World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(Research Article)

Check for updates

Security and privacy challenges of AI-powered coding assistants

Firoz Mohammed Ozman *

Solutions Architect, Enterprise Architecture, Anecca Ideas Corp, Toronto, Canada.

World Journal of Advanced Engineering Technology and Sciences, 2026, 18(01), 331-343

Publication history: Received on 18 December 2025; revised on 25 January 2026; accepted on 28 January 2026

Article DOI: https://doi.org/10.30574/wjaets.2026.18.1.0056

Abstract

The primary aim of the present research is to critically evaluate the security and privacy concerns associated with AI-based coding assistants and to propose evidence-based solutions that enable their safe and responsible utilization. The study contributes to research and practice by providing a systematic discussion of security and privacy issues. The current literature has been applying STS and PhD as independent concepts. However, the literature is limited in demonstrating how AI-based coding assistants change when the two concepts are combined. The methodical review of the selected literature identifies five interconnected themes that summarize the security and privacy of AI-powered coding assistants. These themes are repeatedly reflected in the empirical research, qualitative developer interviews, industry case studies, and conceptual security analyses.

Keywords: AI-powered coding assistants; Secure code generation; Cybersecurity in AI systems; Privacy-by-design; Automation bias; AI governance

1. Introduction

Artificial intelligence (AI) code assistants have become a routine part of the software development process. Code generators based on large language models and related approaches have assisted developers with boilerplate code autogeneration and provided suggestions, while also being more efficient to learn and develop faster (Carter, Dawson, and Oladeji Olaniran, 2025). Beginning with solutions proposed by OpenAI and GitHub, these solutions have gained significant adoption and are based on cloud-hosted models trained on large datasets of source code (Haque, 2025). Despite being identified as efficient and supporting rapid development, these systems must be developed through ongoing interaction with sensitive artefacts, such as proprietary code, credentials, and architectural logic. This has also created security and privacy concerns, which are important alongside performance and usability (Ozman, 2025).

1.1. Problem Statement

Despite the growing popularity of AI-driven coding assistants, they introduce new security and privacy challenges that are not adequately understood or addressed at the system level (Ozman, 2025). These risks include accidental leakage of confidential source code, memorization and copying of sensitive training data, insecure code suggestions, and vulnerabilities resulting from model abuse or immediate manipulation (Ben Yaala & Bouallegue, 2025). Organizational security policies and the software development life cycle (SDLC) are often not configured to evaluate or mitigate threats that are not AI-specific. A lack of empirical and conceptual studies on the same poses a problem for creators, organizations, and regulators in applying such tools for safe deployment and governance.

* Corresponding author: Firoz Mohammed Ozman.

1.2. Research Aim and Objectives

Aim

The primary aim of the present research is to critically evaluate the security and privacy concerns associated with AI-based coding assistants and to propose evidence-based solutions that enable their safe and responsible utilization.

Objectives

- To identify and categorise the significant security threats that AI-based coding assistants pose to software development
- To analyse the problem of privacy in terms of data collection, model training, and real-time transactions on code
- To compare existing technical, organisational, and regulatory controls in relation to the risks
- To propose an evidence-based model of optimal practices toward reducing the risks of security and privacy practices

1.3. Research Questions

- What are the key security threats of AI-based coding assistants during the software development life cycle?
- How does an AI coding assistant impact the privacy of the developers and organisations, both in terms of proprietary and personal data?
- What is the level of mitigation measures that are now in place to control the challenges?
- What are the practical and policy-based strategies that can be applied to enhance the usage of AI-powered coding assistants in a secure and privacy-friendly way?

1.4. Research Rationale

The research is relevant and timely, given the rapid adoption of AI-based tools in mission-critical software systems. The study contributes to research and practice by providing a systematic discussion of security and privacy issues. It offers an advantage to software engineers, cybersecurity experts, and decision-makers who prefer a balance between innovation and risk mitigation. The results would also inform organizational governance systems, help establish ethical and secure AI-assisted programming environments, and thereby promote sustainable and reliable AI-assisted software engineering.

2. Literature Review

2.1. Artificial intelligence-powered coding assistant security threats

Recent literature indicates that AI-based coding assistants pose novel security threats to software development practices. Oh et al. (2024) confirm that malicious AI models can deliberately introduce vulnerable programs with insecure code suggestions, leading programmers to adopt risky habits they may not understand at the time. According to Perry et al. (2023), developers using AI assistants in code may, unconsciously, create less secure code, further compounding this risk. Rajapaksa et al. (2022) present the other side of this risk as an example of AI-based vulnerability detection, raising the dilemma of dual-use technology, since the same tool may be used to enhance or compromise security. Iqbal et al. (2023) also expand on the dangers by defining immediate manipulation, the development of malicious code, and automated exploitation as cybersecurity hazards associated with conversational AI systems. Lakis and Rifai (2025) note that, for practitioners, developers report productivity gains, but these gains are accompanied by hidden vulnerabilities and reduced critical thinking in the resulting code. An amalgamation of these studies reveals that the vulnerabilities of technical models, along with behavioral and contextual abuses, can be exploited to create security threats.

2.2. AI coding assistants are impacting the privacy of developers and organizations.

The privacy of AI coding assistants is increasingly a topic of debate, particularly in business contexts. Although AI code assistants can enhance productivity (Weisz et al., 2025), implementing such systems often involves sharing proprietary code with other cloud-based systems, which poses risks for data disclosure and intellectual property leakage. In this regard, Thaw (2025) concludes that productivity gains are usually achieved at the expense of transparency in data handling and storage. As Pan et al. (2024) reveal, developers are shifting toward selective use, as privacy concerns lead them to avoid selecting AI tools for sensitive tasks, suggesting the development of a sense of responsibility and risk. Pantin (2024) also notes that junior developers may lack experience detecting privacy threats, leaving the organization vulnerable. Sergeyuk et al. (2025) also note that developers remain uncertain about how training data is reused and stored, and whether models memorize it. All these findings culminate in the conclusion that the privacy threat is informational and rooted in trust, knowledge, and organizational regulation.

2.3. Existing mitigation measures

The mitigation practices are currently technical controls, governance mechanisms, and security testing. Samola (2024) discusses the use of AI-driven cybersecurity as a threat-detection approach, and automated monitoring and anomaly detection were considered means of combating new threats. Kshetri (2025) introduces agentic AI as the next stage in the effective response to cyber threats, though questions remain regarding accountability and autonomy. Vulchi and Ackerman (2024) align the OWASP top risks of large language models with mitigation strategies and propose systematic testing and timely system hardening. Ahi et al. (2025) treat mitigation as a governance function, noting the need to balance defensive and offensive AI through policy and management. Sanne (2024) also emphasizes the importance of a high-quality security testing methodology, arguing that the traditional testing methodology should be extended to cover AI-related vulnerabilities. Therefore, current strategies remain fragmented and overly technical and are rarely incorporated into development processes.

2.4. Interventions that are policy and practice-based

A bridge between technical mitigation and practical measures should be created within organizational governance to address the mitigation gap. According to Noor (2025), access control, human-in-the-loop validation, and explicit usage policies are considered best practices for AI-assisted development teams. Graham and Kloss (2025) suggest that optimizing AI-driven CI/CD can enhance security when implemented in a controlled, supervised manner. The article by Ahmad et al. (2022) outlines authentication procedures and provides specific consideration for secure hashing and verification systems to protect artefacts of the development process. Regarding regulations, Fakeyede et al. (2023) and Yusuff (2023) note that data protection regulations, such as GDPR and CCPA, must be followed, and that IT audits and privacy-by-design must be conducted regularly. All of this leads to the conclusion that the secret of successful risk management is the ability to seek the golden mean among technical, organizational, and regulatory responses rather than personal controls.

2.5. Theoretical Framework

The study will integrate Socio-Technical Systems (STS) Theory and Privacy by Design (PbD) to examine AI-assisted code assistants. STS explains that the interaction among AI tools, developers, and organizational environments can pose security-related risks (Thomas, 2024), and PbD emphasizes privacy-related protections throughout the system development life cycle (Obiokafor et al., 2025).

2.6. Literature Gap

The current literature has been applying STS and PbD as independent concepts. However, there is limited literature demonstrating the changes in AI-based coding assistants resulting from combining the two concepts. This gap limits understanding of how collaborative mediation of security and privacy risks could be realized through synergistic socio-technical interactions and entrenched privacy ethics.

3. Materials and Methods

3.1. Search Strategy

An ordered literature review (SLR) was conducted to determine the security and privacy issues related to AI-based coding assistants, including but not limited to GitHub Copilot, CodeWhisperer, IDE-based large language model (LLM) agents, and code LLMs. The search was conducted on 6 January 2026 across the following databases: ACM Digital Library, IEEE Xplore, USENIX, SpringerLink, ScienceDirect, ACL Anthology, OpenReview, and Google Scholar.

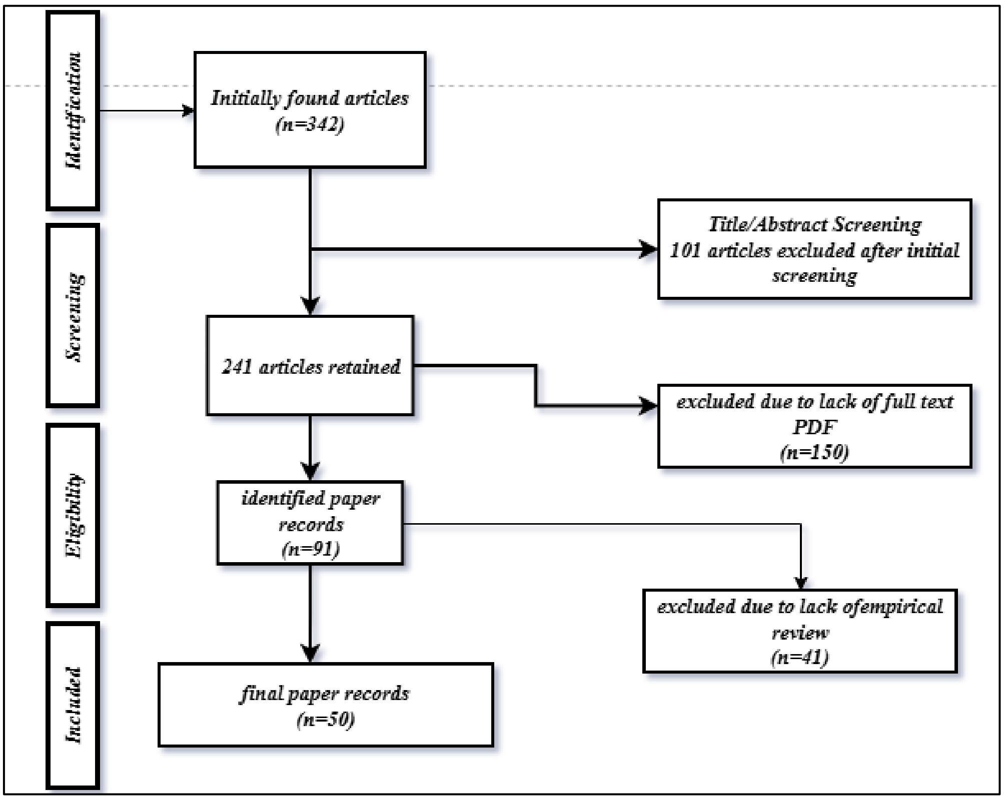
The Boolean operators were used to combine the core query blocks AND (AI coding assistant" OR code assistant OR Copilot OR CodeWhisperer OR "code LLM" OR "LLM for code" OR agentic IDE) AND (security OR vulnerability OR CWE OR insecure code OR insecure prompt injection or insecure indirect prompt injection OR insecure data leakage or privacy or memorization or membership inference or training data extraction or secrets or telemetry or licensing).

Inclusion criteria were: (i) peer-reviewed articles or trustworthy preprints/benchmarks; (ii) an explicit concentration on security/privacy threats or defensive mechanisms about code assistants or code-LLMs; (iii) English language; and

(iv) published in 2021 and 2026 at most, inclusive of foundational privacy attack papers. The inclusion criteria included only opinion articles lacking technical evidence and no-code-LLM articles.

3.2. Study Selection Using PRISMA Framework

The first identification was made using records (n=342). Duplicate records were deleted (n=101). Abstracts and titles were filtered (n =101), and 150 records were filtered out as irrelevant. In the full-text assessment, 91 records were assessed; 41 were excluded due to a lack of empirical or technical support, missing code coverage, or insufficient linkage to security/privacy issues. There were 50 studies in the final corpus.



(Source: self-developed)

Figure 1: Prisma Framework

3.3. Data Analysis Technique

Synthesis was done using a two-stage approach. First, a descriptive mapping of year of publication, location, assistant type, threat type, evaluation method, and benchmarks applied was created. Second, thematic synthesis was carried out based on a security/privacy taxonomy including: (a) insecure code generation (associated with CWEs); (b) prompt and indirect prompt injection in IDEs/agents; (c) privacy leakage and memorization (which includes secrets and PII); (d) training-data extraction and membership inference; (e) supply-chain risks such as hallucinated packages; (f) legal and licensing exposure; and (g) mitigations, such as policy controls, filtering, sandboxing, secret scanning and The risk-to-control links were cross cut across the literature.

4. Results

The methodical review of the selected literature identifies five interconnected themes that summarize the security and privacy of AI-powered coding assistants. These themes recur in the empirical research, qualitative developer interviews, industry case studies, and conceptual security analyses.

4.1. Theme 1: Privacy Threats in AI-Code

One of the most common motifs in the reviewed works is the threat of privacy violations contained in AI-generated code. Madampe, Grundy, and Arachchilage (2025) show that AI program assistants often produce code that mishandles personal or sensitive information, such as insecure credential storage, insufficient anonymization, and incorrect logging.

Equally, James and Castro (2024) note that AI systems trained on large, heterogeneous datasets can inadvertently reproduce data-handling practices that are inconsistent with modern privacy laws, such as the GDPR. These risks are compounded when developers place great trust in AI-generated boilerplate without subjecting it to stringent privacy audits. Research on mobile and IoT ecosystems (Nama, 2023; Menon et al., 2025; Farea et al., 2024) also attests that privacy issues proliferate when AI-generated code is deployed at scale across interconnected systems, thereby exposing user data.

4.2. Theme 2: Developer trust, over-reliance, and less vigilance to security

The second theme concerns developer trust and behavioral reliance on AI coding assistants. Wang et al. (2024) and Cheng et al. (2024) found that developers tend to overestimate the credibility and security awareness of AI tools, particularly when suggestions or recommendations take an assertive tone or are endorsed by online communities. Qualitative evidence presented by Klemmer et al. (2024) indicates that developers may bypass security audits or reviews when AI-generated code appears correct, thereby reducing vigilance regarding security concerns. The initial positive productivity results observed in the enterprise adoption research support this phenomenon (Davila et al., 2024; Arugula, 2024). According to Bird et al. (2022), this change involves a shift from pair programming to automation complacency, in which the developer is confident mainly that the AI has already taken security and privacy considerations into account.

4.3. Theme 3: Insufficient Security Awareness and Contextual Understanding

In the literature, it is consistently noted that AI coding assistants lack a strong understanding of security requirements. As demonstrated by Sherje (2024) and Torka and Albayrak (2024), AI tools are efficient and syntactically correct, but fail to make contextual security decisions, including threat modelling, secure authentication flows, and access-control logic. According to Klemmer et al. (2024) and Pinto et al. (2024), developers typically do not receive warnings when AI-generated code breaches organizational security policies or best practices. Such a lack of contextual security feedback means that developers are once again burdened with an additional cognitive load in assessing risks independently. Moreover, educational research (Becker et al., 2023) warns that inexperienced programmers may learn to replicate unsafe coding patterns generated by AI systems, thereby increasing security debt over the long term within the software ecosystem.

4.4. Theme 4: Ethical, Legal, and Governance Challenges

Several extend beyond technical risks to ethical and governance issues associated with AI-based coding assistants. Anidjar, Packin, and Panezi (2023) contextualize the threat to privacy as part of a broader data-infrastructure issue and argue that AI systems operate within black-box data pipelines that limit accountability. As Maham (2024) and Mushtaq and Hameeda (2025) highlight, a lack of adequate governance structures exposes organizations to regulatory and ethical breaches, particularly in sensitive areas such as the healthcare sector and government mechanisms. Developers are often unclear about accountability in cases of privacy violations arising from AI-generated code. Ali et al. (2025) also show that user perceptions of AI platforms are strongly shaped by fears of surveillance, data misuse, and a lack of transparency; hence, stronger regulatory controls and explainability systems are necessary.

5. Discussion

Altogether, the results indicate that security and privacy issues for AI-enabled coding assistants are socio-technical and arise from the interplay among technical constraints, human behavior, and governance gaps. Although AI tools play a crucial role in improving development efficiency (Arugula, 2024; Sherje, 2024), they also create new avenues for privacy breaches and security risks. According to the literature, AI assistants are not necessarily secure by design, and excessive reliance without institutional protection may only widen existing flaws. Notably, the issues mentioned are universal, and the same problems can be traced across enterprise software, mobile apps, IoTs, and cloud environments, indicating that these risks are structural rather than contextual anomalies.

6. Conclusion

6.1. Summary of Key Findings

The systematic literature review identifies four themes that help outline the privacy and security landscape of an artificial intelligence-powered coding assistant for navigating privacy risk. In this context, developer dependence, along with trust, is evident, as is the limitation of security awareness. Another theme in this literature systematic review is governance and ethical challenges. The evidence supports the use of artificial intelligence tools that improve productivity, while the generation that feels the need to justify security and privacy obligations.

6.2. Linking Findings with Objectives

The research study objective navigates the examination of privacy and security challenges that are integrated into artificial intelligence-focused programming assistants. The prison confirmation findings indicate that challenges extend beyond technical flaws, encompassing regulatory concerns and human-centered risks. Developer experience is isolated in the documentation of the review study, which is directly linked to research focus validation and objective identification.

Recommendations

Based on research synthesis, recommendations guide security-by-design integration processes involving AI coding, with privacy-aware and security-oriented constraints aligned with regulations and recognized standards. The prospect of a mandatory human-in-the-loop review process should be recommended so that organizations can enhance structured code review processes, including an artificial intelligence-generated privacy-sensitive component.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Ahi, K., Agrawal, V., & Valizadeh, S. (2025). Dual-Use of Large Language Models (LLMs) and Generative AI (GenAI) in Cybersecurity: Risks, Defenses, and Governance Strategies. Authorea Preprints. https://www.techrxiv.org/doi/pdf/10.36227/techrxiv.175616948.85236631

[2] Ahmad, J., Mohammad, C. W., & Sadiq, M. (2022, January). Generation of One-Time Password for the Authentication of Software Requirements Using Secure Hash Algorithms. In Proceedings of International Conference on Recent Trends in Computing: ICRTC 2021 (pp. 627–640). Singapore: Springer Nature Singapore. https://www.researchgate.net/profile/Sherin-Zafar/publication/357862568_Applying_Predictive_Analysis_Methods_for_Detection_of_Driver_Drowsiness/links/64d5eda4b684851d3d9e27cf/Applying-Predictive-Analysis-Methods-for-Detection-of-Driver-Drowsiness.pdf#page=624

[3] Alagarsundaram, P. (2023). AI-powered data processing for advanced case investigation technology. Technology, 8(08).https://www.academia.edu/download/123218552/2024_04_WO_029.pdf

[4] Ali, M., Arunasalam, A., & Farrukh, H. (2025). May. Understanding Users' Security and Privacy Concerns and Attitudes Towards Conversational AI Platforms. In 2025 IEEE Symposium on Security and Privacy (SP) (pp. 298–316). IEEE.https://arxiv.org/pdf/2504.06552

[5] Anidjar, L., Packin, N.G., & Panezi, A. (2023). The matrix of privacy: data infrastructure in the AI-Powered Metaverse. Harv. L. & Pol'y Rev., 18, p.59.https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=4363208

[6] Arugula, B. (2024). AI-Powered Code Generation: Accelerating Digital Transformation in Large Enterprises. International Journal of AI, BigData, Computational and Management Studies, 5(2), pp.48–57.https://ijaibdcms.org/index.php/ijaibdcms/article/download/157/164

[7] Becker, B.A., Denny, P., Finnie-Ansley, J., Luxton-Reilly, A., Prather, J., & Santos, E.A. (2023). March. Programming is hard-or at least it used to be: Educational opportunities and challenges of AI code generation. In Proceedings of the 54th ACM Technical Symposium on Computer Science Education, Vol. 1 (pp. 500–506).https://dl.acm.org/doi/pdf/10.1145/3545945.3569759

[8] Ben Yaala, S. & Bouallegue, R. (2025). Vulnerability Detection in Large Language Models: Addressing Security Concerns. Journal of Cybersecurity and Privacy, [online] 5(3), p.71. https://www.mdpi.com/2624-800X/5/3/71

[9] Bird, C., Ford, D., Zimmermann, T., Forsgren, N., Kalliamvakou, E., Lowdermilk, T., and Gazit, I. (2022). Taking Flight with Copilot: Early insights and opportunities of AI-powered pair-programming tools. Queue, 20(6), pp.35-57.https://dl.acm.org/doi/pdf/10.1145/3582083

[10] Carter, W., Dawson, E., & Oladeji Olaniran (2025). AI-Assisted Code Generation: Enhancing Software Development Productivity with Large Language Models. [online] ResearchGate. Available at: https://www.researchgate.net/publication/395473168_AI-Assisted_Code_Generation_Enhancing_Software_Development_Productivity_with_Large_Language_Models

[11] Cevik, A.A., Abu-Zidan, F.M., & Cevik, A.A. (2025). Utilizing AI-powered thematic analysis: methodology, implementation, and lessons learned. Cureus, 17(6).https://www.cureus.com/articles/372677-utilizing-ai-powered-thematic-analysis-methodology-implementation-and-lessons-learned.pdf

[12] Cheng, R., Wang, R., Zimmermann, T., & Ford, D. (2024). "It would work for me too": How online communities shape software developers' trust in AI-powered code generation tools. ACM Transactions on Interactive Intelligent Systems, 14(2), pp.1–39.https://dl.acm.org/doi/pdf/10.1145/3651990

[13] Davila, N., Wiese, I., Steinmacher, I., Lucio da Silva, L., Kawamoto, A., Favaro, G.J.P., & Nunes, I. (2024). April. An industry case study on the adoption of AI-based programming assistants. In Proceedings of the 46th International Conference on Software Engineering: Software Engineering in Practice (pp. 92–102).https://dl.acm.org/doi/pdf/10.1145/3639477.3643648

[14] Fakeyede, O. G., Okeleke, P. A., Hassan, A., Iwuanyanwu, U., Adaramodu, O. R., & Oyewole, O. O. (2023). Navigating data privacy through IT audits: GDPR, CCPA, and beyond. International Journal of Research in Engineering and Science, 11(11), 45–58. https://www.researchgate.net/profile/Olajumoke-Oyewole/publication/384398894_Navigating_Data_Privacy_Through_IT_Audits_GDPR_CCPA_and_Beyond/links/66f6f344f599e0392fa903fc/Navigating-Data-Privacy-Through-IT-Audits-GDPR-CCPA-and-Beyond.pdf

[15] Farea, A.H., Alhazmi, O.H., Samet, R., & Guzel, M.S. (2024). AI-Powered Integrated With Encoding Mechanism Enhancing Privacy, Security, and Performance for IoT Ecosystem. IEEE Access.https://ieeexplore.ieee.org/iel8/6287639/6514899/10646204.pdf

[16] Graham, O., & Kloss, K. (2025). Evaluating the Impact of Reinforcement Learning on Autonomous CI/CD Workflow Optimization. https://www.preprints.org/frontend/manuscript/f30b85a7e439dcc7ef9ec5543ed882b0/download_pub

[17] Haque, M.A. (2025). LLMs: A game-changer for software engineers? BenchCouncil Transactions on Benchmarks Standards and Evaluations, [online] 5(1), pp.100204–100204. https://www.sciencedirect.com/science/article/pii/S2772485925000171

[18] Iqbal, F., Samsom, F., Kamoun, F., & MacDermott, Á. (2023). When ChatGPT goes rogue: exploring the potential cybersecurity threats of AI-powered conversational chatbots. Frontiers in Communications and Networks, 4, 1220243. https://www.frontiersin.org/journals/communications-and-networks/articles/10.3389/frcmn.2023.1220243/pdf

[19] James, A. & Castro, H. (2024). Data Privacy in AI-Powered Personal Assistants.https://www.researchgate.net/profile/Mengkorn-Pum-2/publication/391195561_Data_Privacy_in_AI-Powered_Personal_Assistants/links/680d05e4ded43315573b10d2/Data-Privacy-in-AI-Powered-Personal-Assistants.pdf

[20] John, B. (2025). A Comprehensive Study on Security Challenges and Solutions in AI-Driven Cloud Platforms.https://www.researchgate.net/profile/Beauden-John/publication/388285246_A_Comprehensive_Study_on_Security_Challenges_and_Solutions_in_AI-Driven_Cloud_Platforms/links/6791ee451ec9f9589f59e3f8/A-Comprehensive-Study-on-Security-Challenges-and-Solutions-in-AI-Driven-Cloud-Platforms.pdf

[21] Klemmer, J.H., Horstmann, S.A., Patnaik, N., Ludden, C., Burton Jr, C., Powers, C., Massacci, F., Rahman, A., Votipka, D., Lipford, H.R., & Rashid, A. (2024). December. Using AI assistants in software development: A qualitative study on security practices and concerns. In Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (pp. 2726–2740).https://arxiv.org/pdf/2405.06371

[22] Kshetri, N. (2025). Transforming cybersecurity with agentic AI to combat emerging cyber threats. Telecommunications Policy, [online] 49(6), p.102976. https://www.sciencedirect.com/science/article/pii/S0308596125000734

[23] Lakis, H., & Rifai, A. R. (2025). The Adoption and Impact of AI-Powered Coding Tools Among Swedish Software Developers. https://www.diva-portal.org/smash/get/diva2:1970381/FULLTEXT01.pdf

[24] Madampe, K., Grundy, J., & Arachchilage, N. (2025). June. How Are We Doing With Using AI-Based Programming Assistants For Privacy-Related Code Generation? The Developers' Experience. In Proceedings of the 29th International Conference on Evaluation and Assessment in Software Engineering (pp. 684–689).https://dl.acm.org/doi/pdf/10.1145/3756681.3757035

[25] Madampe, K., Grundy, J., & Arachchilage, N. (2025). AI-based Programming Assistants for Privacy-related Code Generation: The Developers' Experience. arXiv preprint arXiv:2503.03988.https://arxiv.org/pdf/2503.03988

[26] Maham, A. (2024). Advanced Methodologies for Technological Implementation for Ethical Considerations in AI-Powered Healthcare Systems.https://www.theseus.fi/bitstream/handle/10024/863039/Maham_Akhlaq.pdf?sequence=2

[27] Menon, U.V., Kumaravelu, V.B., Kumar, C.V., Rammohan, A., Chinnadurai, S., Venkatesan, R., Hai, H., & Selvaprabhu, P. (2025). AI-powered IoT: A survey on integrating artificial intelligence with IoT for enhanced security, efficiency, and innovative applications. IEEE Access.https://ieeexplore.ieee.org/iel8/6287639/6514899/10929047.pdf

[28] Mushtaq, S. & Hameeda, Q.T.A. (2025). Empowering Public Health: AI-Powered Security Solutions for AI-Driven Challenges. Applied AI Letters, 6(2), p.e119.https://onlinelibrary.wiley.com/doi/pdf/10.1002/ail2.119

[29] Nagaty, K.A. (2023). IoT commercial and industrial applications and AI-powered IoT. In Frontiers of Quality Electronic Design (QED) AI, IoT and Hardware Security (pp. 465–500). Cham: Springer International Publishing.https://www.researchgate.net/profile/Khaled-Nagaty/publication/367025439_IoT_Commercial_and_Industrial_Applications_and_AI-Powered_IoT/links/63d61ee5c97bd76a8244aee8/IoT-Commercial-and-Industrial-Applications-and-AI-Powered-IoT.pdf

[30] Nama, P., (2023). AI-Powered Mobile Applications: Revolutionizing User Interaction Through Intelligent Features and Context-Aware Services. Journal of Emerging Technologies and Innovative Research, 10(01), pp.g611-g620.https://www.researchgate.net/profile/Prathyusha-Nama/publication/385207252_AI-Powered_Mobile_Applications_Revolutionizing_User_Interaction_Through_Intelligent_Features_and_Context-Aware_Services/links/671a62bcedbc012ea13d0a09/AI-Powered-Mobile-Applications-Revolutionizing-User-Interaction-Through-Intelligent-Features-and-Context-Aware-Services.pdf

[31] Noor, N. (2025). Generative AI-assisted software development teams: opportunities, challenges, and best practices. https://lutpub.lut.fi/bitstream/handle/10024/169746/mastersthesis_Nouman_Noor.pdf?sequence=1

[32] Obiokafor, I. N., Ajonuma, M. E., & Aguboshim, F. C. (2025). Integrating Privacy by Design (PbD) in the system development life cycle for enhanced data protection. World Journal of Advanced Research and Reviews, 26(01), 1233-1240. https://www.researchgate.net/profile/Obiokafor-Ifeyinwa/publication/391323032_Integrating_Privacy_by_Design_PbD_in_the_system_development_life_cycle_for_enhanced_data_protection/links/682c91e6026fee1034f951da/Integrating-Privacy-by-Design-PbD-in-the-system-development-life-cycle-for-enhanced-data-protection.pdf

[33] Oh, S., Lee, K., Park, S., Kim, D., & Kim, H. (2024, May). Poisoned chatbot finds work for idle hands: Exploring developers' coding practices with insecure suggestions from poisoned AI models. In 2024 IEEE Symposium on Security and Privacy (SP) (pp. 1141–1159). IEEE. https://arxiv.org/pdf/2312.06227

[34] Ozman, F.M. (2025). A systematic literature review on AI governance platforms: ensuring responsible AI deployment. World Journal of Advanced Engineering Technology and Sciences, [online] 16(2), pp.078–092. doi:https://doi.org/10.30574/wjaets.2025.16.2.1259.

[35] Ozman, F.M. (2025). Systematic literature review on the critical role of data integrity in AI-driven enterprises. World Journal of Advanced Engineering Technology and Sciences, [online] 15(2), pp.1664–1683. doi:https://doi.org/10.30574/wjaets.2025.15.2.0427.

[36] Pan, S., Wang, L., Zhang, T., Xing, Z., Zhao, Y., Lu, Q., & Sun, X. (2024). " I Do not Use AI for Everything": Exploring Utility, Attitude, and Responsibility of AI-empowered Tools in Software Development. arXiv preprint arXiv:2409.13343. https://arxiv.org/pdf/2409.13343

[37] Pantin, C. (2024). The Impact of AI-generated Code on the Future of Junior Developers. https://www.theseus.fi/bitstream/handle/10024/866717/Pantin_Carlos.pdf?sequence=2

[38] Perry, N., Srivastava, M., Kumar, D., & Boneh, D. (2023, November). Do users write more insecure code with AI assistants? In Proceedings of the 2023 ACM SIGSAC conference on computer and communications security (pp. 2785–2799). https://dl.acm.org/doi/pdf/10.1145/3576915.3623157

[39] Pinto, G., De Souza, C., Rocha, T., Steinmacher, I., Souza, A., & Monteiro, E. (2024). April. Developer experiences with a contextualized AI coding assistant: usability, expectations, and outcomes. In Proceedings of the IEEE/ACM 3rd International Conference on AI Engineering-Software Engineering for AI (pp. 81–91).https://dl.acm.org/doi/pdf/10.1145/3644815.3644949

[40] Rajapaksha, S., Senanayake, J., Kalutarage, H., & Al-Kadri, M. O. (2022, December). Ai-powered vulnerability detection for secure source code development. In the International Conference on Information Technology and Communications Security (pp. 275–288). Cham: Springer Nature Switzerland. https://rgu-repository.worktribe.com/OutputFile/2001750

[41] Samola, M. (2024). Enhancing Threat Mitigation in Critical Infrastructure with AI-Powered Cybersecurity Solutions. https://www.researchgate.net/profile/Martins-Amola/publication/390056861_Enhancing_Threat_Mitigation_in_Critical_Infrastructure_with_AI-Powered_Cybersecurity_Solutions/links/67dd7ce23ad6d174c4a453ab/Enhancing-Threat-Mitigation-in-Critical-Infrastructure-with-AI-Powered-Cybersecurity-Solutions.pdf

[42] Sanne, S. H. (2024). Investigations into Security Testing Techniques, Tools, and Methodologies for Identifying and Mitigating Security Vulnerabilities. Journal of Artificial Intelligence, Machine Learning and Data Science, 1(1), 626–631. https://urfjournals.org/open-access/investigations-into-security-testing-techniques-tools-and-methodologies-for-identifying-and-mitigating-security-vulnerabilities.pdf

[43] Sergeyuk, A., Golubev, Y., Bryksin, T., & Ahmed, I. (2025). Using AI-based coding assistants in practice: State of affairs, perceptions, and ways forward. Information and Software Technology, 178, 107610. https://arxiv.org/pdf/2406.07765?

[44] Sherje, N. (2024). Enhancing software development efficiency through AI-powered code generation. Research Journal of Computer Systems and Engineering, 5(1), pp.01–12.https://technicaljournals.org/RJCSE/index.php/journal/article/download/90/86

[45] Stangl, A., Shiroma, K., Davis, N., Xie, B., Fleischmann, K.R., Findlater, L., & Gurari, D. (2022). Privacy concerns for visual assistance technologies. ACM Transactions on Accessible Computing (TACCESS), 15(2), pp.1–43.https://dl.acm.org/doi/pdf/10.1145/3517384

[46] Thaw, T. T. T. (2025). How Effective are AI-powered Code Assistants in Enhancing Developer Productivity?. https://www.theseus.fi/bitstream/handle/10024/895238/Thaw_ThinThuThu.pdf?sequence=2

[47] Thomas, A. (2024). Digitally transforming the organization through knowledge management: A socio-technical system (STS) perspective. European Journal of Innovation Management, 27(9), 437–460. https://www.emerald.com/insight/content/doi/10.1108/EJIM-02-2024-0114/full/pdf

[48] Torka, S. and Albayrak, S., (2024). Optimizing AI-Assisted Code Generation. arXiv preprint arXiv:2412.10953.https://arxiv.org/pdf/2412.10953?

[49] Vulchi, J. R., & Ackerman, E. (2024). Exploring the OWASP Top 10 security risks in LLMs with practical testing and prevention. https://www.researchgate.net/profile/Jaswanth-Vulchi/publication/387271453_Exploring_OWASP_Top_10_Security_Risks_in_LLMs/links/6765ffeb00aa3770e0af498f/Exploring-OWASP-Top-10-Security-Risks-in-LLMs.pdf

[50] Wang, R., Cheng, R., Ford, D., & Zimmermann, T. (2024). June. Investigating and designing for trust in AI-powered code generation tools. In Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency (pp. 1475–1493).https://dl.acm.org/doi/pdf/10.1145/3630106.3658984

[51] Weisz, J. D., Kumar, S. V., Muller, M., Browne, K. E., Goldberg, A., Heintze, K. E., & Bajpai, S. (2025, April). Examining the use and impact of an AI code assistant on developer productivity and experience in the enterprise. In Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (pp. 1–13). https://dl.acm.org/doi/pdf/10.1145/3706599.3706670

[52] Yusuff, M. (2023, May). Ensuring Compliance with GDPR, CCPA, and Other Data Protection Regulations: Challenges and Best Practices. https://www.researchgate.net/profile/Mariam-Yusuff-6/publication/387224965_Ensuring_Compliance_with_GDPR_CCPA_and_Other_Data_Protection_Regulations_Challenges_and_Best_Practices/links/6764be39fb9aff6eaae270f8/Ensuring-Compliance-with-GDPR-CCPA-and-Other-Data-Protection-Regulations-Challenges-and-Best-Practices.pdf

Appendices

Appendix 1: Summary Table

Authors (Year)	Theme	Key Findings	Methodology	Implications
Ahi et al. (2025)	Dual-use AI	LLMs pose both defensive and offensive cybersecurity risks	Conceptual review	Need for AI governance
Ahmad et al. (2022)	Authentication security	OTP with hashing improves requirement security	Experimental	Secure SDLC practices
Alagarsundaram (2023)	AI data processing	AI accelerates investigations but raises privacy risks	Conceptual	Strong access control
Ali et al. (2025)	User trust & privacy	Users fear misuse of conversational AI data	Survey	Transparency essential
Anidjar et al. (2023)	Data infrastructure	AI ecosystems intensify privacy complexity	Legal analysis	Regulatory reform
Arugula (2024)	Enterprise AI coding	AI boosts productivity but increases exposure	Case analysis	Risk-aware adoption
Becker et al. (2023)	Education & AI	AI lowers coding barriers but weakens fundamentals	Empirical	Training redesign
Ben Yaala & Bouallegue (2025)	LLM vulnerabilities	LLMs introduce novel attack surfaces	Technical analysis	Secure model testing
Bird et al. (2022)	Copilot adoption	AI pair-programming reshapes workflows	Industry study	Policy updates needed
Carter et al. (2025)	Productivity	LLMs enhance speed but risk quality	Review	Human oversight required
Cevik et al. (2025)	AI thematic analysis	AI aids analysis but risks bias	Methodological	Validation needed
Cheng et al. (2024)	Trust formation	Community discourse shapes AI trust	Qualitative	Social factors matter
Davila et al. (2024)	Industry adoption	AI improves efficiency yet raises security doubts	Case study	Gradual deployment
Fakeyede et al. (2023)	Data privacy audits	GDPR/CCPA audits reduce exposure	Review	Compliance frameworks
Farea et al. (2024)	Privacy mechanisms	Encoding improves AI security	Experimental	Secure architectures
Graham & Kloss (2025)	CI/CD automation	AI optimises pipelines with governance	Experimental	Controlled autonomy
Haque (2025)	Developer role	LLMs redefine engineering skills	Review	Skill adaptation
Iqbal et al. (2023)	Cyber threats	Chatbots can be weaponised	Threat analysis	Defensive controls
James & Castro (2024)	Personal assistants	AI assistants collect excessive data	Review	Data minimisation
John (2025)	Cloud AI security	AI clouds amplify attack vectors	Review	Zero-trust needed
Klemmer et al. (2024)	Developer security	Developers worry about insecure AI code	Qualitative	Training required

Kshetri (2025)	Agentic AI	Autonomous AI reshapes cyber defence	Policy analysis	Accountability gaps
Lakis & Rifai (2025)	Developer perception	Productivity gains outweigh risks (perceived)	Survey	Risk awareness needed
Madampe et al. (2025a)	Privacy code	AI struggles with privacy-related code	Empirical	Human validation
Madampe et al. (2025b)	Privacy experience	Developers distrust AI privacy outputs	Survey	PbD integration
Maham (2024)	AI ethics	Ethical gaps in AI systems	Conceptual	Ethical frameworks
Menon et al. (2025)	AI-IoT security	AI improves IoT security but increases risk	Survey	Secure integration
Mushtaq & Hameeda (2025)	Public AI security	AI security vital for public sectors	Review	Policy enforcement
Nagaty (2023)	Industrial AI	AI-IoT expands threat surface	Review	Sector regulations
Nama (2023)	Mobile AI apps	Context-aware AI raises privacy risks	Conceptual	User consent
Noor (2025)	Team practices	Best practices mitigate AI risks	Thesis	Governance models
Obiokafor et al. (2025)	Privacy by Design	PbD strengthens SDLC protection	Framework	Proactive privacy
Oh et al. (2024)	Poisoned models	AI can inject insecure code	Experimental	Model vetting
Pan et al. (2024)	Responsible use	Developers limit AI use for safety	Survey	Selective adoption
Pantin (2024)	Junior developers	Juniors overtrust AI	Qualitative	Skill safeguards
Perry et al. (2023)	Insecure code	AI increases insecure outputs	Controlled experiment	Code review essential
Pinto et al. (2024)	Usability	Contextual AI improves UX but hides risk	Case study	Transparency needed
Rajapaksha et al. (2022)	Vulnerability detection	AI detects vulnerabilities effectively	Experimental	Secure AI use
Samola (2024)	Cyber defence	AI enhances threat mitigation	Review	Integrated security
Sanne (2024)	Security testing	Traditional testing insufficient for AI	Review	AI-specific testing
Sergeyuk et al. (2025)	Practical use	Developers uncertain about data reuse	Survey	Policy clarity
Sherje (2024)	Efficiency	AI speeds development	Review	Risk trade-offs
Stangl et al. (2022)	Privacy concerns	Assistive AI raises privacy anxiety	Empirical	User control
Thaw (2025)	Productivity	AI boosts output unevenly	Empirical	Context matters
Thomas (2024)	STS theory	Tech & social factors jointly shape risk	Theoretical	Holistic analysis
Torka & Albayrak (2024)	Optimisation	Optimised AI improves reliability	Technical	Controlled tuning

Vulchi & Ackerman (2024)	OWASP LLM risks	LLM-specific vulnerabilities identified	Testing	Secure design
Wang et al. (2024)	Trust & fairness	Trust linked to transparency	Design study	Explainable AI
Weisz et al. (2025)	Enterprise privacy	Proprietary code exposure risk	Field study	On-prem solutions
Yusuff (2023)	Regulation	Compliance remains challenging	Review	Governance alignment

Appendix 2 Thematic Table

Theme 1 Privacy Risks in AI-Generated Code

Author(s) & Year	Focus Area	Key Findings	Relevance to Theme
Madampe et al. (2025)	Privacy-related code generation	AI assistants frequently generate code with weak data protection, improper storage, and missing consent controls	Core empirical evidence of privacy risks in AI-generated code
Madampe et al. (2025, EASE)	Developer experience study	Developers struggle to identify privacy flaws in AI-generated code without explicit guidance	Shows human–AI interaction amplifies privacy risk
James & Castro (2024)	Data privacy in AI assistants	AI systems may unintentionally reproduce non-compliant data handling practices	Highlights systemic privacy risks from AI training data
Farea et al. (2024)	AI with encoding mechanisms (IoT)	Security and privacy can be enhanced, but default AI outputs remain vulnerable	Demonstrates need for additional safeguards
Menon et al. (2025)	AI-powered IoT survey	Privacy leakage risks increase when AI-generated code is deployed at scale	Shows cascading privacy impact in interconnected systems
Nama (2023)	AI-powered mobile applications	Context-aware AI features raise risks of personal data misuse	Extends privacy concerns to mobile ecosystems

Theme 2 Developer Trust, Over-Reliance, and Behavioural Risk

Author(s) & Year	Focus Area	Key Findings	Relevance to Theme
Wang et al. (2024)	Trust in AI code tools	Developers trust AI suggestions more when tools appear transparent and confident	Explains over-reliance on AI-generated code
Cheng et al. (2024)	Social influence on trust	Online communities reinforce trust even when risks are known	Demonstrates social amplification of misplaced trust
Klemmer et al. (2024)	Security practices study	Developers skip security checks due to confidence in AI output	Shows behavioural reduction in security vigilance

Bird et al. (2022)	Copilot adoption	Early productivity gains mask long-term security risks	Illustrates automation complacency
Davila et al. (2024)	Industry adoption case study	Enterprises adopt AI tools faster than governance controls	Highlights organisational-level trust risks
Pinto et al. (2024)	Contextualised AI assistant usability	Developers assume AI understands security context	Reinforces false assumptions about AI competence

Theme 3 Lack of Contextual Security and Privacy Awareness

Author(s) & Year	Focus Area	Key Findings	Relevance to Theme
Sherje (2024)	AI code generation efficiency	AI improves speed but lacks security reasoning	Shows functional–security trade-off
Torka & Albayrak (2024)	Optimisation of AI-assisted code	Optimisation does not guarantee secure logic	Confirms absence of threat modelling
Klemmer et al. (2024)	Developer interviews	AI tools do not warn about policy or compliance violations	Demonstrates missing contextual safeguards
Becker et al. (2023)	AI in programming education	Students may internalise insecure AI-generated patterns	Highlights long-term security debt risk
Arugula (2024)	Enterprise digital transformation	Security concerns lag behind deployment speed	Shows organisational blind spots
Alagarsundaram (2023)	AI-powered investigations	Contextual misuse can compromise sensitive systems	Extends risk to investigative domains

Theme 4: Ethical, Legal, and Governance Challenges

Author(s) & Year	Focus Area	Key Findings	Relevance to Theme
Anidjar et al. (2023)	Privacy infrastructure & law	AI operates within opaque data pipelines with unclear accountability	Frames privacy risk as governance issue
Maham (2024)	Ethical AI in healthcare	Weak governance leads to privacy and ethical failures	Sector-specific ethical risk
Mushtaq & Hameeda (2025)	AI security in public systems	Security and privacy require policy-driven oversight	Highlights regulatory necessity
Ali et al. (2025)	User attitudes to conversational AI	Users fear surveillance and data misuse	Shows trust erosion from poor governance
John (2025)	AI-driven cloud security	Governance gaps expose platforms to breaches	Links AI coding to cloud security risks
Stangl et al. (2022)	Privacy in assistive technologies	Lack of transparency intensifies privacy concerns	Reinforces need for explainability