https://doi.org/10.2352/EI.2025.37.3.MOBMU-326

AI-Based Vulnerability Scanners: A Cross-Sectional Survey Analysis

Sam Soney Chemparathy[1], **Navaneeth Shivananjappa**[1], **Reiner Creutzburg** [1,2]

[1] **SRH University, School of Technology and Architecture, Sonnenallee 221, D-12509 Berlin, Germany**
[2] **Technische Hochschule Brandenburg, Department of Informatics and Media, Magdeburger Str. 50, D-14770 Brandenburg, Germany**

Email: samsoney.edu@gmail.com, navaneeth.shivananjappa@srh.de, reiner.creutzburg@srh.de, creutzburg@th-brandenburg.de

Keywords: AI-based vulnerability scanners, cybersecurity, AI models, false positives, integration, user survey

Abstract

One major innovation in improving organizations' security measures is the adoption of AI-based vulnerability scanners within the cybersecurity space. The paper analyzes cross-sectional survey research identifying factors that influence the acceptance and use of such advanced tools among cybersecurity professionals. The primary method of gathering data was a structured survey questionnaire that used Likert-scale questions to quantify the participants' opinions objectively. It contained 20 questions based on established models, including TAM, UTAUT, and IDT. In this research, the total number of people who responded to the survey was 49, comprising cybersecurity professionals working in various industry domains. This instrument has measured perceived usefulness, ease of use, performance expectancy, effort expectancy, social influence, facilitating conditions, and the stages of adoption, including awareness, interest, evaluation, trial, and adoption. Our results provide insight into factors that drive or hinder the adoption of AI-based vulnerability scanners, focusing on the significant role of perceived benefits and organizational support. The present paper offers valuable implications for practitioners and researchers who aim to foster AI-driven security solutions within organizational contexts.

Introduction

An evolving cyber threat landscape haunts the organization with growing burdens of discovery and mitigation. While traditional vulnerability scanners were indispensable, heightened threat complexity requires advanced solutions. One such futuristic innovation is an AI-based vulnerability scanner that tends to harness the power of artificial intelligence for speed, accuracy, and adaptability in detecting vulnerabilities.

These AI-based scanners automate, using machine learning algorithms to analyze big data for patterns, attempting to find security threats more quickly than traditional means. The tools can revolutionize cybersecurity since they offer intelligent, proactive threat detection. However, this adoption would depend on the organization's perceived usefulness, ease of use, and readiness.

This research paper outlines these enablers through a cross-sectional survey of cybersecurity practitioners who work across industries. These insights are made with an inherent application of three key theoretical models: the Technology Acceptance Model, the Unified Theory of Acceptance and Use of Technology, and the Innovation Diffusion Theory. All these models provide a common framework to identify technology adoption in organizations.

TAM deals with the perceived usefulness and ease of use [1], while UTAUT constitutes performance expectancy, effort expectancy, social influence, and facilitating conditions [2]. IDT addresses the five stages of innovation adoption: awareness, interest, evaluation, trial, and adoption [3].

Forty-nine cybersecurity professionals were surveyed using 20-item Likert-scale questions [4] designed to quantify participants' opinions objectively. The questionnaire probed familiarity with AI-based scanners, perceptions about effectiveness, problems with traditional and AI-based scanners, and factors influencing acceptance and integration.

This paper analyses cross-sectional survey research to identify key factors that affect cybersecurity professionals' acceptance and usage of such advanced tools, which could provide useful implications for practitioners and researchers. This will also go a long way in understanding drivers and inhibitors of AI-based vulnerability scanners. The findings have useful implications for the diffusion of AI-driven security solutions within organizations, especially perceived benefits, organizational support, and ongoing adaptation to the ever-evolving face of cyber threats.

Objectives

In other words, the main objective will be to assess how perceived usefulness, ease of use, and organizational readiness will impact integrating advanced tools by answering the created four objectives A, B, C, and D below through a questionnaire. This contributes theoretically and practically to an understanding of cyber security through the use of models such as the Technology Acceptance Model (TAM), Unified Theory of Acceptance and Use of Technology (UTAUT), and Innovation Diffusion Theory (IDT).

A structured 20-question questionnaire was prepared to measure the four items listed in the objectives below, based on the Technology Acceptance Model, the Unified Theory of Acceptance and Use of Technology, and the Innovation Diffusion Theory. In its online survey form, this questionnaire was distributed to cybersecurity professionals through various industry networks, online platforms, and professional groups in cybersecurity.

Assess Awareness and Perceptions

It involves the degree to which cybersecurity professionals are aware of the effectiveness, accuracy, and level of integration of AI-based vulnerability scanners relative to other traditional means of carrying out the said tasks.

Identify Benefits and Challenges

Identify the advantages and drawbacks of AI-based vulnerability scanners in adapting to new threats, reducing workload, and handling volumes of data about false positives/negatives.

Evaluate Sector-Specific Performance and Ethical Considerations

Research on various AI-based vulnerability scanners and their performance, applied in finance and healthcare, to describe the identified ethical concerns and organization-wide challenges to adopting such technologies.

Determine Adoption Factors and Expertise Requirements

The key factors affecting the acceptance of AI-based vulnerability scanners include but are not restricted to perceived usefulness, ease of use, and cost-effectiveness; the critical issue is how many skills the implementation and maintenance of such systems require.

The paper discusses the effectiveness, efficiency, and adaptability of AI-based vulnerability scanners for ensuring cybersecurity through survey research. For this purpose, a structured survey questionnaire will be designed.

Literature Review

Recent research has been directed toward applying various artificial intelligence techniques to assess and detect vulnerabilities in software systems [5]. Recent studies have also shown that machine learning and deep learning models are very effective in automatically detecting vulnerabilities in software, which improves efficiency compared to manual methods [6]. These methods can analyze source codes, requirements documents, and other software artifacts to identify security flaws. Residual challenges include the need for high-quality vulnerability datasets and the standardization of evaluation methods [7]. For example, many AI structures have been researched by convolutional neural networks and time series models [8]. Recent surveys by categorizing and analyzing various ML/DL approaches to vulnerability detection pointed to the trends, datasets, and model architectures used [9]. Although promising, AI-based methods enhance careful system development to prevent vulnerabilities. Indeed, current research identifies this problem and thus focuses on improving AI-based vulnerability detection techniques [10]. This paper, therefore, researches factors affecting the cyber-security industry's adoption of an AI-based vulnerability scanner.

While previous research has specifically emphasized the technical competencies of these tools, this is one of the very first studies to apply multi-theory models in examining the broader organizational, technological, and human issues that mold such adoptions. Based on a survey among cybersecurity professionals, an integrated perspective will be employed; hence, the current study will analyze perceived usefulness, organizational readiness, and ethical considerations regarding the integration and effectiveness of AI-driven security solutions. This further sheds light on the field and practical application of AI technologies in cybersecurity.

Methodology

A structured survey questionnaire is prepared to gather primary data for this project. Quantitative responses are sought to assess the effectiveness, efficiency, and adaptability of AI-based scanners in vulnerability assessment.

Thus, those questions will yield specific answers concerning respondents' views on AI-based vulnerability scanners in an organizational setting. For instance, participants' degree of trust in AI-based scanners' capabilities to find vulnerabilities and remediate them could be asked on a Likert scale.

Technology Acceptance Model (TAM)

TAM focuses on how users accept and use a technology [2]. The appropriate questions in this model are familiarity, ease of use, and perceived usefulness.

Questions for the final model include

1. How familiar are you with AI-based vulnerability scanners in cybersecurity?
2. Do you think AI-based vulnerability scanners are more accurate in identifying complex issues than traditional scanners?
3. In your opinion, what expertise is required for organizations to implement and manage AI-based vulnerability scanners effectively?
4. To what extent do you believe AI can enhance the speed of vulnerability detection compared to traditional methods?
5. How adaptable do you think AI-based vulnerability scanners are in handling and analyzing massive volumes of data?
6. In your opinion, how effective are traditional vulnerability scanners in identifying and mitigating cybersecurity threats?

Unified Theory of Acceptance and Use of Technology (UTAUT)

UTAUT can be explained as the aim of explaining user intentions to use information systems and subsequent usage behavior [3]. Questions related to performance expectancy, effort expectancy, social influence, and facilitating conditions come into view here.

The questions created from this model are:

1. In your opinion, how well do AI models integrate with existing cybersecurity frameworks?
2. How confident are you in the ability of AI-based vulnerability scanners to keep pace with continuously evolving cyber threats?
3. To what extent do you believe AI-based vulnerability scanners can enhance the proactive identification of potential threats before exploitation?
4. In your opinion, what challenges might organizations face in integrating AI into their vulnerability scanning processes?
5. How do you perceive the role of AI in addressing zero-day exploits compared to traditional vulnerability scanning methods?

6. To what extent do you believe AI can contribute to reducing the workload associated with cybersecurity vulnerability assessments?

Innovation Diffusion Theory (IDT)

IDT summarized how, why, and at what rate new technologies spread. IDT's central question was about innovation adoption: "the importance of innovation itself, the channels of communication, and the adoption decision-making process."[4].

The questions created from this model are:

1. How crucial is it for cybersecurity solutions to adapt to emerging threats in real-time?
2. Do you believe there are ethical considerations in using AI for vulnerability scanning?
3. What factors do you consider when evaluating the cost-effectiveness of implementing AI-based vulnerability scanners compared to traditional methods?
4. How do you perceive the overall impact of AI on the cybersecurity posture of organizations using AI-based vulnerability scanners?
5. In your organization or experience, what features or improvements would you prioritize in AI-based vulnerability scanners?
6. How concerned are you about false positives and false negatives when using AI-based vulnerability scanners?
7. Have you experienced any challenges with conventional vulnerability scanners adapting to evolving cyber threats?
8. In your experience, how well do AI-based vulnerability scanners perform in various sectors such as finance, healthcare, and government?

Number of Participants

Forty-nine people from the IT industry and cybersecurity domains were surveyed, and their responses are used in work.

Results

AI Vulnerability Scanners technology offers many opportunities but also poses definite challenges. Organizations must face many more new digital threats, and when detecting vulnerabilities, they must call for better and specialized tools. AI has, therefore, revamped the issue of detecting vulnerability so that cybersecurity defense has become reliable, more accurate, and highly adaptable. However, some concerns have been raised regarding the implementation of AI-based scanners.

How familiar are you with AI-based vulnerability scanners in cybersecurity?

The survey leaned more to the familiar side, with 32.7% very familiar and 42.9% somewhat familiar. While 14.3% were not very familiar and 10.2% were not familiar at all.

How effective are traditional vulnerability scanners in identifying and mitigating cybersecurity threats?

Most respondents found traditional scanners somewhat compelling, with 57.1% rating them moderately effective and 22.4% finding them very effective. However, only 12.2% found them ineffective, and 8.2% were not sure.

Have you experienced any challenges with conventional vulnerability scanners in adapting to evolving cyber threats?

22.4% of respondents reported experiencing challenges frequently, while 55.1% encountered them occasionally. 12.2% said they rarely faced challenges, and 10.2% stated they never experienced any.

How crucial is cybersecurity solutions adapting to emerging threats in real-time?

The majority of respondents leaned towards the crucial side, with 26.5% finding it extremely crucial, 42.9% somewhat crucial, while 18.4% finding it not very crucial, and 12.2% saying it was not crucial at all.

To what extent do you believe AI can enhance the speed of vulnerability detection compared to traditional methods?

A significant portion, 32.7%, believed AI can significantly enhance detection speed. 38.8% rated it as moderately effective, 16.3% slightly effective, and 12.2% said it would not enhance speed at all.

Do you think AI-based vulnerability scanners are more accurate in identifying complex issues than traditional scanners?

The responses showed that 30.6% believed AI scanners were more accurate, while 46.9% thought maybe. On the other hand, 14.3% were unsure, and 8.2% did not think AI scanners were more accurate.

In your opinion, how well do AI models integrate with existing cybersecurity frameworks?

28.6% of respondents believed AI models integrate very well with existing cybersecurity frameworks. 49% thought the integration was moderately successful, while 16.3% felt the integration was poor, and 6.1% had no idea.

How concerned are you about false positives and false negatives when using AI-based vulnerability scanners?

A majority expressed concern, with 20.4% being very concerned and 55.1% somewhat concerned. 16.3% said they were not very concerned, and 8.2% were not concerned.

To what extent do you believe AI can contribute to reducing the workload associated with cybersecurity vulnerability assessments?

26.5% of respondents believed AI could reduce the workload a great deal. 46.9% thought it could somewhat help, 12.2% believed AI would have very little impact, and 14.3% thought it would not help at all.

How adaptable do you think AI-based vulnerability scanners are in handling and analyzing massive volumes of data?

The data showed 26.5% thought AI scanners were highly adaptable, 49% rated them as moderately adaptable, 16.3% found them not very adaptable, and 8.2% believed they were not adaptable at all.

In your experience, how well do AI-based vulnerability scanners perform in various sectors such as finance, healthcare, and government?

28.6% of respondents thought AI scanners performed excellently across sectors, while 49% found their performance satisfactory. However, 16.3% rated the performance as poor, and 6.1% had no experience in this area.

Do you believe there are ethical considerations in using AI for vulnerability scanning?

32.7% of respondents identified significant ethical considerations, 36.7% saw some concerns, 16.3% did not perceive any major concerns, and 14.3% were unsure.

In your opinion, what challenges might organizations face in integrating AI into their vulnerability scanning processes?

26.5% of respondents cited technical challenges as a primary concern, 49% pointed to cultural resistance, 18.4% mentioned lack of expertise, and 6.1% identified other challenges.

How do you perceive the overall impact of AI on the cybersecurity posture of organizations using AI-based vulnerability scanners?

22.4% believed AI had a very positive impact, 49% found the impact positive, while 14.3% saw it as neutral, and another 14.3% viewed the impact as negative.

In your organization or experience, what features or improvements would you prioritize in AI-based vulnerability scanners?

22.4% of respondents prioritized faster detection speeds, 51% preferred improved accuracy, 16.3% wanted better integration with existing systems, and 10.2% mentioned other features.

How confident are you in the ability of AI-based vulnerability scanners to keep pace with continuously evolving cyber threats?

29.8% of respondents were very confident, 40.4% were moderately confident, 12.8% were not very confident, and 17% were not confident at all.

To what extent do you believe AI-based vulnerability scanners can enhance the proactive identification of potential threats before exploitation?

27.7% of respondents believed AI could significantly enhance threat identification, 46.8% thought it could moderately improve it, 10.6% said slightly, and 14.9% felt it would not help at all.

What expertise is required for organizations to effectively implement and manage AI-based vulnerability scanners?

21.3% of respondents believed high expertise was needed, 53.2% thought moderate expertise was sufficient, 21.3% said low expertise was enough, and 4.3% thought no expertise was required.

How do you perceive the role of AI in addressing zero-day exploits compared to traditional vulnerability scanning methods?

36.2% of respondents thought AI was much more effective, 38.3% found it somewhat more effective, 19.1% said it was equally effective, and 6.1% believed it was less effective.

What factors do you consider when evaluating the cost-effectiveness of implementing AI-based vulnerability scanners compared to traditional methods?

25.5% of respondents prioritized initial investment costs, 44.7% focused on maintenance and training costs, 23.4% considered return on investment (ROI), and 6.4% identified other factors.

Findings

To calculate the Likert scale-based analysis of the objectives, numerical values are assigned to the responses for the key questions under each research objective.

Very familiar/Very effective/Strongly agree/etc. = 5 Somewhat familiar/Moderately effective/Agree/etc. = 4 Neutral/Equally effective/etc. = 3 Not very familiar/Somewhat ineffective/etc. = 2 Not at all familiar/Ineffective/Strongly disagree/etc. = 1

Average score (on a 1 to 5 scale) for:

Research Objective	Average Likert Score
Assess Awareness and Perceptions	3.94
Identify Benefits and Challenges	3.90
Evaluate Sector-Specific Performance (AI)	4.04
Determine Adoption Factors and Expertise Requirements	3.0

Table 1: Likert Scale Scores for Research Objectives

Assess Awareness and Perceptions

Average Likert Score: 3.94

General Familiarity: 75.6% of the participants had a good understanding of vulnerability scanners-AI, topping the list, while some of the respondents were unaware.

Perception of Traditional Tools: A few would say that conventional scanners work where 22.4% of the surveyed population rarely or never had challenges with conventional scanners, but at least people are curious about other AI-based alternatives to show openness to exploring the potential of new solutions for redressing the deficiencies of tools at hand.

Identify Benefits and Challenges

Average Likert Score: 3.90

Challenges with Conventional Vulnerability Scanners Systems: 77.5% Believed traditional vulnerability scanners often posed problems regarding fast-changing cybersecurity threats. This underlines the demand for solutions that can keep up more dynamically and flexibly, and this is where AI tools could shine.

Benefits and Challenges of AI-based vulnerability Scanners: Although the majority of the surveyed population believes that AI can increase the speed of vulnerability detection and proactive identification of potential threats before exploitation, 75.5% i.e. majority of the population is very concerned and somewhat concerned regarding the concern of increased False Positives and False Negative with AI-based vulnerability scanners

Sector-Specific Performance and Ethical Concerns

Average Likert Score: 4.04

Sector-Specific Performance: 77.6% percent of the population believed that finance, healthcare, and government sectors could benefit from AI-based vulnerability scanners.

Effectiveness of AI for Zero-Day Exploits: 74.5% Respondents feel AI can handle the zero-day vulnerabilities more effectively when compared to usual scanners. This again supports that AI has great potential for detecting and mitigating newly emerging threats, which are difficult to catch with other conventional tools.

Ethical Considerations: 69.4% of the population believe that there will be significant and some ethical concerns when using AI for vulnerability scanning because of the scanner's access to files and folders.

Adoption Factors and Expertise Needs

Average Likert Score: 3.0

Expertise Requirements: 74.5% of the survey shows that High Expertise and Moderate expertise are required when implementing and managing AI-based vulnerability scanners.

Key Drivers for Adoption: The key driver for adopting AI-based vulnerability scanners would be its speed, as responded positively by 71.5% of the surveyed population. Another factor would be its ability to detect zero-day exploits because where 74.5% of the surveyed population believe that AI can effectively detect zero-day exploits.

Significant Concern About False Positives and Negatives

The outcomes are that the participants have different levels of concern for false positives and negatives in AI-based scanners:

Moderate Concern (55%): Over half of respondents are concerned to some degree; the result shows that false positives can be an issue, though not possibly a huge one for most users.

High Concern (20%): 20% of the respondents still expressed high concern about the possibility of false positives and negatives that could thwart confidence in the use of AI-based scanners.

Low Concern (16%): A smaller percentage of the less concerned explain it by trusting the strength of AI tools in handling false positives or not having enough problems with them.

No concern (8%): Some are not concerned at all, probably having very high confidence in the technology or no exposure to false positives.

Adoption Impact: This general concern, particularly about false positives among the ”somatically concerned” and ”very concerned,” underscores the need to improve AI accuracy to invite greater adoptions.

Opportunity for Improvement: There is definite potential if the improvements in AI vulnerability scanners can be made to reduce these eliminations of false positives. That would surely help in increasing the accuracy of detection and probably raise the confidence level of the users, thereby becoming effective for the organizations.

Development Focus: AI developers should reassure highly concerned users by improving precision. Such an AI-based vulnerability scanner will meet the need for and raise confidence in its capabilities by developing an increasingly high level of defense not undermined by a higher level of false alerts.

Evaluate Sector-Specific Performance and Ethical Considerations

Sector-Specific Performance: Twenty-four responses, which involve most respondents, rate AI vulnerability scanners as performing satisfactorily across finance, healthcare, and government. While 14 responses rated performance as excellent, 8 noted poor performance, indicating varying effectiveness across sectors due to differences in system complexity or regulations. A lack of experience in specific sectors (3 responses) indicates gaps in adoption or awareness.

Ethical Considerations: Eighteen respondents identified ethical concerns, with 16 flagging significant issues like privacy and algorithmic bias. While only eight responses saw no major ethical concerns, reflecting confidence in existing safeguards. The division suggests clear ethical standards for AI use in cybersecurity.

Integration Challenges: Cultural resistance is a significant obstacle, as shown by the reluctance of 24 respondents to trust AI. 13 respondents feel technical issues, and nine lack expertise, highlighting the complexity of AI adoption in cybersecurity and indicating the need for workforce upskilling.

AI-based vulnerability scanners have potential across sectors but face performance, ethics, and integration challenges. Addressing cultural resistance, ethical risks, and technical complexity is crucial for broader adoption.

Recommendations

Enhancing Detection Capabilities and Reducing False Positives

To tackle the issue of false positives in vulnerability detection systems, advancements such as the deep learning-based system VulDeePecker have shown promising results. VulDeePecker was tested with a dataset developed explicitly for deep learning vulnerability detection, and the findings indicate its ability to significantly reduce false negatives while maintaining a manageable rate of false positives. When applied to software products like Xen, Seamonkey, and Libav, VulDeePecker uncovered four vulnerabilities not listed in the National Vulnerability Database but were silently patched in later versions by the vendors. Other detection systems largely overlooked these vulnerabilities. This demonstrates that systems like VulDeePecker, leveraging deep learning, can improve the accuracy of vulnerability detection and lower the rate of false positives, thereby strengthening the overall security of software [11].

Addressing Ethical Concerns in System Development

Ethical considerations are essential when developing AI-driven systems, including those used for vulnerability detection. Companies have highlighted the importance of engaging multi-disciplinary teams to examine various perspectives on ethical challenges. Best practices involve clearly defining the purpose of AI systems and assessing their broader societal and operational impacts. Ethical guidelines emphasizing critical quality aspects, such as transparency, fairness, privacy, and explainability, should guide the development process. The findings suggest that organizations should prioritize developing and enforcing ethical standards to ensure that AI systems are built responsibly and align with societal values [12].

This structure ensures clarity and focuses on actionable steps for improving AI-driven vulnerability scanners.

Conclusion

The average score concerning awareness of and perception of the level of AI-driven scanners was about 3.94, showing evidence that most users were better acquainted with the tool and solution. However, a component of the audience needed increased exposure to knowledge in this regard. This has shown further awareness due to the education gap.

Returning to the benefits and challenges, an average score of 3.90 reveals that traditional vulnerability scanners struggle to keep pace with fast-evolving cybersecurity threats. This improves AI-based tools, as they can be more adaptive in solving problems. At the same time, cost-effectiveness and return on investment will be compelling, and they tend to address the long-term benefits over initial implementation costs.

The industry-wide performance of those AI scanners was netting off at 4.04, whose total outlook is intrinsically very positive, especially about zero-day vulnerability detection. Concerns were raised about privacy and algorithmic bias, particularly in financial, health, and government industries. All things being equal, AI perhaps outperforms these traditional tools in concrete areas, but the performance variability due to sector-specific challenges evidences room for improvement. The adoption factor and the expertise requirement averaged 3.0, respectively, raising concerns about the technical expertise required to implement and manage the scanner-based AI process. Most answers registered that high levels of expertise might hamper the adoption process. Most of the other major concerns raised are those where most show at least a moderately high level of false positives and negative threats. This consequence means there would be an enhanced use of the AI scanner's accuracy, giving birth to trust and reliance on the tool. In the bigger picture of rapidly changing threats, AI-enabled vulnerability scanners will most likely be found highly useful yet have to work out issues of expertise requirements, false positives, and ethical concerns. Future efforts should be directed toward detection with increasing accuracy and a corresponding reduction in false positives. More importantly, the responsible use of AI will activate trust and full adoption across industries.

Acknowledgments

This work was supported partially by the European Union in the framework of ERASMUS MUNDUS, Project CyberMACS (Project #101082683) (`https://cybermacs.eu`).

We want to warmly thank Mahipal for his support in reviewing this paper.

References

[1] F. D. Davis and A. Granić, *The Technology Acceptance Model*, 2024.

[2] L. Liu, A. M. Cruz, A. R. Rincon, V. Buttar, Q. Ranson, and D. Goertzen, "What factors determine therapists' acceptance of new technologies for rehabilitation – a study using the Unified Theory of Acceptance and Use of Technology (UTAUT)," *Disability and Rehabilitation*, vol. 37, no. 5, pp. 447-455, Jun. 2014.

[3] A. T. F. Lou and E. Y. Li, "Integrating innovation diffusion theory and the technology acceptance model: The adoption of blockchain technology from business managers' perspective," in *ICEB Jan. 2017 Proceedings*, Dubai, UAE, 2017.

[4] J. Robinson, "Likert scale," in *Springer eBooks*, 2014, pp. 3620-3621.

[5] S. Khan and S. Parkinson, "Review into state of the art of vulnerability assessment using artificial intelligence," in *Computer Communications and Networks*, 2018, pp. 3-32.

[6] S. Kommrusch, "Artificial intelligence techniques for security vulnerability prevention," *arXiv* (Cornell University), Jan. 2019.

[7] Y. Lin *et al.*, "Vulnerability dataset construction methods applied to vulnerability detection: A survey," Jun. 2022.

[8] A. M. S. N. Amarasinghe, W. A. C. H. Wijesinghe, D. L. A. Nirmana, A. Jayakody, and A. M. S. Priyankara, "AI based cyber threats and vulnerability detection, prevention and prediction system," Dec. 2019.

[9] N. S. Harzevili *et al.*, "A survey on automated software vulnerability detection using machine learning and deep learning," *arXiv* (Cornell University), Jan. 2023.

[10] P. S, C. C. B, and L. K. Raju, "Developer's roadmap to design software vulnerability detection model using different AI approaches," *IEEE Access*, vol. 10, pp. 75637-75656, Jan. 2022.

[11] D. Zou, S. Wang, S. Xu, Z. Li, and H. Jin, "VulDeePecker: A deep learning-based system for multiclass vulnerability detection," *IEEE Trans. on Dependable and Secure Computing*, p. 1, Jan. 2019.

[12] N. Balasubramaniam, M. Kauppinen, S. Kujala, and K. Hiekkanen, "Ethical guidelines for solving ethical issues and developing AI systems," in *Lecture Notes in Computer Science*, 2020, pp. 331-346.

Author Biography

Sam Soney Chemparathy holds a Master's in Computer Science with a focus on Cybersecurity from SRH Berlin University. His interests include Cybersecurity, Vulnerability Management, Cloud Security, and ISO standards compliance. He is passionate about modern security challenges and promoting a secure digital environment.

Navaneeth Shivananjappa is a Lecturer at SRH University of Applied Sciences, Berlin School of Technology and Architecture, specializing in the field of Web Application Pentesting and Cyber Security. His research interests include Cybersecurity, Cybersecurity tools, Penetration Testing, Web Application Security, Kubernetes Security, Cloud Security, and Cybersecurity Awareness.

Reiner Creutzburg is a Retired Professor for Applied Computer Science at the Technische Hochschule Brandenburg in Brandenburg, Germany. Since 2019, he has been a Professor of IT Security at the SRH Berlin University of Applied Sciences, Berlin School of Technology. He is a member of the IEEE and SPIE and *chairman of the Multimedia on Mobile Device (MOBMU) Conference at the Electronic Imaging conferences since 2005. In 2019, he was elected a member of the Leibniz Society of Sciences to Berlin e.V. His research interests include Cybersecurity, Digital Forensics, Open Source Intelligence (OSINT), Multimedia Signal Processing, eLearning, Parallel Memory architecture, and Modern Digital Media and Imaging Applications.*

Image Engineering

STUDENT/YP SHOWCASE
PURDUE