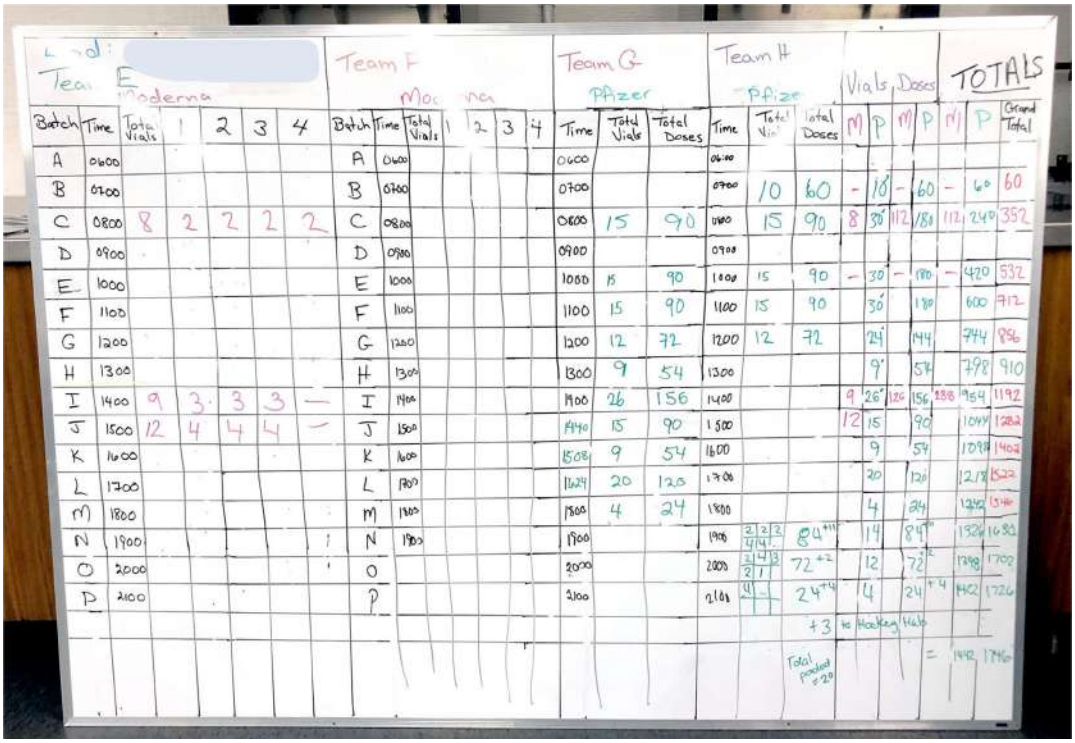
Vaccination clinics have been a successful and essential strategy for bringing the COVID-19 vaccines to the public quickly and effectively . Yet, they can also be stressful and chaotic for frontline workers, which may negatively impact the patient experience. Successfully managing a mass vaccination clinic involves coordinating and communicating information among stakeholders such as pharmacists, nurses, physicians, students, non-clinical staff, security staff, and volunteers in an environment where they may not usually work together so closely . These environments are also typically not designed for mass immunization or supporting the physical and cognitive demands for effectively, efficiently, and safely vaccinating large communities.

One critical task for coordinating a mass vaccine clinic involves managing open vial waste and end-of-day doses , which requires aggregating patient intake with vaccine preparation information while continuously determining the number of doses needed. This task becomes particularly challenging with variations that occur in patient intake, the number of doses available per vial for a vaccine brand, and the desire to minimize waste. While most of the work is completed manually (Figure 1) contributing to a high workload especially if errors occur in tracking or calculations, this demanding task reduces time for frontline workers to spend on maintaining patient safety and immunization needs and supporting medical emergencies.

II. LITERATURE SURVEY

This chapter offers an insight into various important studies conducted by excellent scholars from articles, books, and other sources relevant to the detection of phishing websites. It also provides the project with a theoretical review, conceptual review, and empirical review to demonstrate understanding of the project

A literature survey is an insightful article that presents the existing information including considerable discoveries just as theoretical and methodological commitments to a specific topic.



Mass vaccination clinic doses tracking whiteboard for a single-day vaccination event in the Region of Waterloo, providing two brands of the COVID-19 vaccine. Personal identifying information is redacted.

There is potential for supporting the cognitive workload associated with handling information that is constantly changing in dynamic healthcare settings through the design and implementation of electronic systems. A human factors approach, focusing on users within their work domain combined with systems science, has successfully supported technology design and development in other healthcare settings However, to the best of the authors'

knowledge, there are no implemented electronic systems augmenting decision-making aspects of vaccination clinics.

III. ANALYSIS

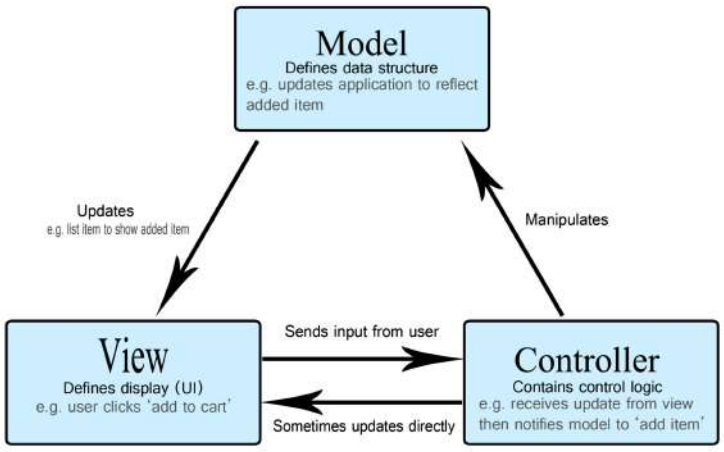
Feasibility study

This chapter describes the various process, methods, and procedures adopted by the researcher to achieve the set aim and objectives and the conceptual structure within which the research was conducted.

The methodology of any research work refers to the research approach adopted by the researcher to tackle the stated problem. Since the efficiency and maintainability of any application are solely dependent on how designs are prepared. This chapter provides detailed descriptions of methods employed to proffer solutions to the stated objectives of the research work.

According to the Merriam-Webster dictionary (11th.Ed), system analysis is "the process of studying a procedure or business to identify its goals and purposes and create systems and procedures that will efficiently achieve them". It is also the act, process, or profession of studying an activity (such as a procedure, a business, or a physiological function) typically by mathematical means to define its goals or purposes and to discover operations and procedures for accomplishing them most efficiently. System analysis is used in every field where the development of something is done. Before planning and development, you need to understand the old systems thoroughly and use the knowledge to determine how best your new system can work.

In ML and statistics, classification method is an approach involving supervised learning where computer program gains information from input and afterward utilizes this figuring out how to characterize new observations. Here are few classification techniques used in the detection of phishing URLs.



IV. DESIGN

System Modelling

System modeling involves the process of developing an abstract model of a system, with each model presenting a different view or perspective of the system. It is the process of representing a system using various graphical notations that shows how users will interact with the system and how certain parts of the system function. The proposed system was modeled using the following diagrams: i. Architecture diagram ii. Use case diagram iii. Flowcharts The proposed system will be implemented using Python Programming language along with different machine learning models and libraries such as pandas, scikit-learn, python who-is, beautiful-Soup, NumPy, seaborn, and matplotlib. Etc.

UML Diagram

Activity diagram is a behavioral diagram. The fig 4.5 shows the activity diagram of the system. It depicts the control flow from a start point to an end point showing various paths which exists during the execution of the activity.

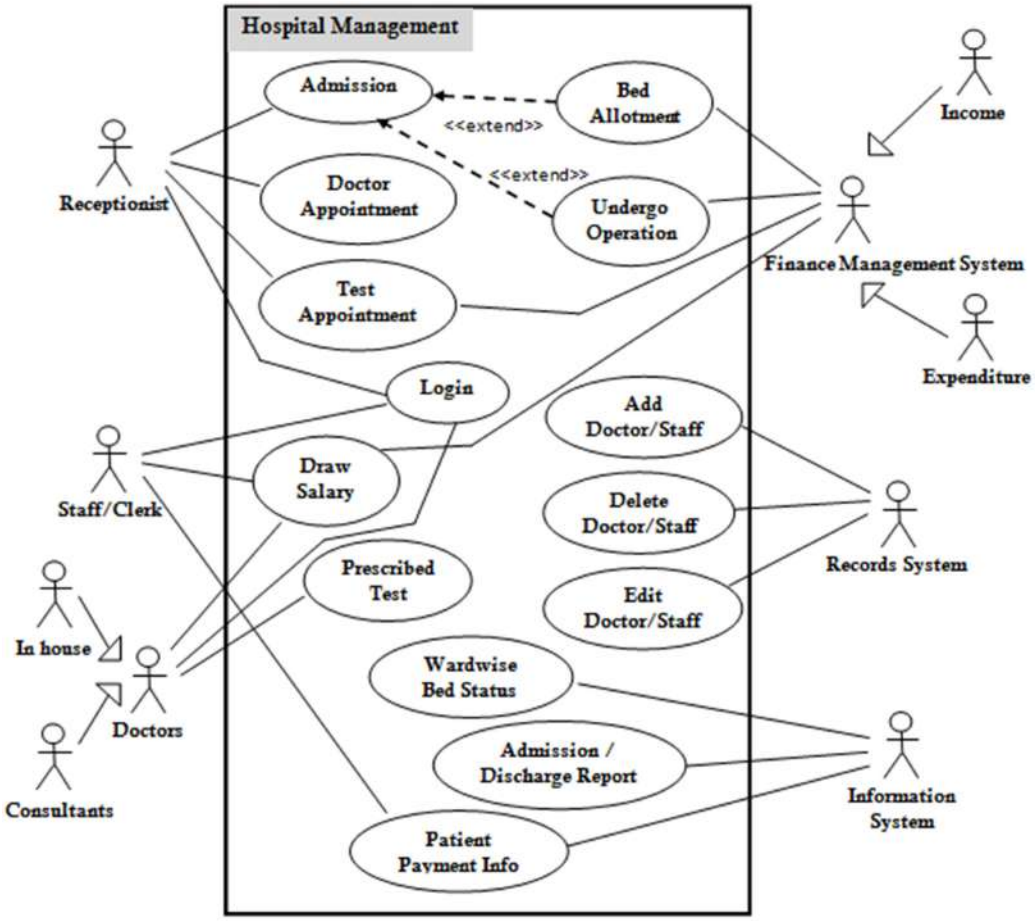
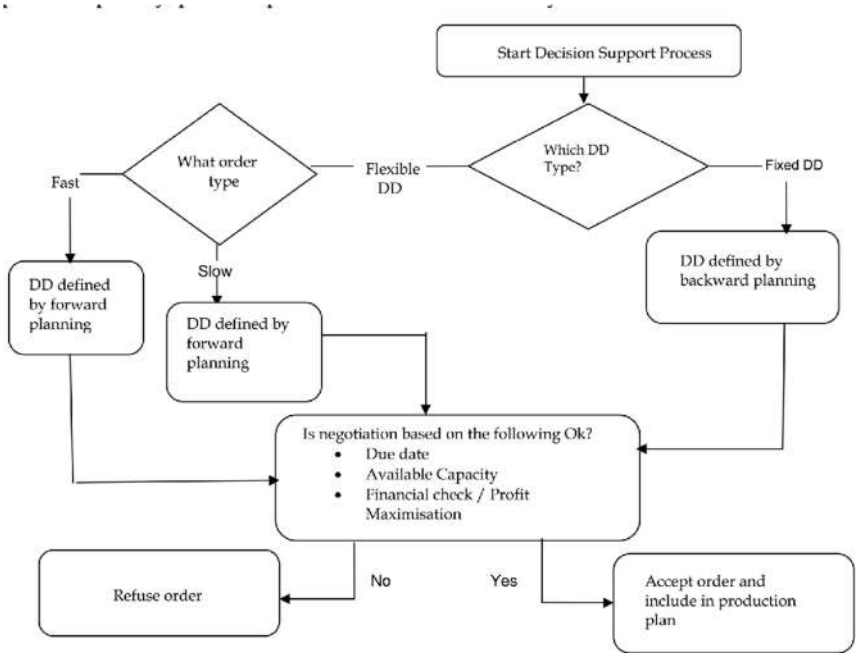


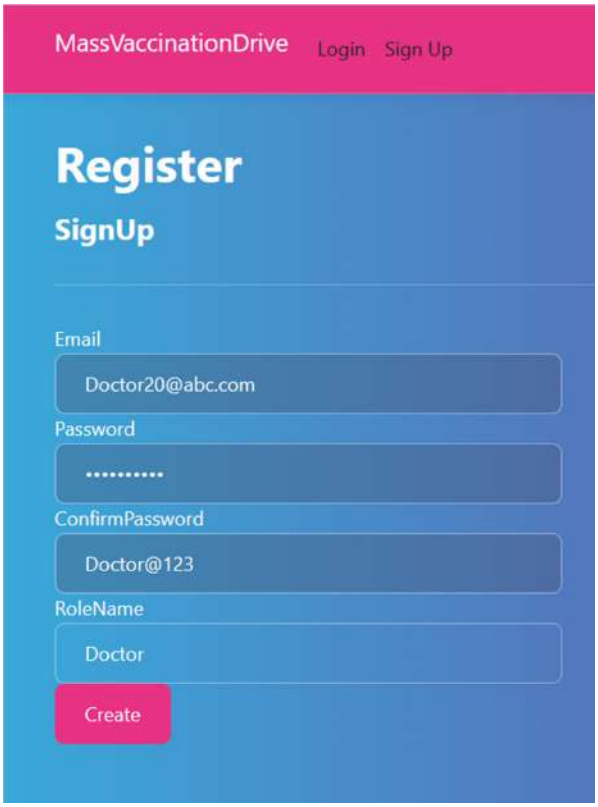
Figure 4.1: UML activity diagram

Data flow diagram



V. RESULTS AND DISCUSSIONS

Screen Shots



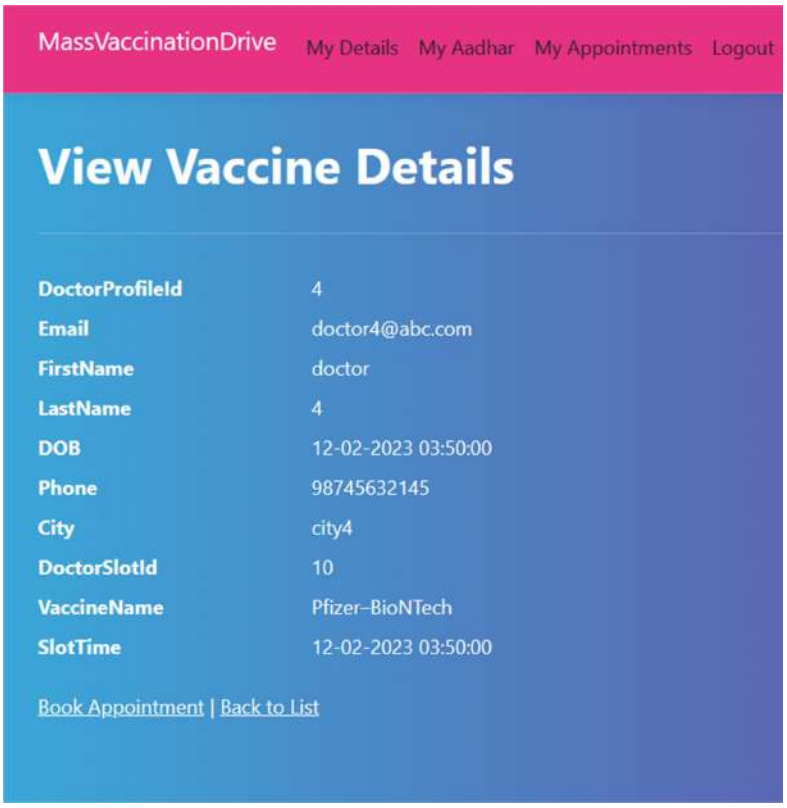
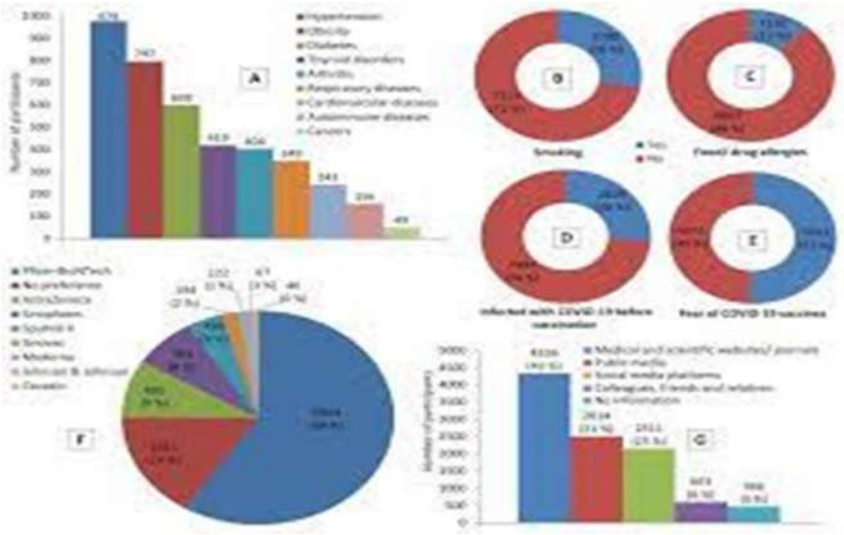


Table and Graphs of results

	Accuracy	Detection Rate
Existing System	76%	67%
Proposed System	96%	97.5%

Performance of the proposed system



Results comparison and graphs

The phishing scam in websites classification model is generated by implementing random forest algorithm, Logistic regression and support vector machine algorithms. The goal of this project is to compare the performance of different classifiers and find out the best approach for classification phishing and non-phishing website. These algorithms were implemented in python.

CONCLUSION AND FUTURE SCOPE

The demonstration of phishing is turning into an advanced danger to this quickly developing universe of innovation. Today, every nation is focusing on cashless exchanges, business online, tickets that are paperless and so on to update with the growing world. Yet phishing is turning into an impediment to this advancement. Individuals are not feeling web is dependable now. It is conceivable to utilize AI to get information and assemble extraordinary information items. A lay person, completely unconscious of how to recognize a security danger shall never invite the danger of making money related exchanges on the web. Phishers are focusing on installment industry and cloud benefits the most.

The project means to investigate this region by indicating an utilization instance of recognizing phishing sites utilizing ML. It aimed to build a phishing detection mechanism using machine learning tools and techniques which is efficient, accurate and cost effective. The project was carried out in Anaconda IDE and was written in Python. The proposed method used four machine learning classifiers to achieve this and a comparative study of the four algorithms was made. A good accuracy score was also achieved.

REFERENCES

[1] Reid G. Smith and Joshua Eckroth. Building ai applications: Yesterday, today, and tomorrow. AI Magazine, 38(1):6–22, Mar. 2017.

[2] Panos Louridas and Christof Ebert. Machine learning. IEEE Software, 33:110–115, 09 2016.

[3] Michael Jordan and T.M. Mitchell. Machine learning: Trends, perspectives, and prospects. Science (New York, N.Y.), 349:255–60, 07 2015.

[4] Steven Aftergood. Cybersecurity: The cold war online. Nature, 547:30+, Jul 2017. 7661.

[5] Aleksandar Milenkoski, Marco Vieira, Samuel Kounev, Alberto Avritzer, and Bryan Payne. Evaluating computer intrusion detection systems: A survey of common practices. ACM Computing Surveys, 48:12:1–, 09 2015.

[6] Chirag N. Modi and Kamatchi Acha. Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: a comprehensive review. The Journal of Supercomputing, 73(3):1192–1234, Mar 2017.

[7] Eduardo Viegas, Altair Santin, Andre Fanca, Ricardo Jasinski, Volnei Pedroni, and Luiz Soares de Oliveira. Towards an energy-efficient anomaly-based intrusion detection engine for embedded systems. IEEE Transactions on Computers, 66:1–1, Jan 2016. 53

[8] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang. Machine learning and deep learning methods for cybersecurity. IEEE Access, 6:35365– 35381, 2018.

[9] Neha R. Israni and Anil N. Jaiswal. A survey on various phishing and anti-phishing measures. International journal of engineering research and technology, 4, 2015.

[10] Pingchuan Liu and Teng-Sheng Moh. Content based spam e-mail filtering. pages 218–224, 10 2016.

[11] N. Agrawal and S. Singh. Origin (dynamic blacklisting) based spammer detection and spam mail filtering approach. In 2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC), pages 99–104, 2016.

[12] Vikas Sahare, Sheetalkumar Jain, and Manish Giri. Survey:anti-phishing framework using visual cryptography on cloud. JAFRC, 2, 01 2015.

[13] S. Patil and S. Dhage. A methodical overview on phishing detection along with an organized way to construct an anti-phishing framework. In 2019 5th International Conference on Advanced Computing Communication Systems (ICACCS), pages 588– 593, 2019.

[14] Dipesh Vaya, Sarika Khandelwal, and Teena Hadpawat. Visual cryptography: A review. International Journal of Computer Applications, 174:40–43, 09 2017.

[15] Saurabh Saoji. Phishing detection system using visual cryptography, 03 2015.

[16] C. Pham, L. A. T. Nguyen, N. H. Tran, E. Huh, and C. S. Hong. Phishing-aware: A neuro-fuzzy approach for anti-phishing on fog networks. IEEE Transactions on Network and Service Management, 15(3):1076–1089, 2018.

[17] K. S. C. Yong, K. L. Chiew, and C. L. Tan. A survey of the qr code phishing: the current attacks and countermeasures. In 2019 7th International Conference on Smart Computing Communications (ICSCC), pages 1–5, 2019. 54

[18] G. Egozi and R. Verma. Phishing email detection using robust nlp techniques. In 2018 IEEE International Conference on Data Mining Workshops (ICDMW), pages 7–12, 2018.

[19] J. Mao, W. Tian, P. Li, T. Wei, and Z. Liang. Phishing-alarm: Robust and efficient phishing detection via page component similarity. IEEE Access, 5:17020–17030, 2017.

[20] G. J. W. Kathrine, P. M. Praise, A. A. Rose, and E. C. Kalaivani. Variants of phishing attacks and their detection techniques. In 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), pages 255–259, 2019.

[21] Muhammet Baykara and Zahit Gurel. Detection of phishing attacks. pages 1–5, 03 2018. [22] Prof. Gayathri Naidu . A survey on various phishing detection and prevention techniques. International Journal of Engineering and Computer Science, 5(9), May 2016.

[23] E. Zhu, Y. Chen, C. Ye, X. Li, and F. Liu. Ofs-nn: An effective phishing websites detection model based on optimal feature selection and neural network. IEEE Access, 7:73271–73284, 2019.

[24] Mahdieh Zabihimayvan and Derek Doran. Fuzzy rough set feature selection to enhance phishing attack detection, 03 2019.

[25] P. Yang, G. Zhao, and P. Zeng. Phishing website detection based on multidimensional features driven by deep learning. IEEE Access, 7:15196–15209, 2019.

[26] T. Nathezhtha, D. Sangeetha, and V. Vaidehi. Wc-pad: Web crawling based phishing attack detection. In 2019 International Carnahan Conference on Security Technology (ICCST), pages 1–6, 2019.