The Nucleus 61, No. 2 (2024) 93-100

https://doi.org/10.71330/thenucleus.2024.1402

www.thenucleuspak.org.pk

The Nucleus

ISSN 0029-5698 (Print)

ISSN 2306-6539 (Online)

A Comprehensive Study on Phishing Attack Detection and Mitigation via Ransomware-as-a-Service (RAAS)

Nimra Ifhtikhar[1], Ahthasham Sajid[1*], Adeel Zafar[2], Atta Ur Rahman[2], Rida Malik[1], Hamza Razzaq[1]

[1]*Department of Cyber Security and Data Science, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan*

[2]*Department of Data Science, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan*

ABSTRACT

Ransomware-as-a-Service (RAAS), a new cybercriminal actor, is making ransomware attacks more potent and widespread. This research comprehensively assesses Ransomware-as-a-Service (RAAS) ecosystem phishing detection and prevention solutions. Seven studies compare RAAS-enabled phishing detection and prevention effectiveness, challenges, and trends. The findings recommend a multi-layered, context-aware approach for organizational resilience to shifting cyber threats. This thorough phishing attack detection and security study examines ransomware-as-a-service. Phishing attacks leverage human weaknesses to steal sensitive data and are becoming more sophisticated. Since RAAS makes ransomware attacks easier, even non-technical people may launch deadly ones. Money is making ransomware assaults more common and severe, putting people, organizations, and key infrastructure at risk. These new attacks must be detected and mitigated to safeguard digital assets. This study compares RAAS ecosystem phishing attack defence detection and mitigation technologies to identify strengths, weaknesses, and emerging trends.

Keywords: *Internet of Things (IoT), Blockchain, Ransomware-as-a-Service (RAAS), Phishing*

1. Introduction

Recent cybercriminal actor ransomware-as-a-service (RAAS) is strengthening and spreading ransomware attacks. According to [1], RAAS systems allow even non-technical users to conduct ransomware operations. Like legal software-as-a-service (SaaS) firms, this business model offers hackers customer support, variable ransomware variants, and user-friendly interfaces. Given the reduced entrance barrier of RAAS, more individuals can start ransomware attacks [1]. The ubiquitous availability of ransomware tools and services has led to several attacks on healthcare, financial, and government businesses [2]. Believes that ransomware attacks will cost $265 billion globally by 2031, demonstrating their financial impact.

A phishing attack uses deceptive emails, messages, or web pages to steal personal information or download malware [3]. Social engineering and contextual information are helping these attacks get smarter. Understanding the complex cyber threat environment is crucial when RAAS and phishing attacks converge, creating a major cybersecurity challenge [3]. Due to RAAS platforms monetizing ransomware, phishing attacks' popularity and complexity, and other aspects, cyber dangers are always evolving. To identify, mitigate, and prevent RAAS-enabled ransomware attacks, significant research and analysis are needed. These attacks are increasing in frequency and severity. The most typical method ransomware spreads in RAAS ecosystems is via phishing attacks, adding to the ever-changing list of risks. A basic process diagram of which is shown in Figure 1. To address that gap, this study compares RAAS phishing attack detection and mitigation methods. It will illuminate phishing attack Defense benefits, disadvantages, and new directions.

This research aims to focus on RAAS phishing detection and prevention. Comparing detection and mitigation solutions in RAAS ecosystem phishing attack defense will reveal strengths, drawbacks, and emerging trends. The research also educates cybersecurity professionals, policymakers, and companies about ransomware threats' dynamic nature and the necessity for proactive defenses. According to [4], knowing how cybercriminals work and their preferred attack pathways is necessary to develop robust cybersecurity strategies that can adapt to changing threat scenarios. By highlighting the challenges and advantages of countering phishing attacks inside RAAS, the research contributes to cyber resilience discussions.

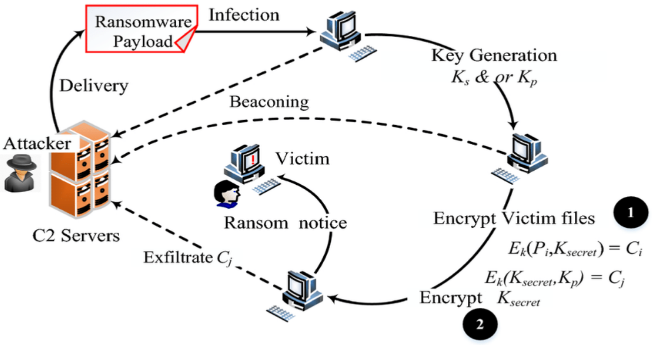

Fig. 1: Typical Ransomware Attack Process [3]

[*] Corresponding author: ahthasham.sajid@riphah.edu.pk

Ransomware spreads largely via phishing attacks in RAAS setups. Cybercriminals employ phishing to propagate ransomware by tricking victims into clicking on infected emails or links. Phishing and RAAS enhance ransomware attacks' impact and make detection and protection harder. Investigating the confluence of RAAS and phishing threats is necessary to design comprehensive defence strategies. This document's structure: A comprehensive study of phishing attack detection and RAAS literature follows. Next, we discuss RAAS frameworks' phishing detection and prevention methods. The parts that follow include case examples, examine present issues, and suggest future paths for this field's practice and study.

2. Literature Review

The objective of this section is to provide a comprehensive overview of all pertinent concepts pertaining to research subjects addressed by previous scholars.

2.1 Ransomware-as-a-Service (RAAS)

When ransomware became lucrative for hackers in the early 2010s, RAAS systems were started. First, RAAS systems were simple and ran on dark web marketplaces and underground forums [5]. Despite their simplicity, these early platforms offered ransomware toolkits and help to hackers. Another research note is that cloud computing has made RAAS systems' user interfaces more complex and intuitive [6].

RAAS ecosystems' various business structures and monetization methods show cybercriminals' entrepreneurial drive. Research reveals that ransomware companies use subscription models. Producers who rent their software to customers or affiliates keep a part of the ransom fees [7]. This revenue-sharing method ensures platform administrators a steady income and motivates affiliates to spread ransomware actively. Affiliates may sell stolen data or provide victims with decryption keys and assistance to make RAAS operations more lucrative and robust [7].

RAAS platforms have democratized ransomware, changing the criminal environment, according to [8]. Only a tiny number of hackers have been able to design and deploy ransomware attacks owing to technical expertise and resources. RAAS systems make ransomware more accessible by providing complete malware creation and distribution options. This democratization of distribution allows anybody, including non-technical people, to initiate ransomware attacks [8]. Due to the lower entrance barrier, ransomware assaults and their harm have increased dramatically.

The exponential rise and enhancement of RAAS systems have changed criminality and challenged traditional cybersecurity methods. Since ransomware has become a commodity via RAAS, [9] suggested reevaluating existing defensive and response methods. Static analysis and signature-based detection struggle to mitigate RAAS-enabled ransomware's adaptability. Thus, RAAS ecosystems need innovative and adaptable cybersecurity solutions to detect, minimize, and prevent ransomware attacks. Cybersecurity specialists, researchers, and legislators must collaborate to develop defences against RAAS threats, which change often.

2.2 Phishing Attacks: Techniques, Trends, and Challenges

The literature is full of phishing assaults that utilize different methods to fool and influence victims. According to [10], email phishing attacks are frequent and include fraudsters posing as trustworthy businesses to obtain personal information or induce consumers to download hazardous files or click on links. The general phishing attack process given by [10] is shown in Figure 1. The research discusses spear phishing, which leverages personal information to make fraudulent messages more persuasive and effective to specific persons or organizations [11]. Also mention the emergence of smishing and vishing as ways to deceive victims into disclosing critical information [12]. Overall, research reveals that phishing attack strategies are complicated and ever-changing, requiring several defense systems.

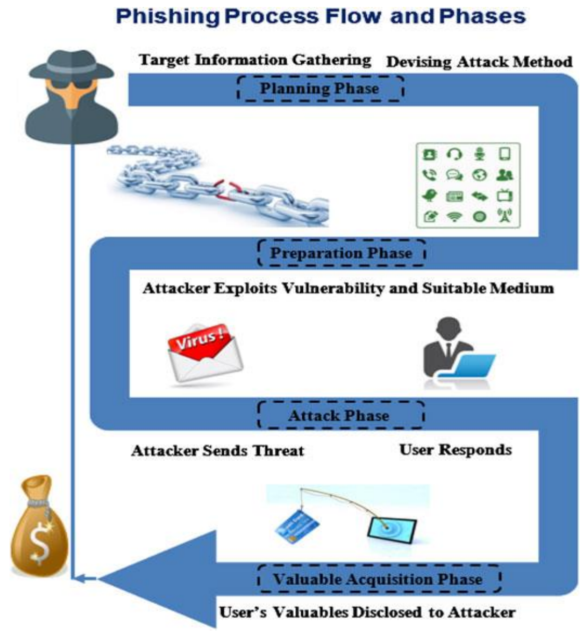
Phishing Process Flow and Phases
Target Information Gathering
Devising Attack Method
Planning Phase
Preparation Phase
Attacker Exploits Vulnerability and Suitable Medium
Virus !
Attack Phase
Attacker Sends Threat
User Responds
Valuable Acquisition Phase
User's Valuables Disclosed to Attacker

Fig. 2: General Phishing Attack Process [10]

Recent phishing trends have shown fraudsters' growing proficiency and versatility, causing major issues for defensive systems. The research addresses pretexting and pretext-based phishing to bypass security and influence human psychology [13]. Another research reports an increase in hybrid phishing attempts [14]. These attacks use email, audio, and text to boost success. Due to mobile devices and social media, research also noted that phishing attacks have spread across many communication channels [15]. These developments demonstrate the necessity for proactive and adaptive RAAS phishing detection and prevention.

Even though cyber security awareness and technology have improved, phishing attacks still plague organizations and individuals worldwide. Another study says the human factor is a major issue in the literature [16]. Despite security measures and technical advances, hackers still use people's biases and misperceptions to deceive and control them. Another study noted that phishing and social engineering schemes change often, making standard detection methods problematic [17]. The anonymity of digital communication channels and the global internet make it hard to identify and punish phishers. A comprehensive plan that includes technical improvements, user education, and stakeholder collaboration is needed to combat phishing attacks.

2.2.1 Detection Methods for Phishing Attacks

Phishing detection must be intelligent and flexible to keep up with the ever-changing threat environment. This section critically examines the main methods, including machine learning, artificial intelligence, heuristic, and behavioural analysis detection approaches from the literature.

2.2.2 Signature-based detection methods

Signature-based detection may stop malicious emails containing links, attachments, or patterns. Known phishing attacks inspired these methods. Studies show how signature-based systems can detect phishing threats [18]. To address new threats, recognized signature databases are updated constantly. One criticizes signature-based detection. They say signature-based detection is reactive and cannot detect zero-day or unknown phishing attempts [19]. Signature-based detection's high false positive rates may also identify benign emails as malicious, frustrating users and disrupting companies.

2.2.3 Heuristic and Behavioral Analysis Approaches

Heuristic and behavioural analysis approaches identify phishing attempts by detecting suspicious actions and attributes rather than preset indications. Polymorphic phishing attacks utilize obfuscation to escape signature-based detection; [20] discuss how well heuristics detect them. Heuristic methods identify and prevent new phishing emails by evaluating their behavior and abnormalities. Also research user behavior and interaction patterns using machine learning methods [21]. It helps detect complicated phishing efforts that mimic actual interactions.

2.2.4 Machine Learning and AI-based Detection Methods

Modern phishing detection systems utilize machine learning and AI to examine massive data sets for detailed patterns that suggest criminal intent. Another research focused on decision trees and support vector machines, two supervised learning approaches that can adapt and learn from new data to improve phishing detection accuracy [22].

According to [23], deep learning algorithms and natural language processing may identify semantic and contextual evidence of phishing intent. False positives, model interpretability, and adversarial attacks limit the potential of machine learning and AI-based phishing detection. These challenges must be studied and improved.

2.3 Mitigation Strategies for Phishing Attacks

A multi-pronged phishing attack mitigation approach that integrates technology and user-centric methods increases cybersecurity. After going through the literature, this section critically analyses user awareness and education initiatives, email filtering and security, multi-factor authentication, and secure communication routes as main mitigation strategies.

2.3.1 User Awareness and Education Programs

User awareness and education campaigns teach phishing detection and response. One author found that continual security training and awareness efforts reduce phishing attempts [24]. Another Stress is that simulated phishing activities may help organizations find and fix vulnerabilities and improve user awareness and resilience. Education initiatives may enhance awareness, but other mitigation strategies are needed to guard against phishing attacks [25].

2.3.2 Email Filtering and Security Protocols

Email filtering and security prevent phishing attacks by automatically analyzing incoming emails for hazardous content and phishing activities. Research examines how effectively advanced email filtering technology can detect and prevent phishing emails using rules, signatures, and heuristics [26]. One discusses using domain-based message authentication, reporting, and conformance (DMARC) protocols to prevent email spoofing and verify email senders [27]. Another says security and email filtering defend against phishing. Advanced attacks that employ social engineering to escape detection may outweigh existing defenses [28].

2.3.3 Multi-factor Authentication and Secure Communication Channels

Multi-factor authentication (MFA) and encrypted communication channels may avoid phishing attempts, which steal user credentials. Research explores how multi-factor authentication (MFA) reduces the effect of phishing attacks by requiring several verifications to access crucial accounts or systems [28]. He designed an IOT-based healthcare MFA, as shown in Figure 2. To avoid unwanted access and interception of sensitive information, [29] recommend encrypted email and messaging systems. Even if multi-factor authentication and encrypted communication channels enhance security, [30] emphasize the need to make implementations simple and integrate them smoothly with existing procedures to increase adoption and compliance.

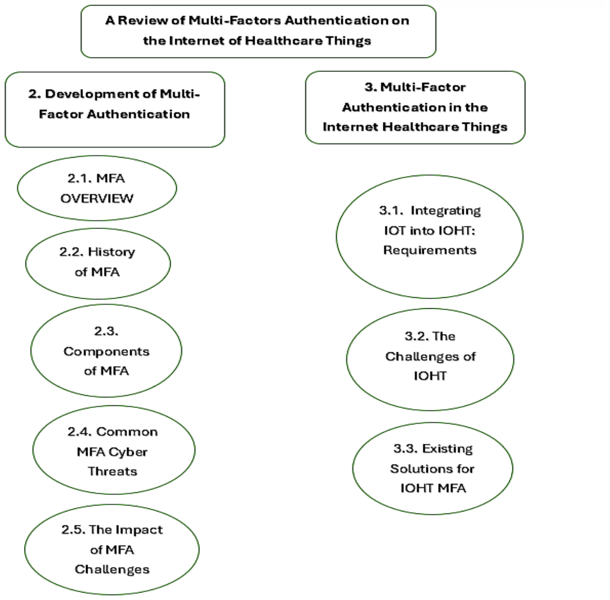
A Review of Multi-Factors Authentication on the Internet of Healthcare Things
2. Development of Multi-Factor Authentication
3. Multi-Factor Authentication in the Internet Healthcare Things
2.1. MFA OVERVIEW
2.2. History of MFA
2.3. Components of MFA
2.4. Common MFA Cyber Threats
2.5. The Impact of MFA Challenges
3.1. Integrating IOT into IOHT: Requirements
3.2. The Challenges of IOHT
3.3. Existing Solutions for IOHT MFA

Fig. 3: MFA IoT: Internet of Healthcare Things [28]

Table 1: Critical Analysis

Ref.	Year	Paper Title	Journal Name	Limitations
[38]	2024	"Reimagining Authentication: A User-Centric Two-Factor Authentication with Personalized Image Verification"	IEEE Access	Limited focus on RAAS-specific challenges
[34]	2022	"Deep Learning for Phishing Detection: Taxonomy, Current Challenges and Future Directions"	IEEE Access	Lack of analysis on machine learning in RAAS contexts
[35]	2022	"Empirical evidence of phishing menace among undergraduate smartphone users in selected universities in Nigeria"	Indonesian Journal of Electrical Engineering and Computer Science	Focuses primarily on user-centric strategies
[31]	2020	"The Ransomware-as-a-Service economy within the darknet"	Computers & Security	Limited focus on phishing attack vectors within RAAS
[32]	2020	"A comprehensive survey of AI-enabled phishing attacks detection techniques"	Telecommunication Systems	Lack of RAAS-specific phishing detection strategies
[36]	2020	"Applicability of machine learning in spam and phishing email filtering: review and approaches"	Artificial Intelligence Review	Limited discussion on evolving phishing tactics
[37]	2020	"An In-Depth Benchmarking and Evaluation of Phishing Detection Research for Security Needs"	IEEE Access	Limited exploration of heuristic approaches in RAAS settings

The "Type of Study" column in this updated table specifies whether the focus was on detection, mitigation, or both. The "Methodology" column lists the precise techniques or approaches utilized in each study. This update offers a more thorough and understandable summary of the state of the field.

2.4 Research Gap

Phishing tactics, trends, and mitigation solutions are well-documented, but there needs to be more study on Ransomware-as-a-Service (RAAS) ecosystems. To prevent sophisticated RAAS-enabled phishing attacks, research focuses on individual mitigation and detection techniques, neglecting strategy interactions and success. Continuous research on RAAS and how it influences phishing attack dynamics is needed to adapt existing tactics to new threats.

This research addresses that requirement by evaluating phishing attack detection and prevention methods, focusing on RAAS challenges. This study combines detection, mitigation, and RAAS operating dynamics to understand the complex relationship between phishing attacks and RAAS systems. This research will also analyze current methodologies' strengths, weaknesses, and trends to improve RAAS ecosystem cybersecurity resilience against phishing assaults by comparison analysis. The study's main purpose is to solve cyber resilience research knowledge gaps so organizations, cybersecurity specialists, and politicians may better comprehend and battle RAAS-enabled cybercrime's ever-changing phishing assaults.

3. Methodology

The method utilized a literature-based comparative analysis examining phishing research to find trends, tactics, and countermeasures. This strategy illuminates the complex dynamics of RAAS-enabled cybercrime by merging study results. The research compares publications using certain criteria to provide a focused and complete examination. Figure 4 below shows a flow diagram for this research.

Inclusion criteria:

- Focus on phishing attack detection and mitigation methods.
- Address the unique challenges presented by RAAS ecosystems.
- Provide empirical evidence or theoretical frameworks for evaluating the effectiveness of the proposed methods.
- Research between 2020-2024

Exclusion Criteria:

- Research before 2020.
- Studies on unspecific phishing detection and mitigation.
- Studies ignoring RAAS platform issues.
- Blogs, news, and opinions to guarantee analytical rigour and trustworthiness.
- Studies without empirical data or theoretical frameworks.

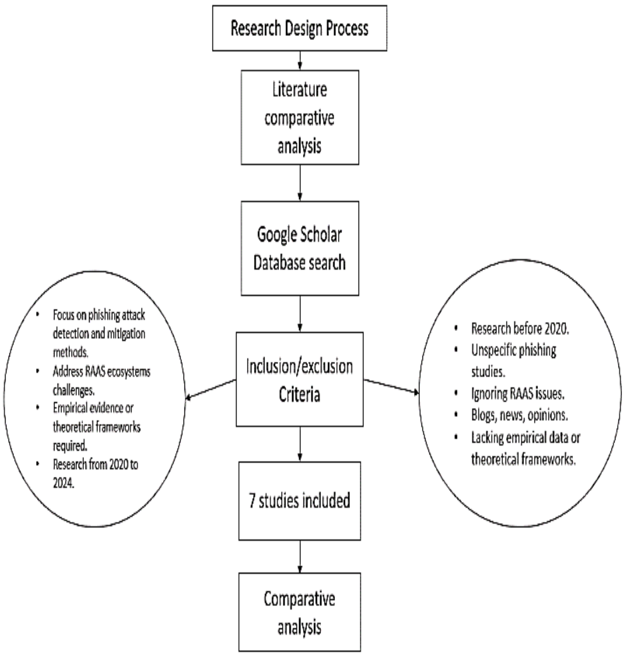
Research Design Process
Literature comparative analysis
Google Scholar Database search
Inclusion/exclusion Criteria
7 studies included
Comparative analysis
Focus on phishing attack detection and mitigation methods.
Address RAAS ecosystems challenges.
Empirical evidence or theoretical frameworks required.
Research from 2020 to 2024.
Research before 2020.
Unspecific phishing studies.
Ignoring RAAS issues.
Blogs, news, opinions.
Lacking empirical data or theoretical frameworks.

Fig. 4: Research Flow Diagram

The method uses IEEE Xplore, Research Gate, and Google Scholar as the main search engines to find relevant studies. Table 2 shows the research keywords and search strings utilized. A total of 7 studies are chosen for analysis.

Table 2: Keywords and Search Strings

Keywords	Search Strings
Phishing Attacks	"Phishing attacks" AND "RAAS"
Phishing Detection Methods	"Phishing detection methods" AND "RAAS"
Mitigation Strategies	"Mitigation strategies" AND "RAAS"
RAAS Ecosystem	"RAAS ecosystem" AND "cybercrime"
Phishing Trends	"Phishing trends" AND "RAAS"
RAAS Challenges	"RAAS challenges" AND "phishing attacks"
Detection Techniques	"Detection techniques" AND "RAAS"
RAAS Evolution	"RAAS evolution" AND "phishing mitigation"

Findings and Trends

This section shows the comparative results of the methodology employed. Table 3 below shows detection methodologies comparatively as discussed by each selected study.

Table 3 Comparative Analysis of Various Phishing Attack Detection Methods in RAAS

Study	Year	Detection Methodologies	Key Findings
[39]	2023	Signature-based, Heuristic	Limited effectiveness against RAAS
[40]	2024	Machine Learning, Behavioral Analysis	Adaptive but not foolproof
[41]	2022	Heuristic, Pattern Recognition	Effective against known threats
[42]	2023	AI-based, Statistical Analysis	High accuracy but complex
[43]	2023	Hybrid Detection, Anomaly Detection	Robust against polymorphic attacks
[44]	2023	Behavioural Analysis, Deep Learning	Context-aware, adaptable
[45]	2023	Feature-based NLP techniques	Limited by data quality

Table 4: Comparative Analysis of Mitigation Strategies Employed in RAAS Environments

Study	Year	Mitigation Strategies	Key Findings
[43]	2023	User Awareness Programs, Email Filtering	Effective but user-dependent
[45]	2023	Multi-factor Authentication, Secure Channels	Robust but resource-intensive
[42]	2023	AI-driven Monitoring, Incident Response	Proactive, reduces impact
[43]	2023	Endpoint Security, Network Segmentation	Comprehensive but complex
[41]	2022	Threat Intelligence, Policy Enforcement	Adaptive, compliance-driven
[39]	2023	Data Encryption, Access Controls	Secure but may hinder usability
[40]	2024	Behavioral Analytics, Real-time Monitoring	Dynamic, real-time response required

Table 5: Emerging Trends in Phishing Attack Techniques within RAAS Ecosystems

Study	Year	Emerging Trends	Key Findings
[41]	2022	Evolving Tactics, Social Engineering	Increasingly sophisticated attacks
[39]	2023	Hybrid Attacks, Multi-channel Campaigns	Diversified and coordinated strategies
[42]	2023	AI-driven Attacks, Context-aware Phishing	Adaptive and targeted
[40]	2024	Polymorphic Malware, Insider Threats	Complex, varied threats
[43]	2023	Automation, RaaS Specialization	Increased efficiency, specialized services
[45]	2023	Cloud-based Attacks, Cross-platform Exploits	Expanding attack surface, broader impact
[44]	2023	Zero-day Exploits, Advanced Evasion Techniques	High-risk, low-detection attacks

4. Discussion Insights from the Comparative Study

A comparison of the chosen studies explains the complicated topography of phishing attack detection, mitigation, and trends in Ransomware-as-a-Service (RAAS) ecosystems.

3.1 Detection Methods

Key findings include the range and complexity of RAAS phishing detection systems. Despite high success rates, machine learning and AI-based phishing threat detection systems are complex and resource-intensive. The adaptive and context-aware heuristic and behavioral analysis approaches may need updates to thwart hackers' ever-changing schemes. Given these disparities, a multi-pronged phishing detection approach that uses the best of various methods is necessary to fight against sophisticated assaults.

3.2 Mitigation Strategies

The research emphasizes the need for phishing mitigation to protect RAAS ecosystems. Real-time monitoring, multi-factor authentication, and user knowledge may minimize phishing. Some solutions sacrifice security and user experience, which are finely balanced. Customize one’s approach to user needs and leverage adaptable and context-aware solutions to create a safe and enjoyable user experience.

The research emphasizes multi-channel campaigns, context-aware phishing, and AI-driven RAAS phishing. These patterns reflect more complex and targeted assaults that exploit system flaws and use sophisticated evasion methods to go undetected. Protecting against RAAS systems' wide phishing attempts is increasingly important due to shifting threats. Threat prediction and reaction need proactive and adaptive defence.

Finally, RAAS phishing complexity is shown by these experiments. Cybersecurity experts, researchers, and organizations must cooperate, analyze, and develop resilient, flexible, and environment-aware detection and mitigation approaches.

5. Challenges and Gaps

4.1 Identified Challenges in Detecting and Mitigating Phishing Attacks in RAAS

The development of RAAS system phishing is an issue. Hackers constantly innovate to break into networks and steal data. AI and context-aware phishing outperform security [48]. In a shifting battlefield, attackers' fast plan changes may test conventional detection methods. Finally, phishing assaults are becoming smarter. Thus, we need mitigation tools that can handle complicated coordinated campaigns, eliminate false positives, and protect user experience.

4.2 Gaps in Existing Literature and Practices:

The analysis also uncovers gaps in RAAS phishing attack detection and prevention expertise. Many studies have studied particular detection and mitigation measures, but only some have synthesized them and tested them in RAAS situations. Researchers need to learn more about how different tactics might work together to boost cybersecurity since present research generally ignores the connection between detection and mitigation measures. Human factors are also important in phishing mitigation techniques; however, RAAS ecosystems have yet to be studied. Human factors include user behavior, awareness, and decision-making [47].

4.3 Limitations of Current Detection and Mitigation Methods

The comparison analysis shows that RAAS phishing detection and mitigation methods have disadvantages. Heuristic and signature-based detection systems handle recognized threats effectively, but they may miss polymorphic phishing attempts with sophisticated evasion methods. Multiple-factor authentication and real-time monitoring offer great mitigation capabilities, but they may need to be more user-friendly and able to survive complicated attacks on human vulnerabilities [46]. Because certain sophisticated detection and mitigation tactics are resource-intensive and may be too much for businesses with limited cybersecurity experience and infrastructure, it is crucial to discover solutions that can be customized.

The comparative analysis showed gaps and problems, underlining the need for research, innovation, and collaboration to build RAAS ecosystem-specific, adaptive, comprehensive, and context-aware phishing attack detection and prevention solutions. Cybersecurity specialists may supplement expertise and assist organizations in resisting RAAS-enabled phishing [49]. Data security and stakeholder confidence in the digital era.

5. Conclusion

Overall, Comparisons of Ransomware-as-a-Service Phishing defence options for the RAAS environment were fascinating. AI detection and machine learning were accurate, but their complexity and resource restrictions needed to be addressed. Although more versatile, heuristic and behavioral analysis needs assault upgrades. User understanding, multi-factor authentication, and real-time monitoring may reduce phishing. Success has come from these techniques. All methods demonstrated the need for security-user satisfaction balancing. RAAS-enabled phishing attempts highlighted the need for adaptive and proactive security. Addressing problems and gaps in practices and literature may help organizations defend against RAAS-enabled phishing, secure sensitive data, and retain digital trustworthiness.

Accurate machine learning and AI identification were challenging and resource-intensive for future study. Behavioral and heuristic analyses were more flexible but required regular assault upgrades. Real-time monitoring, multi-factor authentication, and user awareness reduce phishing. These methods worked well. All these ideas revealed that one must balance security and user enjoyment. Unique RAAS-enabled phishing attempts were found, emphasizing the necessity for proactive and adaptable security. Research suggests RAAS phishing needs a complicated, context-based approach. Cybersecurity researchers must provide robust, adaptable, and user-friendly solutions. Addressing present practices and literature restrictions may increase digital organization data security, RAAS-enabled phishing resistance, and trustworthiness.

Though imperfect, RAAS ecosystem phishing attack detection and mitigation methods are extremely accurate. These methods boost cybersecurity and protect sensitive data from bad actors. Using sophisticated algorithms, behavioural analysis, and hybrid techniques, academics and practitioners have created strong phishing solutions that dramatically reduce risk and damage.

References

[1] J. Zhang and D. Tenney, “The Evolution of Integrated Advance Persistent Threat and Its Defense Solutions: A Literature Review,” Open Journal of Business and Management, vol. 12, no. 1, pp. 293–338, Dec. 2023.

[2] S. Morgan, “Global Ransomware Damage Costs Predicted to Exceed $265 Billion by 2031,” Cybercrime Magazine, Jun. 01, 2021. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

[3] A.K. Jain and B.B. Gupta, “A survey of phishing attack techniques, defence mechanisms and open research challenges,” Enterprise Information Systems, vol. 16, no. 4, pp. 1–39, Mar. 2021.

[4] D.P.F. Möller, “Cyberattacker Profiles, Cyberattack Models and Scenarios, and Cybersecurity Ontology,” Advances in information security, pp. 181–229, Jan. 2023.

[5] Cong, Lin and Grauer, Kimberly and Rabetti, Daniel and Updegrave, Henry, The Dark Side of Crypto and Web3: Crypto-Related Scams (February 14, 2023). Available at SSRN: https://ssrn.com/abstract=4358572

[6] Buerkle, Achim, William Eaton, Ali Al-Yacoub, Melanie Zimmer, Peter Kinnell, Michael Henshaw, Matthew Coombes, Wen-Hua Chen, and Niels Lohse. "Towards industrial robots as a service (IRaaS): Flexibility, usability, safety and business models." *Robotics and Computer-Integrated Manufacturing* 81 (2023) 102484.

[7] Axon, Louise, Arnau Erola, Ioannis Agrafiotis, Ganbayar Uuganbayar, Michael Goldsmith, and Sadie Creese. "Ransomware as a Predator: Modelling the Systemic Risk to Prey." *Digital Threats: Research and Practice* 4, no. 4 (2023): 1-38.

[8] P.H. Meland, Y.F.F. Bayoumy, and G. Sindre, “The Ransomware-as-a-Service economy within the darknet,” Computers & Security, vol. 92, pp. 101762, May 2020.

[9] T. McIntosh, A.S.M. Kayes, Y.P.P. Chen, A. Ng, and P. Watters, “Ransomware Mitigation in the Modern Era: A Comprehensive Review, Research Challenges, and Future Directions,” ACM Computing Surveys, vol. 54, no. 9, pp. 1–36, Dec. 2022.

[10] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, “Phishing Attacks: A Recent Comprehensive Study and a New Anatomy,” Frontiers in Computer Science, vol. 3, no. 1, Mar. 2021.

[11] T. Stojnic, D. Vatsalan, and N. A. G. Arachchilage, “Phishing email strategies: Understanding cybercriminals’ strategies of crafting phishing emails,” Security and Privacy, vol. 4, no. 5, May 2021.

[12] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, “Phishing Attacks: A Recent Comprehensive Study and a New Anatomy,” Frontiers in Computer Science, vol. 3, no. 1, Mar. 2021.

[13] K.F. Steinmetz, A. Pimentel, and W.R. Goe, “Performing social engineering: A qualitative study of information security deceptions,” Computers in Human Behavior, vol. 124, pp. 106930, Nov. 2021.

[14] Goenka, Richa, Meenu Chawla, and Namita Tiwari. "A comprehensive survey of phishing: Mediums, intended targets, attack and defence techniques and a novel taxonomy." *International Journal of Information Security* 23, no. 2 (2024): 819-848.

[15] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, “Phishing Attacks: A Recent Comprehensive Study and a New Anatomy,” Frontiers in Computer Science, vol. 3, no. 1, Mar. 2021.

[16] R. A. M. Lahcen, B. Caulkins, R. Mohapatra, and M. Kumar, “Review and insight on the behavioral aspects of cybersecurity,” Cybersecurity, vol. 3, no. 1, Apr. 2020.

[17] J.W. Bullee and M. Junger, “How effective are social engineering interventions? A meta-analysis,” Information & Computer Security, vol. 28, no. 5, pp. 801–830, Aug. 2020.

[18] A. Shaji. George, A.S. Hovan. George, and T. Baskar, “Digitally Immune Systems: Building Robust Defences in the Age of Cyber Threats,” Zenodo (CERN European Organization for Nuclear Research), vol. 1, no. 4, Aug. 2023.

[19] N. Saxena, E. Hayes, E. Bertino, P. Ojo, K.K.R. Choo, and P. Burnap, “Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses,” Electronics, vol. 9, no. 9, pp. 1460, Sep. 2020.

[20] A.K. Jain and B.B. Gupta, “A survey of phishing attack techniques, defence mechanisms and open research challenges,” Enterprise Information Systems, vol. 16, no. 4, pp. 1–39, Mar. 2021.

[21] A.G. Martín, A. Fernández-Isabel, I. Martín de Diego, and M. Beltrán, “A survey for user behavior analysis based on machine learning techniques: current models and applications,” Applied Intelligence, vol. 51, Jan. 2021.

[22] O. Kayode-Ajala, “Applying Machine Learning Algorithms for Detecting Phishing Websites: Applications of SVM, KNN, Decision Trees, and Random Forests,” International Journal of Information and Cybersecurity, vol. 6, no. 1, pp. 43–61, Mar. 2022.

[23] Z. Zhang, H.A. Hamadi, E. Damiani, C.Y. Yeun, and F. Taher, “Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research,” IEEE Access, vol. 10, pp. 93104–93139, 2022.

[24] A. Sumner, X. Yuan, M. Anwar, and M. McBride, “Examining Factors Impacting the Effectiveness of Anti-Phishing Trainings,” Journal of Computer Information Systems, pp. 1–23, Aug. 2021.

[25] G. Desolda, L.S. Ferro, A. Marrella, T. Catarci, and M.F. Costabile, “Human Factors in Phishing Attacks: A Systematic Literature Review,” ACM Computing Surveys, vol. 54, no. 8, pp. 1–35, Nov. 2022.

[26] P. Mange, A. Lule, and R. Savant, “Advanced Spam Email Detection using Machine Learning and Bio-Inspired Meta-Heuristics Algorithms,” International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 4s, pp. 122–135, 2024.

[27] S. C. Sethuraman, D. P. V. S, T. Reddi, M. S. T. Reddy, and M. K. Khan, “A comprehensive examination of email spoofing: Issues and prospects for email security,” Computers & Security, vol. 131, p. 103600, Nov. 202.

[28] T. Suleski, M. Ahmed, W. Yang, and E. Wang, “A Review of multi-factor Authentication in the Internet of Healthcare Things,” Digital Health, vol. 9, no. 1, May 2023.

[29] K. Mahmood, W. Akram, A. Shafiq, I. Altaf, M.A. Lodhi, and S.H. Islam, “An enhanced and provably secure multi-factor authentication scheme for Internet-of-Multimedia-Things environments,” Computers & Electrical Engineering, vol. 88, p. 106888, Dec. 2020.

[30] M.A. Kafi and T. Adnan, "Empowering Organizations through IT and IoT in the Pursuit of Business Process Reengineering: The Scenario from the USA and Bangladesh," Asian Business Review, vol. 12, no. 3, pp. 67–80, Dec. 2022.

[31] P.H. Meland, Y.F.F. Bayoumy, and G. Sindre, “The Ransomware-as-a-Service economy within the darknet,” Computers & Security, vol. 92, pp. 101762, May 2020.

[32] A. Basit, M. Zafar, X. Liu, A.R. Javed, Z. Jalil, and K. Kifayat, “A comprehensive survey of AI-enabled phishing attacks detection techniques,” Telecommunication Systems, vol. 76, no. 1, Oct. 2020.

[33] D. Jampen, G. Gür, T. Sutter, and B. Tellenbach, “Don’t click: towards an effective anti-phishing training. A comparative literature review,” Human-centric Computing and Information Sciences, vol. 10, no. 1, Aug. 2020.

[34] N.Q. Do, A. Selamat, O. Krejcar, E. Herrera-Viedma, and H. Fujita, “Deep Learning for Phishing Detection: Taxonomy, Current Challenges and Future Directions,” IEEE Access, pp. 1–1, 2022.

[35] M. Ifeanyi Akazue, A. Adimabua Ojugo, R. Elizabeth Yoro, B. Ogheneovo Malasowe, and O. Nwankwo, “Empirical evidence of phishing menace among undergraduate smartphone users in selected universities in Nigeria,” Indonesian Journal of Electrical Engineering and Computer Science, vol. 28, no. 3, pp. 1756, Dec. 2022.

[36] T. Gangavarapu, C.D. Jaidhar, and B. Chanduka, “Applicability of machine learning in spam and phishing email filtering: review and approaches,” Artificial Intelligence Review, vol. 53, Feb. 2020.

[37] A. El Aassal, S. Baki, A. Das, and R.M. Verma, “An In-Depth Benchmarking and Evaluation of Phishing Detection Research for Security Needs,” IEEE Access, vol. 8, pp. 22170–22192, 2020.

[38] Djeki, Essohanam, Jules Dégila, and Muhtar Hanif Alhassan. "Reimagining Authentication: A User-Centric Two-Factor Authentication with Personalized Image Verification." In *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*, pp. 281-285. IEEE, 2024.

[39] Gurukala, Neel Kumar Yadav, and Deepak Kumar Verma. "Feature Selection using Particle Swarm Optimization and Ensemble-based Machine Learning Models for Ransomware Detection." *SN Computer Science* 5, no. 8 (2024): 1-18.

[40] M. Al-Hawawreh, M. Alazab, M.A. Ferrag, and M.S. Hossain, “Securing the Industrial Internet of Things against ransomware attacks: A comprehensive analysis of the emerging threat landscape and detection mechanisms,” Journal of Network and Computer Applications, vol. 223, pp. 103809, Mar. 2024.

[41] Jalil, Sajjad, Muhammad Usman, and Alvis Fong. "Highly accurate phishing URL detection based on machine learning." *Journal of Ambient Intelligence and Humanized Computing* 14, no. 7 (2023): 9233-9251.

[42] J. Zhang and D. Tenney, “The Evolution of Integrated Advance Persistent Threat and Its Defense Solutions: A Literature Review,” Open Journal of Business and Management, vol. 12, no. 1, pp. 293–338, Dec. 2023.

[43] S.K. Hassan and A. Ibrahim, “The role of Artificial Intelligence in Cyber Security and Incident Response”, International Journal for Electronic Crime Investigation, vol. 7, no. 2, Jul. 2023.

[44] A.V. ANDRIU, “Adaptive Phishing Detection: Harnessing the Power of Artificial Intelligence for Enhanced Email Security,” Romanian Cyber Security Journal, vol. 5, no. 1, pp. 3–9, May 2023.

[45] Y. R. Siwakoti, M. Bhurtel, D. B. Rawat, A. Oest, and R. Johnson, “Advances in IoT security: Vulnerabilities, enabled criminal services, attacks and countermeasures,” IEEE Internet of Things Journal, vol. 10, no. 13, pp. 1–1, 2023.

[46] M. Humayun, N. Tariq, Majed Alfayad, Muhammad Zakwan, Ghadah Alwakid, and M. Assiri, “Securing the Internet of Things in Artificial Intelligence Era: A Comprehensive Survey,” IEEE access, pp. 1–1, Jan. 2024.

[47] M. Javed, M.J. Mannan., "Securing smart healthcare cyber-physical systems against blackhole and greyhole attacks using a blockchain-enabled gini index framework," Sensors, vol. 23, no. 23, pp. 9372, 2023.

[48] M. Hassan, "Gitm: A gini index-based trust mechanism to mitigate and isolate sybil attack in rpl-enabled smart grid advanced metering infrastructures," IEEE Access, vol. 11, pp. 62697–62720, 2023.

[49] U. Farooq, Muhammad Asim, Noshina Tariq, Thar Baker, Ali Ismail Awad, "Multi-mobile agent trust framework for mitigating internal attacks and augmenting RPL security," Sensors, vol. 22, no. 12, pp. 4539, 2022.