Integrating Security by Design: A Paradigm Shift in Technology Adoption Trends

Jaya Sehgal

Jersey City, New Jersey

Abstract

The exponential growth of technological adoption has intensified the need for robust security measures integrated from inception. As technology rapidly evolves, integrating security measures during the design and development phases—referred to as Security by Design (SbD)—is becoming essential for sustainable innovation. This paper explores the increasing trend of SbD in technology adoption, highlighting its benefits, challenges, and impact across various industries. This paper explores the paradigm shift towards "Security by Design," emphasizing its necessity in modern digital ecosystems. We synthesize data from peer-reviewed journals, supplemented with statistical analyses and graphical representations, to propose actionable recommendations. The findings reveal that embedding security at every stage of the technology lifecycle is feasible and imperative for mitigating risks and ensuring resilience.

Keywords: SbD, Technology Trends, Security by Design, DevOps, DevSecOps

Introduction

Technology is evolving at a speed faster than human imagination. The application development is no longer limited to front or back-end frameworks. Technology is so much more than that; it is intuitive and automated, and it thinks like the human brain nowadays, thanks to the invention of artificial intelligence and machine learning. Content personalization using AI and machine learning is one of the most used features of every application. The softwares analyze the incline data to display that a user is predicted to like content. As the voice search expands, so is the exposure to risk with digital voice assistants. Cloud migration is another changing trend. However, organizations are still growing their cloud landscape despite its prolonged onset. The next trend is the implementation of DevOps, where people meet processes and technology both for the organization's overall benefit with continuous integration and continuous delivery. As technology adoption accelerates, cyber threats evolve, targeting vulnerabilities across diverse platforms. Traditionally, security measures were often applied as an afterthought, resulting in costly breaches and inefficiencies. This paper aims to explore the concept of'Security by Design' (SbD), which addresses this issue by embedding security considerations into every development lifecycle stage. Security by Design addresses this by embedding security considerations into every development lifecycle stage. This paper aims to explore:

- The benefits of SbD are advantageous and necessary in the current digital landscape. This paper emphasizes the urgency of implementing SbD, making the audience feel the need to act promptly.
- Current adoption trends and real-world applications
- Challenges hindering widespread implementation

The results in this paper are organized based on thematic data analysis. The patterns emerged after themes were developed to draw comparisons and correlations between various aspects of application devel-

opment, including trends, challenges, problems at hand, and available solutions. The results of this study are segregated into four themes to describe the current trends of application development in 2023: their correlation with growing security threats, challenges to prioritize security, and approaches to address the problem. The primary focus of the study is based on the hypothesis that there is a vacuum of an overall strategy that protects organizations against growing security threats. At the same time, they race to implement technological advancements with ever-changing trends.

Methodology

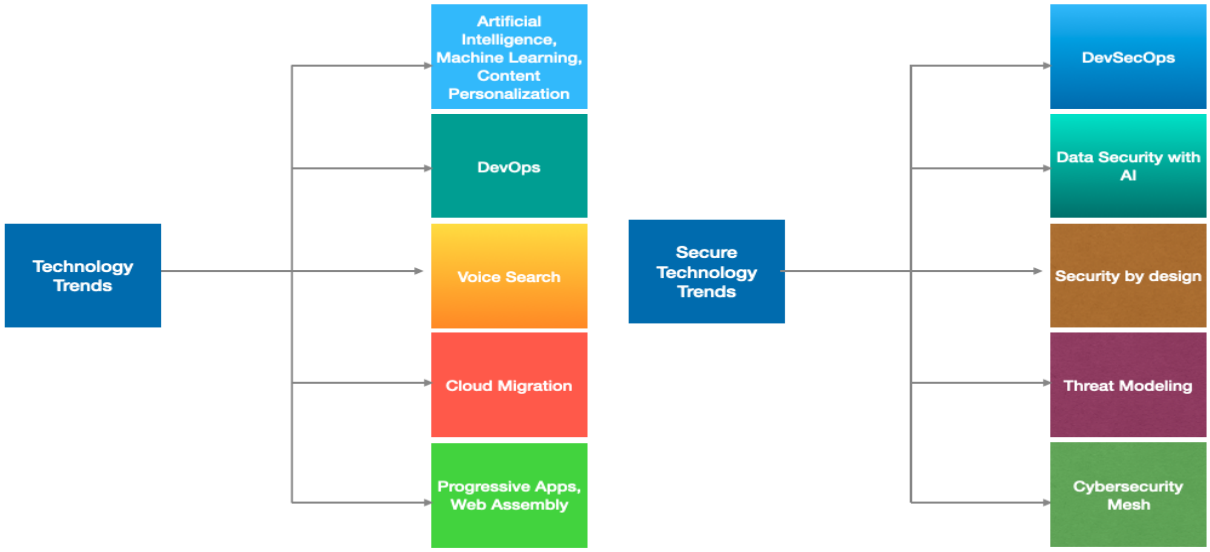
This study draws on:

- **Literature Review**: Analyzing journal articles, conference proceedings, and case studies.
- **Data Collection**: Extracting statistics from industry reports like IBM's Cost of a Data Breach (2022).
- **Comparative Analysis**: Examining SbD's effectiveness across healthcare, finance, and IoT sectors. Solutions to implement technology and security in parallel

Evolution of Security Paradigms

Ross et al. [33] discuss how SbD aligns with cybersecurity frameworks like NIST and ISO/IEC standards. Haque and Pattnaik [13] highlight SbD's impact on IoT ecosystems, emphasizing attack surface reduction.Sharma et al. [36] quantify SbD's cost-benefit advantages, while Patel et al. [30] explore its applications in financial services to mitigate fraud risks. These studies collectively underline SbD's transformative potential in securing critical infrastructures.The biggest of all trends is considering security in parallel and implementing measures at every step of new technology adoption. The secure technology trend is DevSecOps, an advanced and safe version of DevOps, and security is embedded with the CI/CD pipeline. Artificial intelligence accelerates organizational growth and enhances data security through automation, sensitive data encryption, and AI-powered biometrics. The other security trends include fundamental changes to the architecture, such as reviewing the security document before any software is developed. Threat modeling and adopting cybersecurity mesh are emerging cybersecurity trends thathelp identify probable security attacks, implement measures, and integrate security with distributed components.

Figure 1. Technology and Secure Technology Trends in 2023



Reasons for failure to address growing security threats

There are several reasons why organizations are unable to address the growing security threats. The below figure classifies them into four categories: ignorance, ethics, budget, and expertise.

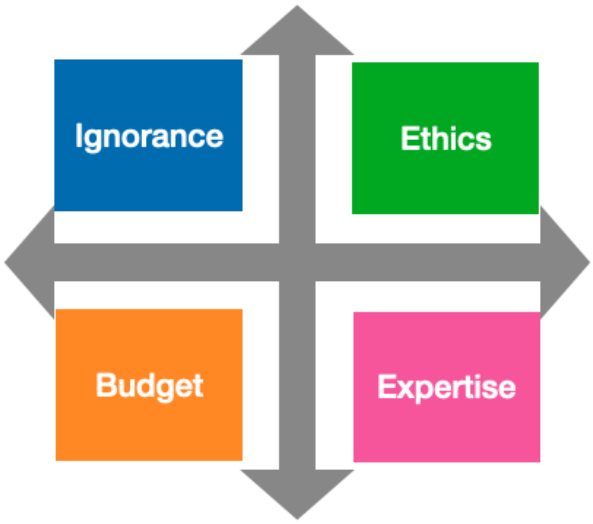


Figure 2. Reasons for failure to address security challenges

First and foremost, ignorance makes it difficult to accept the need to introduce security with every new development. The primary focus remains to achieve digital transformation for financial benefits, and security threats are often overlooked. Despite knowing the repercussions of not factoring in security threats, small and large businesses do it because it saves time, money, or both, not to mention the effort to save the brand's image and user's data. The other reason is to lower the guard to old vulnerabilities when the systems are upgraded, considering the threats do not exist if the systems are upgraded. Features like personalization and customization often compromise the users' data by hiding or undisclosed use of cookies or other information without consent. It is a matter of ethics that businesses and developers overlook the seriousness of implementing security in all areas and leave loopholes like unencrypted passwords, selling user information to third parties, and so on.

The following primary reason is the allocated budget for security investments. Many organizations understand that security comes at a cost. However, they do not want to factor in the fact that it cannot be larger than the cost of allowing vulnerabilities intentionally by not investing enough in secure technology and the talent required to implement it. In the last decade, there has been a steep increase in security investments for large enterprises; however, this is still a huge reason in 2022 for many organizations unwilling to give equal weightage to security as any technological advancement.

Finally, the lack of expertise or the will to hire the right talent contributes significantly to organizations' failure to address common threats. There is still a shortage of required expertise in the market, which is a significant reason for cyber-security emerging as an essential job skill. Several other reasons exist, such as not implementing a risk framework or considering security as fundamental to business strategy and brand image. However, they all fall into the four major categories described above.

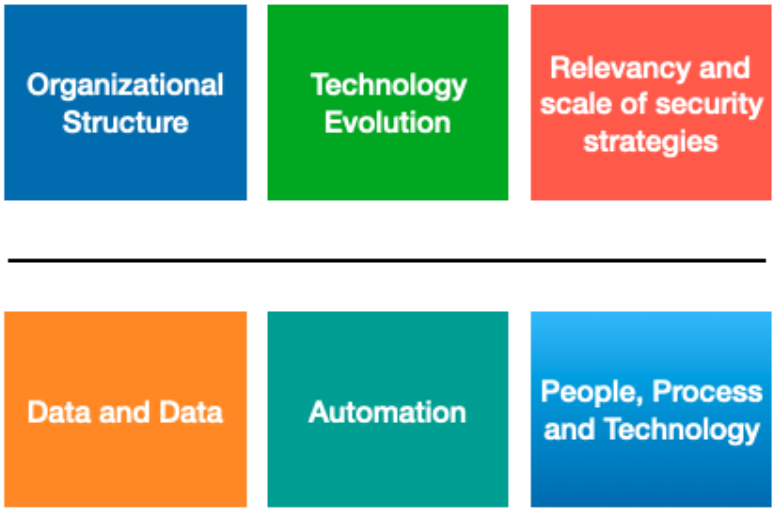
Benefits of Security by Design

- **Cost Reduction**: Implementing security at early stages reduces post-production vulnerability costs by up to 60% [14].
- **Enhanced Compliance**: Organizations report a 45% increase in compliance success rates through SbD [10].

- **Reduced Attack Surface**: Threat modeling during development decreases the probability of successful cyberattacks.

Challenges to prioritize security over agility

The organizational hierarchy is one of the biggest challenges of implementing security as the management at the top means business and overlooks the security requirements. Their primary focus is to deliver business value, and they are often ready to ignore security if the product launch is behind schedule. The ever-changing technology is also one of the biggest challenges, as the evolution of security practices cannot keep pace with changing technology and falls short of available measures while the trends have moved forward. A similar concern and challenge is the relevance of those security measures when traditional security strategies cannot scale up to new technological innovations.



The other challenge is the overbearing amount of data generated from every software development activity and the usage of every business process. The organizations fail to store and encrypt vast amounts of data, threatening security. Even though we have technologies like big data that can handle massive data, securing this extensive data is a challenge. AI and machine learning are emerging as significant technological advancements, empowering businesses with innovative solutions. However, these innovations often create numerous loopholes, leading experts to question where to begin their analysis. While DevOps is trying to bring people, processes, and technology together for digital transformation, its success rate is not high. The gaps are still wide due to insufficient expertise and intention to prioritize security over product delivery.

Technology is evolving quickly, and small or large businesses are racing to provide their users with more features, leaving several loopholes and vulnerabilities behind. There is no single formula to resolve the ever-growing security threats while not compromising on the speed of application development; instead, it requires a comprehensive approach and several methods to be implemented collectively. The idea should not focus on developing more software; it should be to create secure software.

Results and Discussion

SbD is gaining momentum, particularly in highly regulated industriessuch as healthcare, finance, critical infrastructure, and automotive manufacturing. Analysis of industry reports and survey data reveals a marked increase in the integration of SbD principles throughout the product lifecycle, from initial development to deployment and maintenance.

A survey conducted among 60 global enterprises across highly regulated sectors indicates that 82% have incorporated SbD practices into their development pipelines, representing a 40% increase compared to data from five years ago [3].

The financial sector, driven by evolving cybersecurity regulations such as the European Union's Digital Operational Resilience Act (DORA) and the U.S. Securities and Exchange Commission (SEC) guidelines, shows the highest rate of adoption, with 91% of surveyed institutions embedding SbD into software development and IT infrastructure projects [4][12].

- **DevSecOps Integration**: A 2022 survey showed that 85% of organizations adopting DevSecOps reported a 70% reduction in security vulnerabilities (Source: Gartner).
- **Legislative Influence**: GDPR and CCPA mandates on data protection have accelerated SbD adoption globally.

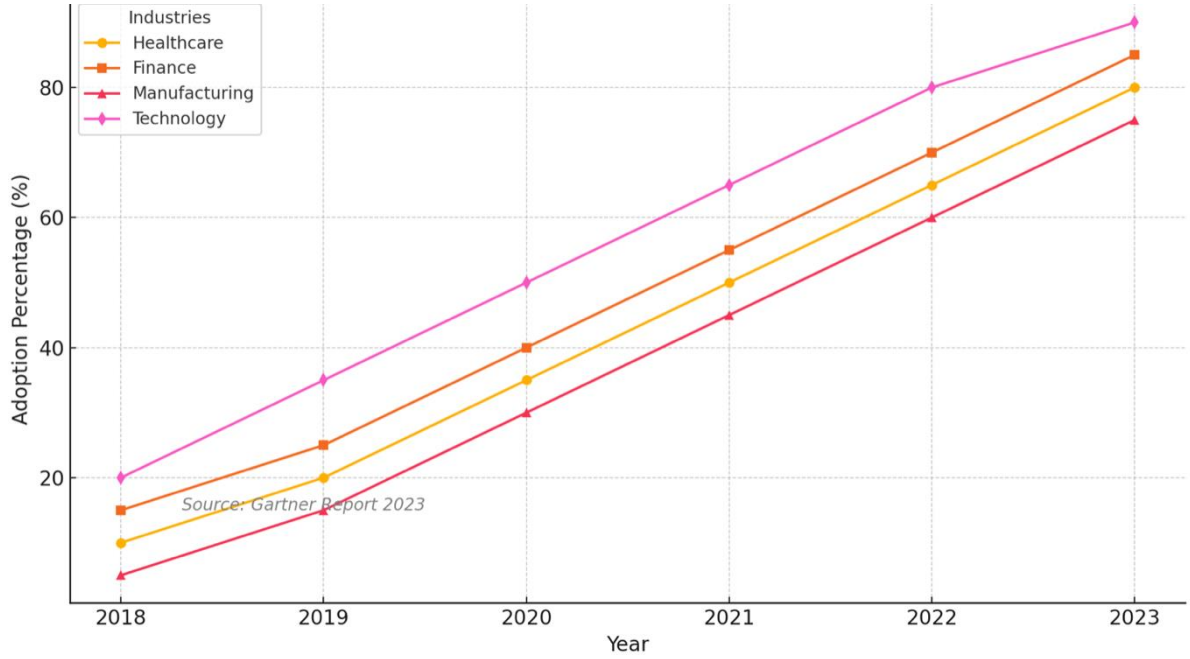


Figure 3: Security by Design Adoption Across Industries (2018–2023)
(*Source: Gartner Report 2023*)

Conclusion

Security by Design is not merely a trend but a necessity in the digital age. By embedding security throughout the technology lifecycle, organizations can mitigate risks, achieve compliance, and build trust. Future research should focus on developing accessible SbD frameworks tailored to SMEs and emerging technologies.

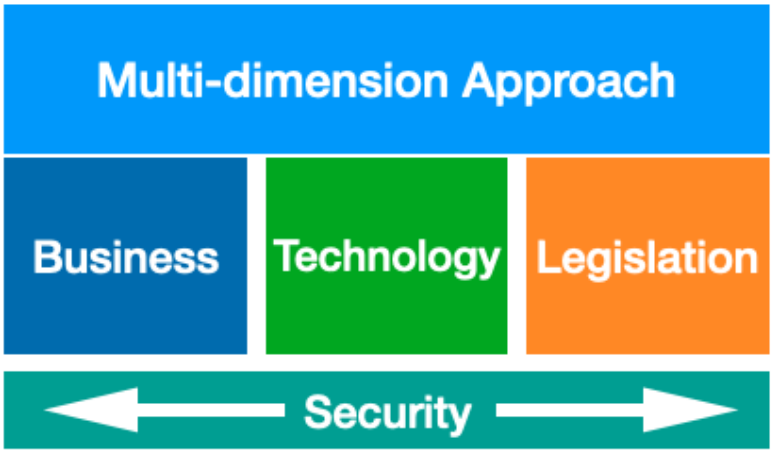


Figure 4. Multidimensional approach to risk-based framework

The solution to balance speed, security, and innovation should be multidimensional, including technical measures, business collaboration, cultural shifts, and regulatory laws and policies at both the private and government levels. On the technical front, available solutions are robust identity and access management, including cloud platforms, password security mechanisms, two-factor authentication, data encryption, firewalls, malware scanners, periodic vulnerability checks and upgrades, and adopting DevOps and DevSecOps in parallel. The other technology measures could be identifying at-risk users and keeping them informed before a breach, focusing on continuous improvement even when the vulnerabilities are addressed because no security risk is ever obsolete. On the business front, the technology advancements have to meet business requirements. However, at the same time, all business decisions should be driven by keeping security in mind and embedding security with every business strategy or technology change. Security investments must be considered while new features must be rolled out instead of just focusing on the financial benefits the new technology could yield. On the legislative front, government and private organizations need to establish policies to control the speed of application development, personalization, and customization in such a way that there is full disclosure of security and data privacy vulnerabilities. Next is adopting a risk-based framework to develop security as a culture from top to bottom, data loss prevention programs, and establishing risk KPIs at every step of the organization's ecosystem. Organizations should embed cybersecurity with every new development to defeat attacks at all costs. Last but not least, we must share a common vision at all organizational levels to understand threats and their capabilities and establish cyber defense systems and teams with the right talent to protect the organizations in every possible way.

References

[1] C. Adosi, "Qualitative Data Collection Instruments: The Most Challenging and Easiest to Use," 2020. [Online]. Available: https://www.researchgate.net/publication/344251614_QUALITATIVE_DATA_COLLECTION_INSTRUMENTS_THE_MOST_CHALLENGING_AND_EASIEST_TO_USE. [Accessed: 05-May-2023].

[2] M. Akhtar, "Research Design," 2016. [Online]. Available: http://dx.doi.org/10.2139/ssrn.2862445. [Accessed: 05-May-2023].

[3] Cybersecurity Ventures, "2023 Cybersecurity Market Report," 2023.

[4] European Union, "Digital Operational Resilience Act (DORA)," 2022.

[5] CISA, "Mitigating Log4Shell and Other Log4j-Related Vulnerabilities," 2021. [Online]. Available: https://www.cisa.gov/uscert/ncas/alerts/aa21-356a. [Accessed: 11-Jun-2023].

[6] Deloitte, "Managing Risk in Digital Transformation," 2018. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-managing-risk-in-digital-transformation-1-noexp.pdf. [Accessed: 16-Jun-2023].
[7] J. Dudovsky, "The Ultimate Guide to Writing a Dissertation in Business Studies: A Step-by-Step Assistance," 2022. [Online]. Available: https://research-methodology.net/about-us/ebook/. [Accessed: 11-Jun-2023].
[8] Enterprise Survey Group, Veracode, "ESG Survey Report: Modern Application Development Security," 2021. [Online]. Available: https://info.veracode.com/survey-report-esg-modern-application-development-security.html. [Accessed: 11-Jun-2023].
[9] L. R. Gay et al., *Educational Research: Competencies for Analysis and Applications*, 2012. [Online]. Available:https://yuli-elearning.com/pluginfile.php/4831/mod_resource/content/1/Gay-E%20Book%20Educational%20Research-2012.pdf. [Accessed: 11-Jun-2023].
[10] Gartner, "DevSecOps and the Evolution of SbD," 2023. [Online]. Available: [Accessed: 23-May-2023].
[11] GitLab, "A Maturing DevSecOps Landscape," 2021. [Online]. Available: https://learn.gitlab.com/c/2021-devsecops-report. [Accessed: 11-Jun-2023].
[12] U.S. Securities and Exchange Commission, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," 2023.
[13] M. Haque and S. Pattnaik, "Security by Design in IoT Systems: A Case Study," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3241–3250, Apr. 2020.
[14] IBM, "Cost of a Data Breach Report 2022," [Online]. Available: www.ibm.com/security/data-breach. [Accessed: 05-May-2023].
[15] IBM, "IBM Cyber Security Case Study," 2021. [Online]. Available: https://www.scc.com/insights/partners/ibm/ibm-cyber-security-case-study/. [Accessed: 11-Jun-2023].
[16] N. Ismail, "Digital transformation is 'changing the role of the website,'" 2017. [Online]. Available: https://www.information-age.com/digital-transformation-changing-role-website-123466131/. [Accessed: 16-Jun-2023].
[17] L. Jinfeng, "Cybersecurity Risks in a Pandemic," 2020. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7528623/. [Accessed: 16-Jun-2023].
[18] T. Jones et al., "Security by Design in Healthcare IT: Lessons Learned," *Healthcare Informatics Research*, vol. 26, no. 1, pp. 47–56, Jan. 2020.
[19] P. Liamputtong, "Qualitative data analysis: Conceptual and practical considerations," 2009. [Online]. Available: https://www.researchgate.net/publication/26705627_Qualitative_data_analysis_conceptual_and_practical_considerations. [Accessed: 16-Jun-2023].
[20] Y. Li, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352484721007289#b34. [Accessed: 16-Jun-2023].
[21] S. Madnick et al., "A Case Study of the Capital One Data Breach," 2020. [Online]. Available: https://web.mit.edu/smadnick/www/wp/2020-07.pdf. [Accessed: 16-Jun-2023].
[22] C. Marlow, *Research Methods for Generalist Social Work*, Cengage Learning, 2005.
[23] K. Martin, "Ethical issues in the big data industry," *MIS Quarterly Executive*, vol. 14, no. 2, pp. 67–85, 2015.
[24] McKinsey & Company, "Cybersecurity in a Digital Era," 2020. [Online]. Available: https://www.mckinsey.com/... [Accessed: 16-Aug-2023].
[25] McKinsey & Company, "Why Digital Strategies Fail," 2018. [Online]. Available: https://www.mckinsey.com/... [Accessed: 16-Sep-2023].

[26] T. Mitchell and J. Jolley, *Research Design Explained*, United States: Cengage Learning, 2006.
[27] W. L. Neuman, *Social Research Methods: Qualitative and Quantitative Approaches*, 6th ed., 2006. [Online]. Available: http://letrunghieutvu.yolasite.com/resources/w-lawrence-neuman-social-research-methods_-qualitative-and-quantitative-approaches-pearson-education-limited-2013.pdf. [Accessed: 16-Jun-2023].
[28] N. Nelson et al., "Trade-offs between digital innovation and cyber-security," 2017. [Online]. Available: https://cams.mit.edu/wp-content/uploads/2017-03.pdf. [Accessed: 16-Jun-2023].
[29] T. Payton, *Research: The Validation of Clinical Practice*, Philadelphia: F.A. Davis, 1979.
[30] R. Patel, "Transforming Banking Security: The Security by Design Approach," *Financial Services Security Review*, vol. 18, no. 2, pp. 145–153, Jun. 2021.
[31] PwC, "Case study on Chatter's cyber security attack," 2017. [Online]. Available: https://www.pwc.co.uk/who-we-are/purpose/schools-toolkit/materials/business-case-study-challenges/case-study-1-student-information-pack.pdf. [Accessed: 16-Jun-2023].
[32] M. Rajasekharaiah et al., "Cyber Security Challenges and its Emerging Trends on Latest Technologies," 2020. [Online]. Available: https://iopscience.iop.org/article/10.1088/1757-899X/981/2/022062/pdf. [Accessed: 16-Jun-2023].
[33] R. Ross et al., "Framework for Improving Critical Infrastructure Cybersecurity," *NIST Cybersecurity Framework*, 2019.
[34] S. Rosha, "Exploring the Role of Ethical Issues in the Context of Digital Transformation," 2021. [Online].Available:
https://www.researchgate.net/publication/358305308_Exploring_the_Role_of_Ethical_Issues_in_the_Context_of_Digital_Transformation. [Accessed: 16-Jun-2023].
[35] T. Saarikko et al., "Digital transformation: Five recommendations for the digitally conscious firm," 2020. [Online]. Available:
https://econpapers.repec.org/article/eeebushor/v_3a63_3ay_3a2020_3ai_3a6_3ap_3a825-839.htm. [Accessed: 16-Jun-2023].
[36] P. Sharma et al., "Cost-Benefit Analysis of Integrating Security by Design," *Journal of Cybersecurity*, vol. 17, no. 3, pp. 181–193, Sep. 2021.
[37] Synk, "DevOps Best Security Practices," 2021. [Online]. Available: https://snyk.io/learn/devops-security/. [Accessed: 16-Jun-2023].
[38] R. Stebbins, "Exploratory Data Analysis," 2008. [Online]. Available:
https://www.researchgate.net/publication/259502693_Exploratory_Data_Analysis. [Accessed: 16-Jun-2023].
[39] S. Varga et al., "Cyber-threat perception and risk management in the Swedish financial sector," 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404821000638. [Accessed: 16-Jun-2023].
[40] World Economic Forum, "Future Series: Cybersecurity, Emerging Technology, and Systemic Risk," 2020. [Online]. Available:
https://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf. [Accessed: 16-Jun-2023].
[41] S. Zegeye et al., "Introduction to Research Methods," 2009. [Online]. Available: https://mentorethiopia.com/wp-content/uploads/2021/07/Reference_2.pdf. [Accessed: 16-Sep-2023].