JAIMT
JOURNAL OF ARTIFICIAL INTELLIGENCE AND MODERN TECHNOLOGY
ISSN: 1595-6261 VOLUME 5, ISSUE 1 (NOV.) 2025
A Peer Reviewed (Refereed) International Journal

USER INTERACTION (UI) SYSTEM FOR PHISHING DETECTION AND VOICE NOTIFICATION

Umejuru Daniel

Department of Computer Science, University of Port Harcourt, Choba, Nigeria

Email: daniel_umejuru@uniport.edu.ng,
https://orcid.org/0009-0007-9843-2248

ARTICLE INFORMATION

Received: 15th September, 2025
Accepted: 13th October, 2025
Published: 20th November, 2025

KEYWORDS: URL, Detection, Notification, Phishing, User Interaction

JOURNAL URL:
https://ijois.com/index.php/jobpef

PUBLISHER: Empirical Studies and Communication (A Research Center)
Website: www.cescd.com.ng

ABSTRACT

Phishing attacks pose a challenge to web user's world all over. These attacks from phishing URLs are many and very disturbing to internet users globally. The curiosity by well-meaning security professionals has led to further research, and thus propels the development of newer systems to solve this lingering challenge. The updated detection and notification systems which are User Interface (UI) friendly are been developed in other to curb the gaps of users experiencing phishing attacks via the Human-Computer Interaction (HCI) approach. This study demonstrates the use of a user interaction system for phishing URL detection and voice notification. A temporal tokenizer was also generated and used for URL text processing which scanned, recognized characters, symbols and redundant tokens. This made it easier to separate specific features from the URL address and return as a list while also identifying directories, keyword arguments, and extensions. VB.NET was used to at the front end while MYSQL database at the backend to accomplish system goals. The proposed system was tested and delivered satisfactory result demonstrating recommendable efficiency

INTRODUCTION

Phishing is an illegal activity that uses fraudulent behavior and technical deception to gain unauthorized access to client-confidential data from users or learning models. Phishing comprises spam mails disguised as genuine with a subject matter or message meant to trick the victims into disclosing sensitive information. In deceptive phishing, email alerts from credit card companies, security departments, banks, suppliers, online payment processors, or IT managers are utilized to take advantage of the uninformed open. The notification requests that the person receiving it, urgently enters or updates their personal data (Meenu 2018). The necessity for data privacy, protection, and prevention against phishing attempts cannot be overstated. Over the years, technological innovation has led to a significant increase in data through social networks (Jain et al., 2020), IoT gadgets, and online transactions. Phishing is one of the oldest techniques still in use today, despite the fact that cybercriminals are constantly coming up with novel methods to gain entry to networks, applications and data without authorization. Learning algorithms are susceptible to these phishing attacks, and hackers employ them to trick them in order to compromise ML detection power (Kumar et al., 2020). Phishing is a type of cybercrime that is expanding rapidly, and when people respond to messages or submit sensitive information to hackers, their data is put at risk (Iwendi et al., 2020).

Phishing

Phishing is a concept, comparable to fishing in which someone will send out hook in hopes that a user will catch it (Subasi and Kremic 2020). The phisher in this case, tricks users of the web into surfing the web so that they can steal sensitive user data. Phishing is the practice of an invader convincing a user, to divulge sensitive information while the scammer impersonates a reliable online platform in an effort to fool or deceive the user. The attacker would have access to all user information, making it easier for the targets to fall for the phisher's trap because they won't be able to tell the difference between legitimate and phishing sites (Shah et al., 2020). Scams such as phishing keep happening with a greater probability of succeeding than other types of attacks due to users' lack of information and awareness. Phishing attacks prey on people's vulnerabilities. It is getting harder to stop phishing attempts, but it is also crucial to develop new strategies for improving phishing detection methods.

Phishing Attacks

Attackers take a number of measures to gather user information. This may entail taking the subsequent actions: planning, compose text message (emails), attack, gather data and fraud (Shie 2020). The fraudster begins to prepare for an attack. The attacker chooses to create a genuine platform that must be replicated and chooses the unfortunate individuals whose data must be obtained. The attack setup platforms must appear to be real at the planning stage in order to entice victims into supplying sensitive information (Maurya and Jain 2020). The attacker or scammer will send text messages to them in the third stage in order to collect

information when the target has been duped by the phisher. The intruder carries out a digital crime like credit card fraud, theft, etc. with the victim's information.

Lifecycle of Phishing Attacks and Cyber Kill Chain

A framework called the "cyber kill chain" was created to describe the many stages of a cyber-attack (Pastor-Galindo et al., 2020). A kill chain includes every stage of an attack, from first access through execution. Among the well-known models created by Lockheed Martin, the Cyber Kill Chain model, which is still in use today by numerous businesses, demonstrates the model's wide spread adoption across a variety of industries that may or may not be connected to cyber security (Baig et al., 2021). As a result, it has demonstrated the stages of a perpetrator, a concept you can use as a model to begin securing your company in accordance with each stage of the cyber kill chain model (AL-Otaibi et al., 2020). The procedures that go into a cyber-attack as well as the steps that adversaries take to accomplish their objective are covered by the created "cyber kill chain". This framework can also be used to follow a phishing attempt, which can be broken down into the following steps:

Theoretical Framework

(a). **Deceptive phishing**: The most frequent type of phishing attack is deceptive phishing, which impersonates an actual platform or webpage and sends text messages (or emails) to the user that look to be authentic (Javed et al., 2020). The malicious links in these text messages (or emails) would instruct the recipient to click on the uniform resource locator URL. The phishing website that the attackers have set up will gather all of the user's login credentials and other sensitive information and send it to the attacker. For instance, the lower case "a" in the email address usercreditcard@amazon.com might be eliminated. Consequently, usercreditcard@mazon.com is used to deceive the user and obtain sensitive information.

(b). **Spear phishing**: The spear phishing attack is comparable to the deceptive phishing kind that only targets one user. The scammers aim to trick someone into giving them private information. A tailored message or email is delivered to the user with the intention of misleading them. The email is personalized to include most of the user's details, such as user name, workplace, designation, and so on (Jain et al., 2020). The most frequently used platform for spear phishing is the social media site like LinkedIn where it is simple for them to find out a user's occupation.

(c). **Whale phishing:** The whaling attack type happens when phishers seek people in positions of power, such as the CEO. Prior to the attack, the perpetrator would spend a great amount of time analyzing the target. The attacker sends an email message to target in order to manipulate them into providing confidential information. Whaling is considered as a very dangerous attack since the people in executive bands have access to the organization's most confidential information. The intruder sends these individuals an email message to trick the recipient into divulging private information (Kumar 2020). Whaling is regarded as a very hazardous attack because executive bands have the ability to access the most sensitive information about the company.

(d). **Pharming:** Pharming is a subset of phishing that does not require a specific person to be the target. Without needing to be specifically targeted, the attacker can harm a huge number of users. There are two techniques to carryout pharming attack: (a). It entails emailing the target codes that change every local host file on the system. The host files would change the URLs into number strings that the system would utilize to access websites. Even though the target user enters a legitimate URL, this may link them to a malicious website. (b). Another pharming attack technique is called DNS cache poisoning, which modifies the website's domain name system tables but leaves the local host files unharmed. This causes a target to be unknowingly diverted to inappropriate web pages. The user would think they are visiting a reliable website, but due to poisoning of the DNS, they would actually be visiting a hostile domain (Mittal et al., 2020).

Phishing Attack Detection Techniques

The use of classification techniques like Artificial Neural Networks (ANN), K-Nearest Neighbors (KNN), and Decision Trees as a method to reduce phishing attacks has been discussed in a number of relevant studies. Alkhalil et al. (2021) conducted study on the phishing attack's lifecycle. His report examines the attack's stages' anatomy, the traits of phishing victims, risks, weaknesses, and cutting-edge phishing tactics. The author supports the significance of raising anti-phishing awareness and developing a better system.

Methodology

VB.NET (Visual Basic.Net) is the adopted methodology used to develop the application. It was used because it is a multiple-paradigm object oriented programming language. It encompasses encapsulation, inheritance and polymorphism and fondly used by programmers because of its vast libraries and functionalities, which allows developers build a wide range of applications, including desktop applications and also web application as applied in this paper.

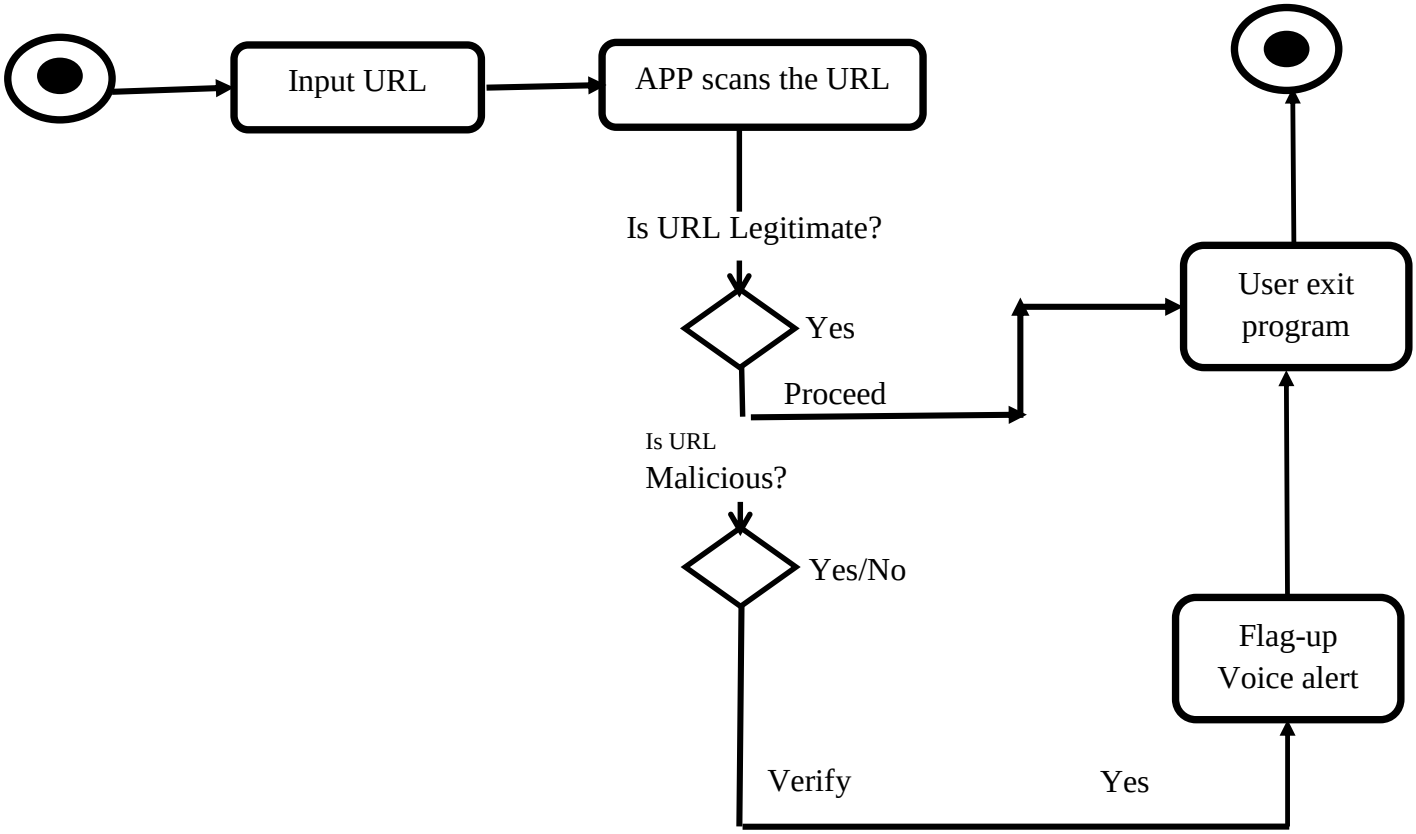

Figure 3.1: Activity Diagram of the System

Activity Diagram depicts the flow of activities. A running non-atomic processing within a state machine is referred to as an activity. An activity results in an action, a change in state, or the return of a value. Activity Diagrams frequently include: activity states, action states, and transitions. It may also have nodes and constraints. Action stages and activity states: An action state is an executable atomic computation that cannot be disassembled. In the Activity diagram below, the process is started, after which the datasets are being loaded and immediately after that, the App scans for URL. If URL isn't present, the process returns to inception for re scanning but if present, it proceeds further to check if URL is legitimate and if yes, the activity flows but if no, it proceeds to flag up a voice alert to notify user of phishing attack detection after which user can exit program.

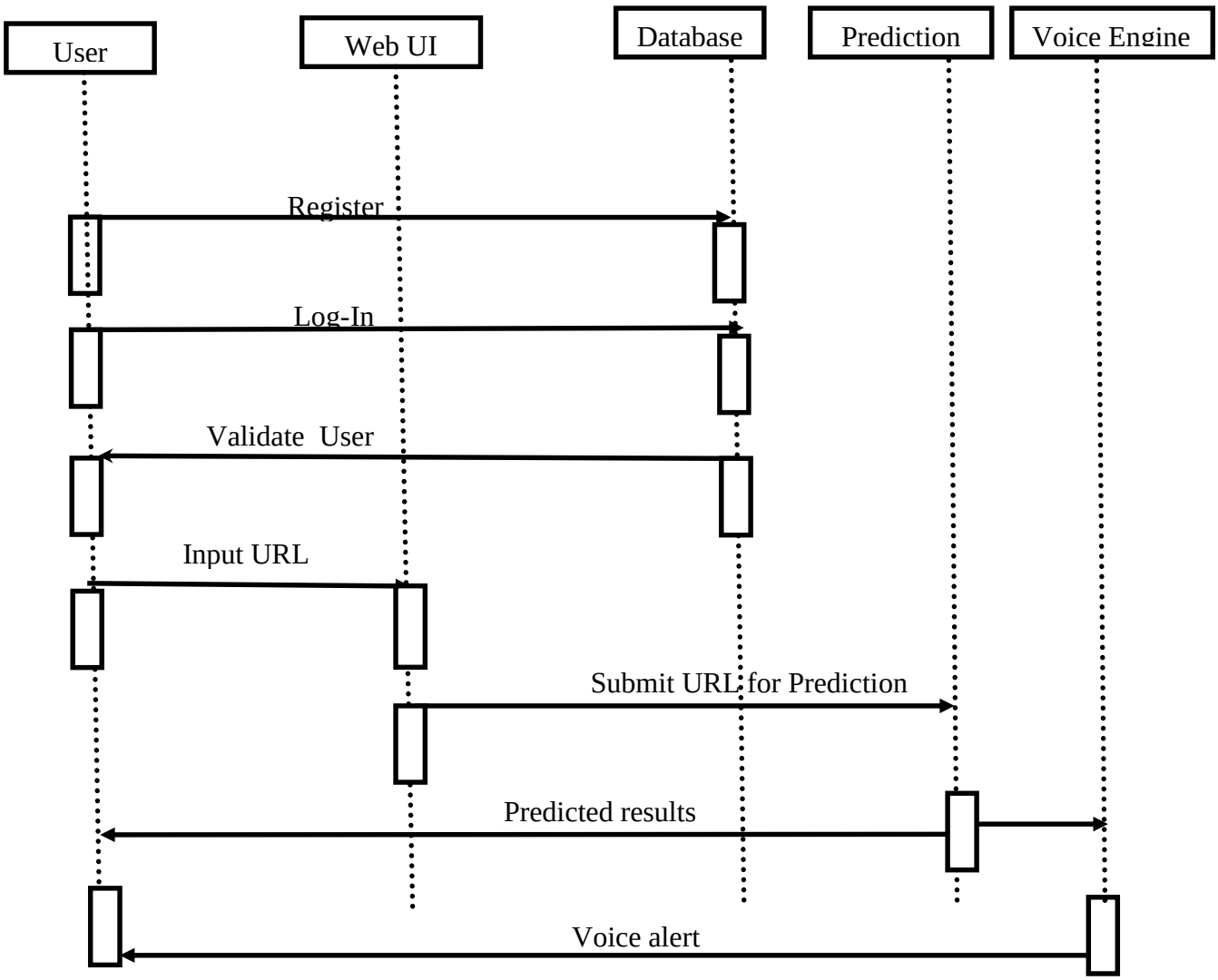

Figure 3.2: Sequence Diagram of the User Interaction

Sequence Diagram showing the step by step sequence of the proposed model. The models sequence diagram which is known as **User Interaction** for the GUI shows how the user interacts with the Web user interface. From the diagram, the user undergoes registration which

is saved directly to the database, after which user logs in upon matching login features and then user gets validated and proceeds to input URL through the web UI. Going further, the URL is being submitted for prediction and predicted results are fed back to user to check if legitimate, or if phishing is also being detected. Finally, user is being notified as voice engine aids to flag up voice alert to user for prompt notification and classification from model, to be either a malicious or trusted URL.

4.0 Results and Discussion

The suggested system used the required programming language VB.NET for the GUI at the front end with MYSQL database at the backend to accomplish system goals.

Figure 4.1: Splash Screen

Figure 4.1 depicts the program splash screen, the first phishing site detection software interface with a progressive bar which displays the percentage that runs from 1 to 100%. The steps vary from 1% to 100%, and the user will be prompted to wait until the user log-in screen appears after it reaches 100%. This is the splash screen that appears when a program is initially launched to notify the user that it has been loaded. The loading progresses as shown in the progressive bar.

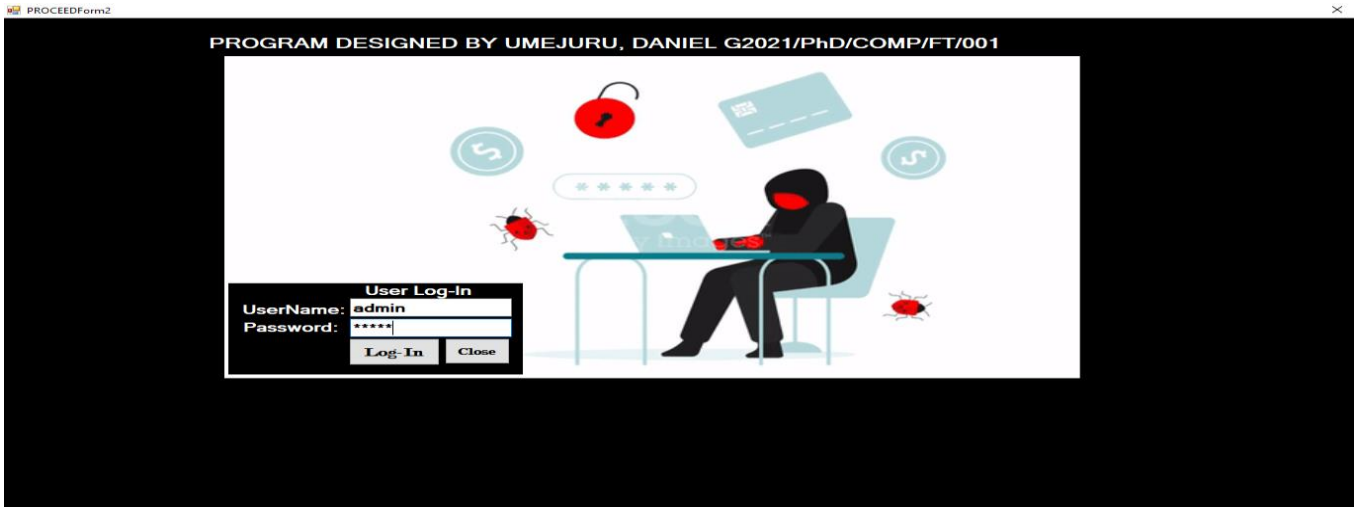

Figure 4.2: Log-in Menu

Figure 4.2 depicts the user log-in menu for usersto supply user name and password; if they match, access will be granted; otherwise, access to the program main menu is denied. If the user enters the wrong user name or password, the application logs off user; but if password matches grants user an authorized access.

Figure 4.3: Program Main Menu

Figure 4.3 shows the program main menu, which has the register menu, report and exit icon. The phishing site registration and prediction icons are found in the pull-down menu of registration panel. The registration pull-down menu simply includes URL site registration and

detection while the report pull-down menu includes URL registration, detection and URL statistics.

Figure 4.4: Phishing URL Address Detection Form

The URL address registration form acquired from the registration module is shown in Figure 4.4 the registration form includes fields URLID, URL address, number of dots, number of dash, atsymbol, URL length, number of underscores, ampersand, hash, percentage symbols, www, number of digits, letters, target and etc. The user is instructed to click analysis and detect icons to search for the most prevalent symbols used by attackers in URL addresses for phishing.

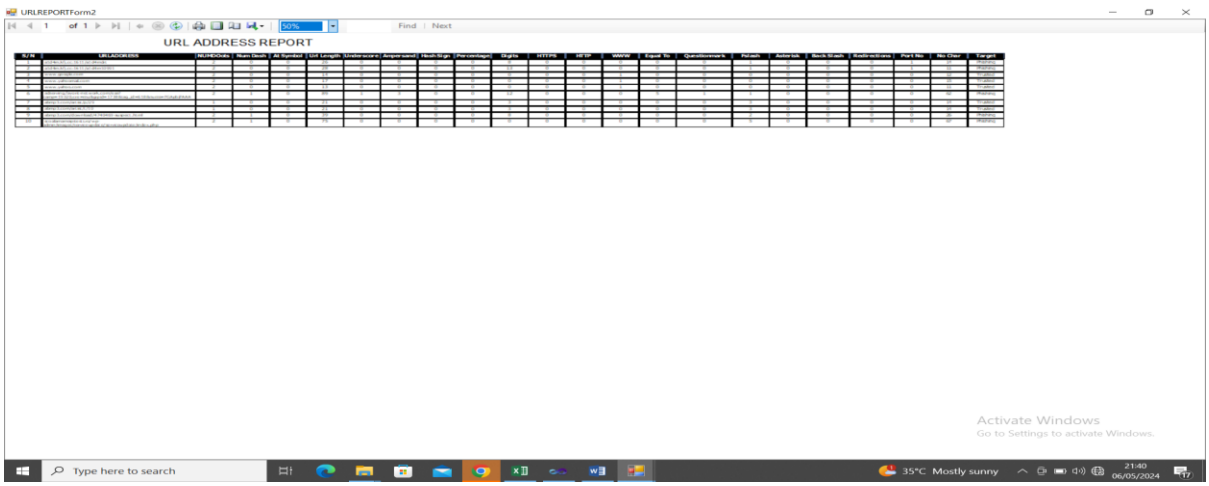

Figure 4.5: URL Address Registration Report

Figure 4.5 above shows URL address registration report with the attributes: URLID, URL address, number of dots, number of dash, atsymbol, URL length, number of underscores,

ampersand, hash, percentage symbols, www, number of digits, letters, target and etc as displayed using VB.NET report viewer control tool. The user has been granted some administrative rights like converting of reports to PDF format, excel or other database supported formats, with an interactive report viewer tools to zoom in/out.

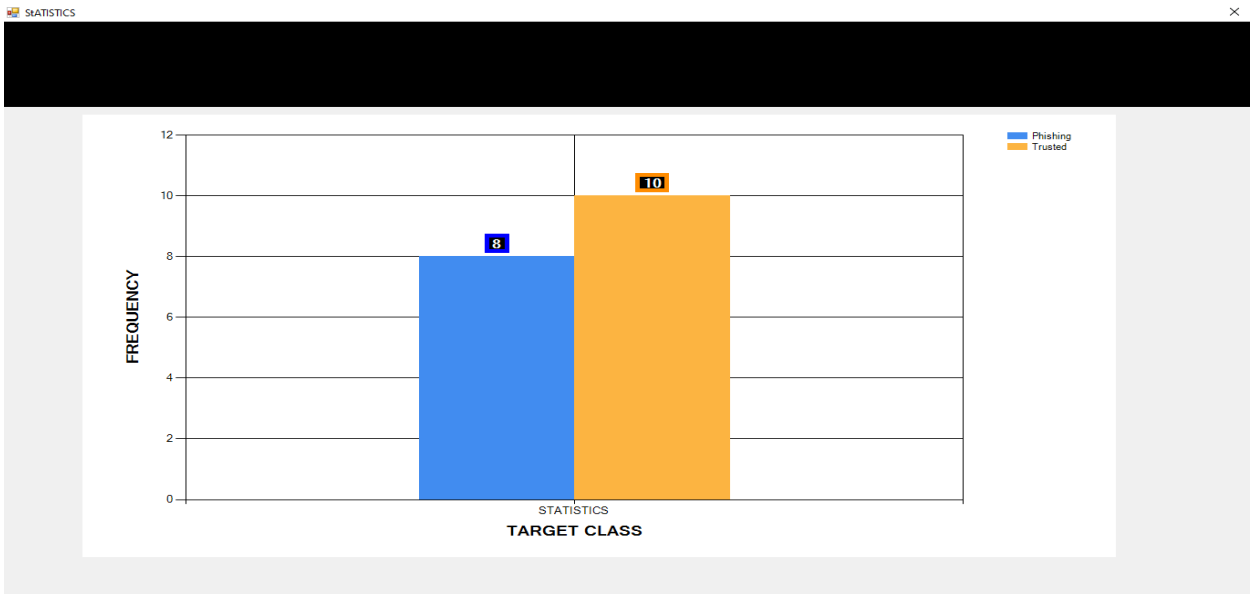

Figure 4.6: Statistic Update Graph

Figure 4.6 above, shows the Statistics update graph with attibutes frequency by target class. It shows the updated record for all phishing or trusted URLS as detected by the system and this helps, to keep a track record of how many phishing or trusted URLS the system has analyzed. From the record above, the system has successfully detected 10 trusted and 8 phishing URLS and this is always updated immediately detection is carried out.

5.0 Conclusion

The user interaction system for phishing URL detection and voice notification is a VB.Net application that was coded to detect phishing or trusted URLs. This is done by inputting the desired URL address and then system checks with the parameters of the URL which are URLID, URL address, number of dots, number of dash, atsymbol, URL length, number of underscores, ampersand, hash, percentage symbols, www, number of digits, letters, target as coded to confirm and based on the checks done; the system detects the URL as either phishing or trusted and gives a target result accompanied by a voice notification to the user which is done for prompt notification. This system is reliable and very efficient as tested and shown, and can be used by individuals and cooperate entities for detection and notification of malicious URLs. It can also be embedded in an anti-virus as an added application.

URLS	CLASS
diaryofagameaddict.com	Phishing
slightlyofficer.net	Trusted
yahoo.com	Trusted
diaryofagameaddict.com	Phishing
divineenterprises.net	Trusted
slightlyofficer.net	Trusted
Kalantzis	Phishing
yahoo.com	Trusted
espdesign.com.au	Phishing
iamagameadict.com	Phishing
rupor.info	Phishing
svision-online.de/mgfi/administrator/components/com_babackup/classes/fx29id1.txt	Phishing
officeon.ch.ma/office.js?google_ad_format=728x90_as	Phishing
sn-gzzx.com	Phishing
sunlux.net/company/about.html	Phishing
outporn.com	Phishing
timothycopus.aimoo.com	Phishing
xindalawyer.com	Phishing
freeserials.spb.ru/key/68703.htm	Phishing
deletespyware-adware.com	Phishing
orbowlada.strefa.pl/text396.htm	Phishing
ruiyangcn.com	Phishing
zkic.com	Phishing
adserving.favorit-network.com/eas?camp=19320;cre=mu&grpid=1738&tag_id=618&nums=FGApbjFAAA	Phishing
cracks.vg/d1.php	Phishing
juicypussyclips.com	Phishing
nuptialimages.com	Phishing
andysgame.com	Phishing
bezproudoff.cz	Phishing
ceskarepublika.net	Phishing
hotspot.cz	Phishing
gmcjjh.org/DHL	Phishing
nerez-schodiste-zabradli.com	Phishing
nordiccountry.cz	Phishing
nowina.info	Phishing
obada-konstruktiwa.org	Phishing
otylkaaotesanek.cz	Phishing

pb-webdesign.net	Phishing
pension-helene.cz	Phishing
podzemi.myotis.info	Phishing

REFERENCES

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Frontiers in Computer Science, 10(6), 1-10, https://doi.org/10.3389/FCOMP.2021.563060.

AL-Otaibi, A. F. and Alsuwat, E. S.(2020) A study on social engineering attacks: phishing attack, International Journal of Recent Advances in Multidisciplinary Research, 7(11), 6374-6380.

Baig, M. S. Ahmed F. and Memon, A. M.(2021) Spear-Phishing campaigns: Link Vulnerability leads to phishing attacks, SpearPhishing electronic/UAV communication-scam targeted, 2021 4th International Conference on Computing & Information Sciences (ICCIS), 1-6, doi: 10.1109/ICCIS54243.2021.9676394.

Iwendi, C. Jalil, Z. Javed, A. R. Reddy, T. Kaluri, R., and Srivastava, G. J. O. (2020) Keysplitwatermark: Zero watermarking algorithm for software protection against cyber-attacks. *IEEE Access,* 8, 72650–72660. doi: 10.1109/ACCESS.2020.2988160

Jagatic, T. Johnson, N. Jakobson, M. Menczer, F.(2020) Social phishing", Communications of the ACM, 50(10), 1-20.

Jain, A. K., Parashar, S., Katare, P., & Sharma, I. (2020). Phishskape: A content based approach to escape phishing attacks. *Procedia Computer Science*, *171*, 1102–1109.

Jain A. K. &Gupta, B. B.(2020). A Novel Approach to Protect Against Phishing Attacks at Client-Side Using Auto-Updated White-list, EURASIP Journal on Information Security, 16(1), 9.

Jain, A. K, Yadav, S. K. and Choudhary, N.(2020) A novel approach to detect spam and smishing SMS using machine learning techniques, International Journal of E-Services and Mobile Applications (IJESMA), 12(1), 21-38.

Javed, A. R., Jalil, Z., Moqurrab, S. A., Abbas, S., and Liu, X. (2020), Ensemble adaboost classifier for accurate and fast detection of botnet attacks in connected vehicles, *Transactions on Emerging Telecommunications Technologies*, 45.

Kumar, A., Chatterjee, J. M., & Díaz, V. G. (2020). A novel hybrid approach of svm combined with nlp and probabilistic neural network for email phishing. International Journal of Electrical and Computer Engineering, 10(1), 486.

Kumar, J., Santhanavijayan, A. Janet, B., Rajendran, B. and Bindhumadhava, B. S. (2020) Phishing website classification and detection using machine learning, International Conference on Computer Communication and Informatics(ICCCI), 45, 3-20.

Maurya, S. and Jain, A. (2020). Deep learning to combat phishing, *Journal of Statistics and Management Systems*, 1–13.

Meenu, S. G.(2018) An enhanced phishing email detection model using machine learning techniques, International journal of emerging technologies and innovative research, 11(5), 523-529, 2018.

Mittal, M., Iwendi, C., Khan, S., and Rehman-Javed, A. (2020). Analysis of security and energy efficiency for shortest route discovery in low-energy adaptive clustering hierarchy protocol using Levenberg–Marquardt neural network and gated recurrent unit for intrusion detection system. *Transactions on Emerging Telecommunications Technologies*, p. e3997.

Pastor-Galindo, J., Nespoli, P., Mármol, F. G. and Martínez Pérez, G. (2020) The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends, in IEEE Access, 8, 10282-10304, doi: 10.1109/ACCESS.2020.2965257.

Shah, B., Dharamshi, K., Patel, M. and Gaikwad, V.(2020) Chrome Extension for Detecting Phishing Websites, International Research Journal of Engineering and Technology (IRJET) 07(03), 40.

Shie, E. W. S. (2020). *Critical analysis of current research aimed at improving detection of phishing attacks,* Selected computing research papers, p. 45.

Shirgave S., Awati C., More R., and Patil S.(2019) A Review on Credit Card Fraud Detection Using Machine Learning, International Journal of Scientific and Technology Research, 8(10), 1217-1220.

Subasi, A., and Kremic, E. (2020). Comparison of adaboost with multiboosting for phishing website detection. Procedia Computer Science, 168, 272–278.

Sundara, P. S., Prabha,S., Vijay, K. B., Julian, B. P. and Kanmani, P.(2022) Phishing attack detection using Machine Learning, Measurement: Sensors, 24, 100476..

Zhang, Y., Hong, J. I., & Cranor, L. F. (2020). Cantina: a content-based approach to detecting phishing web sites. In Proceedings of the 16th international conference on World Wide Web, ACM, 639-648.