Phishing Detection Implementation using Databricks and Artificial Intelligence

Dinesh Kalla
Microsoft | Colorado Technical University
Charlotte, NC 28273

Fnu Samaah
Northeastern Illinois University Harrisburg University
Desplaines, IL 60016

Sivaraju Kuraku, PhD
Uptycs | University of the Cumberlands
Austin, Texas 78758

Nathan Smith
Colorado Technical University
San Diego, California

ABSTRACT
Phishing is a fraudulent activity that includes tricking people into disclosing personal or financial information by impersonating a legitimate company or individual. The increasingly complex nature of phishing has drawn the attention of criminals, who see it as a profitable and simple way to get sensitive information. As a result of the negative impact of phishing assaults on both individuals and companies, efficient detection and prevention measures have been developed. This document overviews numerous approaches for detecting and thwarting phishing attacks. The research introduces the Phishcatch algorithm, which has shown substantial success in identifying phishing emails and alerting consumers to fraudulent attempts. Phishcatch studies user behavior on websites and limits access if any suspicious behavior is found. Phishcatch is a vital instrument in the battle against phishing attempts, with an accuracy and detection rate of 90%. Furthermore, this article explains the steps in developing, testing and implementing successful anti-phishing algorithms.

General Terms
Pattern Recognition, Security Awareness, Stemming and Lemmatization, Cyber Security, Spam Detection, stop words.

Keywords
Phishing, NLTK, Natural Language Processing, Azure Databricks, Spam, Security Situational Awareness, Credential Theft, Python, Machine Learning, Stemming and Lemmatization, Naïve Bayes, Artificial Intelligence.

1. INTRODUCTION
Phishing is a cyber-attack that uses deceit to steal sensitive information from unsuspecting persons, such as passwords or credit card details [1]. This is usually accomplished by creating a phony website or email that looks authentic to deceive people into submitting their personal information [1]. Phishing assaults have been proven to have disastrous outcomes for individuals and corporations. Phishing is predicted to cost the US economy billions yearly [1]. Companies pay direct costs associated with phishing attacks, such as data breaches and productivity loss, while consumers bear indirect costs, such as higher pricing for goods and services [1]. Furthermore, phishing may have severe consequences for individuals, including financial ruin and mental misery.

In the United States alone, phishing attempts cost more than $5 billion in damages in 2018, with businesses bearing the brunt of the losses due to the theft of client data or financial information [1]. Furthermore, these companies frequently suffer brand harm, which causes customers to switch to competing products [1]. Fines are enforced on entities such as healthcare institutions that fail to protect sensitive customer information following regulations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) [1]. Even though anybody may be a victim of phishing, people should be aware of the warning signals of phishing attempts and only supply personal information when they are confident they are dealing with a trustworthy website or organization.

However, the Phishcatch algorithm is one way that can help secure sensitive information internationally, notably in the United States, where phishing causes significant financial losses [1]. The Phishcatch algorithm uses a combination of heuristics and machine learning approaches that are constantly updated to increase its effectiveness [1]. The Phishcatch algorithm has a significant benefit in that it does not rely on signatures or known URLs to detect phishing attempts, making it very successful against new and unknown assaults [12]. Furthermore, the Phishcatch algorithm can detect cross-site scripting (XSS) and man-in-the-middle (MitM) assaults, both of which are becoming more common [12]. The Phishcatch algorithm, which has shown to be a powerful weapon in the battle against phishing, has already been used by several significant corporations. The Phishcatch algorithm's continued growth and enhancement will likely play an important role in protecting sensitive information in the future.

Businesses that accept online payments or have an extensive client base are more likely to be targeted by phishers since they have valuable data [13]. Furthermore, firms that have recently been the victim of a security incident or data breach may be targeted to exploit prospective weaknesses. It is proposed that the PhishCatch algorithm, which employs Machine Learning and the Natural Language Toolkit (NLTK) package, be used to increase the application's performance [3]. Machine learning and artificial intelligence can dramatically improve the Phishcatch algorithm's capacity to detect and thwart phishing assaults. The NLTK library is vital in constructing machine learning models [5]. Emotet is one of the most recent growing cybersecurity threats [18]. As a result, numerous businesses have been tasked with developing a PhishCatch algorithm that uses machine learning and natural language processing to battle the growing volume of phishing emails and cyber threats.

2. PHISHING MECHANISM
Phishing assaults generally carried out using a misleading email with a link to download an infected file, are one of the most common forms of malware [1]. When the user clicks on the link, the virus is triggered and can execute on the user's machine. The characteristics of this sort of malware vary depending on the operating system in use. For example, there are two sorts of Windows viruses: those that penetrate systems using a web browser, known as a "drive-by download," and

those that enter the system via a file downloaded from the internet, known as an "injector" [1].

Regardless of how a phishing assault is carried out, all approaches entail some kind of deceit. Attackers may, for example, send an email purporting to be from a respected institution and request that the receiver click on a link or open an attachment. This link might take the victim to a bogus website designed to steal sensitive information, or the attacker could directly request personal information via a form or email response [1]. Phishing attacks are usually difficult to detect because attackers typically employ genuine-looking logos and graphics in their communications. However, grammatical problems or the sender's email address that does not match the organization's name might be indicators of a phishing email [1].

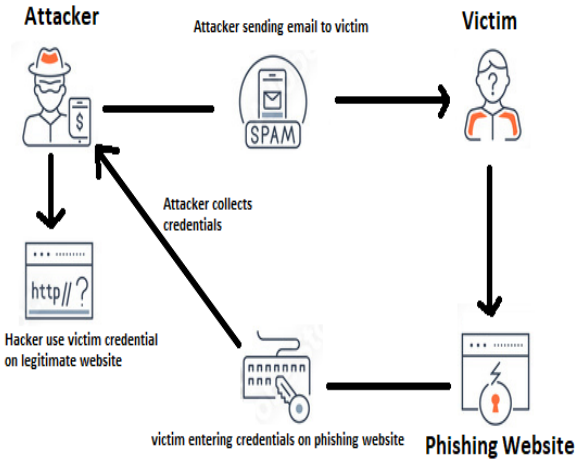

Fig 1: Phishing Mechanism

Phishing attacks are carried out by attackers that send unsolicited communications to users to deceive them into opening an attachment or clicking on a link that may contain malware [3]. The attacker can write the email by hand or use an automated program. These emails frequently come from reputable sources like banks, media sites, or government agencies. They may include attachments that appear to be vital updates or significant information but are actually harmful links or downloads [1]. Such emails are often intended to abuse employees' welfare, such as the promise of better working conditions or a pay raise.

To be successful, phishing attempts must get sensitive information such as usernames and passwords. In phishing assaults, passwords are typically the most targeted information. Attackers also require computer access to conduct phishing assaults, either by sending emails with dangerous attachments or by installing malware on the victim's computer using remote access tools (RATs) [3]. The attackers gather information by disseminating their email addresses, malicious links, and files to understand better how people use their computers and what kind of data they keep online. Following the click of the link, attackers may exploit other vulnerabilities in the compromised machine, such as remote access tools or web browser exploits, to steal victims' financial information, such as bank account numbers and credit card details [1].

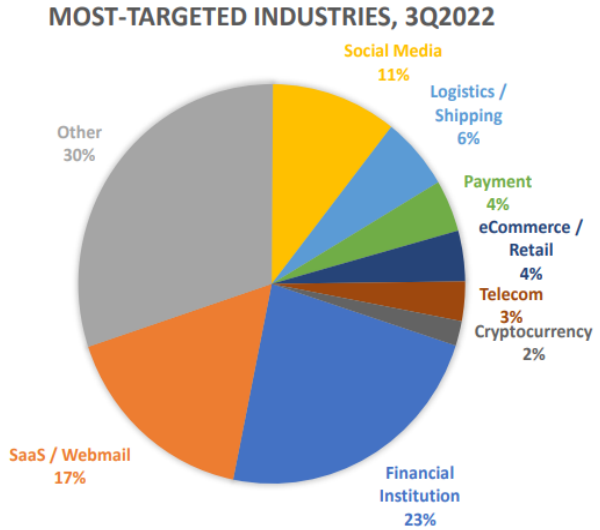

Fig 2: Most Targeted Industries (APWG Q3Report,2022)

Phishing attacks are a continuous and broad danger to individuals and organizations, with some industries being more actively targeted owing to the volume of sensitive information they contain [11]. Financial institutions, social networking platforms, and SaaS/Webmail providers are among the most often targeted businesses due to the vast quantities of personal and financial data they collect that may be exploited to conduct fraud or identity theft [11]. Attackers can acquire access to client credit cards and bank account information and email correspondences by exploiting holes in these firms' security systems [11]. The attackers' primary goal is to get passwords and usernames that may be utilized to compromise the resources and infrastructure of these businesses. However, businesses such as Bitcoin, which have a robust security structure and have yet to be effectively hacked, are not popular targets [11]. Other industries, such as transportation, telecommunications, and eCommerce, may be less commonly attacked since they need more data to be infiltrated, resulting in a significant loss of resources and a compromised security system [11].

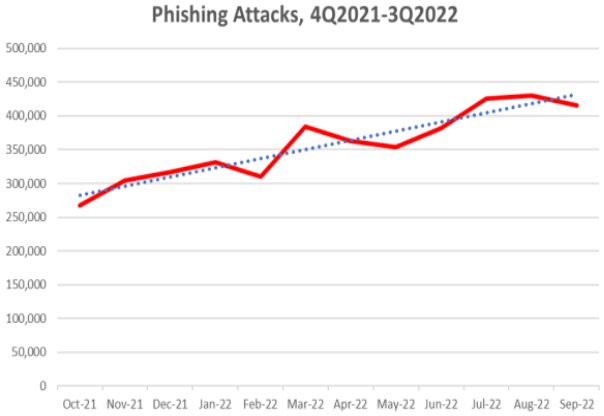

Fig 3: Phishing Attacks 2021-2022 (APWG Q3Report,2022)

From October 2021 to September 2022, the graph above shows a continuous increase in phishing assaults. The number of phishing events increased in the second half of 2021, reaching over 3,000 attacks per day, according to the APWG Trends Report Q3 2022 [4]. This is a concerning trend since attackers are persistent and growing more skilled. According to the

survey, phishing assaults mainly target corporate personnel via social media sites like LinkedIn and Facebook. This method works because many employees have personal profiles on these platforms, and attackers know that if they are already linked with someone at the firm, they are more likely to click on a link or attachment. The increased usage of the internet by organizations and consumers is to blame for the increase in cyberattacks. Cybercriminals use advanced social engineering techniques to trick their victims into clicking on malicious links or opening infected files that appear legitimate files from trusted parties such as banks or email providers, exposing them to malware infections such as ransomware or banking Trojans.

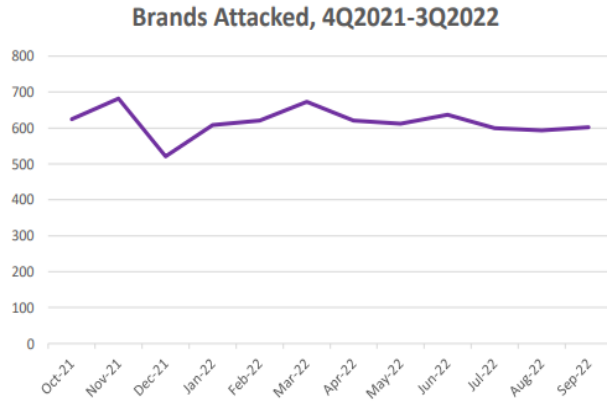

Fig 4: Brands Attacked 2021-2022 (APWG Q3Report,2022)

Phishing assaults on e-commerce and retail enterprises decreased in the third quarter of 2020, but attacks on SaaS stayed constant. This rise might be ascribed to the influence of COVID-19, which required more individuals to work online, creating a bigger pool of possible targets for attackers [1]. Financial institutions were the most targeted industry, accounting for 23.4% of assaults. However, this was down from 27.6% in the previous quarter. Interestingly, December had the fewest phishing assaults of any month, most likely because many businesses take a vacation over the holiday season, giving less potential for attacks [1]. Companies should continually monitor changes in attacker technology and tactics to keep up with developing threats.

3. DIFFERENT TYPES OF PHISHING

3.1 Search Engines Phishing

Phishing through search engines is a technique that uses Google and Bing software to add malicious links to the search engine results pages (SERPs). These malicious links are designed to look like real ones and lure users into clicking them. Phishing through search engines has been around for years, but it is become more common recently due to the increased use of mobile devices and social media platforms like Facebook and Twitter.

3.2 Vishing

Vishing is a phishing assault in which a fraudster calls or texts the victim using their phone number or other information, such as their name and address [1]. The attacker may pretend as an employee of a well-known corporation, such as Apple or Verizon, or a government body, such as the IRS, and ask the victim personal identifying questions [1]. The attacker aims to get sensitive information from the victim, which he or she may subsequently sell on the black market or use to perpetrate identity theft against the victim [1].

Vishing attacks can be challenging to detect because the attacker may employ sophisticated ways to seem official, such as faking the phone number to match the actual organization or agency they claim to represent [1]. Victims may also trust a phone call or text message more than an email or website, rendering them more vulnerable to assault [1].

To avoid vishing attacks, being wary of unsolicited phone calls or text messages is critical, especially if they appear to be from a well-known organization or agency [1]. Personal information, such as passwords or social security numbers, should only be given over the phone or text message if the caller's identity can be verified [1]. If someone has doubts or suspicions, contact the firm or agency immediately using a recognized and trustworthy phone number [1]. Individuals may reduce their vulnerability to vishing attacks and protect their personal and financial information by being aware and taking the required steps.

3.3 Smishing

Smishing is sending fraudulent text messages with URLs that look legitimate but lead to fraud, malware, or other types of cyberattacks [7]. The communications might be sent by attackers impersonating reputable persons, such as business acquaintances, to gather sensitive information like income or working circumstances. Smishing attacks are potent because they use social engineering tactics to generate a feeling of urgency and encourage the victim to act without investigating the message's legitimacy. Individuals and companies can suffer significant repercussions from these assaults, including identity theft, financial loss, and data breaches. As a result, individuals and companies must be aware and take precautions against these sorts of attacks.

3.4 Key logger

Keylogging is capturing every keystroke a computer user makes to obtain sensitive information such as credit card numbers or passwords [2]. The stolen data is typically preserved in a log file for the attacker to retrieve later. Notably, most keylogging data is retained on websites without two-factor authentication, making it more straightforward for attackers to get unauthorized access to critical information [2]. This type of cyber assault, which can result in serious repercussions such as identity theft and financial loss, is frequently used as a weapon for corporate espionage or to get access to sensitive information saved on a victim's computer. As a result, it is critical for computer users to apply robust security measures to protect themselves against keylogging assaults, such as utilizing antivirus software and avoiding questionable internet downloads.

3.5 Social Engineering

Social engineering is a common phishing technique that includes leveraging victims' trust or gullibility to deceive them into disclosing personal information [17]. To persuade victims to provide their passwords or account numbers, attackers may masquerade as customer care representatives or employ other deceit. Unlike other phishing strategies that rely on infrastructure penetration, social engineering persuades individuals to access crucial information willingly. The efficacy of social engineering strategies is based on their capacity to affect victims' psychology and instill a sense of urgency or trust in them, motivating them to reveal sensitive information [18]. Individuals and organizations must thus be aware of the many types of social engineering strategies and take caution when dealing with unknown sources or revealing personal information.

3.6 Domain spoofing

Domain spoofing is a typical phishing method in which attackers establish fake websites that seem identical to authentic ones to collect sensitive information from unsuspecting victims [5]. These websites are meant to appear and feel like the real thing, making it impossible for consumers to tell the difference. Attackers can employ a variety of ways to attract people to their fake websites, such as phishing emails or social media messages with a link to the false website. When a user inputs their login credentials or other sensitive information on the faked website, the attackers can gather and exploit this information to gain access to the real website or carry out other harmful operations. Domain spoofing may have profound effects, ranging from identity theft to financial losses. Thus, users must be aware and cautious when providing personal information online.

3.7 Website forgery

Website forging is a fraudulent practice in which a website that seems real but is phony is created [19]. The fraudster may use stolen identities or data to impersonate an actual website to establish a phony website. The false website might be hosted on another server, and the fraudster will use various tactics to trick the visitor into thinking they are visiting the actual website. This is a typical sort of cyber assault in which the attacker attempts to steal sensitive information from unsuspecting victims. Website forgery is especially problematic since it is sometimes impossible for people to recognize that the website, they are viewing is a fabrication. When a victim inputs personal or financial information on a false website, the attacker can access that information and use it for nefarious reasons. As a result, it is critical for users to be cautious when inputting sensitive information online and to confirm the legitimacy of websites before entering any information.

3.8 Trojan

A Trojan horse is malicious software that may install additional apps on a user's computer without their knowledge or consent [12]. This virus is frequently sent via email attachments or websites that have been hijacked by hackers or malware writers looking to enhance the capabilities of their dangerous programs. Trojan horses are well-known for their ability to disguise themselves as legal applications or software updates, deceiving unwary users into downloading and installing them. Once installed, the Trojan horse can perform a variety of operations on the user's computer, such as stealing personal data, installing further malware, or providing the attacker remote access. As a result, users must be cautious and follow best practices to protect themselves from such unwanted assaults.

3.9 Malware

Malware is a term that refers to any program that is meant to disrupt a computer system or steal personal information from users who unknowingly download it onto their machines, typically without their knowledge or agreement. Cybercriminals generally construct this malware, which is then deployed in a variety of methods, including phishing assaults, spam emails, and keyboard loggers [9]. Phishing assaults have grown in popularity in recent years, and they frequently use malware to infect victims' systems and steal important data. Malware can also be used to carry out other sorts of assaults, such as ransomware and distributed denial-of-service (DDoS) attacks, which can be extremely damaging to organizations and people [10]. As a result, it is critical for people and companies to take precautions against malware, such as installing antivirus software, routinely upgrading software and operating systems, and being wary of strange emails or other communications that may include malware.

3.10 Ransomware

Ransomware is malicious software that encrypts a user's data and prevents them from being accessed until a ransom is paid [5]. This sort of assault may be disastrous for people and businesses, resulting in the loss of critical data and severe financial impact. The attacker encrypts the data, and the victim must pay a ransom to get the decryption key required to open them. This tactic is frequently used to extort money from individuals or businesses. After receiving money, the attacker may or may not supply the victim with the decryption key. The growing prevalence of ransomware attacks emphasizes the importance of proactively protecting personal and business data from cyber threats.

3.11 Malvertising

Malvertising is a cybercriminal practice in which they pay third-party businesses to put advertisements on websites under their control. The advertisements are intended to lure users to the attackers' websites, where they can steal sensitive information or exploit vulnerabilities in the consumers' machines or networks [12]. Users can be directed to these sites by clicking on the advertisement or visiting the website. The attackers can then acquire access to the accounts and passwords of the companies, allowing them to carry out attacks on the firms' systems. This activity is an increasing source of worry for both corporations and people, as it may cause major financial and reputational harm. Users must consequently be attentive and take adequate precautions to protect themselves from such assaults.

3.12 Spear Phishing

Spear phishing is a type of email phishing in which an attacker sends an email to a user posing as a trusted individual, such as an attorney, employer, or university, requesting confidential information such as login credentials, social security numbers, and other personal data that could be used to gain access to accounts or steal money online [15]. Spear phishing is a highly focused kind of phishing that focuses on specific persons or organizations to make the assault look more legitimate and customized. These assaults are frequently effective because the attacker has done research on the target and may use that knowledge to construct a compelling message that seems real.

3.13 Session Hijacking

Session hijacking is a malicious technique to gain unauthorized access to a user's session ID and intercept their data. Attackers achieve this by exploiting vulnerabilities in session management procedures, which can be present in cookies, tokens, or URLs [9]. The attacker can then use this information to impersonate the user, access their confidential information, and carry out unauthorized transactions. Session hijacking is a serious threat that can result in identity theft, account misuse, and financial fraud, among other consequences [9]. To prevent session hijacking attacks, it is essential to ensure proper session management techniques, including session timeouts, secure session storage, and using HTTPS to encrypt session data [8].

3.14 Content injection

Content injection is a cyberattack in which harmful code is placed into genuine website content without the website owner's or user's knowledge or consent [15]. The inserted code may modify or replace current content with malicious code, giving the impression that the website has been altered. Content

injection attacks are designed to steal sensitive data from genuine websites or to divert users to phishing websites where their personal information can be obtained. To carry out the content injection attack and achieve their goals, the attackers may employ a variety of techniques, including cross-site scripting (XSS) and SQL injection (SQLi). Content injection attacks are a severe danger to website owners and users since they can cause data breaches, financial loss, and reputational harm to impacted companies.

3.15 Link Manipulation

Users can be directed to other web pages by using web links. On the other hand, attackers might exploit this feature by building malicious links that redirect visitors to fraudulent sites rather than the intended destination. As a result, attackers can intercept any cookie provided along with the link [15]. This allows them to mimic the user and conduct nefarious activities such as stealing sensitive data or starting fraudulent transactions. As a result, users should be cautious when clicking on links, particularly those they do not recognize or look suspicious. Putting in place security measures like two-factor authentication can also assist to reduce the danger of such assaults.

3.16 Whaling

Whaling is a sort of cyber assault that includes duping consumers into clicking on malware-infected links or advertisements, generally via email or social media postings [19]. The advertisements are frequently directed towards prominent social media sites such as Facebook and Twitter. Attackers often flood a large number of unprotected computers with traffic in order to overwhelm them and cause them to crash or freeze. This may cause severe interruption for organizations and individuals, as well as potential data breaches and data loss. Whaling assaults are growing more complex, with attackers employing social engineering tactics to produce persuasive phishing emails and websites that consumers find difficult to differentiate from legal ones. As a result, companies and individuals must be aware and take proactive actions to defend themselves against whaling assaults.

3.17 Email/spam

Email-based phishing attacks are a common form of cybercrime in which attackers send fraudulent emails that appear to come from a legitimate source, such as a financial institution or an online service, to trick users into divulging sensitive information. This technique is known as email phishing [18]. Despite its prevalence, email phishing attacks have several limitations, including the possibility of emails getting lost in transit or ending up in spam folders, making them less reliable than other phishing attacks. Nonetheless, email phishing remains a popular technique for cybercriminals due to its potential to target a large number of users and its ability to appear trustworthy to victims.

3.18 Web-based delivery

Phishing attempts frequently employ web-based delivery techniques, such as redirecting visitors to fake websites or utilizing pop-ups and malicious code [2]. These assaults can have profound implications, such as money loss, identity theft, and malware installation on victims' machines. Individuals and businesses must take precautions to defend themselves from such assaults, such as learning about the strategies employed by attackers, deploying security software, and keeping alert to strange emails and communications.

4. PURPOSE BEHIND THE PHISHING

4.1 Identity theft

Phishing is a social engineering assault used to gain personal information, particularly login credentials. In this attack, an email or SMS message seems to originate from a trusted source, but it is really delivered by an unknown sender [14]. The email or message may contain what appear to be normal links or attachments. However, they are meant to download malicious software onto the target's computer or mobile device to acquire sensitive information such as login credentials or financial information [14]. These phishing assaults can have major ramifications, including identity theft, financial loss, and malware installation on victims' PCs [14].

4.2 Financial Gain

Phishing is frequently driven by financial gain, with criminals using the scam to trick customers into disclosing their bank account passwords and transferring data [8]. This type of assault is known as "phishing," It involves mimicking emails from financial institutions, banks, and other trustworthy businesses to obtain personal information from unsuspecting victims.

4.3 Password Harvesting

Password harvesting, also known as credential stuffing, is a specific purpose of phishing attacks in which attackers attempt to steal user credentials to gain access to online accounts [9]. Attackers employ automated programs to collect passwords from the machines of a large number of online users without their knowledge or agreement. This occurs when consumers click on links in phishing emails that redirect them to unfamiliar websites where they are requested to input their credentials into an automated form. Attackers utilize this form to acquire the user's login details for future fraudulent operations.

4.4 Gain recognition

Phishing attacks that target high-profile individuals or organizations are often motivated by the desire to gain recognition [17]. Attackers can increase their visibility and notoriety by successfully tricking a well-known entity into revealing sensitive information. This recognition can also lead to attention from other members of the hacking community and potentially lead to financial gain or status within the community. Therefore, high-profile individuals and organizations are at increased risk of becoming targets of phishing attacks due to their status and visibility.

4.5 Exploit security hole

Security vulnerabilities are frequently employed in phishing attacks, in which attackers exploit flaws in an organization's security architecture to obtain unauthorized access to sensitive data [3]. One of the most prevalent methods attackers use is sending seemingly regular emails with links to malicious websites. When a user clicks on the link, the attacker can circumvent security protections and obtain access to sensitive information. These assaults may harm enterprises, resulting in substantial financial losses and reputational damage. As a result, companies must have robust security measures in place to defend themselves from such assaults.

4.6 Brand Tarnishing

Brand tarnishing is a strategy used by attackers to destroy the reputation of businesses or persons by disseminating false or bad information [16]. Attackers use phishing emails that appear to come from a genuine source, such as the targeted firm, but include provocative or objectionable information. Another

technique is to steal client data from the firm and then post it online, which can severely harm the company's reputation. Brand tarnishing is a significant concern since it may result in considerable financial losses and harm the targeted company's reputation.

4.7 Data Theft

Data theft is a primary objective of phishing attacks. Attackers use various tactics to trick individuals into divulging sensitive information like passwords or credit card numbers, allowing them to access the data for their purposes [8]. Malware can also steal data by tricking individuals into downloading it onto their computers or networks. Once the attacker has obtained the data, they can use it to commit identity theft or financial fraud, or sell the information on the black market.

5. CAUSES OF PHISHING

5.1 Security Flaws

Attackers can access systems by exploiting security weaknesses in software and hardware [3]. A design defect is the most prevalent security problem when software is distributed without sufficient testing. Because of this design weakness, attackers can abuse the program and obtain unauthorized computer access.

5.2 Weak passwords

A weak password is not considered a security weakness; instead, the user must generate a strong password and update it frequently. Phishing attacks may readily exploit a weak password [12]. Users and administrators may use weak passwords owing to carelessness in password selection or because they often use basic passwords such as "password" or "123456." Furthermore, individuals frequently use the same password for several accounts, exposing all of their accounts if the password is hacked [8].

5.3 Non-secure desktop

A non-secure desktop does not have the latest security updates. A non-secure desktop that lacks the most recent security patches makes a machine more vulnerable to phishing assaults [7]. Furthermore, users should be aware of the kind and version of their browsers, as certain browsers are more secure than others. If a browser is hacked, it may be used to launch phishing attacks.

5.4 No User Awareness

A non-secure desktop environment employs web browsers such as Internet Explorer 11 and other out-of-date versions that are vulnerable to phishing attempts [5]. Users can prevent this risk by disabling all extensions in Internet Explorer 11 and using contemporary browsers such as Microsoft Edge, Firefox, or Chrome as the default browser in Windows 10/8/7. Users can better defend themselves against phishing attempts and other online hazards by doing so.

5.5 Weak auth or no MFA

Weak authentication methods and the absence of multi-factor authentication (MFA) can expose systems to phishing attacks. Attackers can acquire access to systems through the use of weak password and username combinations, potentially resulting in the theft of sensitive data such as financial and personal information. Files holding sensitive information on individuals, their family members, and workers, which might be exploited for identity theft, may fall into this category. It is critical to deploy robust authentication procedures such as MFA to reduce the dangers of such attacks. [5]

5.6 Access control list

ACL is a set of permissions allocated to a specific object, such as a file or folder, that indicates which people or groups have access to the item and what degree of access they have [5]. ACLs are frequently used to limit access to sensitive data or resources so only authorized users can access them. Suppose an ACL is configured incorrectly or is out of date. In that case, it can lead to security vulnerabilities and raise the risk of phishing attempts by allowing unauthorized users to access sensitive data or network resources. As a result, it is critical to evaluate and update ACLs on a regular basis to ensure that they are correctly set and effective in safeguarding the network against unwanted access.

5.7 Software Updates

Successful phishing assaults are frequently caused by out-of-date software. These are examples of web browsers, antivirus software, and operating systems. When these software packages are not frequently updated, they might become exploitable, exposing the system to attack. To reduce the danger of these sorts of assaults, it is critical to keep software up to date.

5.8 Browser Vulnerabilities

When using a browser like Internet Explorer or Firefox to explore the internet, users are generally requested to install software updates to check for security vulnerabilities in their system each time they visit a website. It is, nevertheless, critical to use caution when upgrading this program. Before installing any updates, users should check whether any security updates are available. This is because attackers may exploit weaknesses in obsolete software and take advantage of users unaware of the latest security upgrades to launch phishing attacks. To reduce the danger of such assaults, it is recommended that all software on a system be maintained up to date.

5.9 Open ports and misconfigured services exposed to the internet

Open ports and misconfigured services on the internet constitute a severe security risk because they allow unprotected traffic from untrusted sources to access devices or computers without authorization, even when firewalls or other security controls are in place. Some frequently used ports, such as 80 (HTTP) and 443 (HTTPS), are exposed to the public, rendering them vulnerable to malevolent actors. Similarly, misconfigured services such as SMTP and FTP can be utilized by anybody on the internet without authorization, raising the danger of phishing attempts. To reduce this risk, it is advised that open ports be secured, and services be correctly configured, as well as employing extra security measures such as network segmentation and intrusion detection systems.

5.10 Poor Endpoint Detection

When endpoint detection is inadequate, phishing attempts may frequently evade security protections and get access to critical information. Maintaining security requires ensuring that a reliable endpoint detection mechanism is in place. Organizations must have the right technologies in place to detect and stop phishing efforts; failing to do so might expose people to fraud [1]. As a result, it is critical to have a well-designed endpoint detection and response system that can detect and respond to phishing assaults.

6. PHISHING DETECTION

6.1 Domain name detection

Detecting phishing attacks using domain names is a common practice to identify fraudulent websites. Legitimate websites are often recognizable by their domain name, which usually matches the company or organization's name. On the other hand, fake websites often contain domain names that resemble legitimate websites but with slight variations that can be difficult to detect. For instance, a domain name like "paypal.com-scam.com" is an example of a fake website created to deceive unsuspecting users into revealing their sensitive information. Therefore, proper domain name detection is crucial in detecting and preventing phishing attacks.

6.2 Language Used

Language detection is another technique that can be used to identify phishing attacks. Typically, phishing emails could be better written in English or use unusual phrases not commonly found in professional communications. If an email appears suspicious because of its language, verifying whether it is a phishing attempt is advisable.

6.3 UI Detection

UI detection, also known as user interface detection, is a method of detecting phishing assaults by inspecting the user interface of a website or email. Fake websites and emails frequently have poor visual quality or misspellings in the text, which might indicate a phishing effort. Users may frequently tell whether a website or email is valid by inspecting its design and layout [18].

6.4 Signature

Many phishing emails must be better designed and have spelling and grammatical mistakes. By checking for these unique email features, analysts can detect phishing efforts. This might include misspellings, grammatical errors, or strange layouts. Employees should be careful when opening emails with strange signatures since they might be phishing efforts.

6.5 Tools to detect

To identify phishing emails, individuals or organizations can use several technologies. These technologies often employ heuristics and machine learning approaches to identify suspected phishing emails. Often utilized tools include PhishMe, KnowBe4, and FireEye [20]. When the program generates an alert, employees must proceed cautiously before opening the email.

6.6 Suspicious attachments

Suspicious email attachment detection is an important component of phishing protection. Suspicious attachments can be recognized by examining the attachment's nature, size, and source. Any attachment that asks the receiver to activate macros should be viewed cautiously, as activating macros can allow malware to execute on the user's device [20]. To avoid potential danger, users should confirm the safety of attachments by contacting the sender personally or via other methods before opening them.

6.7 Suspicious links

Another approach for spotting suspicious links is to move the mouse pointer over the link without clicking on it. This allows consumers to examine the link's actual URL and verify that it matches the displayed content. Furthermore, specific online browsers and email clients include built-in security capabilities that detect and alert users to potentially hazardous links. When clicking on links, be cautious since they might lead to fraudulent websites that steal personal information or install malware on the user's computer.

6.8 A message with a sense of urgency

Attackers frequently employ phishing emails that generate a sense of urgency to trick victims into acting without thinking. They frequently employ fear or hurry to induce panic, causing the victim to act without considering the implications. To prevent falling for these scams, it is critical to be calm and double-check the message's validity before acting.

6.9 Awareness creation

Increasing staff awareness is critical in spotting phishing assaults. Educational seminars and workshops are powerful tools for informing employees about the nature of phishing attempts and how to spot them [8]. To raise employee awareness, IT departments can give a variety of materials such as online training modules, pamphlets, and guidelines. Employees may become essential members of the organization's security team and play a critical role in identifying and stopping phishing attempts if given the required skills and information.

6.10 Unbelievable deals and offers

In numerous ways, unbelievable discounts and offers might lead to questionable phishing efforts. Email verification may entail providing a verification link or prompting the user to enter their email address into a form. Furthermore, phishing efforts may require consumers to check their accounts to claim an offer. Individuals and workers must be watchful and avoid such offers and agreements.

7. PREVENTION OF PHISHING

7.1 Enforcing strong passwords

One of the most effective ways to avoid phishing attempts is to enforce strong passwords. Passwords should be at least eight characters long and comprise a combination of lowercase and uppercase letters, numbers, and symbols. Furthermore, avoid using the same password for different accounts to reduce the risk of unauthorized access to sensitive information [7]. By following these recommended practices, users can lower their chances of falling victim to phishing attempts that leverage weak passwords.

7.2 Implement MFA

Multi-factor authentication (MFA) can significantly reduce the risk of successful phishing attacks by adding a layer of security to the login process. With MFA, users must provide two or more forms of identification when attempting to access their account, such as a password and a text message code. By requiring multiple forms of identification, MFA can make it more challenging for hackers to bypass account security measures with stolen passwords alone [25].

7.3 Creating security awareness programs

Security awareness programs help educate users about protecting themselves from phishing scams and other types of cybercrime. The program teaches them how criminals use social engineering techniques like pretending to be from a company or authority figure, such as an email from a user's bank or credit card company revealing fraud on an account.

7.4 Monitoring open RDP ports

Attackers can use the redirection of Remote Desktop Protocol (RDP) ports to redirect RDP connections, resulting in a denial-of-service attack by consuming network bandwidth and

resources. RDP ports 3389, 3390, 3394, and 4100 are often used. It is recommended to avoid open RDP ports by monitoring them and swiftly shutting them when they are found to be utilized for something other than their original purpose.

7.5 Hardening conditional access policies

Conditional access is a type of access control in which users are permitted access to a resource if specific conditions are satisfied. Location, time of day, device kind, or user identification are examples of such circumstances [8]. Conditional access can be used to restrict access to sensitive information such as social security numbers and credit card data and to guarantee that only authorized individuals have access to customer and financial records.

Using temporary passwords, granted to users depending on predefined criteria, is one form of conditional access. When accessing particular resources, for example, a user may be prompted to submit a temporary password texted to their mobile device. Requiring an extra layer of authentication, this helps to prevent illegal access. Organizations may strengthen their security posture and safeguard sensitive information from unwanted access by introducing conditional access restrictions.

7.6 Security policies

Incorporating security policies, such as those issued by the National Institute of Standards and Technology (NIST), can help avoid phishing attempts. These policies establish best practices for safeguarding systems and sensitive data and should be followed by all workers who have access to member accounts and systems. Such rules should be included in an organization's Information Security Policy and Procedures Manual and other related guidelines and paperwork [25].

7.7 Avoiding clicking links and attachments

Receiving an email with a link or attachment should trigger suspicion, and clicking on it should be done cautiously. Before clicking [10], it is best to confirm the integrity of the link or file by checking the URL or email address with a reliable source. If the link or attachment is opened, ensure it takes the user to the correct page. Otherwise, it is best to approach it with care.

7.8 Spam Guarding

The deployment of spam guarding services at both the organization's email server and user levels is an effective anti-phishing tactic. These tools prevent unsolicited commercial email messages from entering the network and entering emails carrying harmful code, such as viruses or worms, into the computer system.

7.9 Install antivirus and anti-spam software.

Several free antivirus apps may be used to protect computers against malware such as viruses and spyware. Examples include Microsoft Security Essentials, Norton 360, and McAfee's Internet Security package [6]. Additionally, the user should install anti-spam software on their device to filter out unwanted emails and prevent them from reaching the user's inbox without the sender's consent.

8. PHISHING DETECTION IMPLEMENTATION

Several Microsoft Azure technologies are used to create a phishing detection system. Azure Data Factory is used for data migration, allowing files to be transported from many sources to Azure Data Lake gen2. For Python and R language, Azure Databricks is utilized, with all R Language and Python code put in Databricks notebooks..

To run Databricks python note book spark cluster are used Azure Databricks is a fully managed first-party service that enables an open data lakehouse in Azure. With a lakehouse built on top of an open data lake, quickly light up a variety of analytical workloads while allowing for common governance across your entire data estate. Enable key use cases including data science, data engineering, machine learning, AI, and SQL-based analytics.Data Lake Gen 2 is used to store pre- and post-datasets, and Power BI is used to produce telemetry reports by connecting to Data Lake Gen 2.

Data collection is the first stage of the phishing detection implementation. Data is collected from numerous sources and transported to Azure Data Lake Gen2 storage utilizing the Azure data factory tool for data movement. In Azure data factory self hosted integration runtime is use to move data from on prem to Azure Data Lake cloud storage. The obtained dataset is read into CSV format using the Pandas package and labeled. The NLTK library is used for importing stop words and porter stemmer, which are used to delete unnecessary words and locate the word's base root. Regular expressions are used to remove special characters from a dataset.

Following data cleaning, text preparation is carried out, in which email body words are transformed to lowercase, and each word is separated into a separate column. The count vectorizer from the scikit-learn package turns unique words into columns. The primary dataset is then converted into

Boolean variables 0 and 1 for spam and valid emails. Both datasets are then tested using train-test split and the Nave Bayes package. The confusion matrix from the scikit-learn package is used to test and validate predictions. The accuracy score measures the algorithm's accuracy across all 11 datasets.

Emails identified as spam and those not transferred more profoundly into the data lake and Power BI to create a spam detection tool efficiency report. Overall, developing a phishing detection algorithm necessitates using multiple Azure technologies and modules for data cleaning, preprocessing, visualization and testing.

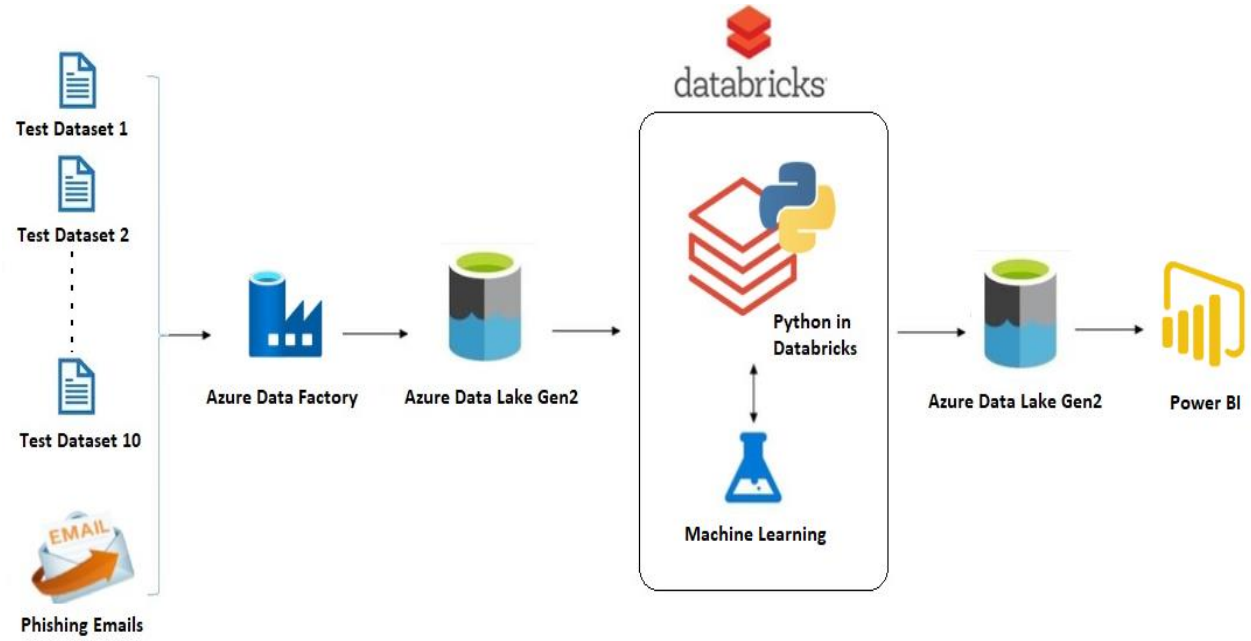

Fig 5: Phishing Detection Implementation

9. EXPERIMENTS AND RESULTS

The research findings reveal that the created phishing detection tool detects phishing emails with excellent efficiency and accuracy. The program was evaluated on 11 datasets, each of which had 500 emails, including a mix of spam and legal emails. The phishing detection tool's total accuracy was 94%, with an efficiency of 92% or higher in most of the tests conducted.

Table 1: Experimental Results

Datasets	Number of Emails	Spam detected	Not Detected	Efficiency
1	500	106	9	0.96
2	500	94	6	0.95
3	500	93	7	0.94
4	500	95	5	0.93
5	500	94	6	0.92
6	500	94	6	0.94
7	500	92	8	0.94
8	500	93	7	0.95
9	500	94	6	0.93
10	500	95	5	0.94
11	500	96	4	0.92
12	5500	1099	16	0.98

When the datasets were split, the accuracy of the prediction model was much lower when compared to the accuracy of the prediction model when evaluated on the entire dataset. According to the findings, the greater the dataset, the more accurate the prediction model. Furthermore, Fig. 7 depicts the efficacy of the phishing detection tool, which reveals that the tool was more than 92% efficient in most of the tests done. The tool was determined to be 94% efficient and accurate on average. Finally, the experimental findings show that the created phishing detection tool successfully identifies phishing emails and may be used to safeguard individuals and businesses from phishing assaults.

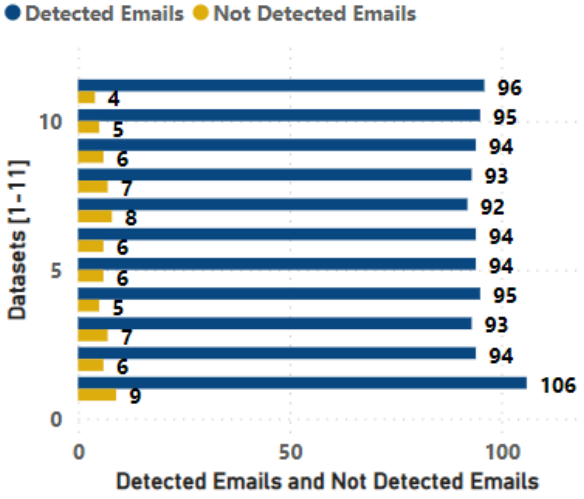

Fig 6: Phishing Detected vs Not Detected

The phishing detection tool's effectiveness was assessed by testing it on 11 datasets, each comprising 500 emails (5,500). As shown in Fig 7, the developed prediction model was more

than 92% efficient in most of the experiments and 94% efficient and accurate on average.

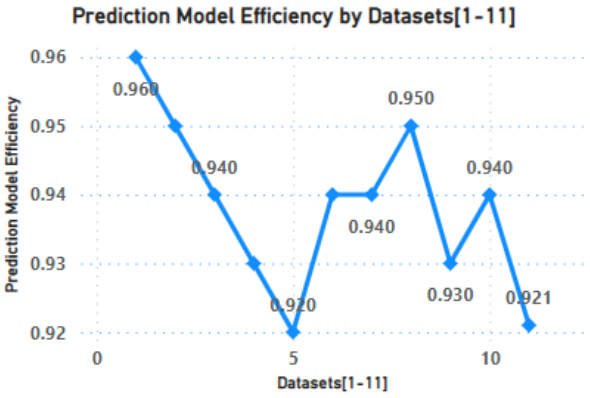

Fig 7: Efficiency of the Phishing Detection Tool

Furthermore, the prediction model's accuracy was in the 96% to 92% range for split datasets with 500 emails each. The prediction model's accuracy was 98% for the whole dataset of 5,500 emails. These findings suggest that the greater the dataset, the more accurate the prediction model will be.

10. CONCLUSION

Overall, this research paper highlights the importance of taking proactive measures to prevent phishing attacks. It also provides valuable insights into developing and testing a phishing detection algorithm using Natural Language Processing and Python. While the algorithm demonstrates high accuracy in detecting phishing emails, there is still room for improvement, particularly in considering attachments and subject lines. Future research could focus on integrating these tools with popular email services and developing real-time alert systems for users. Overall, this paper contributes to the ongoing efforts to improve cybersecurity and protect against phishing attacks.

11. REFERENCES

[1] Akinyelu, A. A. (2019). Machine learning and nature-inspired based phishing detection: a literature survey. International Journal on Artificial Intelligence Tools, 28(05), 1930002.

[2] Chan, J. M., Van Blarigan, E. L., Langlais, C. S., Zhao, S., Ramsdill, J. W., Daniel, K., ... & Winters-Stone, K. M. (2020). Feasibility and acceptability of a remotely delivered, web-based behavioral intervention for men with prostate cancer: a four-arm randomized controlled pilot trial. Journal of medical Internet research, 22(12), e19238.

[3] Dinesh K; Nathan S. "Study and Analysis of Chat GPT and its Impact on Different Fields of Study." Volume. 8 Issue. 3, March - 2023, International Journal of Innovative Science and Research Technology (IJISRT), www.ijisrt.com. ISSN - 2456-2165, PP :- 827-833. https://doi.org/10.5281/zenodo.7767675

[4] Hakim, Z. M., Ebner, N. C., Oliveira, D. S., Getz, S. J., Levin, B. E., Lin, T., ... & Wilson, R. C. (2021). The Phishing Email Suspicion Test (PEST) is a lab-based task for evaluating the cognitive mechanisms of phishing detection. Behavior research methods, 53, 1342-1352.

[5] Homayoun, S., Dehghantanha, A., Ahmadzadeh, M., Hashemi, S., Khayami, R., Choo, K. K. R., & Newton, D. E. (2019). DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer. Future Generation Computer Systems, pp. 90, 94–104.

[6] Kalla, D., & Samaah, F. (2020a). Chatbot for Medical Treatment using NLTK Lib. *IOSR Journal of Computer Engineering*, *22*(1), 50–56. https://doi.org/10.9790/0661-2201035056

[7] Lopez-Aguilar, P., & Solanas, A. (2021). The Role of Phishing Victims' Neuroticism: Reasons Behind the Lack of Consensus. Int'l J. Info. Sec. & Cybercrime, 10, 75.

[8] Marzuki, K., Hanif, N., & Hariyadi, I. P. (2022). Application of Domain Keys Identified Mail, Sender Policy Framework, Anti-Spam, and Antivirus: The Analysis on Mail Servers. International Journal of Electronics and Communications Systems, 2(2), 65-73.

[9] Mishra, S., & Soni, D. (2021). Dsmishsms-a system to detect smishing sms. Neural Computing and Applications, pp. 1–18.

[10] Negassa, M. D., Mallie, D. T., & Gemeda, D. O. (2020). Forest cover change detection using Geographic Information Systems and remote sensing techniques: a spatiotemporal study on Komto Protected Forest priority area, East Wollega Zone, Ethiopia. Environmental Systems Research, 9, 1-14.

[11] Oesch, S., & Ruoti, S. (2020, August). That was then; this is now: A security evaluation of password generation, storage, and autofill in browser-based password managers. In Proceedings of the 29th USENIX Conference on Security Symposium (pp. 2165-2182).

[12] Petelka, J., Zou, Y., & Schaub, F. (2019, May). Put your warning where your link is: Improving and evaluating email phishing warnings in Proceedings of the 2019 CHI conference on human factors in computing systems (pp. 1-15).

[13] Qwaider, S. R. H. (2019). ANALYSIS AND EVALUATION OF CYBERSECURITY TECHNIQUES FOR SOCIAL ENGINEERING (Doctoral dissertation).

[14] Riadi, I., Umar, R., Busthomi, I., & Muhammad, A. W. (2022). Block-hash of blockchain framework against man-in-the-middle attacks. Register: Jurnal Ilmiah Teknologi Sistem Informasi, 8(1), 1-9.

[15] Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning-based phishing detection from URLs. Expert Systems with Applications, 117, 345-357.

[16] Sharma, A., Gupta, P., & Noida, I. (2020). COVID 19 PANDEMIC: IMPACT ON BUSINESS AND CYBER SECURITY CHALLENGES. Journal of Emerging Technologies and Innovative Research (JETIR), 7(7).

[17] Shen, G., Link, S. S., Tao, X., & Frankfort, B. J. (2020). Modeling a potential SANS countermeasure by manipulating the translaminar pressure difference in mice. npj Microgravity, 6(1), 19.

[18] Kuraku, S.; Kalla, D. Emotet Malware–A Banking Credentials Stealer. Iosr J. Comput. Eng. 2020, 22, 31–41.

[19] Xu, D. (2019). Jamming-assisted legitimate surveillance of suspicious interference networks with successive interference cancellation. IEEE Communications Letters, 24(2), 396–400.

[20] Yathiraju, N., Jakka, G., Parisa, S. K., & Oni, O. (2022). Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security: A Survey of Social Engineering Attacks and Steps for Mitigation of These Attacks. In Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security (pp. 110-132). IGI Global.

[21] Zhang, L., Tan, S., Wang, Z., Ren, Y., Wang, Z., & Yang, J. (2020, December). Viblive: A continuous liveness detection for a secure voice user interface in an IoT environment. In Annual Computer Security Applications Conference (pp. 884-896).