The Evolution of Phishing Attacks: Spoofed Email Detection Technique Using Slam Model

Shivani Sompura[a], Pooja Shah[b]

[a]Post Graduate student,Gandhinagar Institute of Technology, Khatraj-Kalol Road, Moti Bhoyan, Gandhinagar district, Kalol, Gujarat 382721
[b]Assistant Professor, Gandhinagar Institute of Technology, Khatraj-Kalol Road, Moti Bhoyan, Gandhinagar district, Kalol, Gujarat 382721

Abstract

Phishing is a type of identity theft in which Internet users are duped into disclosing personal information such as login credentials, credit/debit card details, and so on. In recent years, researchers have created a variety of anti-phishing technologies. However, the issue persists. As a result, this study paper provides a thorough examination of phishing attack strategies and detection procedures. The research was divided into three phases: a first phishing attack, knowledge transfer using a mixed-approach, and a second phishing attack with new material. Following data validation and analysis, it was discovered that people's degree of cyber security awareness improved dramatically. The proportion of people that opened the phishing email fell by 71.5%. As a result, the proposed technique can improve cyber security in many organisations and sectors/industries by identifying E-mail spoofing with the SLAM model. It will also assist various users in avoiding phishing assaults while using the Internet for their daily activities, and new tactics will advise administrators in detecting phishing risks such as email spoofing.

Keywords: Phishing, Theft, Anti phishing, Spoofing, Detection, SLAM Model.

1. Introduction

The advancement of technology and communication systems ushered in a new era of digital movement. People and businesses today rely nearly entirely on technology for their operations. It improved efficiently, but this approach has also increased the risk of threats; the growing use of technology means that crucial infrastructure components are vulnerable to phishing attempts. [1, 2].

Technology has made everyone's life much easier. People can get anything with a single click and store data in one place. However, it has also become a nightmare because it has made it easy for hackers to steal data through phishing assaults. This situation is becoming increasingly severe as a result of the massive surge in cybercrime.

Hackers deploy various sorts of social engineering assaults; securing the information of vital infrastructure and databases from such disruption and attacks is critical, and will be one of the primary issues in the future. Phishing is one of the most well-known social engineering attacks. It is often used by hackers to entice victims to give sensitive and personal information. [3, 4].

Terrorists use phishing attacks to promote propaganda and disinformation, raise funds, plan campaigns, and offer information on them. In the future, they may attempt to launch attacks on the country's essential infrastructure. As a result, fighting them with intelligent systems capable of detecting, evaluating, and responding to phishing assaults have become a need [23].

Furthermore, phishing assaults are not localised; they are a global hazard that poses a threat to any system in the globe at an increasing rate. This is why we require creative techniques such as the faked E-mail strategy using the SLAM model, which provides learning power to software and will aid humans in combating such attacks. [11, 15].

The purpose of this study is to present applying spoofed e-mail detection techniques for phishing attacks, to demonstrate how these techniques can be effective for detection & prevention of phishing attacks, as well as to give the scope for future world.

2. Phishing: Definition, Need, Lifecycle and Issues.

2.1. Phishing Attack and Issues

Phishing is a type of cyber assault that employs email, phone, or text messages to encourage people to provide personal or sensitive information, such as passwords, credit card information, and social security numbers, as well as information about a person or organisation [1].

Phishing is a type of identity theft that deceives Internet users into disclosing personal information; in recent years, researchers have created a variety of antiphishing solutions. However, the issue persists. As a result, this study provides a thorough examination of phishing attack strategies and detection procedures [13].

Phishing attacks are typically carried out through the use of emails. The word "fishing" is derived from the words "password harvesting" and "fishing for passwords." "Brand spoofing" is another term for it. Phishers are con artists. The term 'phishing' was first used on January 2, 1996. During the 1990s, hackers would pose as AOL administrators and phish for login credentials in order to gain free internet access. Phishing began to evolve at a rapid pace in the 2000s and 2010s. Phishing was the most common cyber crime in 2020, according to the FBI's 2020 Internet Crime Report, with over 240,000 victims and a loss of more than $50 million. And the number of victims has more than doubled since 2019 and is almost ten times higher than in 2018[17].

Phishing accounts for more than 80% of all "social actions," another term for social engineering attacks, making it by far the most common sort of such an attack. Furthermore, the survey claims that 96% of social acts are sent by email, with only 3% delivered via website and 1% submitted via phone or text. Phishing attacks are typically carried out via email [23].

With an understanding of the specific environment, the detection technique analyses the many hazards that may exist in the given area. It then aids in the development and execution of plans to fight harmful assaults or threats. A wide range of diverse activities are engaged in detecting strategy for defending the concerned entity as well as rapid response to a danger landscape. These could include decreasing the environment's attraction to potential attackers, identifying vital locations and sensitive information, executing preventative controls to ensure attacks are costly, attack detection capability, and reaction and response capabilities. The detection technique also does technical analysis to determine the paths and regions that the attackers could target [5, 6].

The spoofing approach provides the much-needed confidence that operations and activities can be carried out without fear of danger. It aids in the most efficient use of security strategy and resources. It also aids in enhancing the effectiveness of security resources and security expenses, particularly in vital places [7, 8].

Phishing dangers saturate every company and are not usually directly under the authority of IT. Business leaders are pushing forward with digital business initiatives, and those leaders are making technology-related risk decisions on a daily basis. Increased phishing risk exists, but so are data security solutions [12].

The phishing system is critical for the government and other organisations that have a direct impact on the wellbeing and safety of the nation - or the planet - or the organisation. Phishing assaults on governments, military organisations, defence suppliers, and individuals are beginning to augment or replace physical attacks, placing nations at risk [13].

Antivirus software and firewalls no longer prevent these attacks. The risk of cyber attacks is continually increasing, and it is no longer a question of "if" but rather "when" it will occur for businesses and institutions. This is why a spoofing e-mail detection system is so critical. Security is vital because it includes everything related to protecting our data from cyber attackers who wish to steal it and use it to inflict harm. This can include sensitive data, information from government and industry, personal information, personally identifiable information (PII), and intellectual property [22].

One of the most difficult aspects of e-mail security is ensuring the safety of our data. Ransomware, phishing attacks, malware attacks, and other threats are examples of challenges. India ranks 10th in the world in terms of local cyber-attacks, with 121 million occurrences already recorded in 2021 [3].

List of the top challenges of cyber attack system:

- Ransom ware attacks
- IOT attacks
- Cloud attacks
- Phishing attacks
- Block chain and Crypto currency attacks
- Software vulnerabilities
- Machine learning and AI attacks
- BYOD policies
- Insider attacks
- Outdated hardware
- Intelligence/awareness

2.2. Lifecycle of Phishing Attacks

The lifecycle of phishing attack is shown in Figure 1. A Phishers uses following steps to take the user's credential:

Step 1: Planning and Setup: First, the Phishers identifies the target organisation and prepares the technical strategy to acquire secret information.

Step 2: Phishing Site Construction: Then, Phishers creates a phishing website that looks similar to the official website. Various online tools are available which generate a replica of a well-known website (HTTrack Website Copier- Free Software Offline Browser (GNU GPL) 2017). Cui et al. found that 90% of the malicious sites are the replica or modification of previous phishing attacks (Cui et al. 2017). After constructing the website, Phishers uploads these files to a web-hosting server.

Step 3: Phishing Spreading: Then, attacker chooses the appropriate distribution method to spread the link of the phishing website. Later, Section 3 will discuss the various phishing distribution methods.

Step 4: Installation: The fake link redirects the user to the malicious website where the user may end up providing credentials. The fake link may install some malicious software on user's system.

Step 5: Data collection: Phishers can access the data filled by the Internet user. Moreover, malicious software can also send the information stored at user's system.

Step 6: Break-Out: After receiving the user's credentials, the cybercriminals delete all the evidence, that is, the phishing websites, email accounts, and so on. The attacker can use user's credential (e.g. credit card details, username, password, etc.) for malicious purposes [28].

2.3. Motivation of Attackers

Following are the intentions of attackers behind the phishing attack

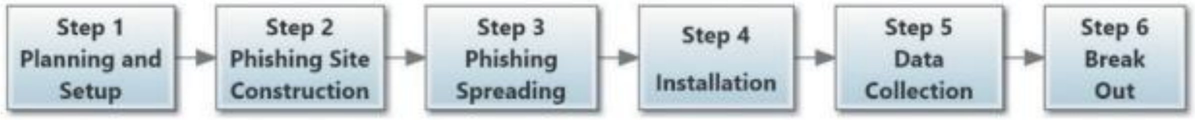

Fig. 1: Lifecycle of Phishing Attack

- Financial benefits: Stealing money from the end users is the main reason to perform phishing attacks.
- Impersonate identity: Attackers mimic the identity of legitimate user/enterprise to execute illegal projects.
- Gaining Fame and dignity: Web criminals may attack Internet users to achieve the fame and recognition.

3. The Impact of Spoofed E-Mail Technique with SLAM Model

Because the scope of risks has increased beyond what people can manage, it is now critical to automate threat detection and management. The spoof e-mail detection technique assists in automatically analysing online traffic and investigating questionable activity. SLAM can detect assaults before attackers have access to important information. In addition, the AI engine continuously learns from the huge amounts of data it analyses. This form of lifelong learning enables the organisation of the defence system to be automated, allowing it to tackle prospective attacks on its own. Detection is seen as a science that discovers solutions to complicated situations that cannot be solved without the use of intellect. Some strategic applications in the realm of cyber are increasing as a result of the manner in which computers replicate human intelligence activity. such as thinking, learning, planning etc [4, 7, 8].

The impact of spoofed email detection technique can be significant and can help mitigate the risks associated with spoofed emails. Some of the benefits of detecting spoofed emails include:

1. Reduced phishing attacks: By detecting spoofed emails, organizations can prevent phishing attacks that attempt to trick recipients into revealing sensitive information or downloading malware.

2. Improved security posture: Detecting spoofed emails can improve the overall security posture of an organization, as it helps to identify and block malicious emails before they can do harm.

3. Protection against BEC attacks: Spoofed email detection techniques can also help protect against business email compromise (BEC) attacks, where attackers impersonate high-level executives or vendors to trick employees into making fraudulent financial transactions.

4. Enhanced reputation: By preventing spoofed emails from being delivered, organizations can protect their brand reputation and avoid damage to their image caused by fraudulent emails being sent under their name.

5. Compliance with regulations: Many regulations, such as SLAM and HIPAA, require organizations to implement measures to protect personal and sensitive data. Detecting spoofed emails can help organizations comply with these regulations and avoid fines or legal penalties.

Overall, faked email detection systems can have a substantial impact and can assist organisations in reducing the risks connected with these types of assaults. Implementing advanced email security solutions, such as SLAM, can assist organisations in detecting and preventing the delivery of spoofed emails, resulting in a safer and more secure email environment [25, 26].

3.1. Spoofed e-mail Detection

The general problem of simulating intelligence has been simplified to specific sub-problems.
Which have certain characteristics or capabilities that an intelligent system should exhibit? The Following techniques have received the most attention.

- Sender Policy Framework (SPF): SPF is a DNS-based email authentication system that determines whether or not the transmitting IP address is authorised to send emails on behalf of the domain. SPF works by defining a list of authorised sending servers in DNS records, which email servers can use to validate the sender's IP address.
- Domain Keys Identified Mail (DKIM): DKIM is another DNS-based email authentication mechanism that employs cryptographic signatures to authenticate the authenticity of email messages. DKIM works by adding a digital signature to the email's header, which can be checked by the recipient's email server to confirm that the message was not tampered with in transit.
- Domain-based Message Authentication, Reporting, and Conformance (DMARC): DMARC is a DNS-based email authentication protocol that combines SPF and DKIM to give a full email authentication solution. DMARC allows domain owners to establish policies for how their emails should be handled if they fail SPF or DKIM checks, such as being rejected or sent to a quarantine folder.
- Content-based filtering: Content-based filtering is a technique for detecting phishing attacks and other malicious activity by analysing the content of emails. This can include inspecting the email's subject line, body text, and links for suspicious content.
- Machine learning and artificial intelligence (AI): Machine learning and artificial intelligence (AI) can be used to analyse massive amounts of email data and find trends that suggest phishing attacks or other harmful behaviour. This can include analysing email headers, IP addresses, and user behaviour to detect and prevent malicious activities [27, 28].

Overall, there are several different types of spoofed email detection techniques that organizations can use to protect against email spoofing and phishing attacks. Implementing a combination of these techniques can provide a comprehensive email security solution that helps protect against a range of threats.

Many solutions for safeguarding data across networks and the Internet have been created (for example, antivirus software, firewalls, encryption, secure protocols, and so on); yet, adversaries are always developing new ways to attack network systems. A detection and prevention system (DPS) is a software or hardware device installed within a network that can detect and prevent potential intrusions. DPSs perform four essential security functions: monitoring, detection, analysis, and response to unauthorised activity [14, 20].

4. Application Of Spoofed E-Mail Detection with SLAM

According to Wang et al. (2008), the application of Heuristic Technology, which means "the knowledge and skills that use some methods to determine and intelligently analyse codes to detect the unknown virus by some rules while scanning," is the future of anti-virus detection technology. According to scholarly literature, AI approaches have a wide range of applications in preventing cybercrime. For example, neural networks are being used to identify and prevent intrusions, but there are also plans to use neural networks in "Denial of Service (DoS) detection, computer worm detection, spam detection, zombie detection, malware classification, and forensic investigations." SLAM Heuristics, Data Mining, Neural Networks, and AISs techniques have also been applied to next-generation anti-virus technologies. Some IDSs use intelligent agent technology which is sometimes even combined with mobile agent technology. Mobile intelligent agents can travel among collection points to uncover suspicious cyber activity. This section will briefly present related work and some existing [21].

In the context of phishing, the terms S, L, A, and M refer to the various components of an email message that can be analyzed to detect phishing attempts.

S (Sender): The sender of an email can be a key indicator of whether the email is legitimate or a phishing attempt. Phishing emails often use spoofed sender addresses to appear as though they are coming from a trusted source. By analyzing the sender's email address and other metadata, such as the sender's IP address or email authentication records (such as SPF or DKIM), the SLAM method can determine whether an email is likely to be legitimate or not.

One common tactic is to include a real company's address inside their fake one. For example, the sender's email might be @emcom.bankofindia.com, where the scammer is pretending to be from Bank of America, using the real company's URL in a new domain to trick you.

You can quickly determine whether the email is a scam by searching the address used. You'll likely find warnings that tell you it is a phishing email.

L (Links): Phishing emails often contain links that direct users to fake login pages or other malicious websites. By analyzing the URLs of these links, the SLAM method can determine whether they are likely to be legitimate or part of a phishing attempt. For example, the SLAM method can check whether the domain name matches the sender's email address or whether the URL uses HTTP or HTTPS protocol.

Hover Over Links (L) Before Clicking:

A popular way scammers get their target's information is with the use of hyperlinks. Many people believe their anti-virus filters will protect them from clicking these links, but they do not. Anti-virus software can filter any attachments that may contain malware, but in the case of a hyperlink, the actual link is not unsafe. What's unsafe is the site it takes you to if you click on it.

These links can come in many different forms: text links, images or buttons within the email. Before clicking on a link, you need to hover over it to see the URL. Noticing a sketchy URL will immediately tell you that the email is a scam.

A (Attachments): Phishing emails may also contain malicious attachments, such as infected files or malware. By analyzing the content and file type of attachments, the SLAM method can determine whether they are likely to be legitimate or part of a phishing attempt. You used to be able to tell if an attachment was OK based on the type of file it was. Not anymore. Criminals can now infect all types of files with malware, including PDFs,and who wouldn't quickly click a file labelled as a sales order or invoice? File attachments are widely used in phishing emails simply because they work.

Never open an unexpected or strange file attachment. Actually, never open any attachment without first scanning it with an anti-virus/anti-malware application.

M (Message Text): The message text of a phishing email can contain clues that indicate whether it is a legitimate message or a phishing attempt. For example, phishing emails may use urgent or threatening language to encourage users to click on a link or open an attachment. By analyzing the language and tone of the message, the SLAM method can identify these types of phishing attempts and block them.

Overall, by analyzing the sender, links, attachments, and message text of an email, the SLAM method can help identify and block phishing attempts before they can do harm.

Carefully Read the Message (M)

We all do it — scan through messages without reading them fully. Especially in the work environment, where we have hundreds of things to process. Though efficient, this can be unsafe if you come across a phishing email. When scanning the email, you will likely miss small spelling or grammatical errors that can indicate it's a scam. Even reading through the email, these errors can be difficult to spot, because our brains can automatically process words even if they're incorrect. That is why it's important to be thorough in order to catch any potential red flags in the email.

If you don't have time to read the email carefully, don't take any actions (clicking a link or downloading an attachment) until you can [23].

5. Challenges in Phishing Attacks

The main challenge is the difficulty in developing a solid model of what acceptable behaviour is and what an attack is; as a result, they may generate a high number of false positive alarms, which may be caused by atypical behaviour that is actually normal and authorised, because normal behaviour can change easily and quickly. The active application of Artificial Intelligence is not the only challenge that organisations and cyber defence experts must face. Others are the result of flaws in the present security methodology [12].

- Distant infrastructure. Today, systems communicate across continents, sending sensitive data AI over the world. These transfers don't undergo sufficient protection and are easier to break into.
- Manual detection. Human teams don't have 24/7 focus on security threats and suspicious patterns. Most of the time, systems go unmonitored.
- Reactivity of security teams. Most security experts focus on facing threats rather than predicting them.
- Dynamic treats. Hackers have many strategies for hiding their locations, IPs, identities, and methods. The cyber defence field, on the other hand, is a lot more transparent and open for research – data, created by businesses, is easily accessible by criminals.
- An intrusion detection system, no matter how efficient, may be disabled by attackers if they can learn how the system works.
- Another problem involves supplying intrusion detection systems that will conform to legal regulations, security requirements and/or service-level agreements in real world.
- Social engineering tactics. Phishing attacks often use social engineering tactics to trick users into divulging sensitive information or clicking on malicious links. These tactics can be difficult to defend against because they rely on exploiting human psychology and emotions.
- Sophisticated techniques. Phishing attacks can be sophisticated and difficult to detect, with attackers using techniques like spear-phishing or whaling to target specific individuals or organizations. These attacks can be customized to include convincing language, logos, and other elements that make them appear legitimate.
- Use of encryption and obfuscation. Attackers may use encryption and obfuscation techniques to hide malicious payloads or evade detection by security software. This can make it difficult to detect and block phishing attempts before they reach their intended target.

6. The Way Forward in Phishing Detection

It's no wonder that cyber security is a top issue for all organisations, especially at a time when the world is going digital. Phishing detection professionals are hard at work developing innovative solutions to give a comprehensive and effective defence system. It requires considerably more care. Given human limits and the intelligence of agents such as computer viruses and worms, network-centric systems require intelligent cyber sensor agents that detect, evaluate, and respond to cyber threats in a timely manner [23].

With SLAM tools here are few predictions on how it will change (enhance) the cyber defence system?

- Using machine learning and artificial intelligence: By analysing massive amounts of data and discovering patterns and anomalies, machine learning and artificial intelligence can be used to detect phishing attempts. These technologies can aid in the detection of new and developing phishing assaults that standard signature-based detection methods may miss.
- Organisational collaboration and information sharing can help to improve phishing detection and response. Sharing threat intelligence and best practises, as well as working on incident response and remediation activities, can be examples of this.
- User education and awareness: In the fight against phishing attacks, user education and awareness is crucial. To assist users in recognising and avoiding phishing attacks, organisations should provide frequent training and awareness programmes.

Furthermore, much more study is needed before we can build reliable, deployable intelligent agent systems capable of managing distributed infrastructures. In the future, researchers must look for a theory of group utility function that will allow groups of agents to make judgements. It is advised that teams not only look for preventive phishing assaults, but also consult with technology to plan an aftermath [22].

7. Conclusion

Spoofed E-mail detection is regarded as one of the most encouraging advances in the information age and cyber security. The rapid growth of information technology has a significant positive impact and brought many conveniences into our lives. However, it also resulted in difficult-to-manage concerns, such as the advent of cybercrime. As a result, security execution is improved, and the system is better protected against an increasing number of refined cyber attacks. As technology advances, so do criminal cases. Every day, we see an increase in the number and diversity of cyber crimes, as modern technology makes it easy for criminals to fulfil their objectives.

Organisations anticipate that hackers will begin actively exploiting AI in the near future, and let's face it, standard technologies can't handle such dangers. As it stands, most businesses are unprepared to deal with extremely intelligent viruses, malware, ransomware, and other types of cyber attacks. One thing is certain: implementing some detective and preventive solutions can already help firms spend less time and effort on daily security duties while also better preparing them for emerging hazards. IT is both a weapon against present dangers and a long-term investment. Because technology is becoming more widely available, there will soon be no reason for any organisation to put off using this strategy. Instead than waiting for custom tools to accomplish large-scale security,

This study has briefly reviewed accomplishments made thus far in the field of implementing faked e-mail detection algorithms for preventing cybercrime, their obstacles and desired qualities, as well as the scope to route forward in cyber security.

Acknowledgement

I would like to convey my heartfelt gratitude to Professor and staff members of the Department of Computer Engineering for allowing me to conduct my study and for her assistance and encouragement throughout the process.

I would also want to thank Dr. H.N Shah, the Director of Gandhinagar Institute of Technology, for giving me the opportunity to do this research.

References

1. D. Dasgupta, (2006) “Computational Intelligence in Cyber Security”, IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety (CIHSPS 2006), pp. 2–3

2. H. Chen, F. Y. Wang, (2005) “Guest Editors' Introduction: Artificial Intelligence for Homeland Security”, IEEE intelligent systems, Vol. 20, No. 5, pp. 12–16.

3. Selma Dilek1, Hüseyin Çakır2 and Mustafa Aydın3 (2015) “Applications Of Artificial Intelligence Techniques To Combating Cyber Crimes: A Review”. International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, No. 1, January 2015.

4. E. Tyugu, (2011) “Artificial intelligence in cyber defence”, 3rd International Conference on Cyber Conflict (ICCC 2011), pp. 1–11.

5. KINGSLEY CHIMEZIE AMADI, Machine Learning as a Strategic Initiative for Cyber Defence Dissertation Manuscript July 2020.

6. Ishaq Azhar Mohammed, Artificial Intelligence For Cyber Security: A Systematic Mapping Of Literature International Journal Of Innovations In Engineering Research And Technology [IJIERT] Sept 2020.

7. Suyash srivastav, Bijoy benny, Artificial Intelligence (A. I) and its application in Cyber Security, June 15, 2021.

8. Florentina - Loredana Dragomir, Artificial Intelligence Techniques Cyber Security, International Scientific Conference "Strategies XXI" (2017).

9. Dimitar Stevo Bogatinov, Mitko Bogdanoski and Slavko Angelevski “AI based Cyber Defence for more secure Cyber Space” 2016.

10. L. Hong, (2008) “Artificial Immune System for Anomaly Detection”, IEEE International Symposium on Knowledge Acquisition and Modelling Workshop, pp. 340 – 343.

11. X. B. Wang, G. Y. Yang, Y. C. Li, D. Liu, (2008)” Review on the application of Artificial Intelligence in Antivirus Detection System”, IEEE Conference on Cybernetics and Intelligent Systems, pp. 506 509.

12. Artificial Intelligence, wikipedia.org/wiki/Artificial_intelligence, (24/12/2021)

13. L. Phillips, H. Link, R. Smith, L. Weiland, (2006) Agent-Based Control of Distributed Infrastructure Resources, U.S. Department of Energy, Sandia National Laboratories, USA.

14. M. R. Stytz, D. E. Lichtblau, S. B. Banks, (2005) “Toward using intelligent agents to detect, assess, and counter cyber attacks in a network-centric environment”, Ft. Belvoir Defence Technical Information Centre, 1. Edition, Alexandria, VA.

15. J. Helano, M. Nogueira, (2006) “Mobile Intelligent Agents to Fight Cyber Intrusions”, the International Journal of Forensic Computer Science (IJoFCS), Vol. 1, pp. 28-32.

16. E. Herrero, M. Corchado, A. Pellicer, A. Abraham, (2007) “Hybrid multi agent-neural network intrusion detection with mobile visualization”, Innovations in Hybrid Intelligent Systems, Vol. 44, pp. 320 328.

17. C. Bitter, D.A. Elizondo, T. Watson, (2010) “Application of Artificial Neural Networks and Related Techniques to Intrusion Detection”, IEEE World Congress on Computational Intelligence (WCCI 2010), pp. 949 – 954.

18. E. S. Brunette, R. C. Flemmer, C. L. Flemmer, (2009) “A review of artificial intelligence”, Proceedings of the 4th International Conference on Autonomous Robots and Agents, pp. 385 392.

19. J. S. Russell, P. Norvig, (2003) Artificial Intelligence: A Modern Approach, 2nd edition, Upper Saddle River, Prentice Hall, New Jersey, USA.

20. G. Luger, W. Stubblefield, (2004) Artificial Intelligence: Structures and Strategies for Complex Problem Solving, 5th edition, Addison Wesley.

21. Thanh Cong Truong, Quoc Bao Diep and Ivan Zelinka, “Artificial Intelligence in the Cyber Domain: Offense and Defence”, 2020.

22. A. Patel, M. Taghavi, K. Bakhtiyari, J. Celestino Júnior, (2012) “Taxonomy and Proposed Architecture of Intrusion Detection and Prevention Systems for Cloud Computing”, Y. Xiang et al. (Eds.), Springer-Verlag Berlin Heidelberg, pp. 441 458.

23. Amr Kayid, “The role of Artificial Intelligence in future Technology” (March 2020).

24. Ankit Kumar Jain & B. B. Gupta (2021): A survey of phishing attack techniques, defence mechanisms and open research challenges, Enterprise Information Systems.

25. Guo, Z., Cho, J.-H., Chen, I.-R., Sengupta, S., Hong, M., & Mitra, T. (2022). SAFER: Social Capital-Based Friend Recommendation to Defend against Phishing Attacks. Proceedings of the International AAAI Conference on Web and social media, 16(1), 241-252

26. Wu, H.; Guo, X.; Jiang, D.; Guo, X.; Lv, T.; Luo, H. GNSS Spoofing Identification and Smoothing Localization Method for GNSS/Visual SLAM System. Appl. Sci. 2022, 12, 1386

27. Gupta, B.B., Arachchilage, N.A.G. & Psannis, K.E. Defending against phishing attacks: taxonomy of methods, current issues and future directions. Telecommun Syst 67, 247–267 (2018).

28. Jain, Ankit Kumar, and B.B. Gupta. "Phishing Detection: Analysis of Visual Similarity Based Approaches." *Security and Communication Networks* 2017 (2017).