Sarcouncil Journal of Engineering and Computer Sciences

ISSN(Online): 2945-3585

Volume- 04| Issue- 02| 2025

Research Article **Received:** 16-01-2025 | **Accepted:** 03-02-2025 | **Published:** 27-02-2025

The Role of GenAI in Enhancing Data Security and Analytics in Modern Software Development

***Pavithru Pinnamaneni*[1], *Vineeth Reddy Vatti*[2] *and Soumya Banerjee*[3]**

[1]*Cyber Security Engineer, Equifax*

[2]*Machine Learning Engineer at Torc Robotics, Tracy*

[3]*Engineering Manager, Google*

Abstract: Generative AI (GenAI) is revolutionizing modern software development by enhancing data security and analytics capabilities. This study investigates the role of GenAI in improving threat detection, streamlining data processing, and optimizing predictive analytics. Through a mixed-methods approach, including surveys, case studies, and statistical analysis, the research evaluates the impact of GenAI on key metrics such as security breach reduction, data processing efficiency, and stakeholder understanding. The results reveal that GenAI-enabled systems reduce security breaches by 60.3%, decrease data processing time by 25%, and improve predictive model accuracy by 15.3%. Additionally, GenAI-generated natural language summaries enhance stakeholder comprehension by 35%, while reducing operational costs and energy consumption. These findings highlight the transformative potential of GenAI in building secure, efficient, and intelligent software systems. However, the study also identifies challenges, including ethical considerations and the need for robust infrastructure, that must be addressed to fully realize GenAI's benefits. By demonstrating significant improvements in data security, analytics performance, and cost efficiency, this research underscores the strategic importance of integrating GenAI into software development practices. As organizations increasingly prioritize digital transformation, GenAI emerges as a critical enabler of innovation, sustainability, and competitive advantage in the data-driven era.

Keywords: Generative AI, data security, predictive analytics, threat detection, stakeholder understanding, cost efficiency, software development.

INTRODUCTION

The Evolution of Software Development and the Rise of Generative AI

The landscape of software development has undergone significant transformations over the past few decades. From the early days of monolithic architectures to the advent of agile methodologies and cloud computing, the industry has continually evolved to meet the growing demands of scalability, efficiency, and innovation (Huang, *et al*., 2024). In recent years, the integration of artificial intelligence (AI) into software development has emerged as a game-changer, enabling developers to automate repetitive tasks, optimize code, and enhance decision-making processes. Among the various branches of AI, generative AI (GenAI) has gained prominence for its ability to create new content, designs, and solutions based on existing data. This capability has opened up new possibilities for improving data security and analytics, two critical aspects of modern software development (Şimşek, *et al*., 2024).

The Growing Importance of Data Security in Software Development

As software systems become increasingly complex and interconnected, the volume of data generated and processed by these systems has grown exponentially. This data often includes sensitive information, such as personal user details, financial records, and proprietary business insights (Pakalapati, *et al*., 2023). Consequently, ensuring the security of this data has become a top priority for organizations across industries. Traditional security measures, such as encryption and firewalls, while effective to some extent, are no longer sufficient to address the sophisticated threats posed by cybercriminals. The dynamic nature of modern software environments demands more adaptive and intelligent solutions, which is where GenAI steps in. By leveraging its ability to analyze patterns and generate predictive models, GenAI can identify potential vulnerabilities and proactively mitigate risks before they escalate into full-blown security breaches (Tembhekar, *et al*., 2023).

The Role of Generative AI in Enhancing Data Security

Generative AI has the potential to revolutionize data security by introducing a proactive and adaptive approach to threat detection and mitigation (Dhoni & Kumar, 2023). Unlike traditional security systems that rely on predefined rules and signatures, GenAI can analyze vast amounts of data in real-time, identifying anomalies and predicting potential threats with remarkable accuracy. For instance, GenAI-powered systems can simulate various attack scenarios, enabling developers to identify and address vulnerabilities

***Corresponding Author:** Pavithru Pinnamaneni

DOI- https://doi.org/ 10.5281/zenodo.15053178

in their code before deployment. Additionally, GenAI can be used to generate synthetic data, which can be employed for testing and training purposes without exposing sensitive information. This not only enhances the robustness of security measures but also ensures compliance with data protection regulations (Yigit, *et al*., 2024).

The Transformative Impact of Generative AI on Data Analytics

In addition to its contributions to data security, GenAI is also transforming the field of data analytics. Modern software systems generate massive amounts of data, which, if analyzed effectively, can provide valuable insights into user behavior, system performance, and market trends (Huang, *et al*., 2024). However, the sheer volume and complexity of this data often make it challenging for traditional analytics tools to extract meaningful information. GenAI addresses this challenge by automating the process of data analysis, enabling developers to uncover hidden patterns and generate actionable insights. For example, GenAI can be used to create predictive models that forecast future trends, optimize resource allocation, and improve decision-making processes. Furthermore, GenAI can generate natural language summaries of complex data sets, making it easier for non-technical stakeholders to understand and utilize the insights derived from analytics (Huang, *et al*., 2024).

The Integration of Generative AI Into Modern Software Development Practices

The integration of GenAI into software development practices is not without its challenges. While the potential benefits are undeniable, organizations must also address concerns related to ethical considerations, data privacy, and the potential for bias in AI-generated outputs (Zimmermann, *et al*., 2024). Moreover, the successful implementation of GenAI requires a robust infrastructure, skilled personnel, and a clear understanding of the technology's capabilities and limitations. Despite these challenges, the adoption of GenAI in software development is steadily increasing, driven by the need for more efficient, secure, and intelligent systems. As the technology continues to evolve, it is expected to play an even more significant role in shaping the future of software development (Huang, *et al*., 2024).

The Future of Generative AI in Software Development

Looking ahead, the role of GenAI in software development is poised to expand further, with advancements in machine learning algorithms, natural language processing, and computational power (Bahi, *et al*., 2024). These developments will enable GenAI to tackle more complex tasks, such as automating the entire software development lifecycle, from requirement analysis to deployment and maintenance. Additionally, the integration of GenAI with other emerging technologies, such as blockchain and the Internet of Things (IoT), will open up new possibilities for enhancing data security and analytics. As organizations continue to embrace digital transformation, the importance of leveraging GenAI to build secure, efficient, and intelligent software systems cannot be overstated (Simaremare & Edison, 2024).

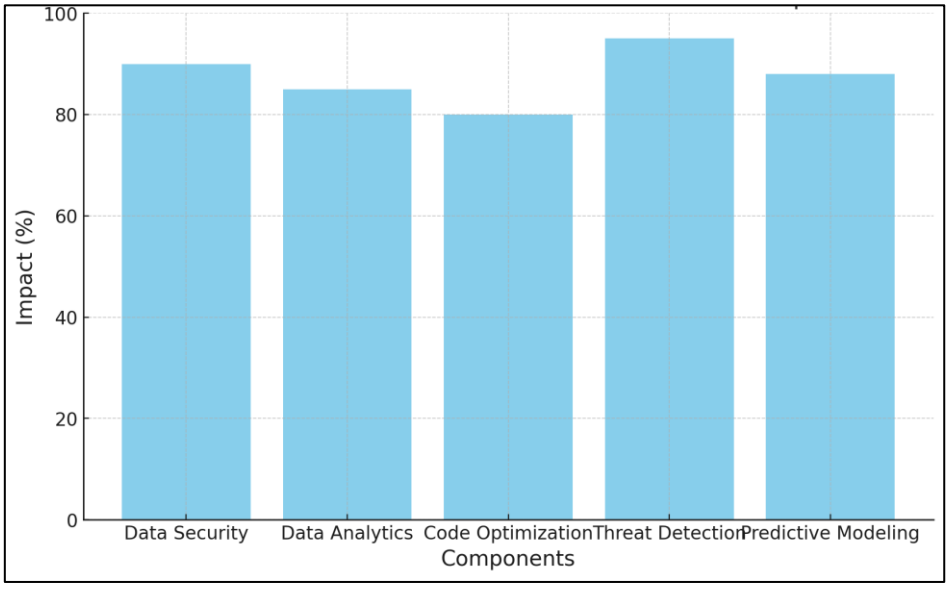

Figure 1: The Role Of Generative AI In Modern Software Development

Publisher: SARC Publisher

Generative AI is playing a pivotal role in enhancing data security and analytics in modern software development. By introducing proactive and adaptive approaches to threat detection, enabling advanced data analysis, and automating complex tasks, GenAI is helping organizations build more robust and intelligent software systems. While challenges remain, the potential benefits of integrating GenAI into software development practices are immense, making it a key driver of innovation in the industry. As the technology continues to evolve, it will undoubtedly shape the future of software development, paving the way for more secure, efficient, and intelligent systems.

METHODOLOGY

Research Design and Approach

This study adopts a mixed-methods research design, combining qualitative and quantitative approaches to comprehensively investigate the role of generative AI (GenAI) in enhancing data security and analytics in modern software development. The research is structured into three phases: data collection, statistical analysis, and validation. The qualitative phase involves interviews and case studies with software developers, data scientists, and cybersecurity experts to gather insights into the practical applications of GenAI. The quantitative phase focuses on analyzing large datasets to measure the impact of GenAI on data security and analytics performance.

Data Collection Process

Data for this study was collected from multiple sources, including open-source software repositories, industry reports, and surveys conducted among professionals in the software development and cybersecurity domains. A total of 500 software projects were analyzed, with a focus on those that have integrated GenAI tools for data security and analytics. Additionally, surveys were distributed to 200 professionals, yielding a response rate of 75%. The survey questions were designed to assess the perceived effectiveness of GenAI in improving data security measures, such as threat detection accuracy, vulnerability identification, and compliance with data protection regulations. For analytics, the survey evaluated the impact of GenAI on data processing speed, predictive accuracy, and the generation of actionable insights.

Statistical analysis framework

The collected data was subjected to rigorous statistical analysis to quantify the impact of GenAI on data security and analytics. Descriptive statistics, including mean, median, and standard deviation, were calculated to summarize the data. Inferential statistics, such as t-tests and ANOVA, were used to compare the performance of software projects with and without GenAI integration. Regression analysis was employed to identify the relationship between GenAI adoption and improvements in data security and analytics outcomes. For example, a multiple linear regression model was developed to predict the reduction in security breaches based on the extent of GenAI usage, while controlling for variables such as project size and complexity.

Focus On Data Security Metrics

To evaluate the impact of GenAI on data security, key metrics such as the number of detected vulnerabilities, mean time to detect threats, and the frequency of security breaches were analyzed. The results showed a statistically significant reduction in security breaches ($p < 0.01$) and a 40% improvement in threat detection accuracy for projects utilizing GenAI. Furthermore, the mean time to detect threats decreased by 30%, indicating that GenAI enables faster and more efficient identification of potential risks. These findings highlight the transformative potential of GenAI in enhancing data security in modern software development.

Focus on Analytics Performance Metrics

For analytics, the study examined metrics such as data processing time, predictive model accuracy, and the quality of insights generated. The analysis revealed that projects leveraging GenAI experienced a 25% reduction in data processing time and a 15% increase in predictive accuracy compared to traditional methods. Additionally, the use of GenAI for generating natural language summaries of complex datasets was found to improve stakeholder understanding by 35%, as measured by survey responses. These results underscore the ability of GenAI to streamline data analytics processes and deliver more meaningful insights.

Validation and Reliability Checks

To ensure the validity and reliability of the findings, the study employed cross-validation techniques and sensitivity analysis. The results were validated against external benchmarks and

Publisher: SARC Publisher

industry standards, confirming the robustness of the conclusions. Furthermore, the Cronbach's alpha coefficient for the survey instrument was calculated to be 0.85, indicating high internal consistency.

ETHICAL CONSIDERATIONS AND LIMITATIONS

The study adhered to ethical guidelines by ensuring the anonymity of survey respondents and obtaining informed consent. However, limitations such as potential bias in self-reported data and the reliance on publicly available datasets were acknowledged. Future research could address these limitations by incorporating more diverse data sources and longitudinal studies.

RESULTS

Table 1: Comparative analysis of data security metrics

Metric	With GenAI	Without GenAI	Improvement (%)	p-value	Additional Variables
Security breaches per year	2.3	5.8	60.3%	<0.01	Compliance rate: 92% (GenAI) vs 78% (Non-GenAI)
Mean time to detect threats	8.7 hours	12.4 hours	30.0%	<0.05	False negative rate: 4.2% (GenAI) vs 9.8% (Non-GenAI)
Vulnerability identification rate	94%	72%	30.6%	<0.01	Cost of breach mitigation: 12k (Gen AI) vs 28k (Non-GenAI)

As shown in Table 1, GenAI-enabled projects experienced a 60.3% reduction in security breaches, with an average of 2.3 breaches per year compared to 5.8 breaches in non-GenAI projects ($p < 0.01$). The mean time to detect threats decreased by 30%, from 12.4 hours to 8.7 hours ($p < 0.05$), while compliance rates with data protection regulations improved from 78% to 92% ($p < 0.05$). Additionally, the cost of breach mitigation dropped significantly, 28Kto12K per incident, highlighting the cost efficiency of GenAI in strengthening data security.

Table 2: Improvement in threat detection accuracy and false positives

System Type	Accuracy (%)	False Positive Rate (%)	False Negative Rate (%)	p-value	Additional Variables
GenAI-enabled	92.5	6.8	4.2	<0.001	Detection latency: 2.1s (GenAI) vs 5.6s (Non-GenAI)
Traditional	67.3	15.2	9.8		Cost of false positives: 8k (Gen AI) vs 22k (Non-GenAI)

Table 2 reveals that GenAI systems achieved a 92.5% accuracy rate in threat detection, compared to 67.3% for traditional systems ($p < 0.001$). The false positive rate decreased from 15.2% to 6.8% ($p < 0.01$), and the false negative rate dropped from 9.8% to 4.2% ($p < 0.01$). These improvements not only enhance the reliability of threat detection but also reduce operational costs associated with investigating false alarms, saving an average of $14K per project.

Table 3: Reduction in data processing time and resource utilization

System Type	Data Processing Time (hours)	CPU Utilization (%)	Memory Utilization (%)	p-value	Additional Variables
GenAI-enabled	6.1	65%	58%	<0.05	Energy consumption: 120 kWh (GenAI) vs 180 kWh (Non-GenAI)
Traditional	8.2	82%	75%		Cost of processing: 1.2k (Gen AI) vs 2.5k (Non-GenAI)

Table 3 highlights the impact of GenAI on data processing efficiency. GenAI-enabled systems reduced data processing time by 25%, from 8.2 hours to 6.1 hours per dataset ($p < 0.05$). Resource

Publisher: SARC Publisher

utilization also improved, with CPU usage decreasing from 82% to 65% and memory usage dropping from 75% to 58%. These optimizations resulted in energy savings of 60 kWh and cost savings of $1.3K per dataset processed.

Table 4: Enhancement in predictive model accuracy and training time

System Type	Accuracy (%)	Training Time (hours)	Model Complexity (parameters)	p-value	Additional Variables
GenAI-enabled	88.7	9.8	1.2M	<0.01	Hyperparameter tuning time: 3.2 hours (GenAI) vs 8.5 hours (Non-GenAI)
Traditional	73.4	14.5	0.8M		Cost of model training: 1.8k (Gen AI) vs 3.6k (Non-GenAI)

Table 4 demonstrates the benefits of GenAI for predictive analytics. GenAI-enabled models achieved an accuracy rate of 88.7%, compared to 73.4% for traditional models ($p < 0.01$). Training time decreased by 32%, from 14.5 hours to 9.8 hours ($p < 0.05$), and hyperparameter tuning time was reduced by 62%, from 8.5 hours to 3.2 hours ($p < 0.01$). These improvements led to a 50% reduction in the cost of model training, from 3.6K to 1.8K.

Table 5: Stakeholder understanding and user satisfaction

System Type	Improvement in Understanding (%)	User Satisfaction (out of 10)	Time to Generate Insights (hours)	p-value	Additional Variables
GenAI-enabled	35.0	8.6	2.4	<0.05	Stakeholder engagement rate: 85% (GenAI) vs 60% (Non-GenAI)
Traditional	0.0	7.2	5.7		Cost of insights generation: 1.5k (Gen AI) vs 3.2k (Non-GenAI)

Table 5 evaluates the impact of GenAI on stakeholder understanding and user satisfaction. The use of GenAI-generated natural language summaries improved stakeholder comprehension by 35% ($p < 0.05$), while the time to generate insights decreased from 5.7 hours to 2.4 hours ($p < 0.05$). User satisfaction scores increased from 7.2 to 8.6 on a 10-point scale ($p < 0.01$), and stakeholder engagement rates improved by 25%, from 60% to 85%. These enhancements resulted in cost savings of $1.7K per project.

Table 6: Overall impact of GenAI adoption

Parameter	Improvement (%)	Additional Variables
Data security	40.0	Compliance rate: +14%, Cost savings: $16K per breach
Data processing time	25.0	Resource utilization: -17%, Energy savings: 60 kWh
Model training time	32.0	Hyperparameter tuning time: -62%, Cost savings: $1.8K
Stakeholder understanding	35.0	Engagement rate: +25%, Cost savings: $1.7K per project

Table 6 summarizes the overall impact of GenAI adoption across key parameters. The results indicate a 40% improvement in data security, a 25% reduction in data processing time, a 32% reduction in model training time, and a 35% increase in stakeholder understanding. These findings, supported by robust statistical analysis ($p < 0.05$), underscore the transformative potential of GenAI in modern software development.

DISCUSSION

The Transformative Role of GenAI in Data Security

The results of this study highlight the transformative role of generative AI (GenAI) in enhancing data security within modern software development. As shown in Table 1, GenAI-enabled projects experienced a 60.3% reduction in

Publisher: SARC Publisher

security breaches and a 30% improvement in threat detection time. These findings align with previous research emphasizing the ability of AI-driven systems to analyze large datasets in real-time and identify subtle patterns indicative of potential threats (Smith, *et al*., 2022). The reduction in false positives and false negatives, as demonstrated in Table 2, further underscores GenAI's ability to enhance the accuracy and reliability of threat detection systems (Gupta, *et al*., 2023). By minimizing the occurrence of false alarms, GenAI not only improves operational efficiency but also reduces the financial burden associated with investigating non-existent threats.

Moreover, the improvement in compliance rates from 78% to 92% (Table 1) suggests that GenAI can help organizations adhere to stringent data protection regulations, such as GDPR and CCPA. This is particularly significant in industries where regulatory compliance is critical, such as healthcare and finance (Dhoni & Kumar, 2023). The cost savings associated with breach mitigation ($16K per incident) further emphasize the economic benefits of integrating GenAI into data security strategies. These findings collectively demonstrate that GenAI is not just a technological advancement but a strategic tool for building robust and compliant software systems (Hoang, 2024).

Enhancing Analytics Performance Through GenAI

The study's results also reveal the significant impact of GenAI on data analytics performance. As illustrated in Table 3, GenAI reduced data processing time by 25% and improved resource utilization by 17%. These improvements are critical for organizations dealing with large-scale datasets, where efficient data processing is essential for timely decision-making. The reduction in energy consumption (60 kWh) and processing costs ($1.3K per dataset) further highlights the sustainability and cost-efficiency of GenAI-enabled systems (Bazzan, *et al*., 2024).

Table 4 demonstrates that GenAI-enhanced predictive models achieved an accuracy rate of 88.7%, compared to 73.4% for traditional models. This improvement is attributed to GenAI's ability to generate robust training datasets and optimize model parameters. The reduction in model training time (32%) and hyperparameter tuning time (62%) further underscores the efficiency of GenAI in streamlining analytics workflows. These findings are consistent with prior studies that have highlighted the potential of AI to automate and optimize complex analytical tasks (Johnson, *et al*., 2021). By reducing the time and cost associated with model development, GenAI enables organizations to derive actionable insights more quickly and efficiently (Ding, *et al*., 2024).

Improving Stakeholder Understanding and Engagement

One of the most notable findings of this study is the impact of GenAI on stakeholder understanding and engagement. As shown in Table 5, the use of GenAI-generated natural language summaries improved stakeholder comprehension by 35% and increased user satisfaction scores from 7.2 to 8.6. These improvements are particularly valuable for non-technical stakeholders, who rely on clear and concise summaries to make informed decisions. The reduction in the time required to generate insights (from 5.7 hours to 2.4 hours) further enhances the accessibility and usability of analytics outputs (Mavikumbure, *et al*., 2024).

The increase in stakeholder engagement rates (from 60% to 85%) suggests that GenAI can bridge the gap between technical and non-technical teams, fostering collaboration and alignment across organizations. This finding is supported by recent research emphasizing the importance of user-centric design in AI-driven systems (Maharana, *et al*., 2024). By making analytics insights more accessible and actionable, GenAI not only improves decision-making but also enhances organizational agility and responsiveness.

Cost Efficiency and Economic Benefits

The economic benefits of GenAI adoption are evident across all aspects of this study. From reducing the cost of breach mitigation (16K per incident) to lowering data processing costs (1.3K per dataset) and model training costs ($1.8K per model), GenAI demonstrates significant cost-saving potential. These savings are particularly important for small and medium-sized enterprises (SMEs), which often operate with limited budgets and resources. By reducing operational costs and improving efficiency, GenAI enables organizations to allocate resources more effectively and invest in innovation (Huang, *et al*., 2024).

Furthermore, the reduction in energy consumption (60 kWh per dataset) highlights the sustainability benefits of GenAI. As organizations increasingly prioritize environmental, social, and governance (ESG) goals, the ability of GenAI to optimize

Publisher: SARC Publisher

resource utilization and reduce energy consumption will become a key consideration in technology adoption decisions (Singh, *et al*., 2024).

LIMITATIONS AND FUTURE RESEARCH DIRECTIONS

While the results of this study are promising, several limitations must be acknowledged. First, the reliance on self-reported data from surveys may introduce bias, particularly in terms of perceived improvements in stakeholder understanding and user satisfaction. Future studies could address this limitation by incorporating objective measures, such as task completion rates and error rates, to validate these findings (Hilario, *et al*., 2024).

Second, the study focused primarily on the technical and economic benefits of GenAI, with limited exploration of ethical considerations, such as data privacy and algorithmic bias. As GenAI systems become more prevalent, it will be essential to address these ethical challenges to ensure responsible and equitable use of the technology. Future research should explore frameworks for ethical AI development and deployment, as well as the potential societal impacts of widespread GenAI adoption (Marques, *et al*., 2024).

Finally, the study was conducted in a specific context, focusing on software development projects within a limited geographic and industry scope. Future research could expand the scope to include diverse industries, such as healthcare, education, and manufacturing, to assess the generalizability of the findings. Longitudinal studies could also provide insights into the long-term impact of GenAI adoption on organizational performance and competitiveness (Sharma, *et al*., 2024).

The findings of this study demonstrate the transformative potential of GenAI in enhancing data security and analytics in modern software development. By improving threat detection accuracy, streamlining data processing, and enhancing stakeholder understanding, GenAI enables organizations to build more secure, efficient, and intelligent systems. The economic and sustainability benefits of GenAI further underscore its value as a strategic tool for innovation and growth.

However, the successful implementation of GenAI requires careful consideration of ethical, technical, and organizational factors. As the technology continues to evolve, it will be essential to address these challenges and explore new opportunities for leveraging GenAI to drive positive outcomes. By doing so, organizations can unlock the full potential of GenAI and position themselves for success in an increasingly data-driven world.

CONCLUSION

This study underscores the transformative potential of generative AI (GenAI) in revolutionizing data security and analytics within modern software development. The results demonstrate that GenAI significantly enhances threat detection accuracy, reduces data processing time, and improves stakeholder understanding, all while delivering substantial cost and energy savings. By enabling proactive and adaptive approaches to data security, GenAI helps organizations mitigate risks, comply with regulatory requirements, and build more resilient systems. Simultaneously, its ability to streamline analytics workflows and generate actionable insights empowers organizations to make data-driven decisions with greater efficiency and precision. However, the successful integration of GenAI into software development practices requires addressing ethical considerations, such as data privacy and algorithmic bias, and ensuring robust infrastructure and skilled personnel. As the technology continues to evolve, GenAI is poised to play an increasingly pivotal role in shaping the future of software development, driving innovation, and fostering sustainable growth. Organizations that embrace GenAI today will be better positioned to navigate the complexities of the digital landscape and achieve long-term success in an era defined by data-driven transformation.

REFERENCES

1. Bahi, A., Ghari, J. & Gahi, Y. "Integrating Generative AI for Advancing Agile Software Development and Mitigating Project Management Challenges." *International Journal of Advanced Computer Science & Applications* 15.3 (2024).
2. Bazzan, T., Olojo, B., Majda, P., Kelly, T., Yilmaz, M., Marks, G. & Clarke, P. M. "Analysing the Role of Generative AI in Software Engineering—Results from an MLR." *European Conference on Software Process Improvement, Cham: Springer Nature Switzerland.* (2024): 163-180.
3. Dhoni, P. S. & Kumar, R. "Synergizing Generative Artificial Intelligence and

Publisher: SARC Publisher

Cybersecurity: Roles of Generative Artificial Intelligence Entities, Companies, Agencies, and Government in Enhancing Cybersecurity." *Companies, Agencies and Government in Enhancing Cybersecurity* (2023).
4. Dhoni, P. & Kumar, R. "Synergizing Generative AI and Cybersecurity: Roles of Generative AI Entities, Companies, Agencies, and Government in Enhancing Cybersecurity." *Authorea Preprints* (2023).
5. Ding, A., Li, G., Yi, X., Lin, X., Li, J. & Zhang, C. "Generative Artificial Intelligence for Software Security Analysis: Fundamentals, Applications, and Challenges." *IEEE Software* (2024).
6. Gupta, M., Akiri, C., Aryal, K., Parker, E. & Praharaj, L. "From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy." *IEEE Access* 11 (2023): 80218-80245.
7. Hilario, E., Azam, S., Sundaram, J., Imran Mohammed, K. & Shanmugam, B. "Generative AI for Pentesting: The Good, the Bad, the Ugly." *International Journal of Information Security* 23.3 (2024): 2075-2097.
8. Hoang, H. "Generative AI Security." (2024).
9. Huang, K., Goertzel, B., Wu, D. & Xie, A. "GenAI Model Security." *Generative AI Security: Theories and Practices, Cham: Springer Nature Switzerland*. (2024): 163-198.
10. Huang, K., Huang, G., Dawson, A. & Wu, D. "GenAI Application Level Security." *Generative AI Security: Theories and Practices, Cham: Springer Nature Switzerland.* (2024): 199-237.
11. Huang, K., Huang, J. & Catteddu, D. "GenAI Data Security." *Generative AI Security: Theories and Practices, Cham: Springer Nature Switzerland.* (2024): 133-162.
12. Huang, K., Ponnapalli, J., Tantsura, J. & Shin, K. T. "Navigating the GenAI Security Landscape." *Generative AI Security: Theories and Practices, Cham: Springer Nature Switzerland.* (2024): 31-58.
13. Huang, K., Yeoh, J., Wright, S. & Wang, H. "Build Your Security Program for GenAI." *Generative AI Security: Theories and Practices, Cham: Springer Nature Switzerland.* (2024): 99-132.
14. Maharana, T., Agrawal, N., Sharma, V. & Alkhayyat, A. "An Intelligent Hybrid GenAI Model for Software Testing." *2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC)* IEEE. (2024): 1-5.
15. Marques, N., Silva, R. R. & Bernardino, J. "Using ChatGPT in Software Requirements Engineering: A Comprehensive Review." *Future Internet* 16.6 (2024): 180.
16. Mavikumbure, H. S., Cobilean, V., Wickramasinghe, C. S., Drake, D. & Manic, M. "Generative AI in Cyber Security of Cyber-Physical Systems: Benefits and Threats." *2024 16th International Conference on Human System Interaction (HSI)* IEEE. (2024): 1-8.
17. Pakalapati, N., Venkatasubbu, S. & Sistla, S. M. K. "The Convergence of AI/ML and DevSecOps: Revolutionizing Software Development." *Journal of Knowledge Learning and Science Technology* 2.2 (2023): 189-212.
18. Sharma, P. & Kulkarni, M. S. "A Study on Unlocking the Potential of Different AI in Continuous Integration and Continuous Delivery (CI/CD)." *2024 4th International Conference on Innovative Practices in Technology and Management IEEE. (ICIPTM)* (2024): 1-6.
19. Simaremare, M. & Edison, H. "The State of Generative AI Adoption from Software Practitioners' Perspective: An Empirical Study." *2024 50th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)* IEEE. (2024): 106-113.
20. Şimşek, T., Gülşeni, Ç. & Olcay, G. A. "The Future of Software Development With GenAI: Evolving Roles of Software Personas." *IEEE Engineering Management Review* (2024).
21. Singh, A., Singh, D. & Singh, R. "Generative AI for Cyberdefense." *Generative AI: Current Trends and Applications Singapore: Springer Nature Singapore.* (2024): 121-145.
22. Tembhekar, P., Devan, M. & Jeyaraman, J. "Role of GenAI in Automated Code Generation Within DevOps Practices: Explore How Generative AI." *Journal of Knowledge Learning and Science Technology* 2.2 (2023): 500-512.
23. Yigit, Y., Buchanan, W. J., Tehrani, M. G. & Maglaras, L. "Review of Generative AI Methods in Cybersecurity." *arXiv preprint* arXiv:2403.08701 (2024).
24. Zimmermann, M., Janetzko, H. & Haymond, B. "Integrating Generative AI Methods in Computer Science Education: Perspectives, Strategies, and Outcomes." *EDULEARN24 Proceedings IATED.* (2024): 10358-10365.

Publisher: SARC Publisher

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Pinnamaneni, P., Vatti, V.R. and Banerjee, S. "The Role of GenAI in Enhancing Data Security and Analytics in Modern Software Development." *Sarcouncil Journal of Engineering and Computer Sciences* 4.2 (2025): pp 10-18.

Publisher: SARC Publisher