European Journal of Computer Science and Information Technology,13(24),76-88, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Mobile Automation Architecture: A Cross-Industry Impact Analysis on Financial Services, Retail, and Healthcare Sectors

Charanpreet Singh Hora
Pune University, India

doi: https://doi.org/10.37745/ejcsit.2013/vol13n247688 Published May 20, 2025

Citation: Hora C.S. (2025) Mobile Automation Architecture: A Cross-Industry Impact Analysis on Financial Services, Retail, and Healthcare Sectors, *European Journal of Computer Science and Information Technology*,13(24),76-88

Abstract: *This article examines the transformative impact of mobile automation architecture across critical industries including banking, retail, healthcare, telecommunications, and travel sectors. The article explores how automation frameworks address industry-specific challenges while identifying universal principles applicable across sectors. Through analysis of implementation methodologies, security protocols, and performance optimization techniques, this article reveals how mobile automation serves as both a technical solution and strategic business enabler. The article demonstrates that while industries prioritize different aspects of mobile automation—financial services emphasize security and compliance, retail focuses on performance scalability, and healthcare prioritizes data privacy—successful implementations share common architectural approaches. This article contributes to the growing body of knowledge on digital transformation strategies by providing a comprehensive cross-industry analysis of mobile automation implementations, offering practitioners and researchers insights into effective architectural frameworks that balance industry-specific requirements with universal best practices.*

Keywords: Mobile automation architecture, cross-industry implementation, automated security testing, regulatory compliance, digital transformation

INTRODUCTION

Evolution of Mobile Applications in Business Operations

The landscape of business operations has undergone a significant transformation with the integration of mobile applications across various sectors. Mobile applications have evolved from simple utility tools to comprehensive business solutions that drive organizational growth and customer engagement [1]. This evolution has reshaped how businesses interact with their customers, manage internal processes, and deliver

services in industries including banking, retail, healthcare, and telecommunications. The shift toward mobile-centric business models have created new opportunities for operational efficiency while simultaneously introducing complex challenges related to performance, security, and user experience that must be addressed through systematic approaches to mobile application development and testing.

The Critical Role of Mobile Automation Architects

Mobile Automation Architects have emerged as essential stakeholders in the development and maintenance of mobile applications across industries. Research indicates how these specialists bridge the gap between business requirements and technical implementation by designing frameworks that ensure mobile applications meet quality standards while reducing time-to-market [2]. These architects develop strategies for automated testing that span the entire application lifecycle, from development to deployment and maintenance. Their expertise enables organizations to implement consistent testing methodologies that address industry-specific challenges while maintaining the agility required to adapt to changing market demands and technological advancements in the mobile space.

Growing Significance of Automated Testing for Mobile Platforms

Automated testing has become increasingly crucial as mobile applications grow in complexity and business criticality. The diversity of devices, operating systems, and network conditions presents substantial challenges for ensuring consistent application performance and user experience. Comprehensive automated testing frameworks allow organizations to validate application functionality across multiple platforms while identifying potential issues before they impact end users. This approach to quality assurance has become particularly important in industries where mobile applications handle sensitive data or critical functions, such as financial services and healthcare, where failures can have significant consequences for both businesses and their customers.

Research Scope and Objectives

This research examines the implementation and impact of mobile automation architecture across key industries, with particular focus on banking, retail, healthcare, telecommunications, and travel sectors. The study aims to identify both industry-specific challenges and common patterns in mobile automation implementation that transcend sectoral boundaries. By analyzing different approaches to mobile automation architecture, this research seeks to establish a comprehensive understanding of best practices that can be applied across industries while recognizing the unique requirements of each sector. The findings aim to provide practical insights for Mobile Automation Architects and organizational leaders seeking to enhance their mobile application quality assurance strategies in an increasingly mobile-centric business environment.

European Journal of Computer Science and Information Technology,13(24),76-88, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Theoretical Framework and Methodology

Defining Mobile Automation Architecture

Mobile automation architecture represents the structured approach to automating the testing and functionality validation of mobile applications across different platforms and devices. This architectural framework encompasses the tools, processes, and methodologies that enable organizations to implement systematic automation solutions for mobile applications [3]. The architecture typically includes multiple layers that address different aspects of mobile automation, from the infrastructure layer that manages device farms and simulators to the script layer that defines test cases and validation criteria. A comprehensive mobile automation architecture considers not only the technical implementation but also the integration with development processes, enabling continuous testing and delivery pipelines that align with modern software development practices.

Key Automation Frameworks and Technologies

The landscape of mobile automation is supported by diverse frameworks and technologies that address specific testing needs and use cases. These frameworks can be categorized based on their approach to interacting with mobile applications, their compatibility with different platforms, and their ability to integrate with existing development tools and processes. Popular open-source frameworks offer flexibility and customization options, while commercial solutions often provide enhanced capabilities for enterprise-scale implementation. The selection of appropriate frameworks depends on factors such as the complexity of the application under test, the required level of test coverage, and the technical expertise available within the organization. The technological ecosystem continues to evolve with innovations that address emerging challenges in mobile application testing.

Critical Success Factors in Cross-Industry Implementation

The successful implementation of mobile automation architecture across different industries relies on several critical factors that transcend specific technical approaches. These factors include organizational commitment to quality assurance, alignment between business objectives and testing strategies, and the establishment of clear governance models for automation initiatives. The adoption of mobile automation requires not only technological readiness but also cultural alignment that values quality and efficiency. Cross-industry implementation success depends on the ability to balance standardization for consistency with customization for industry-specific requirements. Organizations that achieve this balance can establish mobile automation as a strategic capability rather than merely a tactical solution for testing activities.

Evaluation Metrics for Automation Effectiveness

Measuring the effectiveness of mobile automation initiatives requires a structured approach to defining and tracking relevant metrics. These metrics should encompass both technical aspects, such as test coverage and execution efficiency, and business outcomes, such as reduced time-to-market and improved customer satisfaction [4]. A comprehensive evaluation framework might include indicators related to defect detection

efficiency, automation coverage across different test types, and the return on investment for automation initiatives. The selection of appropriate metrics depends on the specific objectives of the automation program and should align with broader organizational goals. Effective measurement not only demonstrates the value of automation but also provides insights for continuous improvement of the automation architecture.

Table 1: Implementation Framework Comparison [3, 4, 5]

Implementation Aspect	Traditional Approach	Mobile Automation Architecture	Key Benefits
Testing Strategy	Limited Manual Testing	Comprehensive Automation	Consistency & Coverage
Infrastructure	Physical Device Labs	Cloud-Based Device Farms	Scalability & Efficiency
Integration	Siloed Testing Phase	DevOps Pipeline Integration	Continuous Feedback
Measurement	Basic Pass/Fail Metrics	Evaluation Framework	Strategic Insight
Security Testing	Periodic Audits	Automated Validation	Continuous Risk Assessment

Financial and Banking Sector Applications

Security Automation Challenges and Solutions

The financial and banking sector faces unique security challenges in mobile application deployment due to the sensitive nature of financial data and transactions. Security automation in this domain must address vulnerabilities at multiple levels, including network communication, data storage, authentication mechanisms, and third-party integrations [5]. Common challenges include implementing secure communication protocols that protect data in transit while maintaining performance, automating penetration testing to identify potential vulnerabilities before deployment, and ensuring secure coding practices throughout the development lifecycle. Solutions have emerged that integrate security automation directly into the continuous integration and continuous deployment (CI/CD) pipeline, allowing financial institutions to detect security issues early in the development process. These automated approaches enable financial organizations to maintain robust security postures while accelerating their development cycles to meet market demands.

Regulatory Compliance Testing Methodologies

Financial institutions operate within strict regulatory frameworks that necessitate comprehensive compliance testing of mobile applications. These regulations vary by jurisdiction but typically address areas such as data privacy, information security, transaction monitoring, and customer due diligence. Automated compliance testing methodologies enable financial organizations to systematically validate adherence to

these complex regulatory requirements throughout the application lifecycle. These methodologies typically incorporate rule-based validation systems that check application behaviors against predefined compliance criteria. The integration of compliance testing into automated testing frameworks allows for continuous verification, reducing the risk of non-compliance and associated penalties. Financial organizations increasingly adopt risk-based approaches to compliance testing, focusing automation efforts on high-risk areas that have significant regulatory implications.

Real-Time Fraud Detection Systems Integration

The integration of real-time fraud detection systems with mobile banking applications represents a critical application of automation in the financial sector. These systems leverage advanced analytics to identify suspicious transactions or activities as they occur, requiring seamless integration with mobile application frameworks [6]. Automated testing for fraud detection integration must validate both technical implementation and functional effectiveness across diverse scenarios. Testing frameworks must simulate various fraud patterns to ensure detection mechanisms function correctly while minimizing false positives that could impact legitimate customer transactions. The real-time nature of these systems presents unique challenges for automation, requiring test environments that can accurately replicate production loads and response times. Successful implementation depends on close collaboration between fraud detection specialists, mobile application developers, and automation architects to ensure comprehensive test coverage.

Case Studies of Successful Implementation in Major Financial Institutions

Major financial institutions have demonstrated significant benefits from implementing comprehensive mobile automation architectures. These organizations have leveraged automation to address specific challenges in the banking sector while achieving broader business objectives related to customer experience and operational efficiency. Case studies reveal common patterns in successful implementations, including phased approaches that begin with high-value test cases before expanding to comprehensive coverage, cross-functional teams that combine domain expertise with technical skills, and adaptive frameworks that evolve with changing business requirements and technological capabilities. These implementations highlight how mobile automation can serve as a strategic enabler for financial institutions, supporting rapid innovation while maintaining the security and reliability essential in financial services. The most successful organizations establish clear governance structures for their automation initiatives, ensuring alignment with business priorities and continuous improvement based on measurable outcomes.

Table 2: Industry-Specific Mobile Automation Priorities [5, 6, 7, 8]

Industry	Primary Automation Focus	Key Challenges	Primary Success Metrics
Financial Services	Security Testing & Compliance	Real-time Fraud Detection	Security & Compliance Adherence
Retail	Performance Optimization	High-Traffic Load Handling	Transaction Completion & Response Time
Healthcare	Patient Data Security	Regulatory Compliance	Data Protection & Access Control
Telecommunications	Service Activation	Cross-Network Performance	Service Reliability
Travel	Multi-Language Support	Notification Reliability	Booking Completion & Consistency

Retail and Healthcare: Contrasting Implementation Approaches

Performance Optimization for High-Traffic Retail Scenarios

The retail sector presents unique challenges for mobile automation architecture, particularly during high-traffic periods such as sales events and holiday shopping seasons. Performance optimization in retail mobile applications requires automation frameworks that can simulate and validate application behavior under extreme load conditions [7]. These frameworks must test not only the application itself but also its integration with backend systems that manage inventory, payment processing, and order fulfillment. Effective automation strategies in retail environments focus on identifying performance bottlenecks through systematic load testing and continuous monitoring. Advanced testing approaches incorporate real-world usage patterns to create realistic test scenarios that reflect actual customer behaviors. Mobile automation architects in retail environments must balance the need for comprehensive performance validation with the rapid deployment cycles that characterize the industry, creating optimization strategies that maintain application responsiveness even during peak traffic periods.

Patient Data Security and Regulatory Compliance in Healthcare

Healthcare mobile applications handle highly sensitive patient information, requiring specialized approaches to automation that prioritize data security and regulatory compliance [8]. Unlike retail applications, healthcare solutions must adhere to stringent regulatory frameworks such as HIPAA in the United States and similar regulations globally. Automation frameworks in healthcare must incorporate validation of consent management, data encryption, access controls, and audit logging to ensure compliance with these regulations. Testing methodologies must verify that patient data remains protected throughout the application lifecycle, including during data transmission, storage, and processing. Mobile automation in healthcare extends beyond functional testing to include comprehensive security validation, ensuring that

applications maintain robust protection against potential vulnerabilities that could compromise patient information or violate regulatory requirements.

Cross-Platform Consistency Testing Strategies

Both retail and healthcare sectors face challenges in maintaining consistent user experiences across diverse mobile platforms, yet their approaches to cross-platform testing reflect their different priorities. Retail organizations typically emphasize visual consistency and transactional accuracy across platforms to maintain brand identity and ensure conversion optimization. Healthcare applications, however, focus on functional consistency to ensure that critical features such as medication management and appointment scheduling work reliably regardless of the user's device. Automation frameworks addressing cross-platform consistency must validate applications across different operating systems, screen sizes, and hardware capabilities. Effective strategies incorporate visual testing tools that can identify inconsistencies in user interface elements while confirming that core functionality behaves as expected across platforms. Mobile automation architects in both sectors must develop testing frameworks that balance comprehensive coverage with efficient execution to support rapid development cycles.

Privacy Protection Methodologies

Privacy protection represents a critical concern in both retail and healthcare mobile applications, though with distinct emphases reflecting sector-specific requirements. Retail applications must protect customer purchase history, payment information, and preference data, while healthcare applications manage more sensitive medical records and personal health information. Automation frameworks for privacy testing validate that applications collect only necessary data, implement appropriate consent mechanisms, and maintain proper data segregation. These frameworks must verify that privacy controls function as intended across various user scenarios and application states. Testing methodologies include automated validation of privacy policy implementation, data minimization practices, and user consent management. Mobile automation architects must develop comprehensive testing strategies that address privacy considerations at every level of the application, from user interface components to backend data storage and processing systems.

Telecommunications and Travel Industries: Network Considerations

Service Activation Automation Strategies

The telecommunications and travel industries rely heavily on service activation processes that must be seamless, reliable, and scalable across diverse network conditions. Service activation automation in these sectors requires sophisticated frameworks that can validate complex provisioning workflows and integration points between multiple systems [9]. In the telecommunications sector, service activation involves configuring network elements, updating customer profiles, and activating features across distributed infrastructure. Travel industry applications must similarly coordinate service activation across booking systems, payment processors, and service provider networks. Automation strategies in both sectors must address the challenge of testing service activation across varied network topologies and conditions,

ensuring that customers can successfully activate and use services regardless of their location or connectivity status. Effective automation frameworks incorporate comprehensive validation of the entire service activation lifecycle, from initial request through confirmation and usage verification.

Network Performance Simulation Techniques

The reliability of mobile applications in telecommunications and travel industries depends significantly on their ability to function across diverse network conditions. Network performance simulation techniques enable organizations to systematically test applications under various bandwidth, latency, and stability scenarios [10]. These simulation frameworks create controlled testing environments that replicate real-world network conditions, allowing developers to identify potential issues before they impact customers. Advanced simulation approaches incorporate geographic distribution patterns that reflect the actual movement of users across different network coverage areas. This is particularly important for travel applications, where users frequently transition between network types and coverage zones. Mobile automation architects must develop testing strategies that encompass both ideal and degraded network conditions, validating application behavior and implementing appropriate fallback mechanisms for scenarios with limited connectivity.

Multi-Language and Multi-Currency Testing Frameworks

Both telecommunications and travel industries serve global audiences, necessitating robust approaches to testing applications across multiple languages and currencies. Multi-language testing frameworks must validate not only text translation but also localization elements such as date formats, number formatting, and cultural preferences. Similarly, multi-currency testing must verify accurate conversion, display, and processing of different currencies throughout the application. Automation challenges in this domain include maintaining test efficiency across numerous language and currency combinations while ensuring comprehensive coverage of localization features. Effective frameworks implement parameterized testing approaches that separate test logic from localization data, allowing efficient validation across multiple markets. Mobile automation architects in these industries must collaborate closely with localization specialists to ensure that automated tests accurately reflect language and currency requirements for each target market.

Real-Time Notification Systems Reliability

Real-time notification systems play a crucial role in both telecommunications and travel mobile applications, providing users with timely updates about service status, account changes, and travel itineraries. Testing these notification systems requires automation frameworks that can validate message delivery, content accuracy, and timing across various channels such as push notifications, SMS, and in-app alerts. The reliability of these systems becomes particularly critical during service disruptions or travel changes, when timely communication can significantly impact customer experience. Automation strategies must verify notification behavior under various application states and network conditions, ensuring that critical messages are delivered even in challenging connectivity scenarios. Mobile automation architects must develop comprehensive testing approaches that validate the entire notification pipeline, from event

triggering through delivery confirmation, while accounting for platform-specific implementation differences in notification handling.

Future Trends and Emerging Technologies

AI and Machine Learning in Mobile Automation

Artificial intelligence and machine learning represent transformative forces in the evolution of mobile automation architecture. These technologies are reshaping how organizations approach test case generation, execution prioritization, and defect analysis. AI-powered automation systems can identify patterns in application behavior and test results, enabling more intelligent test selection and execution strategies. Machine learning algorithms can analyze historical test data to identify high-risk areas that require more intensive testing, optimizing resource allocation while maintaining comprehensive coverage. Natural language processing capabilities are enabling the creation of test cases from user stories and requirements documents, streamlining the transition from specification to validation. As these technologies mature, mobile automation frameworks will increasingly incorporate self-healing mechanisms that can adapt to application changes without manual intervention, reducing maintenance overhead and accelerating development cycles.

Predictive Testing Methodologies

Predictive testing methodologies leverage data analytics to anticipate potential issues before they manifest in production environments [11]. These approaches analyze historical defect patterns, code changes, and user behavior to identify areas of the application with elevated risk, allowing organizations to focus testing efforts where they will provide the greatest value. Predictive models can estimate defect density in different application components, prioritize test cases based on their likelihood of revealing defects, and forecast potential performance bottlenecks under projected user loads. The integration of predictive capabilities into mobile automation frameworks enables more efficient test planning and execution, particularly in complex applications with extensive feature sets. As organizations accumulate more comprehensive testing data, the accuracy and utility of these predictive models will continue to improve, further enhancing the effectiveness of mobile automation initiatives.

DevOps Integration Strategies

The convergence of mobile automation with DevOps practices is reshaping how organizations approach the entire application lifecycle. Integrated DevOps pipelines incorporate automated testing as a continuous activity rather than a discrete phase, enabling immediate feedback on code changes and reducing time-to-market for new features. Mobile automation frameworks designed for DevOps environments emphasize integration with continuous integration/continuous delivery (CI/CD) tools, containerization technologies, and infrastructure-as-code solutions. These integrations enable the creation of consistent, reproducible test environments that accurately reflect production conditions. Advanced DevOps implementations incorporate feature flags and canary deployments that rely on automated testing to validate new functionality with limited user exposure before full release. The evolution of mobile automation within

DevOps ecosystems is driving the development of more collaborative workflows that unify development, testing, and operations perspectives throughout the application lifecycle.

Cloud-Based Mobile Automation Solutions

Cloud-based platforms are emerging as essential enablers for scalable mobile automation across diverse device types and operating systems. These solutions provide access to extensive device farms that would be impractical for most organizations to maintain internally, enabling comprehensive testing across the fragmented mobile ecosystem. Cloud platforms offer elastic resources that can accommodate variable testing loads, from routine regression testing to intensive pre-release validation. The distributed nature of cloud infrastructure facilitates geographically dispersed testing that can validate application performance across different regions and network conditions. Integration capabilities with existing development and testing tools allow organizations to leverage cloud resources while maintaining their established workflows and practices. As cloud-based mobile automation solutions continue to evolve, they will increasingly incorporate specialized capabilities for performance testing, security validation, and accessibility compliance, providing comprehensive testing solutions that address the full spectrum of mobile application quality requirements.

Table 3: Emerging Technologies Impact [11, 12]

Emerging Technology	Current State	Projected Impact	Application Potential
AI/ML in Testing	Early Adoption	Self-Healing Tests	High Across Industries
Predictive Testing	Limited Implementation	Risk-Based Optimization	High in Finance & Healthcare
DevOps Integration	Varied Maturity	Continuous Testing	High Across Industries
Cloud-Based Solutions	Growing Adoption	Enhanced Coverage	High Across Industries
Knowledge Transfer	Emerging Practice	Cross-Industry Learning	High with Adaptation

Research Implications and Recommendations

Industry-Specific Best Practices

The research findings reveal distinct patterns of effective mobile automation implementation across different industry sectors. In financial services, best practices emphasize security-first automation frameworks that integrate compliance validation throughout the testing lifecycle. Retail organizations benefit most from performance-focused approaches that prioritize user experience under variable load conditions. Healthcare implementations demonstrate the importance of privacy-centric testing methodologies that validate both regulatory compliance and data protection measures. Telecommunications and travel sectors show strongest results when implementing network-resilient automation frameworks that

account for variable connectivity scenarios. These industry-specific approaches reflect the unique business priorities and regulatory environments of each sector, suggesting that mobile automation architects should tailor their strategies to address industry-specific challenges rather than pursuing generic implementation models. Organizations should evaluate and adapt these practices according to their specific business context while maintaining core quality assurance principles.

Cross-Industry Knowledge Transfer Opportunities

Despite industry-specific differences, significant opportunities exist for cross-industry knowledge transfer in mobile automation methodologies [12]. Financial sector approaches to security automation can benefit healthcare organizations facing similar data protection challenges. Retail expertise in performance optimization under high-traffic conditions offers valuable insights for travel applications managing seasonal demand fluctuations. The research identifies several domains where cross-industry learning presents particular value, including test environment management strategies, continuous integration approaches, and test data generation methodologies. Successful knowledge transfer requires contextual adaptation rather than direct transplantation of practices, with particular attention to how industry-specific requirements might necessitate modification of approaches. Organizations should establish structured mechanisms for identifying, evaluating, and adapting practices from other sectors, potentially through industry forums, collaborative research initiatives, or engagement with consultants having cross-sector experience.

Organizational Implementation Guidelines

Effective implementation of mobile automation architectures requires a structured organizational approach that addresses both technical and cultural dimensions. The research findings support a phased implementation model that begins with high-value test cases before expanding to comprehensive coverage. Organizations should establish clear governance structures that define roles, responsibilities, and decision-making processes for mobile automation initiatives. Cross-functional teams combining domain expertise with technical skills demonstrate superior outcomes compared to siloed approaches that separate business and technical considerations. Executive sponsorship proves essential for securing necessary resources and addressing organizational resistance to automation adoption. Implementation roadmaps should incorporate both quick wins to demonstrate value and longer-term strategic initiatives that build lasting capabilities. Organizations must also develop appropriate metrics frameworks that measure both technical effectiveness and business impact, enabling data-driven refinement of automation strategies over time.

Research Limitations and Future Directions

This research provides valuable insights into mobile automation implementation across industries but contains several limitations that suggest directions for future investigation. The study focused primarily on larger organizations with established mobile presences, leaving questions about how findings might apply to smaller organizations or those early in their mobile journey. The rapidly evolving technology landscape creates challenges for establishing enduring best practices, suggesting a need for longitudinal studies that track implementation effectiveness over time. Future research should explore how emerging technologies

such as edge computing and 5G networks might reshape mobile automation requirements and approaches. Additional investigation into the relationship between mobile automation maturity and business outcomes would provide valuable insights for organizations seeking to justify investment in advanced automation capabilities. Comparative studies of automation approaches across different geographic regions could reveal how cultural and regulatory factors influence implementation success. The field would also benefit from more detailed examination of skill development and team structures that enable effective mobile automation implementation in different organizational contexts.

CONCLUSION

This thorough article analysis of mobile automation architecture across key industries demonstrates the strategic significance of systematic automation approaches in enabling organizations to deliver secure, reliable, and high-performing mobile applications. The article reveals both industry-specific implementation patterns and universal principles that transcend sectoral boundaries, providing a foundation for effective mobile automation strategies in diverse business contexts. Financial services organizations benefit from security-focused automation frameworks, retail from performance-oriented approaches, healthcare from privacy-centric methodologies, and telecommunications from network-resilient testing strategies. Despite these differences, opportunities for cross-industry knowledge transfer exist, particularly in test environment management, continuous integration, and test data generation. As mobile applications continue to evolve as critical business enablers, organizations must develop structured implementation approaches that address both technical and cultural dimensions while remaining adaptable to emerging technologies and changing market requirements. The future of mobile automation will increasingly incorporate artificial intelligence, predictive testing methodologies, seamless DevOps integration, and cloud-based solutions, further enhancing the strategic value of automation as a cornerstone of digital excellence across industries.

REFERENCES

[1] Tairov I., Donchev I (2023) , "Mobile Applications Use for Business Growth," in 2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T). https://ieeexplore.ieee.org/document/10238668/footnotes#footnotes

[2] Leonardo Militano; Anastasios Zafeiropoulos, et al.(2021) , "AI-powered Infrastructures for Intelligence and Automation in Beyond-5G Systems," in 2021 IEEE Globecom Workshops (GC Wkshps), . https://ieeexplore.ieee.org/document/9682117

[3] Seth P., Rane N., et al. (2018) "Uberisation of Mobile Automation Testing," in 2017 International Conference on Intelligent Computing and Control Systems (ICICCS),. https://ieeexplore.ieee.org/abstract/document/8250706

[4] Capitán L.(2018) ; Birgit Vogel-Heuser, "Metrics for Software Quality in Automated Production Systems as an Indicator for Technical Debt," in 2017 13th IEEE Conference on Automation Science and Engineering (CASE). https://ieeexplore.ieee.org/abstract/document/8256186

[5] Traynor P., Butler K, et al. (2017) , "FinTechSec: Addressing the Security Challenges of Digital Financial Services," in IEEE Security & Privacy, 15 (5) https://ieeexplore.ieee.org/abstract/document/8055676

[6] Shaymardanov T.A., Vavrenyuk A.B. (2022) , "Development of an Anti-fraud System with Real-Time Analytics," in 2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), April 20. https://ieeexplore.ieee.org/abstract/document/9755691

[7] Guo A.;Yuan C., et al.(2018) , "Research on SDN/NFV Network Traffic Management and Optimization based on Big Data and Artificial Intelligence," 18th International Symposium on Communications and Information Technologies (ISCIT), 27 December. https://ieeexplore.ieee.org/abstract/document/8587985

[8] Jaigirdar F.T., Rudolph C., et al.(2021) , "Risk and Compliance in IoT-Health Data Propagation: A Security-Aware Provenance-Based Approach," in 2021 IEEE International Conference on Digital Health (ICDH), 08 November . https://ieeexplore.ieee.org/abstract/document/9581214

[9] Inam R., Karapantelakis A., et al. (2015) , "Towards Automated Service-Oriented Lifecycle Management for 5G Networks," in 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA), October 26. https://ieeexplore.ieee.org/document/7301660

[10] Suzuki Y., Yokota T, et al. (2016) , "Performance Improvement of Large-Scale Interconnection Network Simulator by Using GPU," in 2015 Third International Symposium on Computing and Networking (CANDAR), March 7. https://ieeexplore.ieee.org/abstract/document/7425438

[11] Sarro F. (2018), "Predictive Analytics for Software Testing," in IEEE Transactions on Software Engineering, 02. https://ieeexplore.ieee.org/document/8452801/references#references

[12] Massey A.P., Montoya-Weiss M.(2022), "A Knowledge Exchange Perspective of Technology Transfer," in Proceedings of the Thirtieth Hawaii International Conference on System Sciences, August 6. https://ieeexplore.ieee.org/document/661576