Defending Against Phishing Attacks on Cloud-Systems: What Has Been Studied?

Carlos Eduardo Araújo Cardoso Cidrão, Oskar Hermansson and Simon Hacks[a]
Department of Computer and Systems Sciences, Stockholm University, Stockholm, Sweden

Keywords: Phishing, Cloud, Cyber Defense, Systematic Literature Review.

Abstract: Phishing attacks, a cybercrime where attackers deceive victims into revealing personal and financial information, present significant threats to cloud-based systems. Securing these environments has become paramount with the growing adoption of cloud services. This study addresses the research question: ”What is the overall perception of strategies in scientific publications to counter phishing attacks targeting cloud services?” Using a systematic literature review approach, the research synthesized findings from 13 selected scientific articles, focusing on technical and social defense strategies against phishing.

The study highlights the human factor as a critical vulnerability despite existing technical solutions like advanced authentication, IDS (Intrusion Detection System), and machine learning. Effective defense requires combining technical measures with user education and adapting to evolving phishing strategies. It calls for greater integration of social aspects into technical solutions and targeted research on cloud-specific defenses and AI’s role in phishing mitigation.

1 INTRODUCTION

Phishing is a cybercrime where fraudsters ”fish” for information. Users can also be tricked into sending money to the fraudster. This cyberattack is usually initiated via messages containing a clickable link to a deceptive website. The website appears legitimate to the user but is controlled by the fraudster. Phishing is a term that was first introduced in 1996 and has evolved since then (Chaudhry et al., 2016).

Cloud-based systems originated from a project at MIT in 1963, funded by DARPA, which aimed to create a computer solution for multiple simultaneous users, an early form of cloud computing (Surbiryala and Rong, 2019). These systems have evolved significantly, offering functionalities beyond multi-tenancy, such as resource pooling and scalability, where users can adjust computing power as needed (Surbiryala and Rong, 2019). Delivery models include Infrastructure-as-a-Service (IaaS), providing computing infrastructure over the internet; Platform-as-a-Service (PaaS), offering a platform for developing cloud solutions; and Software-as-a-Service (SaaS), delivering complete software services like Dropbox and Office365 directly to end-users over the internet (Surbiryala and Rong, 2019).

Cloud services are becoming more and more popular. Consequently, security becomes one of the primary concerns for users due to a lack of resources and expertise in the area (Chiew et al., 2018). As cloud services’ popularity and information richness increase, they become more attractive targets for phishing attacks (Chiew et al., 2018). For example, phishing within cloud services generally occurs outside the environment through social engineering, which can be a phishing attack. These types of cyberattacks are often characterized by the difficulty of identifying them with external programs that monitor security within a system (Rakotondravony et al., 2017; Prasad et al., 2022). Thus, it is a type of attack that is hard to identify through conventional security systems within cloud services, while phishing attacks are common (Prasad et al., 2022). While defending against phishing in cloud environments and classical environments share many commonalities, there are differences due to the distributed nature of cloud environments, shared responsibility between providers and users, and the heightened complexity of securing dynamic, multi-tenant infrastructures against increasingly sophisticated attack vectors.

However, previous research in this field has primarily focused on the technical aspects of cybersecu-

[a] https://orcid.org/0000-0003-0478-9347

Cidrão, C. E. A. C., Hermansson, O. and Hacks, S.
Defending Against Phishing Attacks on Cloud-Systems: What Has Been Studied?.
DOI: 10.5220/0013140000003899

In *Proceedings of the 11th International Conference on Information Systems Security and Privacy (ICISSP 2025) - Volume 1*, pages 234-241
ISBN: 978-989-758-735-1; ISSN: 2184-4356

rity (Prasad et al., 2022; Abusaimeh, 2020; Butt et al., 2023). At the same time, to the best of our knowledge, there are limited studies elaborating on the social aspects. To get a better overview of the existing research and to control if we are missing out on social factors, this study provides an overview of existing research on phishing defense strategies. Accordingly, we formulate our research question: *"What is the overall perception of strategies in scientific publications to counter phishing attacks targeting cloud services?"*

This article comprehensively synthesizes existing defense strategies against phishing attacks targeting cloud systems, encompassing both technical and social approaches. It identifies key gaps in integrating social aspects into technical solutions and emphasizes the need for tailored strategies specific to cloud service models like SaaS, PaaS, and IaaS. To illustrate this, we give the needed background on phishing and detail the notion of cloud systems, followed by related work elaborating on similar issues. Next, we detail how we conducted our systematic literature review and present the findings based on the scientific literature. Before we conclude the work, we discuss the findings and indicate future research directions.

2 BACKGROUND

2.1 Phishing

Phishing is a cyberattack that employs various methods to deceive victims into revealing information, which is then illicitly used by the fraudster. The logic behind this kind of cyberattack is that the attacker uses "bait" to lure and "fish" for the victim's personal information. Since phishing was first introduced in the 1990s, fraudsters have developed new methods and media, making it one of the primary attack vectors hackers use. Phishing has continued to be widely used, and "spear phishing" has become the most common vector for distributing malware (Alabdan, 2020).

SaaS and webmail were the main focus for fraudsters in the early years, accounting for one-third of all cyberattacks (Alabdan, 2020). Regarding the financial aspects of phishing, services to create customized phishing pages are sold for three to twelve US dollars, indicating that it is relatively inexpensive for a fraudster to launch a phishing attack. It also appears that a common method for fraudsters to cash out their proceeds is through gift cards. The Federal Bureau of Investigation (FBI) estimated that the total loss due to phishing in 2018 was almost 50 million US dollars, affecting tens of thousands of organizations and individuals (Alabdan, 2020).

A successful phishing attack follows a five-step lifecycle (Shaikh et al., 2016): (1) Planning and Setup, where the fraudster gathers information about the target; (2) Phishing, involving the sending of manipulated emails that appear legitimate to trick the victim into clicking a malicious link; (3) Infiltration, where clicking the link installs malware on the victim's device, granting the attacker access to the system; (4) Data Collection, during which the attacker extracts valuable information, potentially including financial data; and (5) Exfiltration, where the attacker removes traces of the attack to avoid detection and evaluates the attack's success for future optimization.

Various strategies can be employed to counter phishing (Chaudhry et al., 2016). On the client side, robust password management is pivotal, e.g., by encouraging users to use unique passwords generated by a password management system. This also includes electronic communication filtering, content filtering, and encryption to ensure data integrity. Installing firewalls, filters, antivirus, and antimalware technologies is recommended to strengthen endpoint security and reduce the reception of known phishing attempts. The importance of digital certificates and secure email protocols is also stressed. Immediate communication upon identifying phishing attacks, preparation for security breaches, and support from specialized units are critical measures. Additionally, training end-users to recognize phishing attempts is the most fundamental strategy for combating phishing.

On the server side, implementing authentication methods, such as two-factor or multi-factor authentication, is essential to enhance security levels (Chaudhry et al., 2016). Website personalization is highlighted as another strategy to improve user safety. It also stressed that participating in and contributing to security research communities to report and share information on security incidents is effective. This underscores the necessity for close collaboration between system administrators, law enforcement agencies, and other stakeholders within a trusted community to detect and prevent phishing attacks early.

2.2 Cloud-Services

Cloud-based computing is a category of utility computing; a computer should be a public utility accessible to the general population (Filipe and Obaidat, 2009). This idea evolved into using computers to share resources over the internet with end customers (Antonopoulos and Gillam, 2010). Cloud computing is (Antonopoulos and Gillam, 2010): *"A model of service delivery and access where dynamically scalable and virtualized resources are provided* *as a service over the Internet."* This definition outlines what a cloud-based system should perform, the characteristics it should possess, and how the service should be delivered. Cloud systems enable companies to leverage computing power they do not own by outsourcing their IT infrastructure to third-party providers (Antonopoulos and Gillam, 2010).

Deployment models are part of cloud systems and include different ways to store data in public, private, or hybrid infrastructures. The public model makes the cloud accessible to the general public, potentially through a company selling its cloud services to individuals and businesses. The private model is intended for a specific organization, with access restricted to authorized personnel. The hybrid model is more complex, combining two or more clouds, both public and private, where each user is a unique entity with different access levels within the system (Goyal, 2014).

As companies increasingly migrate their systems to the cloud, they encounter new challenges related to cybersecurity, as stored data gets more vulnerable to cyberattacks such as phishing and malware. The potential damage is substantial since the data often includes customer purchases, ongoing orders, addresses, and personal identification numbers. Humayun et al. (Humayun et al., 2022) emphasize that while companies can protect themselves with security programs specific to cloud systems, they must still adhere to best practices to enhance cybersecurity.

Despite the operational differences between cloud systems and traditional data centers, cloud environments encounter the same threats because these systems often use the same technology as traditional data centers. Tripathy et al. (Tripathy et al., 2020) argue that organizations find it more challenging to maintain visibility and control over data in the cloud, as unauthorized individuals can access the cloud and add new data without the organization's knowledge. Such unauthorized access can cause significant harm to a cloud-based system. Additionally, fraudsters seek to exploit vulnerabilities in a program's Application Programming Interface (API) keys to access an organization's cloud systems and infect other organizations using the same provider. Fraudsters employ various types of SQL attacks to access data stored in the system's database (Tripathy et al., 2020).

2.3 Related Work

Butt et al. (Butt et al., 2023) conducted a scientific study to identify cloud-based email phishing attacks, concluding that phishing poses a significant threat to cloud systems. They argue that a robust framework integrating machine learning and deep learning techniques can help defend phishing in cloud environments. Therefore, they suggest that future research explore advanced deep learning models and expand with more training data to cover more phishing email cases.

Another study identifies the security risks associated with cloud-based systems, such as data placement, data segregation, and user rights within a cloud system (Balani and Varol, 2020). It is suggested that companies adopt best practices for user authentication, clear service-level agreements (SLA), transparency among cloud service providers, and standardization of security measures. They emphasize the importance of developing security standards for all cloud-based systems to promote safe usage.

Prasad et al. (Prasad et al., 2022) explore effective methods for detecting phishing URLs, where logistic regression has proven particularly effective with an accuracy of 94%. The study highlights the importance of continuing to develop deep learning algorithms to improve the ability to classify and counter phishing attacks. The authors suggest further exploration of reinforcement learning mechanisms for monitoring cloud environments and developing more sophisticated defenses against evolving phishing methods.

Abusaimeh (Abusaimeh, 2020) presents a comprehensive study on authentication attacks in cloud services and corresponding defense mechanisms. The author examines various attacks, such as phishing, and how cloud services can defend against them. The significance of robust authentication systems for improving cloud security is central to achieving good security. Solutions such as multi-factor authentication and image-based passwords are proposed as effective methods to counter phishing. Future research shall broaden the range of studies to include a greater variety of defense mechanisms, indicating a continuous need for innovation and development of security measures against the ever-changing threats in cloud services.

Previous research in cloud-based cybersecurity highlights the continuous development and adaptation needed to defend against phishing attacks. These studies indicate that it is crucial to quickly identify security problems and challenges due to cloud services' ever-changing nature. Despite progress in identifying and combating phishing attacks, these studies emphasize the need for further research to strengthen defense mechanisms in cloud services. Our work aims to provide a systematic overview of the research to identify future research directions better.

Table 1: Search Terms.

Search Terms	Articles
”SaaS” AND ”phishing”	2
”PaaS” AND ”phishing”	1
”IaaS” AND ”phishing”	4
”phishing detection techniques”	58
”phishing” AND ”cloud”	300

3 RESEARCH METHOD

A qualitative approach is applied as a document study to answer the research question. This study follows Kitchenham and Charters (Kitchenham et al., 2007), focusing on scientific articles about phishing attacks on cloud services. This approach aims to map existing research in this area. Kitchenham and Charters (Kitchenham et al., 2007) describe this research strategy as a structured method for conducting literature reviews to systematically collect, review, and synthesize existing research in a field. This is relevant to understanding and identifying patterns, trends, and potential knowledge gaps in the research on phishing attacks against cloud services. As a database, this study relies on Scopus as it is a curated list of scientific venues that ensures the quality of the included articles, e.g., that they have undergone a scientific peer review.

The search terms are presented in table 1. Only articles published from 2014 to 2024 were included to focus on relevant research from the past decade; the articles must be available, written in English, and have gone through a peer-review process. After gathering the articles by the search terms ($n = 365$), duplicates were removed ($n = 363$), and the articles' abstracts and titles that meet the inclusion criteria[1] were reviewed ($n = 26$). Subsequently, a deeper full-text review was conducted ($n = 7$). Based on the remaining articles, snowballing resulted in $n = 13$ articles to be included in our results.

Next, we performed a content analysis (Denscombe, 2017), following Johannesson & Perjons (Johannesson and Perjons, 2014) six steps: (1) select a sample of text material, (2) break down the sample into units, (3) develop categories for analysis, (4) code the units according to the categories, (5) count the frequency of the units for each category, and (6) analyze the text with the frequency aspect in mind.

4 RESULTS

The coding yielded four themes, including six categories and 25 identified codes (cf. online appendix[2]). Following, we present our findings in more detail.

4.1 Defense Methods

Technical Methods. The identified codes show various technical defense methods against phishing in cloud services. One such method is various types of *software security*, including antivirus and antimalware technologies that prevent, detect, and remove malicious software. There is also a focus on *communication security*, where techniques such as electronic communication filtering and secure email protocols are used to filter and encrypt data exchanged over corporate networks, ensuring data integrity and enhancing trust in internal data (Chaudhry et al., 2016).

Network security has also been central among the articles, with examples such as firewalls, Intrusion Detection Systems (IDS), and various filters to monitor and protect the network from malicious traffic. Additionally, the importance of *system and data protection* is emphasized, focusing on password management, digital certificates, two-factor authentication, and regular operating system updates.

The *cloud security* code aims to highlight various discussed defense methods, such as blockchain technology, security layers for cloud storage, dynamic resource allocation, IP reputation monitoring, blacklisting, and user access controls. For instance, Vayansky and Kumar (Vayansky and Kumar, 2018) discuss that phishing can be stopped before it reaches the user through blacklisting or by blocking phishing websites. Furthermore, Chandra et al. (Chandra et al., 2015) mention that their solution includes a detailed user access control mechanism that ensures secure data file transfer, making it impossible to force entry into their system. The study by Karthika et al. (Karthika et al., 2023) used a solution called ”Phish Block” to detect phishing URLs within cloud-based systems. This was achieved by leveraging blockchain technology, whose immutable structure ensures that data stored in the blockchain cannot be altered. The researchers' solution also uses homographic URL detection through smart contract algorithms. Therefore, there are many different technical defense methods that individuals can utilize to achieve the desired result.

[1] (1) Relation to cloud systems. (2) Documentation of phishing attacks. (3) Primary study.

[2] https://github.com/simonhacks/Cloud_Phishing/blob/main/ICISSP___Cloud_Security.pdf

Social Methods. Based on the identified codes, the study shows three main groups within this category. Among these three groups, *education* was the most important and frequently mentioned in the articles. Attributes such as preparation, training, knowledge, and test cases were central to these articles. One aspect of Vayansky and Kumar's (Vayansky and Kumar, 2018) solution was that they proposed educating system stakeholders through game-based learning to identify phishing attacks. Another article supporting user training with game-based learning argues that training against phishing using comics and games is effective through empirical research (Goel et al., 2017). Other articles that mention the concept of social engineering do so more in passing as their solutions are more technically oriented (Althamary and El-Alfy, 2017; Allodi et al., 2019).

Algorithmical Methods. Research in this area has mainly focused on *machine learning*. Machine learning encompasses various techniques discussed in the articles. For example, the decision tree algorithm, Naive Bayes model, and Support Vector Machine (SVM) are directly applied in a proposed solution (Preethi et al., 2023). Jha et al. (Jha et al., 2022) use SVM in conjunction with an object detection model, "You-Only-Look-Once" (YOLO), to handle the TF-IDF representation of HTML web pages. A similar solution is found in another study where researchers use SVM along with "Adaline" and "Backpropagation" algorithms to improve the detection speed and classification of phishing attacks (Chaudhry et al., 2016).

It can be concluded that there are widespread and robust machine learning methods that various researchers frequently use to achieve the desired results. In most studies, researchers speak favorably about using the decision tree algorithm, SVM, and the Naive Bayes model for machine learning.

4.2 Evaluation

Criteria. Different evaluation criteria have been used to assess the *performance* of technical defense methods across all articles. These include detection rate, accuracy, precision, recall, and F1-score. These metrics are central to evaluating how effectively the techniques can identify phishing attacks. For example, accuracy measures the overall proportion of correct identifications compared to the total number of cases tested (Preethi et al., 2023), while precision and recall focus on how well the system identifies actual phishing URLs and avoids false positives (Jha et al., 2022). The F1-score combines precision and recall to provide a balanced view of system performance. Additionally, Top-k Match Accuracy and AUC (Area Under Curve) are used to assess specific applications like visual similarity analysis and logo recognition (Jha et al., 2022). These metrics help comprehensively understand the techniques' performance in various scenarios.

The *effectiveness* of defense methods is evaluated through measures such as processing delay, cost-effectiveness, and resource efficiency. Processing delay is critical to ensure the system can detect phishing attacks in real-time (Preethi et al., 2023). Cost-effectiveness and resource efficiency assess how well the systems use available resources and manage costs, which is crucial for long-term sustainability and practical implementation (Chandra et al., 2015; Wu et al., 2017; Gutierrez et al., 2018).

The *reliability* of defense methods is analyzed through metrics like false positives, misclassification rate, Matthew's Correlation Coefficient (MCC), and confusion matrix. These metrics help us understand how often the system makes incorrect classifications and its reliability in identifying actual threats (Chaudhry et al., 2016; Karthika et al., 2023; Preethi et al., 2023). MCC and the confusion matrix provide deeper insights into system performance by showing the distribution of correct and incorrect classifications.

User behavior is also assessed to understand how users impact the effectiveness of defense systems. Metrics such as users' ability to follow security advice and training effectiveness evaluate how accurately users follow security instructions and how well training programs work (Chaudhry et al., 2016). Opening rates and click rates analyze how often users interact with phishing messages, providing insights into the credibility of the messages. Additionally, manipulation checks, sufficiency threshold, and heuristic versus systematic processing examine users' cognitive processes and decision-making (Goel et al., 2017). Emotional and motivational drivers are also assessed to understand how user behavior affects system effectiveness (Goel et al., 2017). These aspects are important for developing defense strategies considering technical and human factors.

4.3 Challenges

Technical Challenges. The identified codes reveal various technical challenges in defending against phishing within cloud services. *Machine learning* faces issues with efficiency and precision, where defense methods can vary in accuracy and performance, resulting in both positive and negative outcomes (Prasad et al., 2022). Machine learning models require large amounts of data for training and must be continuously updated to address new phishing techniques (Jha et al., 2022). Preethi et al. (Preethi et al., 2023) emphasize that continuous updating is critical to handle new phishing strategies, but these processes are resource-intensive and require constant monitoring. Advanced phishing strategies further complicate detection, necessitating continual adaptation of machine learning models (Gutierrez et al., 2018; Vayansky and Kumar, 2018). Limitations in URL detection and lack of adaptability are additional problems affecting detection efficiency (Karthika et al., 2023).

In *cloud security*, the complexity of shared responsibility between cloud users, cloud providers, and potentially third parties creates difficulties in maintaining a uniform level of security (Prasad et al., 2022). Phishing attacks leveraging cloud services can be harder to detect as they often appear more legitimate and have fewer random URLs, requiring models to adapt to these sophisticated attacks (Jha et al., 2022). *Blockchain* presents technical challenges such as implementation complexity, high computational costs, and limited scalability (Karthika et al., 2023). These factors make it challenging to integrate blockchain technology effectively into security solutions.

Social Challenges. In this code, there was no outlier in the frequency of codes as seen in the previous categories. The coding identified four main groups within the codes. Within the *user-related challenges* code, the study found inefficiency in browser extensions and toolbars, as 35-45% of users still clicked on phishing emails despite these additions, which also ties into another challenge highlighted in this thesis, namely the disregard of warning systems and user errors (Goel et al., 2017).

Goel et al. (Goel et al., 2017) also discuss the short-term effect of *education and training* in connection with phishing IQ tests. The researchers claim that it can have a counterproductive effect, as a phishing IQ test might cause fear of phishing instead of the desired effect of making users better at identifying phishing attempts. Another challenge the study presents is that people make quick and intuitive decisions based on their first impression of a situation due to *cognitive limitations*. In this case, it can negatively affect users as a fraudster might trick them into clicking on a link they believe is legitimate when it is not (Loxdal et al., 2021; Goel et al., 2017).

The study also highlights *individual and cultural differences* in the reception of a phishing attack. Goel et al. (Goel et al., 2017) emphasize that people from different cultures receive phishing training in various ways. For example, the study showed that people from the USA responded well to training, while those from Sweden and India did not have the same positive effect. Overall, the study reveals that there were not many articles addressing the social challenges of phishing.

5 DISCUSSION

Our results show that firewalls, Intrusion Detection Systems (IDS), and secure email protocols are proven effective in protecting cloud services from malicious phishing attacks in scientific studies. Implementing advanced authentication methods, such as two-factor authentication and digital certificates, has also been critical in maintaining robust security and enhancing data integrity within cloud services (Chaudhry et al., 2016). Thus, defense methods against phishing within cloud services are actively developed. Another prominent trend is that researchers often combine multiple techniques to leverage their complementary strengths. For example, combining machine learning techniques such as SVM and decision trees has improved detection capabilities and reduced false positive results (Preethi et al., 2023). This strategy involves using different algorithms and techniques to take advantage of their benefits, resulting in more robust and effective security systems.

Further, studies have shown that integrating various machine learning techniques, such as Naive Bayes and SVM, can handle the complexity of phishing attacks more effectively (Chaudhry et al., 2016). By combining these techniques, security systems can better predict and identify potential phishing attacks. Despite these advancements, significant challenges must be overcome. Implementing these techniques requires extensive data collection and processing, which can be resource-intensive in terms of time and infrastructure. There is also a need to continuously update and adjust algorithms to handle the constantly evolving phishing strategies.

Another important insight from the study is the critical role that user education and awareness play in preventing phishing attacks. Several researchers have emphasized that technical solutions must be complemented with user education programs, which have been shown to reduce the risk of successful phishing attacks (Chaudhry et al., 2016). Education programs that include various forms of training, including traditional training sessions, interactive seminars, and game-based learning, have proven particularly effective. These methods enhance users' ability to identify phishing attempts by creating an engaging and practical learning environment (Vayansky and Kumar, 2018). Despite this, challenges remain, such as the short-term effect of education programs and cultural differences in the receptiveness to training, which need to be addressed to maximize the effectiveness of these programs (Goel et al., 2017). Additionally, phishing attacks leveraging cloud services are often harder to detect as they can appear more legitimate and use less random URLs. This requires continuously adapting and updating security systems to handle these sophisticated attacks (Jha et al., 2022).

Although technical solutions are essential, the study shows that the human factor is crucial in effectively combating phishing attacks. Employees' ability to identify and respond to phishing attempts is one of the most critical aspects of maintaining security within an organization. This is emphasized by Goel et al. (Goel et al., 2017), who point out that regular and updated training programs tailored to the organization's specific needs and cultural context can significantly reduce the risk of successful phishing attacks. This study highlights a significant gap in the analyzed studies focusing solely on technical solutions. While technical systems can offer high accuracy in detecting phishing attacks, it is crucial not to underestimate the social aspect of security. Lapses in user education and awareness can lead to the failure of even the most advanced technical solutions. Therefore, security strategies must integrate comprehensive educational efforts to ensure that users are well-prepared to identify and manage phishing attempts (Goel et al., 2017).

6 CONCLUSION

This study aimed to identify the mapped strategies in previous research to understand the general perception surrounding them. The findings indicate that the general perception of phishing attacks on cloud services involves manipulating users deceived by fraudsters. Many researchers described phishing as a form of social engineering. Despite this, most of the proposed solutions to remediate phishing focused on technical aspects. At the same time, we found some studies elaborating on the social aspect of phishing, such as user education, to counter the effectiveness of a phishing attack. The consensus was that technical solutions address much of the problem with simple phishing traps and virtually make it impossible to penetrate a cloud system with the various technical protections implemented within the systems. Therefore, there is no significant focus on the social aspect of a phishing attack; instead, the emphasis is on the technical solutions an organization can employ.

There are limitations to this study. Firstly, there was not much research specifically related to the study's focus, which meant the authors often had to look for sources on related topics. This may be because the authors chose to base their selection of articles solely on the Scopus database; relevant research may exist in other databases. Additionally, the predetermined criteria for article selection can be retrospectively criticized since much research that considered the social aspect could have been done before 2014.

Kitchenham and Charter (Kitchenham et al., 2007) discuss researcher bias and publication bias, which refer to the tendency for positive results to be more likely to be published than negative ones, as well as the researchers' impartial interpretation of data. This factor could have affected the study's results despite the authors' efforts to read the articles impartially. It is challenging to remain completely unbiased throughout an entire literature analysis.

This work has identified the general strategies for countering phishing in cloud-based systems. It has become clear that there is a significant need to develop the mindset around the social aspects of technical solutions against phishing, as much evidence points to the human factor being the most significant and most volatile risk in phishing attacks on cloud services. The authors suggest that future research should emphasize integrating social aspects into technical solutions, as it is not enough to create a robust technical solution without providing individuals using the system with the right conditions.

The development of artificial intelligence (AI) further complicates this area. As AI has become increasingly advanced in recent years (especially generative AI), fraudsters can use AI to emulate a person's signature, writing style, or voice, making it even more challenging to identify a phishing attempt. Therefore, future research should also focus on the social aspects of AI and phishing.

ACKNOWLEDGEMENTS

This work has received funding from European Union's HORIZON research and innovation programme under the Grant Agreement no. 101138583.

REFERENCES

Abusaimeh, H. (2020). Security attacks in cloud computing and corresponding defending mechanisims. *Interna-*

tional Journal of Advanced Trends in Computer Science and Engineering, 9(3).

Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. *Future internet*, 12(10):168.

Allodi, L., Chotza, T., Panina, E., and Zannone, N. (2019). The need for new antiphishing measures against spear-phishing attacks. *IEEE Security & Privacy*, 18(2):23–34.

Althamary, I. A. and El-Alfy, E.-S. M. (2017). A more secure scheme for captcha-based authentication in cloud environment. In *2017 8th International Conference on Information Technology (ICIT)*, pages 405–411. IEEE.

Antonopoulos, N. and Gillam, L. (2010). *Cloud computing*, volume 51. Springer.

Balani, Z. and Varol, H. (2020). Cloud computing security challenges and threats. In *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, pages 1–4. IEEE.

Butt, U. A., Amin, R., Aldabbas, H., Mohan, S., Alouffi, B., and Ahmadian, A. (2023). Cloud-based email phishing attack using machine and deep learning algorithm. *Complex & Intelligent Systems*, 9(3):3043–3070.

Chandra, J. V., Challa, N., and Pasupuleti, S. K. (2015). Intelligence based defense system to protect from advanced persistent threat by means of social engineering on social cloud platform. *Indian Journal of Science and Technology*.

Chaudhry, J. A., Chaudhry, S. A., and Rittenhouse, R. G. (2016). Phishing attacks and defenses. *International journal of security and its applications*, 10(1):247–256.

Chiew, K. L., Yong, K. S. C., and Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, 106:1–20.

Denscombe, M. (2017). *The good research guide: For small-scale social research projects*. McGraw-Hill Education (UK).

Filipe, J. and Obaidat, M. S. (2009). *E-business and Telecommunications: International Conference, ICETE 2008, Porto, Portugal, July 26-29, 2008, Revised Selected Papers*, volume 48. Springer Science & Business Media.

Goel, S., Williams, K., and Dincelli, E. (2017). Got phished? internet security and human vulnerability. *Journal of the Association for Information Systems*, 18(1):2.

Goyal, S. (2014). Public vs private vs hybrid vs community-cloud computing: a critical review. *International Journal of Computer Network and Information Security*, 6(3):20–29.

Gutierrez, C. N., Kim, T., Della Corte, R., Avery, J., Goldwasser, D., Cinque, M., and Bagchi, S. (2018). Learning from the ones that got away: Detecting new forms of phishing attacks. *IEEE Transactions on Dependable and Secure Computing*, 15(6):988–1001.

Humayun, M., Niazi, M., Almufareh, M. F., Jhanjhi, N., Mahmood, S., and Alshayeb, M. (2022). Software-as-a-service security challenges and best practices: A multivocal literature review. *Applied Sciences*, 12(8):3953.

Jha, B., Atre, M., and Rao, A. (2022). Detecting cloud-based phishing attacks by combining deep learning models. In *2022 IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*, pages 130–139. IEEE.

Johannesson, P. and Perjons, E. (2014). *An introduction to design science*, volume 10. Springer.

Karthika, R., Valliyammai, C., and Naveena, M. (2023). Phish block: A blockchain framework for phish detection in cloud. *Computer Systems Science & Engineering*, 44(1).

Kitchenham, B., Charters, S., et al. (2007). Guidelines for performing systematic literature reviews in software engineering version 2.3. *Engineering*, 45(4ve):1051.

Loxdal, J., Andersson, M., Hacks, S., and Lagerström, R. (2021). Why phishing works on smartphones: A preliminary study. In *54th Annual Hawaii International Conference on System Sciences, HICSS 2021*, pages 7173–7182. ScholarSpace.

Prasad, V. K., Dansana, D., Mishra, B. K., and Bhavsar, M. (2022). Intensify cloud security and privacy against phishing attacks. *ECS Transactions*, 107(1):1387.

Preethi, P., Ramadevi, P., Akshaya, K., Sangamitra, S., and Pritikha, A. (2023). Analysis of phishing attack in distributed cloud systems using machine learning. In *2023 Second International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT)*, pages 1–5. IEEE.

Rakotondravony, N., Taubmann, B., Mandarawi, W., Weishäupl, E., Xu, P., Kolosnjaji, B., Protsenko, M., De Meer, H., and Reiser, H. P. (2017). Classifying malware attacks in iaas cloud environments. *Journal of Cloud Computing*, 6:1–12.

Shaikh, A. N., Shabut, A. M., and Hossain, M. A. (2016). A literature review on phishing crime, prevention review and investigation of gaps. In *2016 10th international conference on software, knowledge, information management & applications (SKIMA)*, pages 9–15. IEEE.

Surbiryala, J. and Rong, C. (2019). Cloud computing: History and overview. In *2019 IEEE Cloud Summit*, pages 1–7. IEEE.

Tripathy, D., Gohil, R., and Halabi, T. (2020). Detecting sql injection attacks in cloud saas using machine learning. In *2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, pages 145–150. IEEE.

Vayansky, I. and Kumar, S. (2018). Phishing–challenges and solutions. *Computer Fraud & Security*, 2018(1):15–20.

Wu, W., Hu, S., Yang, X., Liu, J. K., and Au, M. H. (2017). Towards secure and cost-effective fuzzy access control in mobile cloud computing. *Soft Computing*, 21:2643–2649.