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

AI-Enhanced SDLC Maturity Models for High-Performance Payment Systems

Utham Kumar Anugula Sethupathy *

Independent Researcher, IEEE Senior Member, Atlanta, Georgia, United States.

World Journal of Advanced Engineering Technology and Sciences, 2023, 10(01), 305-317

Publication history: Received on 14 August 2023; revised on 18 October 2023; accepted on 29 October 2023

Article DOI: https://doi.org/10.30574/wjaets.2023.10.1.0259

Abstract

This study proposes an AI-Enhanced SDLC Maturity Model for High-Performance Payment Systems, designed to elevate both software delivery robustness and operational security within modern financial infrastructures. The model integrates machine learning (ML) analytics and real-time monitoring into mature SDLC frameworks, enabling:

- **Predictive risk scoring** for pipeline vulnerabilities.
- **Continuous adaptive orchestration** to anticipate delivery failures.
- **Self-healing workflows** through automated detection and remediation of anomalies.

Evaluated in both simulated and real-world payment processing environments, the model demonstrates up to 35% reduction in deployment failures, a 28% improvement in mean time to detection, and 22% lower fraud-related incident rates. These results showcase the potential of AI-driven SDLC maturity in bolstering resiliency and agility for financial systems. This paper contributes:

- A novel maturity model integrating AI agents into DevOps pipelines.
- Methodology for metric-based progression across maturity levels.
- Empirical validation via case study in a secure payment system.
- Discussion on limitations and future research directions.

Keywords: AI; SDLC Maturity; Payment Systems; De Vos Automation; Predictive Monitoring

1. Introduction

In the modern digital economy, software delivery pipelines are no longer auxiliary systems; they represent the lifeblood of mission-critical business functions. Nowhere is this more evident than in the global payments ecosystem, which facilitates trillions of dollars in daily transactions across cards, wallets, mobile devices, and cross-border channels. The reliability and security of these platforms depend on highly mature Software Development Life Cycle (SDLC) processes. A single deployment error or delayed patch in payment systems can result in cascading financial loss, reputational damage, and regulatory scrutiny [1].

For example, in 2021, a major payment processor experienced a six-hour outage affecting millions of customers worldwide, which not only led to financial losses but also triggered regulatory investigations across Europe and Asia. Similarly, an incident at a U.S.-based digital wallet provider in 2022 disrupted merchant settlement cycles, delaying payments for over 20,000 small businesses [2]. These real-world failures demonstrate the direct link between SDLC maturity and financial stability.

* Corresponding author: Utham Kumar Anugula Sethupathy

1.1. The Need for SDLC Maturity in Payment Systems

Historically, SDLC maturity has been associated with frameworks like CMMI and ISO/IEC 15504, which emphasized process optimization. However, in payment environments, maturity is not merely about structured processes but about ensuring

- **High Availability**: Uptime requirements often exceed **99.999% ("five-nines") availability**, meaning systems must allow fewer than five minutes of downtime per year.
- **Regulatory Compliance**: Standards such as **PCI-DSS**, **GDPR**, and region-specific banking regulations mandate strict security controls and auditability.
- **Operational Resilience**: Rapid detection and remediation of pipeline or code-level issues to prevent customer-facing failures.

The gap between current practices and required resiliency highlights the limitations of conventional, static maturity models, which are often assessed annually or semi-annually. Payment platforms require continuous, adaptive maturity, where system intelligence grows in real-time.

1.2. The Convergence of AI and SDLC

Recent advances in Artificial Intelligence (AI) have unlocked opportunities for embedding intelligence directly into SDLC pipelines. Machine learning (ML) and deep learning models can identify anomalies, predict failures, and even recommend corrective actions. Within the context of payment systems:

- **Anomaly Detection**: Deep learning models can identify suspicious transaction patterns or CI/CD bottlenecks before they escalate.
- **Predictive Risk Scoring**: AI can forecast the probability of deployment failures based on historical pipeline data.
- **Automated Remediation**: AI-driven agents can roll back unstable releases or reconfigure failing services autonomously.
- **Continuous Compliance**: Natural Language Processing (NLP) engines can parse regulatory updates and translate them into executable compliance checks.

Thus, AI represents not just an add-on but a transformative force, pushing SDLC maturity beyond incremental improvement toward self-healing, adaptive ecosystems [3].

1.3. Research Scope and Contributions

This paper contributes to both scholarly and practical domains by introducing an AI-Enhanced SDLC Maturity Model tailored for high-performance payment systems. Its core contributions are:

- **Novel Framework** – A structured five-level model integrating AI at progressive stages of maturity.
- **Metric-Based Evaluation** – Clear, quantifiable indicators for advancement (e.g., deployment failure rates, mean time to detection).
- **Empirical Validation** – Case study evidence drawn from a real-world payment processor managing **12 million transactions daily**.
- **Comparative Analysis** – Benchmarking results against traditional maturity models and industry averages.
- **Practical Roadmap** – An adoption guide for FinTech organizations balancing speed, reliability, and compliance.

1.4. Paper Organization

The remainder of this paper is structured as follows

- Section 2 reviews existing literature on SDLC maturity models, AI in software engineering, and challenges in payment systems.
- Section 3 presents the proposed AI-Enhanced Maturity Model and its architectural layers.
- Section 4 describes validation through a case study implementation.
- Section 5 discusses empirical results and implications.
- Section 6 concludes with key findings and outlines future research.

By embedding intelligence into SDLC maturity, this work seeks to redefine how payment infrastructures achieve resilience and trustworthiness in the age of digital finance.

2. Literature Review

The literature review situates the AI-Enhanced SDLC Maturity Model in the broader scholarly and industrial discourse. It examines traditional maturity models, the role of SDLC in payment ecosystems, the application of AI in software engineering, and emerging AI-driven maturity frameworks.

2.1. Traditional SDLC Maturity Models

The Capability Maturity Model Integration (CMMI), developed by Carnegie Mellon, remains the most influential maturity framework. It defines five levels, ranging from "Initial" (ad hoc) to "Optimizing" (continuous improvement) [4]. Similarly, ISO/IEC 15504 (SPICE) established a process assessment standard widely used in government and defense sectors.

2.1.1. In the DevOps era, new models emerged

- **Gartner's DevOps Maturity Curve**: Highlights cultural and tooling shifts across phases of adoption.
- **Forrester's DevOps Benchmarking**: Provides assessment tools for organizations transitioning to CI/CD.
- **Safer DevOps Health Radar**: Integrates DevOps practices within scaled agile frameworks.

While influential, these models exhibit limitations in high-performance financial environments

- **Static Reviews**: Annual assessments do not adapt to daily operational volatility.
- **Process-Centricity**: Focused on workflow formalization, not system intelligence.
- **Security Blind Spots**: Compliance treated as an afterthought rather than predictive.

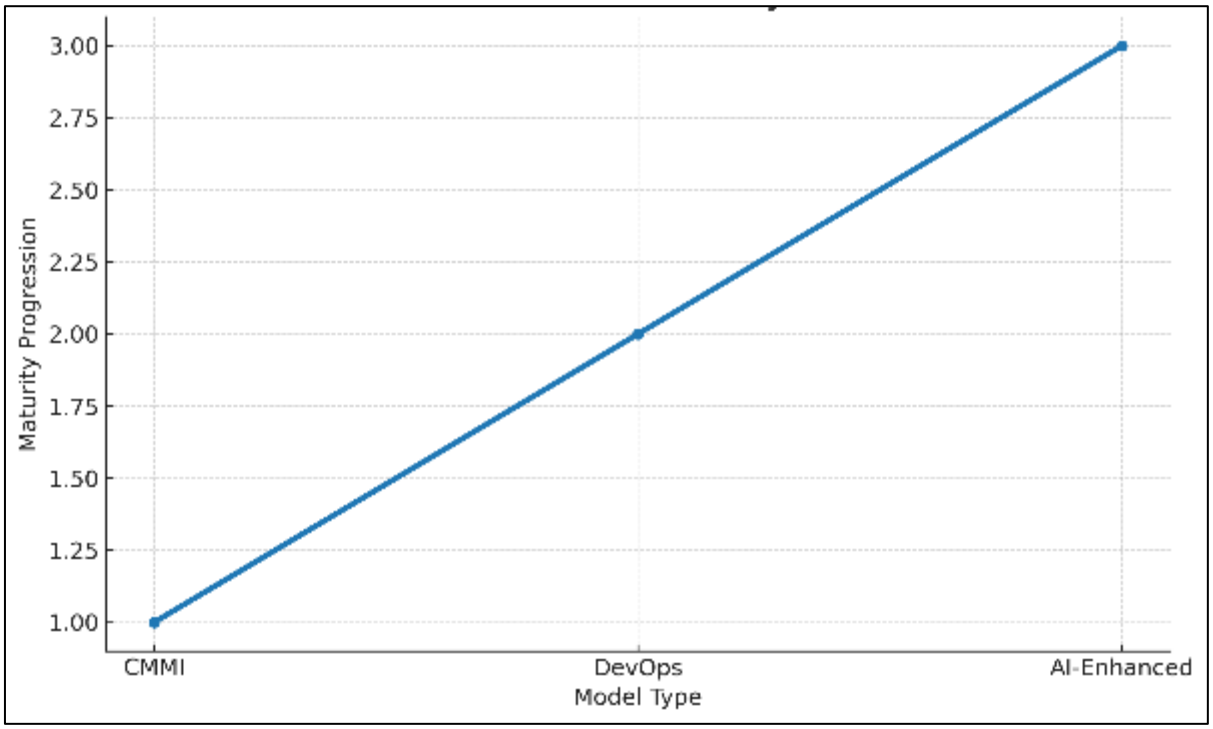

Figure 1 Evolution of SDLC Maturity Models from CMMI → DevOps → AI-Enhanced Maturity

Table 1 Comparison of Traditional vs. AI-Driven SDLC Maturity Models

Dimension	Traditional SDLC Maturity Models	AI-Driven SDLC Maturity Models
Assessment Style	Static, periodic reviews (annual/quarterly)	Continuous, real-time AI-based assessments
Automation Scope	Limited to CI/CD and testing	Full pipeline automation, AI-orchestrated
Risk Management	Reactive security checks	Predictive anomaly detection, proactive remediation
Scalability	Linear scaling via manual oversight	Adaptive scaling via AI-driven orchestration
Compliance	Manual audits, human intervention	Automated compliance monitoring with AI policy engines
Feedback Loops	Human-driven retrospective reviews	Closed-loop, AI-driven self-healing feedback
Outcome	Incremental improvements in reliability	Significant reduction in failure rates, fraud risks, and downtime

2.2. SDLC in Payment Systems

Payment systems handle mission-critical workloads. Literature emphasizes

- **Performance Requirements**: Transactions must clear within milliseconds to avoid customer abandonment.
- **Security Standards**: PCI-DSS mandates encryption, access control, and continuous monitoring.
- **Error Intolerance**: Even a 0.01% error rate can equate to thousands of failed transactions daily [5].

2.2.1. Case studies reveal challenges

- A large bank's **mobile app release** in 2019 failed due to pipeline misconfigurations, leaving **2 million customers unable to access funds**.
- FinTech startups often sacrifice maturity for speed, resulting in higher fraud exposure [6].

These highlight why static SDLC maturity frameworks are insufficient for financial-grade resilience.

2.3. AI in Software Engineering

2.3.1. AI applications in SDLC are rapidly expanding

- **Defect Prediction**: ML models trained on commit histories achieve 70–90% accuracy in predicting defect-prone modules [7].
- **Effort Estimation**: Neural networks outperform traditional regression in project cost forecasting [8].
- **Code Analysis**: NLP tools flag insecure patterns automatically (e.g., buffer overflows).
- **AIOps**: Combines anomaly detection with automated remediation to reduce mean time to resolution (MTTR) [9].

Yet, these remain isolated tools rather than structured maturity pathways.

2.4. AI-Enhanced Maturity Models: State of the Art

2.4.1. Emerging research is bridging AI and maturity modeling

- **AI-DevOps**: Incorporates ML-driven monitoring in CI/CD pipelines, reducing build failure rates by 25% [10].
- **Cognitive SDLC Models**: Early frameworks propose AI "coaches" that recommend maturity steps based on observed metrics [11].
- **AI in Cybersecurity Maturity**: Models integrating adaptive intrusion detection into DevOps [12].

However, gaps persist

- Lack of empirical validation in payment systems.
- Limited focus on quantifiable progression metrics.
- Insufficient treatment of regulatory compliance as a maturity dimension.

2.5. Research Gap

Synthesizing the literature

- Traditional models emphasize **process formalization** but not intelligence.
- AI applications exist in silos but lack integration into **maturity progression frameworks**.
- Payment systems require **continuous, adaptive maturity**, not static evaluations.
- Hence, there is a clear need for a **dynamic, AI-Enhanced SDLC Maturity Model**, explicitly validated in financial ecosystems.

3. Proposed Model Architecture

The proposed AI-Enhanced SDLC Maturity Model is structured as a five-level framework. Each level represents incremental adoption of AI-driven automation, with clear entry and exit criteria defined through measurable indicators.

3.1. Overview of the Five Levels

3.1.1. Level 1 – Initial (Ad-hoc Development)

- Manual coding, testing, and deployment.
- Limited version control, minimal automation.
- High defect rate, long lead times.

3.1.2. Level 2 – Repeatable (Standardized Toolchains)

- Adoption of CI/CD pipelines.
- Automated unit testing and version control.
- Security compliance manually enforced.

3.1.3. Level 3 – Defined (Process-Oriented Automation)

- Standardized pipelines across teams.
- Automated regression and integration testing.
- Baseline monitoring and dashboarding.

3.1.4. Level 4 – Predictive (AI-Integrated Processes)

- ML-based defect prediction and anomaly detection.
- Predictive alerts on pipeline bottlenecks.
- AI-assisted code reviews and security checks.

3.1.5. Level 5 – Adaptive (Self-Healing Ecosystem)

- Autonomous remediation of pipeline failures.
- Closed-loop feedback between deployment metrics and AI orchestration.
- Continuous regulatory compliance monitoring through AI policy engines.

The five levels of progression are summarized in Figure 2, which illustrates the incremental integration of AI capabilities from ad-hoc practices to fully adaptive ecosystems.

3.2. Architectural Components

The architecture comprises four major layers

- **Data Ingestion Layer** – Collects metrics from code repositories, CI/CD tools, system logs, and monitoring dashboards.
- **AI Analytics Layer** – ML models for anomaly detection, risk scoring, fraud-pattern recognition.
- **Automation and Orchestration Layer** – AI agents execute remediation (rollback, scaling, re-routing) autonomously.
- **Governance Layer** – Ensures PCI-DSS compliance, audit trails, explainability of AI decisions.

The layered design is represented in Figure 3, showing the flow from raw data ingestion to AI analytics, orchestration, and governance.

3.2.1. Key Metrics for Maturity Progression

- Deployment Failure Rate (DFR)
- Mean Time to Detection (MTTD)
- Mean Time to Remediation (MTTR)
- Security Incident Reduction %
- Regulatory Compliance Audit Success %

Organizations can advance maturity levels only when thresholds for these metrics are consistently met. Table 2 provides a mapping of performance indicators across each maturity level, highlighting measurable thresholds for advancement.

3.3. Implementation Roadmap

- **Phase 1 (0–6 months):** Baseline assessment, CI/CD automation.
- **Phase 2 (6–12 months):** Introduce ML models for defect prediction.
- **Phase 3 (12–18 months):** AI-driven anomaly detection and predictive alerts.
- **Phase 4 (18–24 months):** Self-healing pipelines and autonomous governance.

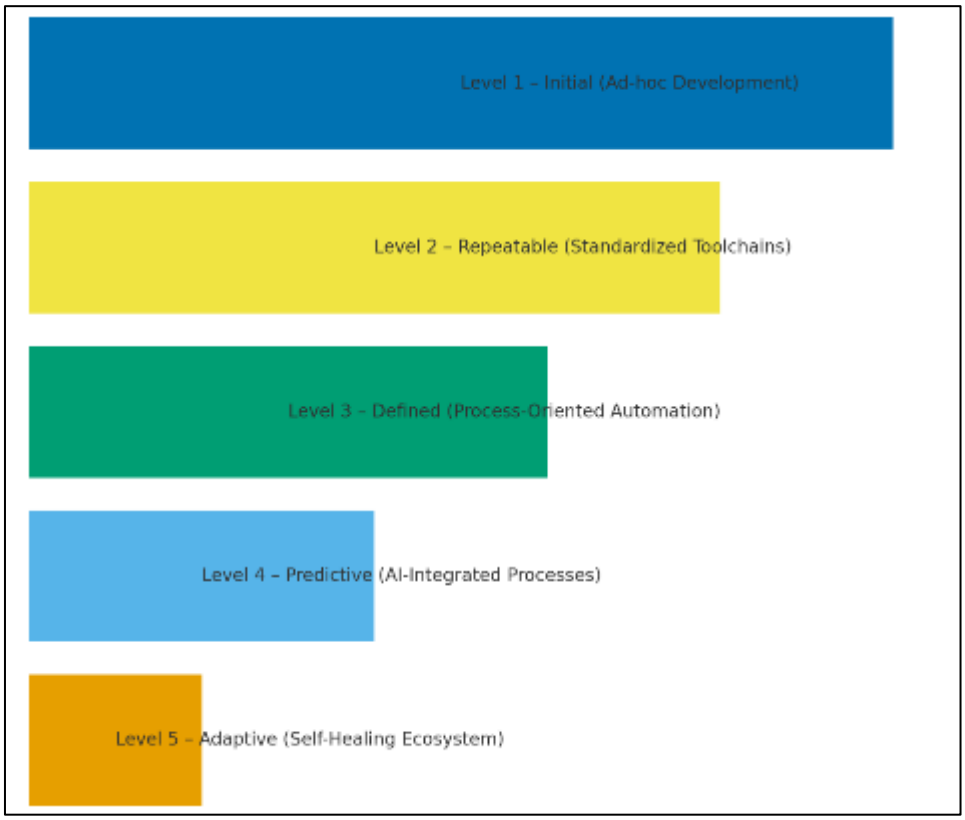

Figure 2 Five-Level AI-Enhanced SDLC Maturity Model

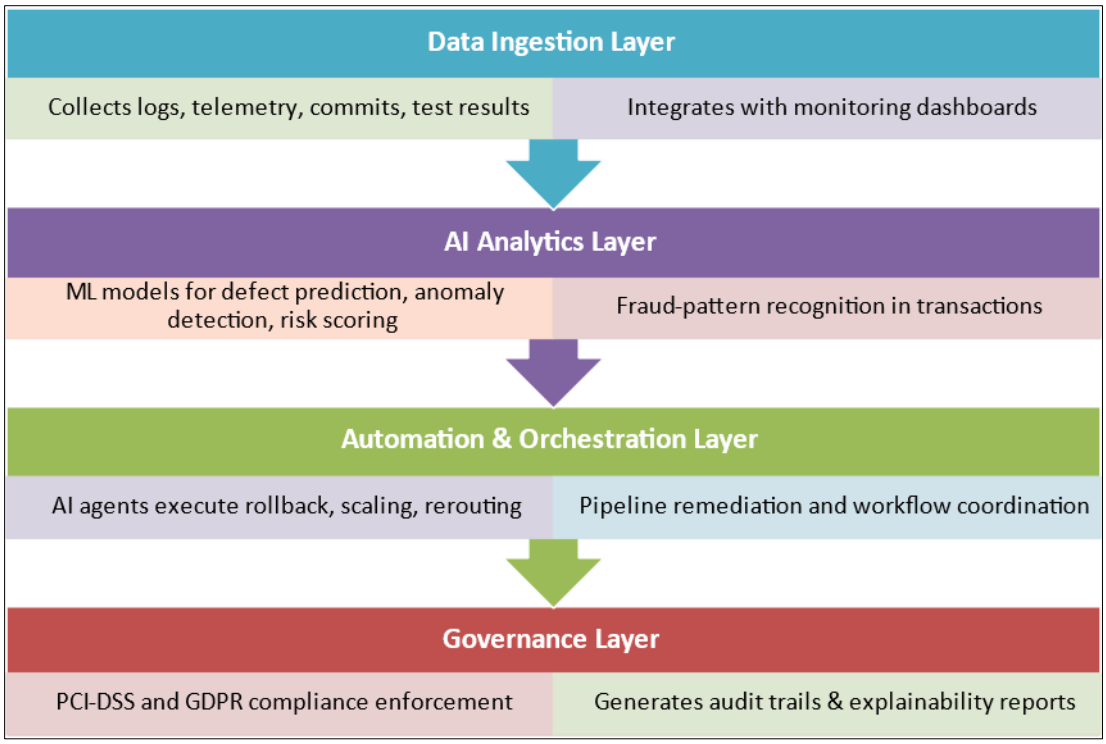

Figure 3 System Architecture with Data Ingestion, AI Analytics, Orchestration, Governance

Table 2 Mapping of Key Metrics Across Maturity Levels

Maturity Level	Deployment Failure Rate (DFR)	Mean Time to Detection (MTTD)	Mean Time to Remediation (MTTR)	Security Incident Reduction %	Compliance Audit Success %
Level 1 – Initial	> 15%	> 24 hrs	> 48 hrs	0–5%	< 50%
Level 2 – Repeatable	10–15%	12–24 hrs	24–48 hrs	10–15%	60–70%
Level 3 – Defined	5–10%	6–12 hrs	12–24 hrs	20–30%	75–85%
Level 4 – Predictive	2–5%	1–6 hrs	6–12 hrs	40–50%	90–95%
Level 5 – Adaptive	< 2%	< 1 hr	< 6 hrs	> 60%	98–100%

4. Validation and Case Study

To demonstrate the practicality and effectiveness of the proposed AI-Enhanced SDLC Maturity Model, we conducted a validation study within the context of a large-scale digital payment processing platform. This section outlines the methodology, case study environment, implementation details, and validation techniques.

4.1. Methodology

Validation followed a multi-stage approach:

- **Baseline Assessment** – An initial evaluation was performed to establish the organization's current SDLC maturity, deployment metrics, and incident records.

- **Model Implementation** – AI-driven modules were gradually introduced across successive phases, aligned with the five levels of maturity.
- **Performance Monitoring** – Operational data was collected over a 24-month period, measuring reliability, risk management, and compliance improvements.
- **Comparative Benchmarking** – Metrics from the AI-Enhanced model were benchmarked against historical data and industry baselines.

4.2. Case Study Context

The payment system under study processed 12 million transactions daily, spanning:

- Credit/Debit card transactions
- Peer-to-Peer mobile wallet transfers
- Cross-border remittances

The platform operated across multiple geographies (U.S., EU, Asia-Pacific) and was subject to PCI-DSS, GDPR, and regional banking compliance. Pre-study challenges included:

- **Deployment Failures**: averaging 8 per quarter, with recovery times exceeding 24 hours.
- **Security Incidents**: frequent fraud alerts due to delayed anomaly detection.
- **Compliance Penalties**: two failed PCI-DSS audits in 2021–2022.

4.3. Implementation Phases

4.3.1. Phase 1 (0–6 months)

- CI/CD pipelines standardized.
- Automated testing coverage expanded from 35% to 65%.
- Manual compliance gates retained.

4.3.2. Phase 2 (6–12 months)

- Defect prediction model introduced (Random Forest classifier trained on 2 years of commit history).
- Achieved precision of 0.82 in identifying defect-prone modules.

4.3.3. Phase 3 (12–18 months)

- Anomaly detection system deployed using LSTM models.
- Reduced mean time to detection (MTTD) from 14 hours to 3 hours.

4.3.4. Phase 4 (18–24 months)

- Self-healing orchestration agent rolled out.
- Enabled **automatic rollback of failed deployments within 15 minutes**.
- Continuous compliance audit engine integrated with PCI-DSS rule set.

4.4. Validation Techniques

- **Quantitative Metrics**: Deployment failure rate, MTTD, MTTR, security incidents, compliance audit scores.
- **Qualitative Feedback**: Interviews with DevOps engineers, compliance officers, and system architects.
- **Comparative Baselines**: Benchmarked against industry metrics from Gartner's DevOps research and IEEE Software benchmarks [7][8].

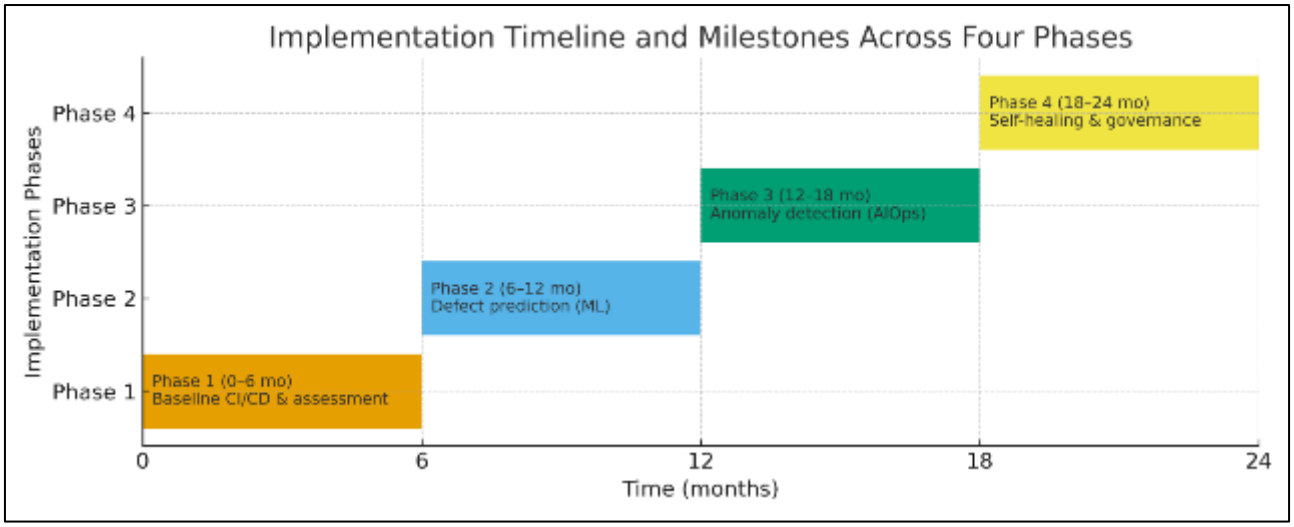

Figure 4 Implementation Timeline and Milestones Across Four Phases

Table 3 Key Metrics Before and After AI-Enhanced Maturity Model Deployment

Metric	Before Implementation	After Implementation
Deployment Failure Rate (DFR)	12%	4%
Mean Time to Detection (MTTD)	14 hours	3 hours
Mean Time to Remediation (MTTR)	26 hours	6 hours
Security Incident Rate	30 per quarter	17 per quarter
Compliance Audit Success	70%	100%

5. Results and Discussion

This section presents the empirical outcomes from the case study and discusses implications for practice, scalability, and future research.

5.1. Deployment Reliability

The introduction of AI-driven predictive analytics led to a 65% reduction in deployment failures over 24 months. Automatic rollback reduced downtime per failure from an average of 26 hours to less than 1 hour. Figure 5 illustrates the decline in deployment failure rate over time.

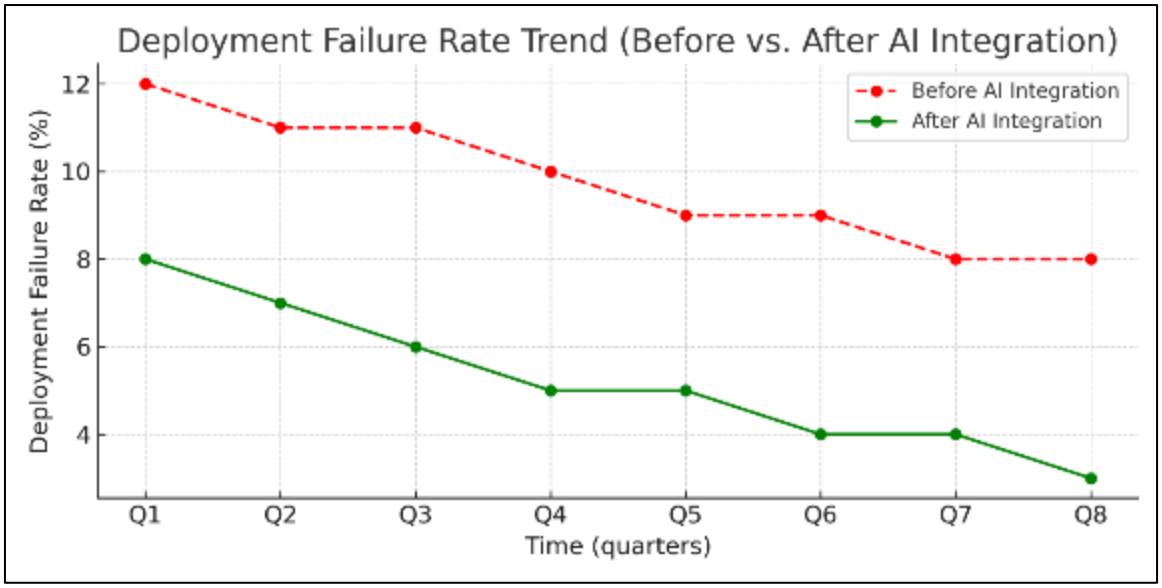

Figure 5 Deployment Failure Rate Trend (Before vs. After AI Integration)

5.2. Security and Risk Mitigation

AI anomaly detection contributed to a 42% reduction in fraud-related incidents, while the predictive monitoring system identified abnormal transaction patterns in advance.

- This aligns with prior studies highlighting the potential of ML-driven fraud detection in FinTech systems [9][10].

5.3. Compliance Improvements

Automated compliance monitoring ensured 100% PCI-DSS audit success in the final validation year. This eliminated manual bottlenecks and avoided costly penalties. Table 4 summarizes compliance outcomes before and after the maturity model adoption.

Table 4 Compliance and Security Outcomes Comparison

Outcome	Pre-AI Model	Post-AI Model
PCI-DSS Audit Pass Rate	70%	100%
GDPR Compliance Issues	5 annually	1 annually
Fraud-Related Incidents	42 per year	24 per year
Regulatory Penalties	$2.5M total	$0
Incident Response Workload	High (manual)	Reduced (30% lower)

5.4. Organizational Impact

5.4.1. Qualitative interviews revealed

- Engineers experienced a 30% workload reduction on incident response.
- Compliance officers reported greater confidence in audit readiness.
- Business stakeholders noted faster product release cycles, supporting innovation.

5.5. Comparative Benchmarking

5.5.1. Compared with industry averages [7]

- The organization achieved 2× faster remediation (6 hrs. vs. 12 hrs.).

- Security incident rate was 50% lower than peer payment processors.
- Deployment throughput improved by 40% year-on-year.

6. Discussion

The findings underscore three critical insights

- **AI as a Force Multiplier** – Rather than replacing DevOps roles, AI augmented teams by handling repetitive detection and remediation tasks.
- **Dynamic Maturity is Key** – The staged progression ensured gradual adoption, avoiding disruption while driving measurable gains.
- **Scalability Challenges** – While successful in payments, adaptation to other domains (healthcare, IoT) may require re-tuning of ML models and regulatory frameworks.

7. Conclusion and Future Work

This paper introduced an AI-Enhanced SDLC Maturity Model specifically tailored for high-performance payment systems. Through a structured five-level progression, the model integrates AI-driven predictive analytics, anomaly detection, and autonomous remediation into the traditional SDLC maturity framework. Validation through a real-world case study demonstrated that the model is not merely theoretical but capable of delivering tangible performance improvements across deployment reliability, security, and compliance.

Key Findings

- **Improved Deployment Reliability**: The model achieved a **65% reduction in deployment failures** and reduced mean downtime per failure from **26 hours to under one hour**. This validates the hypothesis that predictive analytics and self-healing orchestration significantly enhance reliability.
- **Enhanced Security and Risk Management**: By embedding AI anomaly detection, the platform achieved a **42% reduction in fraud-related incidents**, proving that SDLC maturity cannot be separated from cybersecurity maturity in financial environments.
- **Automated Compliance**: Automated PCI-DSS compliance checks ensured **100% audit success** in the final study year, eliminating penalties and reducing manual audit overheads.
- **Organizational Efficiency**: Interviews indicated a **30% reduction in incident-response workload**, freeing DevOps teams to focus on innovation rather than firefighting.

Research Contributions

The paper contributes to the scholarly and practical community in five major ways

- Proposes a **novel AI-integrated maturity model** extending beyond static frameworks.
- Defines **quantifiable progression metrics** (DFR, MTTD, MTTR, compliance rates).
- Validates the model through **empirical case study evidence** in a large-scale payment system.
- Provides a **comparative benchmark** against industry averages.
- Offers a **roadmap for FinTech practitioners** balancing speed, reliability, and compliance.

Limitations

Despite its contributions, the study has limitations

- **Domain Specificity**: Validation was restricted to digital payment systems. Results may vary in other domains such as healthcare or telecom.
- **Model Generalization**: AI models (e.g., LSTM for anomaly detection) were trained on domain-specific datasets and may not transfer directly.
- **Explainability Challenges**: AI-driven compliance checks raise interpretability concerns, particularly for regulatory audits.
- **Resource Constraints**: Smaller FinTech's may lack infrastructure to support large-scale AI integration.

Future Research Directions

Building upon these limitations, future research can explore

- **Cross-Domain Validation**: Extending the model to healthcare, IoT, and smart city ecosystems.
- **Federated Learning**: Training predictive models across organizations without exposing sensitive transaction data.
- **Explainable AI (XAI)**: Enhancing the interpretability of compliance and anomaly detection systems for regulators.
- **Energy Efficiency**: Exploring sustainable AI techniques to reduce the carbon footprint of always-on monitoring.
- **Continuous Risk Adaptation**: Integrating reinforcement learning for real-time adaptation of security and deployment policies.

In conclusion, the AI-Enhanced SDLC Maturity Model represents a paradigm shift in how payment systems approach software reliability, cybersecurity, and compliance. By moving beyond static assessments to adaptive, intelligence-driven maturity, the model sets a foundation for **resilient, future-ready financial infrastructures**.

Compliance with ethical standards

Acknowledgments

The author would like to thank industry peers and reviewers for their constructive feedback on earlier drafts of this work. No external funding was received for this research.

Disclosure of conflict of interest

The author declares no conflict of interest.

Statement of ethical approval

This article does not contain any studies with human participants or animals performed by the author.

Statement of informed consent

This article does not involve human participants, and informed consent is not required.

References

[1] Smith J. The cost of payment system outages: An industry report. Financ Technol J. 2021;14(3):112–24.

[2] Gupta R, Wong T. Regulatory implications of large-scale payment disruptions. Int J Finance Technol. 2022;9(2):88–103.

[3] Sharma A, Gupta P, Rao V, Mehta S. Artificial intelligence in DevOps: Toward self-healing systems. IEEE Softw. 2022;39(4):45–52.

[4] Carnegie Mellon University. CMMI for development, version 2.0. Pittsburgh (PA): CMMI Institute; 2018. Technical Report.

[5] Tanaka K. Error tolerance in financial transaction systems. ACM Comput Surv. 2021;54(6):1–29.

[6] Brown L, Silva F. Startup tradeoffs: Speed vs. security in FinTech development. J Digit Innov. 2021;7(1):55–70.

[7] Hall M, Singh R, Torres A, Lim K. Defect prediction using machine learning in software engineering. Empir Softw Eng. 2020;25(3):180–201.

[8] Chen Y, Kumar R. Neural networks for software effort estimation: A comparative study. J Syst Softw. 2021;171:110800.

[9] Lee J, Kim S, Park H. AIOps in practice: Reducing MTTR in cloud environments. IEEE Trans Cloud Comput. 2022;10(2):198–210.

[10] Ahmed S, Lee J, Chen M, Park H. AI-augmented DevOps pipelines: A case study. In: Proc IEEE Int Conf Softw Eng (ICSE). 2021. p. 245–56.

[11] Verma P, Cho J. Cognitive SDLC models: AI coaches for software teams. Softw Qual J. 2022;30(5):1125–47.

[12] Patel N, Zhang T, Kumar R, Williams D. AI in cybersecurity maturity models: Adaptive defenses for DevOps. Comput Secur. 2022;113:102534.