Sarcouncil Journal of Multidisciplinary

ISSN(Online): 2945-3445

Volume- 05| Issue- 07| 2025

Review Article **Received:** 05-06-2025 | **Accepted:** 28-06-2025 | **Published:** 17-07-2025

Engineering Secure Financial Portals: A Case Study in Credit Line Increase Process Digitization

Sandeepa Genne
Northwestern Polytechnic University, USA

Abstract: Digital transformation in financial services calls for strong security systems that strike a compromise between regulatory compliance and customer experience. Replacing outdated systems with contemporary cloud-native alternatives, this post shows the successful deployment of a secure web-based portal for credit line increase (CLI) processes at a large financial institution. The platform uses AWS Lambda for scalability, Spring Boot microservices for backend operations, React for dynamic frontend interfaces, multi-layered encryption, real-time identity verification, and automatic fraud detection systems to ensure financial rules compliance while keeping operational efficiency. The architectural design highlights domain-specific engineering philosophies customized for financial services needs. Implementation results show major increases in fraud prevention capacity, customer satisfaction indicators, and processing efficiency. The case emphasizes how careful integration of current technologies may completely transform traditional banking practices while preserving security integrity. Studies indicate that building a successful FinTech portal calls for thorough consideration of security systems, legal constraints, and user experience design. Beyond personal deployments, the ramifications provide financial institutions pursuing digital transformation projects with ideas for negotiating difficult security and compliance settings.

Keywords: FinTech security, microservices architecture, credit line management, digital banking transformation, secure portal engineering.

INTRODUCTION

An Overview of Financial Services' Digital Transformation

Over the previous ten years, the financial services sector has experienced a remarkable digital revolution that has changed how companies engage with clients and offer products. Changing consumer expectations, technical developments, and the great need for operational efficiency in an ever more competitive market have all propelled this evolution. Recent research has shown that smart and strong fintech software solutions have become quite effective in empowering digital banking services and boosting financial inclusion across many socioeconomic groups (Patel, A., & Satapathy, S. K. 2023). Beyond just digitalizing current procedures, this change is a complete reimagining of financial service distribution systems.

Secure Portals' Crucial Function in Contemporary Banking Infrastructure

Portals are the lifeblood of the modern banking system, the interface between financial institutions and their customers. They have to balance multiple competing demands - regulatory compliance, high security standards, user-friendly interfaces, and integration with existing systems. In cloud-based systems where data privacy and system security are a big concern for banks and other financial institutions using cloud infrastructure, this challenge is even more pronounced (Mahalle, A. *et al*., 2018). The architectural decisions made in building these portals have a big impact on corporate risk and customer trust.

Problem Statement: Legacy Credit Line Increase Processes and Their Limitations

Old-school banking shows its clunkiest side when it comes to handling credit line increases. Paperwork piles up, processes drag on, and applications bounce between departments like a game of hot potato. There's no visibility into where an application stands—it's like being transported back to the age of fax machines. The result? Missed opportunities, wasted resources, and frustrated customers. As for risk management, it's just as outdated—trying to spot fraud with legacy tools is like bringing a butter knife to a gunfight. Real-time decision-making? Not even close.

Goals and Scope of the Research

The creation and use of a secure online portal at a large financial institution is investigated in this paper, which also looks at the complete digitization of credit line increase procedures. The main goals include analyzing the security systems needed for safeguarding sensitive financial information, estimating the technical infrastructure required for safe financial portals, assessing how digital transformation affects customer happiness and operational efficiency, and pinpointing best practices for fusing contemporary technologies with already established banking infrastructure. Both technical implementation specifics and strategic issues for financial institutions engaging

***Corresponding Author:** Sandeepa Genne

DOI- https://doi.org/10.5281/zenodo.16031935

in comparable digital transformation projects are within the scope.

Brief Introduction to the Case Study Institution

The case study organization is a major banking firm that supports millions of clients spread over several geographical areas. The institution started an extensive digital transformation project facing growing pressure to modernize customer-facing services while still adhering to tight security and compliance guidelines. Because of its high customer interaction frequency and potential for major operational improvements, the credit line increase procedure was chosen as a pilot project. This project was strategically placed as a learning experience for more general digital transformation initiatives, thanks to the institution's dedication to using cloud-native technologies and microservices design.

Thesis Statement: How Secure Portal Engineering Can Revolutionize Traditional Banking Processes

According to this paper, if done appropriately with domain-specific considerations for financial services, secure portal design can completely transform conventional banking methods. Simultaneous financial institution gains in customer experience, operational efficiency, and risk management can be realized by way of deliberate architectural design, strong security execution, and judicious technological selection. Beyond mere technological deployment, the change includes organizational reorganization, legal adaptation, and the definition of new paradigms for financial service delivery in the digital age.

REVIEW OF LITERATURE AND THEORETICAL STRUCTURE

Evolution of Digital Banking Platforms and Customer Self-Service Portals

From basic online account viewing features, the development of digital banking systems has evolved to include thorough self-service ecosystems that let consumer's complete difficult financial transactions independently. Early implementations emphasized information display and basic transaction functionality; current platforms combine complex features, including real-time analytics, customized financial guidance, and automatic decision-making algorithms. Modern digital banking transformation methods highlight the need to provide uniform customer experiences across several channels while preserving operational efficiency and security integrity (IE Digital, 2022). This development mirrors more general technical improvements as well as shifting consumer expectations for financial services' immediacy, openness, and control.

Applications of Security Frameworks in Financial Technology

Financial technology security frameworks have developed to meet increasingly complex cyber threats while also allowing innovation and customer convenience. Multi-layered strategies combining artificial intelligence and data mining technologies for threat detection and prevention have replaced conventional perimeter-based security models (Bhargava, N. *et al*., 2021). These systems include authentication methods, encryption algorithms, anomaly detection systems, and continuous monitoring functions developed especially for financial settings. While reducing false positives that could impede legitimate client transactions, the integration of machine learning algorithms has enhanced the real-time detection of fraudulent activity.

Guidelines for Regulation Compliance

Financial institutions have to simultaneously negotiate compliance systems and complex legal frameworks across many countries. The Payment Card Industry Data Security Standards (PCI DSS) impose operational and technological standards on businesses that process payment card information, whereas the Sarbanes-Oxley (SOX) Act focuses on internal controls and the accuracy of financial reporting. The General Data Protection Regulation (GDPR) makes managing customer data protection and consent more difficult for businesses that operate in or serve European markets. These regulatory frameworks assist the operational systems, data management techniques, and architectural decisions made by digital banking networks taken collectively.

Prior Research on Banking Process Digitization

Academic and commercial research has thoroughly recorded several methods for digitalizing banking operations, hence highlighting both triumphs and obstacles in transformation projects. Studies continually emphasize the need for customer-centric design, perfect integration with current systems, and strong change management techniques. Studies show that successful digitizing projects demand a delicate balance between operational stability and technical innovation, with special attention to retaining service continuity throughout transition phases. The literature also underlines the essential part that employee

Publisher: SARC Publisher

engagement and organizational culture play in reaching sustainable digital transformation results.

Theoretical Underpinnings of Financial Secure System Design

Theoretical underpinnings for secure system design in finance come from several fields, including finance risk management, computer science, and information security. Important concepts are defense-in-depth techniques, zero-trust architecture models, and continuous verification approaches, assuming no implicit trust inside system limits. Rather than retrofitted additions, these conceptual frameworks stress the need to develop security solutions that are built into the system's architecture. Using these guidelines in financial situations calls for more thought on maintaining an audit trail, ensuring transaction integrity, and meeting regulatory compliance demands specific to the financial services industry.

Gap Analysis: The Need for Domain-Specific Engineering Solutions

Even with major progress in broad security and digital change plans, big holes still exist in meeting the special needs of financial services. Regular fixes often miss the mark on the specific rules, risk issues, and tricky operations that banks deal with. Studies show we need engineering methods that build in financial know-how from the start instead of trying to tweak general answers after they're set up (Bhargava, N. *et al*., 2021; IE Digital, 2022). This problem shows up in areas like handling transactions in real time, complex okay processes, and working with old bank systems, which are still key to daily work.

SYSTEM ARCHITECTURE AND TECHNICAL IMPLEMENTATION

Overview of the CLI Portal Architecture

Credit line increase portals need architectural designs that balance many technical needs while meeting financial sector limits. The design uses a multi-tier structure where display, business rules, and data layers work on their own, making it easier to build and fix parts. Small services make up the main structure, with each service having its own life cycle and update schedule. These design choices let teams change single parts without causing problems for the whole system. This is key when dealing with money transfers, and it must always be available.

Table 1: Technology Stack Components for CLI Portal Implementation (Santiago, R. & Goyal, R. 2025; Sbarski, P., & Kroonenburg, S. 2017)

Layer	Technology	Purpose	Key Features
Frontend	React	User Interface	Component-based, Virtual DOM, State Management
Backend	Spring Boot	Microservices	RESTful APIs, Service Discovery, Circuit Breakers
Serverless	AWS Lambda	Event Processing	Auto-scaling, Pay-per-use, Stateless Functions
Monitoring	CloudWatch	Observability	Metrics, Logs, Alerts, Dashboards
API Gateway	Spring Cloud Gateway	API Management	Routing, Rate Limiting, Authentication
Cache	Redis	Performance	In-memory Storage, Session Management
Database	PostgreSQL	Data Persistence	ACID Compliance, Replication, Backup

Backend Infrastructure: Spring Boot Microservices Design Patterns

Because of its extensive ecosystem and track record of dependability in business settings, Spring Boot has become the preferred platform for deploying microservices (Santiago, R. & Goyal, R. 2025). The credit assessment service, approval workflow engine, and notification dispatcher each function as autonomous microservices, communicating through well-defined interfaces. Domain boundaries align with business capabilities rather than technical considerations, ensuring that credit policy changes affect only relevant services. Circuit breaker patterns prevent cascading failures when downstream services experience issues, while service mesh technologies manage inter-service communication security and routing complexities.

Frontend Development: React-Based Dynamic User Interfaces

React's component architecture played a key role in building modular user interfaces that react to changes in backend state. The Virtual DOM reconciliation process cuts down on browser repaints during frequent updates, which is typical in financial apps where real-time data guides user choices. Strategies for component composition allow for code reuse across different parts of the portal while keeping distinct visual hierarchies for

Publisher: SARC Publisher

various user roles. To boost performance, the team put code splitting and dynamic imports into action. This reduced initial bundle sizes and improved time-to-interactive metrics, which are crucial to keep customers engaged.

Cloud Infrastructure: Using AWS Lambda for Serverless Computing

Serverless computing through AWS Lambda transforms traditional deployment models by eliminating server management overhead and enabling granular cost control (Sbarski, P., & Kroonenburg, S. 2017). Lambda functions execute discrete tasks such as document parsing, risk score calculation, and third-party API interactions. Event-driven invocation patterns align naturally with user-initiated actions in the credit line process. Despite the inherent latency issues of serverless architectures, consistent performance is ensured by cold start improvements, such as providing concurrency for key tasks. Because Lambda functions are stateless, careful session management techniques utilizing external storage systems are required.

Monitoring and Observability: CloudWatch Implementation

Good monitoring goes beyond simple uptime checks; it calls for full awareness of application behavior and corporate indicators. CloudWatch gathers logs from several microservices to allow event correlation over service boundaries during incident investigation. Custom metrics track domain-specific indicators like approval processing length and decision accuracy rates. Ranging from stakeholder alerts to scaling changes, alarm configurations set off automated responses to unusual patterns. Distributed tracing exposes request flows through the microservices maze, highlighting bottlenecks that conventional monitoring could miss.

Designing APIs and Integrating Them with Older Banking Systems

RESTful API design principles guide external interface specifications, though pragmatic deviations accommodate legacy system constraints. Message transformation layers translate between modern JSON payloads and legacy format requirements, often involving fixed-width records or XML structures. Asynchronous patterns using message queues decouple the responsive web portal from slower mainframe processing cycles. Compensating transaction patterns handle scenarios where legacy systems lack native rollback capabilities. Implementations of API gateways impose rate limitations and uniform security requirements on disparate backend systems.

Performance Optimization Strategies

User experience is immediately affected by database query performance; therefore, thorough index planning and query plan analysis are needed. Through event-driven invalidation, Redis caching maintains cache coherency while lowering database load for often-accessed reference data. For geographically distributed users, CDN deployment for static assets uses edge sites to help minimize latency. Connection pooling tuning based on seen usage patterns and garbage collecting optimization for JVM-based microservices constitute application-level optimizations. Load testing scenarios simulate peak usage periods, hence disclosing performance deterioration patterns that direct capacity planning decisions.

SECURITY ENGINEERING AND COMPLIANCE FRAMEWORK

Multi-layered Security Architecture

Financial sites call for deep defense approaches wherein network, application, and data layers simultaneously deploy security controls. Modern implementations use deep learning algorithms to find unusual access patterns (Sheth, H. S. 2022) and blockchain-based authentication systems. Network segmentation isolates vital processing components from public-facing interfaces, while application firewalls scan traffic patterns for possible exploitation attempts. Database encryption supplements network security, guaranteeing that compromised perimeter defenses cannot expose sensitive financial records. Such layered approaches admit that single-point security measures necessarily fall under complex attack scenarios.

Table 2: Multi-layered Security Framework Components (Sheth, H. S. 2022; Cui, M. *et al*., 2021)

Security Layer	Implementation	Protection Scope	Technology
Network	Firewall, VPC	Perimeter Defense	AWS Security Groups
Application	WAF, Input Validation	Code Injection, XSS	OWASP Standards
Authentication	Multi-factor, Biometric	Identity Verification	OAuth 2.0, SAML
Encryption	TLS 1.3, AES-256	Data Protection	HSM, Certificate Management
Behavioral	ML Models	Fraud Detection	Deep Learning Algorithms

Publisher: SARC Publisher

Audit	Immutable Logs	Compliance Tracking	Blockchain Integration

Data Encryption Protocols (At-rest and In-transit)

Beyond basic TLS implementations, encryption techniques for financial information include dynamic encryption methods that change with threat environments. Additional security layers for especially sensitive activities are provided by sophisticated cryptographic technologies, including chaotic sequence generation (Cui, M. *et al*., 2021). Hardware security modules are used by Atrest encryption for key management, hence preventing unapproved access even with a physical server compromise. Employing certificate pinning and mutual TLS authentication, transit encryption gets rid of man-in-the-middle attack channels. Key rotation schedules balance security demands against operational complexity, with automated processes reducing human error risks.

Identity Verification and Authentication Mechanisms

Through multifactor implementations integrating behavioral analytics and biometric markers, modern authentication goes beyond simple username-password combinations. Device fingerprinting generates distinct identifiers using hardware characteristics, browser settings, and network characteristics. Based on transaction features and past user trends, risk-based authentication dynamically alters verification needs. Passwordless authentication methods improve user experience through push notifications and cryptographic difficulties while lowering credential theft threats. Identity federation allows safe third-party integrations without revealing main authentication credentials.

Authorization and Role-based Access Control

Granular permission models show organizational structures and legal standards unique to financial activities. By including contextual elements like transaction amounts, time limits, and geographic restrictions, attribute-based access control broadens conventional role definitions. Temporal permissions allow temporary elevated privileges for particular activities without permanent role changes. Enforcement of segregation of duties lowers internal fraud concerns by stopping single users from finishing whole transaction chains. Privileges are changed by dynamic authorization based on adherence requirements and real-time risk assessments.

Fraud Detection Integration and Real-time Monitoring

Machine learning models identify variances that indicate fraudulent activity prior to completion by examining transaction patterns across several dimensions. Real-time scoring engines assess hundreds of risk elements within milliseconds, therefore balancing fraud prevention against consumer friction. Behavioral biometrics find account takeover attempts by monitoring mouse actions, navigation patterns, and typing styles. Integration with external threat intelligence improves internal detection capacity with industry-wide attack pattern recognition. Algorithms for minimizing false positives lower permissible transaction interruptions while keeping high fraud capture rates.

Compliance Mapping to Financial Regulations

Regulatory issues are a main driver of architectural choices in system design, which in turn requires that we have full alignment between technical controls and compliance requirements. We use automated compliance tools that check transactions against regulatory rules prior to processing, which in turn prevents violations that may result in large penalties. We put in audit trails that include the details required for regulatory audits while respecting data minimization. We have designed our cross-border transaction handling to include jurisdiction-specific requirements, which we adapt to regulatory differences in various operating regions. We do regular compliance assessments, which check for ongoing adherence as regulations change and as we make changes to the system.

Table 3: Regulatory Compliance Mapping (Mahalle, A. *et al*., 2018)

Regulation	Requirement Category	Technical Control	Implementation
PCI-DSS	Card Data Protection	Encryption, Tokenization	Vault Services
SOX	Financial Reporting	Audit Trails, Access Control	Immutable Logging
GDPR	Data Privacy	Consent Management, Data Deletion	Privacy API
AML	Anti-Money	Transaction Monitoring	Pattern Analysis

Publisher: SARC Publisher

	Laundering		
KYC	Identity Verification	Document Validation	AI-based Verification
Basel III	Risk Management	Capital Calculation	Real-time Analytics

Security Testing and Vulnerability Assessment Approaches

Continuous security validation involves the use of automated scanning tools as well as manual penetration testing, which is aimed at finding business logic vulnerabilities. Red team exercises are like practice sessions that simulate clever attack scenarios, thus helping you to find loopholes in your security that even regular testing may not be able to detect. Static code analysis looks for possible security holes in the development phase, thus saving money on the fixes as compared to when the issues are found in production. Dynamic application security testing checks the application while it is running to see how it behaves if it is under attack; hence, risks related to configuration and injection can be detected. Responsible disclosure programs provide rewards to external security researchers who are able to find vulnerabilities before bad guys use them."

RESULTS AND IMPACT ANALYSIS

Quantitative Metrics: Reduction in Processing Time

Improvements in processing times are essential success factors for financial services digital transformation projects. When compared to manual legacy procedures, the implementation of the CLI portal significantly decreased the end-to-end processing time. These enhancements result from the removal of interdepartmental handoffs that previously caused bottlenecks, automated decision engines, and parallel processing capabilities. Instant customer alerts take the place of conventional mail-based communications, and real-time data validation avoids downstream rework cycles. Application submission to initial response, full processing cycles, and customer notification delays are just a few of the time-based metrics that measurement systems monitor.

Customer Satisfaction Improvements and User Experience Metrics

Function of Quality Structured methods for converting client needs into quantifiable satisfaction metrics is offered by deployment strategies (Thompson, D. M. M., & Fallah, M. H. 1989). Reduced friction points, clear navigation patterns, and visible status tracking throughout the application process are examples of improvements to the user experience. Surveys of customer satisfaction show advancements in a number of areas, such as communication clarity, speed, and simplicity of use. Increased customer advocacy after portal adoption is shown by Net Promoter Scores. For started applications, behavioral analytics show higher completion rates and lower abandonment rates.

Fraud Detection Enhancement Statistics

Advanced fraud detection capabilities leveraging artificial intelligence demonstrate marked improvements over rule-based legacy systems. Machine learning models identify complex fraud patterns that traditional threshold-based systems overlooked, while maintaining acceptable false positive rates. Real-time scoring enables immediate intervention for high-risk applications rather than post-facto detection. Integration with industry-wide threat databases enhances pattern recognition capabilities beyond institutional boundaries. Performance analysis reveals improved detection accuracy across various fraud typologies, including identity theft, synthetic identities, and application manipulation attempts.

System Performance and Scalability Achievements

Modernizing infrastructure results in quantifiable gains in performance across important technical metrics. Architectural robustness is demonstrated by response time consistency under various load scenarios, and auto-scaling features manage demand spikes without degrading. Database query optimization and caching strategies reduce resource consumption per transaction. Microservices architecture enables independent scaling of system components based on actual usage patterns rather than peak capacity provisioning. System behavior under stress circumstances surpassing anticipated growth scenarios is validated by load testing.

Cost-Benefit Analysis of the Digital Transformation

Financial analysis reveals compelling returns on digital transformation investments through multiple value streams. Operational cost reductions stem from decreased manual processing requirements, reduced error rates requiring correction, and lower infrastructure costs through cloud adoption. Revenue enhancements result

Publisher: SARC Publisher

from increased application volumes enabled by improved customer experience and faster processing capabilities. Risk mitigation benefits manifest through enhanced fraud prevention and improved compliance adherence. Despite initial implementation investments, modern designs are favored in comparison to the total cost of ownership.

Operational Efficiency Gains

Increases in workforce productivity allow employees to shift from repetitive processing duties to more valuable customer engagement activities. Automated workflows provide uniform policy application across all applications while doing away with tedious manual tasks. Transparency in decision-making and thorough audit trails are advantageous for exception handling procedures. Errors in system synchronization and redundant data entry are decreased by integration efficiency. Digital workflows that standardize processes increase quality nd consistency, and lessen the need for new hires to receive training.

Comparative Analysis with Legacy System Performance

Direct comparisons between legacy and modern implementations reveal transformational improvements across multiple dimensions. Legacy batch processing constraints disappear with real-time processing capabilities, enabling immediate customer responses. Manual paper-based workflows requiring physical document handling contrast sharply with digital document management and automated verification. System availability improves from business-hours-only legacy access to continuous availability with planned maintenance windows. Error rates decline through automated validation and system-enforced business rules replacing manual checking procedures.

Table 4: Performance Metrics Comparison Framework (Thompson, D. M. M., & Fallah, M. H. 1989; Kuttiyappan, D., & Rajasekar, V. 2024)

Metric Category	Legacy System Characteristics	Modern Portal Characteristics	Improvement Focus
Processing	Batch-based, Manual Steps	Real-time, Automated	Speed, Efficiency
Availability	Business Hours Only	24/7 Access	Customer Convenience
Scalability	Fixed Capacity	Dynamic Auto-scaling	Demand Management
User Interface	Terminal/Paper-based	Web/Mobile Responsive	User Experience
Integration	Point-to-point	API-driven	Flexibility
Fraud Detection	Rule-based	AI-enhanced	Accuracy, Speed
Monitoring	Reactive	Proactive, Predictive	Issue Prevention

CONCLUSION

The digital change in the increase in credit line through safe portal implementation shows the transforming capacity of modern engineering practices in financial services. Successful integration of Microservices architecture, cloud-native technologies, and advanced security structure sets new benchmarks for customer-affected banking applications. This technological progress is fundamentally extended beyond the process of digitization for rehabilitation of how financial institutions interact with customers while maintaining regulatory compliance and safety integrity. The convergence of Spring Boot microservices, React-based interfaces, and AWS serverless computing creates scalable solutions that are favorable for developing market demands. Multinational security implementation addresses the contemporary danger landscape by enabling spontaneous user experiences by incorporating artificial intelligence and real-time fraud detection capabilities. The results validate the adoption of that strategic technology when aligned with domain-specific requirements, providing simultaneous improvement in operational efficiency, customer satisfaction, and risk management dimensions. Financial institutions pursuing similar changes should recognize that success requires a comprehensive architectural scheme, a strong security structure, and careful integration with the existing infrastructure. Implications extend into the ecosystem of financial services, establishing new expectations for digital service distribution and showing that the obstacles of the heritage system do not need to disrupt innovation when proper engineering solutions are implemented.

REFERENCES

1. Patel, A., & Satapathy, S. K. "Empowering digital banking services and enhancing financial inclusion using smart and robust fintech software solutions." *2023 World*

Publisher: SARC Publisher

Conference on Communication & Computing (WCONF). IEEE, (2023).
2. Mahalle, A., Yong, J., Tao, X., & Shen, J. "Data privacy and system security for banking and financial services industry based on cloud computing infrastructure." *2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design ((CSCWD))*. IEEE, (2018).
3. Bhargava, N., Bhargava, R., Rathore, P. S., & Agrawal, R. "Artificial Intelligence and Data Mining Approaches in Security Frameworks*"*. *John Wiley & Sons*, (2021).
4. IE Digital, "Three Strategies for Modernising Digital Banking," (2022). https://iedigital.com/wp-content/uploads/2022/09/ie_Modernising-Digital-Banking.pdf
5. Santiago, R. & Goyal, R. "Spring System Design in Practice: Build Scalable Web Applications Using Microservices and Design Patterns in Spring and Spring Boot," *Packt Publishing*, (2025), https://ieeexplore.ieee.org/book/10989054
6. Sbarski, P., & Kroonenburg, S. "Serverless architectures on AWS: with examples using Aws Lambda*"*. *Simon and Schuster*, (2017).
7. Sheth, H. S. K., Ilavarasi, A. K., & Tyagi, A. K. "Deep Learning, blockchain based multi-layered Authentication and Security Architectures." *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*. IEEE, (2022)
8. Cui, M., Zhang, C., Chen, Y., Zhang, Z., Wu, T., & Wen, H. "Multilayer dynamic encryption for security OFDM-PON using DNA-reconstructed chaotic sequences under cryptanalysis." *IEEE Access* 9 (2021): 18052-18060.
9. Thompson, D. M. M., & Fallah, M. H. "QFD-a starting point for customer satisfaction metrics." *IEEE International Conference on Communications, World Prosperity Through Communications*,. IEEE, (1989).
10. Kuttiyappan, D., & Rajasekar, V. "AI-enhanced fraud detection: Novel approaches and performance analysis." *AI-Enhanced Fraud Detection: Novel Approaches and Performance Analysis* (2024).

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

Cite this article as:
Genne, S. "Engineering Secure Financial Portals: A Case Study in Credit Line Increase Process Digitization" *Sarcouncil Journal of Multidisciplinary* 5.7 (2025): pp 563-570.

Publisher: SARC Publisher