# Combatting Phishing Attacks in the Internet of Things (IoT)

Hafsa Rafique, Reamsha Khan

University of Management and Technology, Lahore, Pakistan

**Correspondence:**
Saad Abdullah: reamshakhan1122@gmail.com

**Article Link:** https://www.brainetwork.org/index.php/jcai/article/view/29

**DOI:** https://doi.org/10.69591/jcai.1.2.4

JCAI
ISSN (P):3007-3049
ISSN (E):3007-3057
JOURNAL OF COMPUTING AND ARTIFICIAL INTELLIGENCE
ARTIFICIAL INTELLIGENCE
Published by
Beyond Research Advancement and Innovation Network

**Volume 1, Issue 2, 2023**

**Funding**
No

**Citation:** Rafique, H., & Khan, R. (2023). Combatting phishing attacks in the internet of things (IoT), *Journal of Computing and Artificial Intelligence, 1*(2), 42-59.

**Conflict of Interest:** Authors declared no Conflict of Interest

**Acknowledgment:** No administrative and technical support was taken for this research

**Article History**

**Submitted: Sep** 08, 2023
**Last Revised:** Oct 12, 2023
**Accepted: Nov** 28, 2023

**An official Publication of**
**Beyond Research Advancement &**
**Innovation Network, Islamabad, Pakistan**

# Combatting Phishing Attacks in the Internet of Things (IoT)

Hafsa Rafique[1], Reamsha Khan[1*],

[1]University of Management and Technology, Pakistan

## Abstract

Phishing is the most popular and substantial Internet risk today's era, in which attackers attempt to obtain business credentials by using malware or social engineering. The capability to identify phishing attacks with great precision has always been a great issue. Recent progress in phishing detection procedures has caused the development of several new methods that are specially built for phishing detection when accuracy is critical. The phishing problem is extensive because there are many ways to carry out such an attack, suggesting that one solution will not be enough.

***Keywords:*** phishing attack; prevention techniques; phishing stages; countermeasures;

## Introduction

Phishing is a different kind of network-attack in which the invader makes duplication of a current Web page to trick consumers into filing individual, commercial, or key data to what they consider is their service provider's Online platform (e.g., through specially designed e-mails or instant messages). Phishing scams have received significant attention in recent years, a significant danger to worldwide Internet security. Phishing [1] is an automated identity theft scheme that makes use of human nature and the Internet to trick millions of people and steal significant sums of money. In the 4th month of 2004, the IT industry research Gartner assessed that 1.8000,000 Americans had already submitted their personal information to phishers. The main goal of these campaigns is to exploit system weaknesses, which can be either technical or due to user ignorance, which implies that researchers must defend against these attacks on both a technical and a user level.

[*] Corresponding Author: reamshakhan1122@gmail.com

Phishers take advantage of the human tendency to overlook vital warning messages. The lack of public awareness regarding phishing attacks are also one of the key reasons why phishing attacks have been as successful as shown in the Fig below. Phishers' goal is to expose connected gaps to perform successful outbreaks whenever a researcher arises with a procedure to avoid these attacks. The following are the incentives behind these events:

**Login authorization theft:**

The phisher uses fake electronic mail as a cautioning notice to change passwords and provides a link to snip login details from users of online sites such as Amazon, and Gmail.

**Banking credentials theft:**

Online login credentials and credit cards details such as card number, expiration and issuance dates, cardholder's name, CVV number, and other famous financial intermediaries such as PayPal. Collecting Info: Info corresponding to email and phone numbers is required through straight-promoting firms.

**Figure 1**
*Phishing Attack*

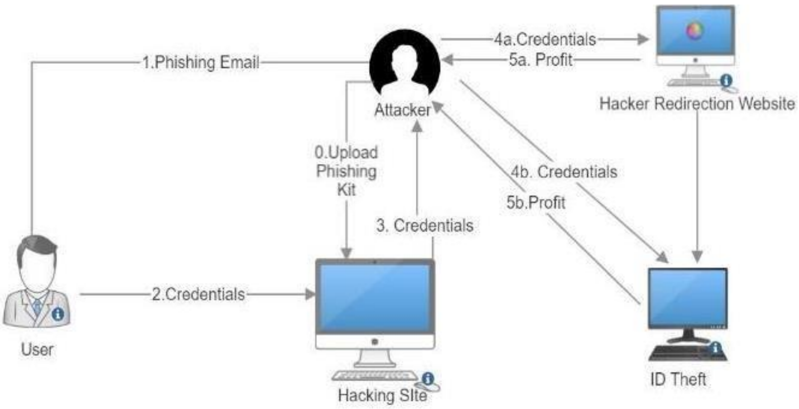


Fig 1. Phishing Attack

## Literature Review

According to a review of the literature, there are several phishing classes and anatomies. The author provides a summary of phishing techniques, but fails to identify vectors and the situations in which they arise. [2] [3] classifies attack initiation strategies, victim data gathering techniques, and attack communication channels; though, the research creates no attempt to classify anti-phishing techniques. Author [4] focused primarily on countermeasures and categorized them according to where they were used. In their consideration of client-server authentication mechanisms, they also neglect the impact of the communication medium. [5]

Server-side, browser-side, and online training anti-phishing solutions are all dependent on the system architecture. The classification of tactics, on the other hand, is far too broad to be useful. In an email, the author [6] presents a countermeasure categorization scheme, however, they disregard additional attack settings. This paper [7] presents a comprehensive picture of technical phishing defenses without taking into consideration emerging communication platforms and developing attack strategies that ended the last few years. Although the first to completely analyze the subject of phishing and give a framework for researching the attack and its defenses, this author [7] was the first to provide a framework for investigating the bout and its resistance. Instead of focusing on attack stages, the current study examines countermeasures for phishing strategies. Existing research on countermeasures has concentrated on phishing problems in specific communication media without methodically assessing the sharing of countermeasure groups across statement media, according to our literature assessment. For example, divide anti-phishing strategies used on websites into 3 categories: browser plugins and anti-phishing toolbars, digital signature and trust dissemination systems, and content-based detection tools [8].

## Phishing Methodology

This method is divided into 5 stages:

**Stage A:** The target group or a single individual is chosen, and the setup and planning process begins. It's up to them at that point to learn more about the company and its network. It may be done by going to the site in person or by watching the network activity. The next step is to set up the bouts through a manual technique, such as a website or email with malicious hyperlinks that can redirect the victim to a phoney web page.

**Step B:** This stage is used to direct these faked emails to their intended recipients, such as acting as a reputable financial institution and asking that the client update particular information immediately by clicking on a dangerous link. Emails may be sent to identify employees of a company.

**Step C:** When the victim goes on the false link, all these malwares is installed on the system, allows hackers to take control of the machine and modify its settings, or change access permissions. In rare cases, it may redirect to a bogus website that requires authentication.

**Step D:** The required data is recovered after hackers get a link to the user's device, and if the employer provides the attacker with his account information, the attacker may now access the user's account.

**Step E:** The phisher eliminates all evidence, including the false website accounts, after obtaining the required information. They also keep note of how far their attack progressed in order to improve future strikes.

## Methods & Techniques of Phishing

Phishing as a whole may be divided into 3 components:

1. Medium
2. Vector
3. Technical approach

Some directions are only suitable for specific media, although some technological techniques are only appropriate for specific attack trajectories. The vector is the opportunity of the bout and is typically mandatory by the medium. The medium used by an attacker to communicate with their victims is known as the phishing attack. This type of attack is usually carried out through social engineering techniques and attack methods such as cross-site scripting. In order to increase their chances of success, the attacker typically uses these techniques in combination with other methods.

### A. Medium:

In phishing attacks, the medium is the 1st thing to study. The medium controls the categories of techniques are used. The tool in which an attacker cooperates with the objective is mentioned as the media. There are 3 primary media via which this contact might occur:

1. Speak
2. SMS/MMS
3. Internet

The best popular method for people to connect and express info is through ability to speak, which includes speaking and the use of language. It is frequently specified that the use of words is what differentiates one person from another. As a result, this medium is used to trick people into revealing personal info to others. SMS is type of communication entails sending brief messages via a mobile. MMS evolved from this, allowing the transmission of content other than writing, such as pictures, videos, or auditory samples. This medium offers phishers a variety of handy ways to communicate with targets and obtain their personal information.

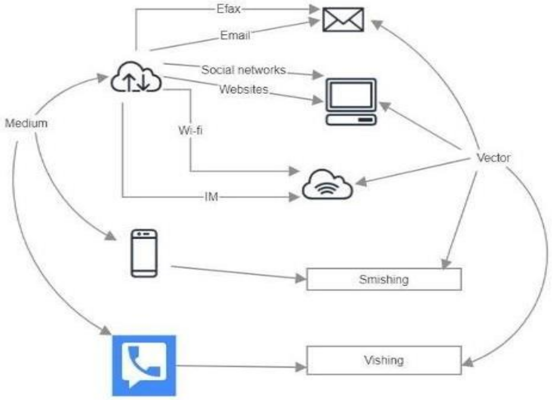
The internet is the final media to be evaluated. The internet's always-changing and expanding nature means that new channels of communication are being invented, from its origin as the ARPANET [9]. This collection of message techniques is conveniently accessible in one place and includes anything from electronic mail to Instagram, which permits phishers to "hook" potential victims [10].

### B. Vectors

These are defined over the medium exploited through the invader. As shown in the figure below.

**Figure 2**

*Medium and Vectors*



### *C. Vishing*

This phishing technique, known as vishing, utilizes voice communication. While using a phone for fraudulent activities is not a novel concept, it has become more prevalent with the advent of voice over IP (VoIP) technology. Vishing takes advantage of the ability to spoof phone numbers, making calls appear to originate from legitimate sources. VoIP enables the masking of the caller's actual location, thereby deceiving victims into sharing sensitive information. Because of the low cost of calls, there are a variety of reasons why this type of phishing is effective, for example:

1. Acceptance of automatic phone systems (automation).
2. Call centers: due to the widespread usage of call centers, individuals have grown familiar with outsiders get in touch and bidding personal information. This also makes phishers with external inflections less doubtful.
3. Target age: a bigger part of the worlds can be extended by mobile than by electronic mail.

### *D. Smishing Vector*

The vector of smishing is SMS [11] as a communication channel. This is when phishing assaults are carried out through a short message service. This procedure is used in 2 different ways. The 1st tactic requires transfer a message pretending as a reliable authority (e.g., bank, etc.). After that, the target is sent to a forged website or contact number, where they are requested to login or provide personal information. As soon as this occurs, attackers can take use of the information they've gathered. The alternative method comprises sending a victim a Text with infection or a link to a malware-infected website. The phisher may then carry out their attack, which might entail anything from gathering the target's contacts and messages to setting up a botnet or acquiring access to authentication codes for logins or transactions once the malware has been installed.

### *E. Email*

The internet, naturally, is the media that has the broadest diversity of flight path. E-mail is the 1st vector to consider (email). This attack vector sends specially produced emails to target users, persuading them to do events that will give the attacker access to their personal information. Besides, it conceals the sender's geographic location. When exploiting this vector, phishers can use a variety of technological tactics, such as address spoofing and so on. Also, it conceals the sender's geographic location. When exploiting this vector, phishers can use a variety of technological tactics, such as address spoofing and so on. As it shown below.

**Figure 3**

*Email Phishing*

## Phishing Attack Approaches

A phisher must first investigate their victim to generate high-quality phishing emails that are relevant to the target. A phisher can accomplish this aim in a variety of ways. The first is browser sniffing, which determines which websites the target usually visits by measuring access time. Cookies, DNS cache, and URLs are all investigated. If the access time for a given resource is too short, if the site is brief, the target is likely to visit it frequently. The attacker must sniff this data to gain access to it. To embed JavaScript, you must first utilize a website with advertising or another method. For example, a Hyper (HTML) email sends a script that will notify the phisher of the attack. Site accessibility times. The phisher may now create an email to seem as though it came from a site the victim is acquainted with using this information.

### *A. Categories of Phishing Attack detection*

**1.** Deep learning

**2.** Machine learning

**3.** Scenario-based

**4.** Hybrid learning

#### *1. Deep learning*

Recent advancements in deep learning (DL) methodologies suggest that the categorization of phishing websites using deep neural networks (NN) should outperform conventional machine learning (ML) methods. DL approaches such as feed-forward deep neural networks and convolutional neural networks (CNN) have been employed for cybersecurity intrusion detection.

In a study by the authors [12], they proposed an anti-phishing framework relying on a DL-based phishing detection model implemented at the Internet Service Provider (ISP) level to ensure comprehensive security. They utilized enhanced dynamic rule induction [13], which they claim is the first machine learning and deep learning algorithm used as an anti-phishing tool. Additionally, Mao et al. developed a learning-based approach for selecting page layout comparisons to identify phishing sites. They established rules and constructed a phishing page classifier using traditional learning algorithms such as Support Vector Machines (SVM) and Decision Trees (DT) to analyze page layout aspects effectively.

Regarding datasets, the author [14] provided the largest dataset, comprising 1528 phishing websites, followed by Open Phish with 613 phishing websites, Alexa with 1600 legitimate websites, payment gateway with 66 valid websites, and top banking websites with 252 legitimate websites. Tests were conducted on various datasets, including one obtained from [source], which contained 2000 web content entries (1000 phishing and 1000 legitimate).

### 2. Machine learning

The author [15] devised an Adaptive Neuro-Fuzzy Inference System-based resilient approach with integrated features for detecting and protecting against phishing attacks. Meanwhile, authors [16] introduced the Phish Bench benchmarking framework, enabling examination and analysis of current characteristics for phishing detection under various test conditions, including unified framework design, datasets, classifiers, and performance metrics. In [17], the authors proposed a phishing website detection approach based on Particle Swarm Optimization (PSO). Their method suggests utilizing PSO to weigh different website features, leading to enhanced accuracy in identifying phishing websites. The proposed PSO-based website characteristics aim to identify distinct aspects of sites, considering their significance in distinguishing phishing from legitimate websites. Additionally, in [18], researchers presented research focusing on feature selection for identifying phishing websites, claiming to have obtained the 47-feature phishing email dataset from paper [19].

### 3. Scenario-based

In their paper [20], the authors outlined several approaches to detect phishing attacks. They conducted a comprehensive review of existing methods, including ML-based, NML-based, NN-based, and behavior-based detection approaches. Using stick phishing as a model, they demonstrated how their proposed technique operates and evaluated the learning outcomes of the game based on observational data gathered from students' interactions [21]. Additionally, they highlighted the potential benefits of this information for the general public in terms of preparing for and preventing phishing attacks, as well as implementing policies to mitigate further misuse by phishers.

## Hybrid learning based

The author [15] suggested a hybrid threat detection approach that utilized SHLR. A three-step procedure was suggested by the authors: (1) The majority of websites disclosed in a search query's results are legal if the web page domain matches the domain name of the websites found in the query's results, and (2) character characteristics' heuristic criteria are legal. (3) A machine learning model to determine whether the internet page is legitimate or a phishing attack. To detect a phishing effort, the authors [22] used LR, DT, and RF techniques, and they believe the RF is a [23] much superior way of detection.

## Countermeasures:

### *A. Ontology:*

Ontology is a model that represents a set of concepts in a certain field in addition to the semantic relationships between those concepts [24]. Modeling new terminology, phrases, or expressions used in phishing emails as concepts and semantic connections in an ontology might help identify them. Phishing scams are getting more complex. The textual information used to launch the assaults is mutated in particular, making it harder to categorize them using traditional anti-phishing measures. Phishers, for example, frequently modify the text of phishing emails to prevent detection when confronted with traditional content-based defenses [25].

However, if the semantic linkages between ideas are well specified, the chances of identifying new types of phishing emails may improve. By recognizing meaning-based signals pointing to phishing and reasoning about phishing, ontological semantics can improve natural language understanding. To date, ontology has been used in only a few anti-phishing strategies. To increase the accuracy of classifier-based anti-phishing systems, this author [26] presents an ontology-based approach.

If the generated properties match those of known phishing emails, the e-mail is passed to an ontology, which then combines a set of related ideas in the detection process [27]. Create a knowledge representation system that can identify between different types of fraud, such as phishing.

### B. Honeypots:

These are security devices whose value is consequent from their capability to be probed and hacked. Honeypots are frequently set up as a trap to collect suspicious information. They are set to gather info on hackers, develop outlaw databases, and/or block suspicious sites. To contest phishing assaults, many honeypot-based methods have been developed [28]. The main concept behind these methods is to intentionally offer phishers honey tokens that appear to be authentication data (e.g. fingerprinted credentials).

### C. Client-server authentication

Client-server authentication between clients and servers is used in client-server authentication. The simplicity and robustness of this technique are advantages. Mutual authentication has been performed using a trusted device such as a smartphone [29]. This method not only reduces the reliance on users during the validation process but also provides protection against other types of attacks, such as Man-in-the-Middle (MITM) attacks. Additionally, an Identity-based Signature Scheme has been employed to enhance the security of email transmission.

### D. Email-authentication

This approach targets the enhancement of phishing attacks at the email level. The fundamental concept is that if recipients do not receive a fake email, they are less likely to fall victim to fraud [30]. Phishing emails are often detected using filters and content analysis tools before reaching recipients. For instance, training filters like Bayesian filters can effectively block a significant portion of phishing emails [31]. Moreover, companies like Microsoft and Yahoo have developed email authentication methods such as Sender ID and Domain Keys to verify the legitimacy of received emails and prevent sender information spoofing. Widespread adoption of these techniques could help reduce the volume of spam emails being sent [32].

### E. Browser-integrated tools

Phishing detection mechanisms often involve comparing the URL of a webpage in the address bar against a blacklist of known fake site URLs. In browsers like Microsoft Internet Explorer (IE) 7, the address bar turns red to signal the loading of a malicious page. Additionally, academic tools like Spoof Guard and Pwd Hash [33] are recognized for their integration into browsers to mitigate phishing attacks. Spoof Guard [34] detects phishing signs such as disguised URLs by scanning online pages. Pwd Hash [35], on the other hand, generates domain-specific passwords that can't be used on any other domain.

## Future work

Phishing is a gateway for malware and ransomware of all types. Ransomware is used in malware assaults on businesses, and ransomware operators demand a large ransom in return for not releasing stolen data, which is a new trend in 2020. Phishing schemes in 2020 are preying on unprepared users by imitating COVID-19 and healthcare-related institutions and individuals. Instead of thinking about reactive ways to battle once a phishing attempt has occurred, it is better to secure doors at our end and be proactive in defense. An automatic reporting function can be included so that phishing assaults are reported to the organization from the user's end, such as a bank or government agency.

## Conclusion

Finally, this article demonstrates that phishing is a present and important global issue. Phishing is still one of the most common malware infection vectors, the most common way of breach infiltration, and the most common method of social engineering assaults. There's also the concerning trend of the number of phishing sites found towards the end of the year increasing. 2019 had the greatest levels of activity since 2016. As technology evolves, the scope of phishing vectors is expected to widen, presenting new opportunities for malicious actors to exploit. These bad actors will likely innovate and employ novel methods, such as utilizing voice assistants like Amazon's Alexa for sound squatting, to conduct more sophisticated phishing attacks. This research indicates that phishing attack services are available to anybody for a fee. From the ancient to the cutting-edge, a full overview of the many types of phishing efforts is provided. Each type of assault is thoroughly detailed and addressed.

## References

[1] J. Hong, “The state of phishing attacks,” *Commun. ACM*, vol. 55, no. 1, pp. 74–81, Jan. 2012, doi: 10.1145/2063176.2063197.

[2] R. Wetzel, “Tackling phishing,” *Bus. Commun. Rev.*, vol. 35, no. 2, pp. 46–49, 2005.

[3] G. Ollmann, “The vishing guide,” *IBM Glob. Technol. Serv.*, pp. 1–16, 2007.

[4] L. Yang, J. Zhang, X. Wang, Z. Li, Z. Li, and Y. He, “An improved ELM-based and data preprocessing integrated approach for phishing detection considering comprehensive features,” *Expert Syst. Appl.*, vol. 165, p. 113863, 2021.

[5] H. Huang, J. Tan, and L. Liu, “Countermeasure techniques for deceptive phishing attack,” in *2009 International Conference on New Trends in Information and Service Science*, IEEE, 2009, pp. 636–641. https://ieeexplore.ieee.org/abstract/document/5260965/

[6] A. Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg, and E. Almomani, “A survey of phishing email filtering techniques,” *IEEE Commun. Surv. Tutor.*, vol. 15, no. 4, pp. 2070–2090, 2013.

[7] M. Jakobsson and S. Myers, *Phishing and countermeasures: understanding the increasing problem of electronic identity theft*. John Wiley & Sons, 2006. Available: https://books.google.com/books?hl=en&lr=&id=xxAbEcNlIwwC&oi=fnd&pg=PR3&dq=M.+Jakobsson+and+S.+Myers,+Phishing+and+countermeasures:+understanding+the+increasing+problem+of+electronic+identity+theft.+John+Wiley+%26+Sons,+2006.&ots=JXgKxwEqoA&sig=ieyZ4jtwkN79jOnh0H8aQyURj5M

[8] M. Chandrasekaran, K. Narayanan, and S. Upadhyaya, “Phishing email detection based on structural properties,” in *NYS cyber security conference*, Albany, New York, 2006, pp. 2–8.

[9] V. Ra, B. G. HBa, A. K. Ma, S. KPa, P. Poornachandran, and A. Verma, “DeepAnti-PhishNet: Applying deep neural networks for phishing email detection,” in *Proc. 1st AntiPhishing Shared Pilot 4th ACM Int. Workshop Secur. Privacy Anal.(IWSPA)*, Tempe, AZ, USA, 2018, pp. 1–11. Available: https://www.researchgate.net/profile/M-Kumar-2/publication/326211143_DeepAnti-PhishNet_Applying_Deep_Neural_Networks_for_Phishing_Email

_Detection_CEN-AISecurityIWSPA-2018/links/5d2317d5458515c11c1c15d9/DeepAnti-PhishNet-Applying-Deep-Neural-Networks-for-Phishing-Email-Detection-CEN-AISecurityIWSPA-2018.pdf

[10] R. Dantu, S. Fahmy, H. Schulzrinne, and J. Cangussu, “Issues and challenges in securing VoIP,” *Comput. Secur.*, vol. 28, no. 8, pp. 743–753, 2009.

[11] S. Mishra and D. Soni, “SMS phishing and mitigation approaches,” in *2019 twelfth international conference on contemporary computing (ic3)*, IEEE, 2019, pp. 1–5. Available: https://ieeexplore.ieee.org/abstract/document/8844920/

[12] S. Maurya and A. Jain, “Deep learning to combat phishing,” *J. Stat. Manag. Syst.*, vol. 23, no. 6, pp. 945–957, Aug. 2020, doi: 10.1080/09720510.2020.1799496.

[13] N. Abdelhamid, F. Thabtah, and H. Abdel-Jaber, “Phishing detection: A recent intelligent machine learning comparison based on models content and features,” in *2017 IEEE international conference on intelligence and security informatics (ISI)*, IEEE, 2017, pp. 72–77. Available: https://ieeexplore.ieee.org/abstract/document/8004877/

[14] S. Bell and P. Komisarczuk, “An Analysis of Phishing Blacklists: Google Safe Browsing, OpenPhish, and PhishTank,” in *Proceedings of the Australasian Computer Science Week Multiconference*, Melbourne VIC Australia: ACM, Feb. 2020, pp. 1–11. doi: 10.1145/3373017.3373020.

[15] M. A. Adebowale, K. T. Lwin, E. Sanchez, and M. A. Hossain, “Intelligent web-phishing detection and protection scheme using integrated features of Images, frames and text,” *Expert Syst. Appl.*, vol. 115, pp. 300–313, 2019.

[16] A. Das, S. Baki, A. El Aassal, R. Verma, and A. Dunbar, “SoK: a comprehensive reexamination of phishing research from the security perspective,” *IEEE Commun. Surv. Tutor.*, vol. 22, no. 1, pp. 671–708, 2019.

[17] W. Ali and S. Malebary, “Particle swarm optimization-based feature weighting for improving intelligent phishing website detection,” *IEEE Access*, vol. 8, pp. 116766–116780, 2020.

[18] S. Hutchinson, Z. Zhang, and Q. Liu, “Detecting Phishing Websites with Random Forest,” in *Machine Learning and Intelligent Communications*, vol. 251, L. Meng and Y. Zhang, Eds., in Lecture

Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 251. , Cham: Springer International Publishing, 2018, pp. 470–479. doi: 10.1007/978-3-030-00557-3_46.

[19] A. K. Tyagi and G. Aghila, "A wide scale survey on botnet," *Int. J. Comput. Appl.*, vol. 34, no. 9, pp. 9–22, 2011.

[20] J. Mao *et al.*, "Detecting phishing websites via aggregation analysis of page layouts," *Procedia Comput. Sci.*, vol. 129, pp. 224–230, 2018.

[21] A. Begum and S. Badugu, "A Study of Malicious URL Detection Using Machine Learning and Heuristic Approaches," in *Advances in Decision Sciences, Image Processing, Security and Computer Vision*, vol. 4, S. C. Satapathy, K. S. Raju, K. Shyamala, D. R. Krishna, and M. N. Favorskaya, Eds., in Learning and Analytics in Intelligent Systems, vol. 4. , Cham: Springer International Publishing, 2020, pp. 587–597. doi: 10.1007/978-3-030-24318-0_68.

[22] 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)*, IEEE, 2019, pp. 588–593. Available: https://ieeexplore.ieee.org/abstract/document/8728356/

[23] A. Niranjan, D. K. Haripriya, R. Pooja, S. Sarah, P. Deepa Shenoy, and K. R. Venugopal, "EKRV: Ensemble of kNN and Random Committee Using Voting for Efficient Classification of Phishing," in *Progress in Advanced Computing and Intelligent Engineering*, vol. 713, B. Pati, C. R. Panigrahi, S. Misra, A. K. Pujari, and S. Bakshi, Eds., in Advances in Intelligent Systems and Computing, vol. 713. , Singapore: Springer Singapore, 2019, pp. 403–414. doi: 10.1007/978-981-13-1708-8_37.

[24] M. Pandey and V. Ravi, "Detecting phishing e-mails using text and data mining," in *2012 IEEE International Conference on Computational Intelligence and Computing Research*, IEEE, 2012, pp. 1–6. Available: https://ieeexplore.ieee.org/abstract/document/6510259/

[25] "Zeszyty Naukowe Dolnośląskiej Wyższej Szko\ly Przedsiębiorczości i Techniki. Studia z Nauk Technicznych, - Google Search." Available:

https://www.google.com.pk/search?q=Zeszyty+Naukowe+Dolno%C5%9Bl%C4%85skiej+Wy%C5%BCszej+Szko%5Cly+Przedsi%C4%99biorczo%C5%9Bci+i+Techniki.+Studia+z+Nauk+Technicznych%2C&sca_esv=e2da69de12d3bb4c&sca_upv=1&gl=pk&source=hp&ei=RLtBZougON6ji-gPgeufiA4&iflsig=AL9hbdgAAAAAZkHJVCQAGc2OGDhvWmhf0vlgTQSxI6SV&ved=0ahUKEwiL0oHeh4qGAxXe0QIHHYH1B-EQ4dUDCBU&uact=5&oq=Zeszyty+Naukowe+Dolno%C5%9Bl%C4%85skiej+Wy%C5%BCszej+Szko%5Cly+Przedsi%C4%99biorczo%C5%9Bci+i+Techniki.+Studia+z+Nauk+Technicznych%2C&gs_lp=Egdnd3Mtd2l6Im1aZXN6eXR5IE5hdWtvd2UgRG9sbm_Fm2zEhXNraWVqIFd5xbxzemVqIFN6a29cbHkgUHJ6ZWRzacSZYmlvcmN6b8WbY2kgaSBUZWNobmlraS4gU3R1ZGlhIHogTmF1ayBUZWNobmljem55Y2gsSABQAFgAcAB4AJABAJgBAKABAKoBALgBA8gBAPgBAvgBAZgCAKACAJgDAJIHAKAHAA&sclient=gws-wiz

[26] M. Bazarganigilani, “Phishing E-Mail detection using ontology concept and naive Bayes algorithm,” *Int. J. Res. Rev. Comput. Sci.*, vol. 2, no. 2, p. 249, 2011.

[27] K. Kerremans, Y. Tang, R. Temmerman, and G. Zhao, “Towards ontology-based e-mail fraud detection,” in *2005 portuguese conference on artificial intelligence*, IEEE, 2005, pp. 106–111. Available: https://ieeexplore.ieee.org/abstract/document/4145934/

[28] S. Li and R. Schmitz, *A novel anti-phishing framework based on honeypots*. IEEE, 2009. Available: https://ieeexplore.ieee.org/abstract/document/5342609/

[29] S. Das, A. Kim, Z. Tingle, and C. Nippert-Eng, “All About Phishing: Exploring User Research through a Systematic Literature Review.” arXiv, Aug. 16, 2019. Available: http://arxiv.org/abs/1908.05897

[30] D. Florêncio and C. Herley, “Password Rescue: A New Approach to Phishing Prevention.,” in *HotSec*, 2006. Available: https://www.usenix.org/event/hotsec06/tech/full_papers/florencio/florencio.pdf

[31] H. Sharma, E. Meenakshi, and S. K. Bhatia, “A comparative analysis and awareness survey of phishing detection tools,” in *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, IEEE, 2017,

pp. 1437–1442. Available: https://ieeexplore.ieee.org/abstract/document/8256835/

[32] "Enhancing IOT security: Proactive phishing website detection using Deep Neural Networks case study: smart home | Journal of Telecommunications and the Digital Economy." https://search.informit.org/doi/abs/10.3316/informit.T2024040300010891240159221

[33] S. Yousif Mohammed *et al.*, "A Two-Stage Hybrid Approach for Phishing Attack Detection Using URL and Content Analysis in IoT," *BIO Web Conf.*, vol. 97, p. 00059, 2024, doi: 10.1051/bioconf/20249700059.

[34] A. K. Mishra, A. K. Tripathy, S. Saraswathi, and M. Das, "Prevention of Phishing Attack in Internet-of-Things based Cyber-Physical Human System," in *High Performance Vision Intelligence*, vol. 913, A. Nanda and N. Chaurasia, Eds., in Studies in Computational Intelligence, vol. 913. , Singapore: Springer Singapore, 2020, pp. 15–32. doi: 10.1007/978-981-15-6844-2_2.

[35] N. Z. Jhanjhi, M. Humayun, and S. N. Almuayqil, "Cyber security and privacy issues in industrial internet of things.," *Comput. Syst. Sci. Eng.*, vol. 37, no. 3, 202. Available: https://cdn.techscience.cn/ueditor/files/TSP_CSSE-37-3/TSP_CSSE_15206/TSP_CSSE_15206.pdf