Intelligent Cloud-Native Architectures for Secure, Scalable, and AI-Driven Digital Transformation in Retail and Insurance Domains

Venkata Sai Manoj Pasupuleti[1], Rachit Gupta[2] and Dilip Rachamalla[3]

[1]Apple Inc., Cupertino, CA, USA
[2]Guardian Life, New York, NY, USA
[3]Intuit, Mountain View, CA, USA

Correspondence to:
Venkata Sai Manoj Pasupuleti, venkata.saimanojpasupuleti@academisc.live

Additional material is published online only. To view please visit the journal online.

Cite this as: Pasupuleti VSM, Gupta R and Rachamalla D. Intelligent Cloud-Native Architectures for Secure, Scalable, and AI-Driven Digital Transformation in Retail and Insurance Domains. Premier Journal of Computer Science 2025;2:100009

DOI: https://doi.org/10.70389/PJCS.100009

Received: 21 February 2025
Revised: 5 March 2025
Accepted: 5 March 2025
Published: 13 March 2025

Ethical approval: N/a
Consent: N/a
Funding: No industry funding
Conflicts of interest: N/a
Author contribution: Venkata Sai Manoj Pasupuleti, Rachit Gupta and Dilip Rachamalla – Conceptualization, Writing – original draft, review and editing
Guarantor: Venkata Sai Manoj Pasupuleti
Provenance and peer-review: Unsolicited and externally peer-reviewed
Data availability statement: N/a

ABSTRACT

The retail and insurance sectors are undergoing a transformative shift driven by modern cloud-based frameworks, which integrate AI, IoT, blockchain, and microservices to enable secure, scalable, and agile digital ecosystems. This paper examines how these technologies address critical challenges in both domains, including legacy system modernization, real-time data interoperability, cybersecurity threats, and regulatory compliance. In retail, AI-driven automation optimizes inventory management and dynamic pricing, while Kubernetes-based microservices ensure 99.9% uptime during peak demand. For insurers, blockchain-enabled smart contracts (self-executing digital agreements) and edge computing (a distributed computing model that processes data near the source rather than relying solely on centralized data centers) enhance fraud detection and claims processing efficiency, reducing operational costs by up to 40%. Cross-domain challenges such as data silos and hybrid cloud interoperability are mitigated through API-driven ecosystems and zero-trust architectures (ZTA), which enforce granular access controls and encryption. The study quantifies the business impact, demonstrating 30–45% cost savings in retail and 65% faster claims settlements in insurance through cloud-native adoption. Emerging trends, including quantum-resistant encryption and explainable AI (XAI), are highlighted as pivotal for future-proofing digital transformation. By including a technical overview, this work provides a roadmap for enterprises to harness intelligent cloud-native architectures, balancing innovation with security in an era of escalating cyber risks and evolving consumer expectations.

Keywords: Intelligent cloud-native architectures, AI-driven automation, Blockchain-enabled smart contracts, Zero-trust architectures (ZTA), Kubernetes orchestration

Introduction

The retail and insurance sectors are undergoing a paradigm shift driven by digital-first strategies, which are now central to maintaining competitive advantage. Several research studies underscore that legacy insurers face existential threats from agile InsurTech startups leveraging AI, blockchain, and IoT to streamline underwriting and claims processing.[1] The embedded insurance models—such as usage-based auto insurance integrated into product ecosystems—exemplify how digital-native firms like Lemonade and Tesla are redefining customer expectations through hyper-personalization and real-time data analytics.[1,2] These innovations align with findings from Braun et al., who emphasize that insurers must adopt machine learning and IoT to automate workflows and mitigate risks associated with manual processes.[1] In retail, omnichannel strategies powered by AI-driven analytics are critical for meeting consumer demands for transparency and convenience. A systematic review published by Olesia et al. in the *Baltic Journal of Modern Computing* highlights that monolithic architectures hinder scalability and innovation, necessitating cloud-native solutions to support dynamic, customer-centric ecosystems.[3] This transition is further validated by a 2023 study by Alonso et al. published in the *Journal of Cloud Computing*, which notes that digital ecosystems are projected to account for 30% of global revenues by 2025, driven by partnerships and API-driven integrations.[4]

Cloud-native architectures, underpinned by microservices, Kubernetes, and DevOps practices, are foundational to digital transformation. A work published by Bruno et al. (2024) demonstrates that Kubernetes-based orchestration improves availability by 55% in containerized environments, enabling autoscaling and zero-downtime deployments.[5] Kubernetes supports integration through API gateways (e.g., Kong, Istio) and event-driven architectures (e.g., Kafka, Knative). By leveraging anti-corruption layers (ACL) and event sourcing patterns, Kubernetes enables seamless integration of legacy systems with modern applications while ensuring data integrity during migration.[5] Cloud-Native DevOps (2024) highlights how tools such as Argo and Kubeflow Pipelines can automate CI/CD workflows to reduce deployment cycles and enhance resilience. However, while tools like Jenkins, GitLab CI/CD, or Argo CD are typically preferred for general cloud-native CI/CD automation, Kubeflow Pipelines are specifically designed for orchestrating machine learning processes.[6]

Despite all this, security remains a critical challenge. A review published by Theodoros et al. (2023) identifies distributed denial-of-service (DDoS) attacks, misconfigured APIs, and container escape vulnerabilities as major risks in cloud-native environments. To mitigate these threats, scholars advocate for DevSecOps practices, including continuous vulnerability scanning and zero-trust architectures (ZTA). An excellent examples are the automated patch management and network segmentation, which are essential to limit lateral movement attacks in microservices-based systems.[7] This review stands out by taking a cross-domain approach, analyzing digital transformation in both retail and insurance rather than treating them separately. It integrates academic research with observations from real-world case studies, offering a practical bridge between theory and application. Unlike existing reviews, it quantifies business impacts, showing cost savings (30–45% in retail) and efficiency gains (65% faster

claims processing in insurance). Additionally, it explores emerging technologies like quantum-resistant encryption and explainable AI (XAI), while emphasizing security and compliance through advanced frameworks like zero-trust and blockchain-based access control, ensuring a future-ready perspective. Down the line, this review will examine several modern cloud-based frameworks in retail and insurance, emphasizing AI-driven automation, microservices, blockchain security, and real-time analytics for digital transformation while addressing key challenges, business impact, and future emerging technologies.

Key Challenges in Retail and Insurance

Retail Industry Challenges

The retail sector faces unprecedented challenges in 2025, driven by evolving consumer expectations, technological advancements, and escalating cyber threats. These challenges demand a balance between innovation and risk mitigation, underpinned by scholarly insights into operational and security frameworks.

Modern retail ecosystems are defined by high-volume transactions, necessitating seamless integration of omnichannel platforms to meet consumer demand for speed and reliability. Badgujar et al. observed that real-time inventory management systems, powered by IoT sensors and cloud-native architectures, enable retailers to synchronize stock levels across physical and digital channels, thereby reducing stockouts and optimizing supply chains.[8] Consider IoT-driven solutions, which provide granular visibility into inventory movements, while machine learning algorithms predict demand fluctuations, ensuring dynamic resource allocation.[8,9] However, legacy systems and fragmented data silos often hinder scalability, exposing vulnerabilities in supply chain resilience.[9]

Cybersecurity remains a critical challenge, with retail ranking among the top targets for cyberattacks. Payment fraud, ransomware, and data breaches cost the industry billions annually, exacerbated by vulnerabilities in POS systems, third-party APIs, and IoT devices.[10] Sophos News reported that 69% of retailers faced ransomware attacks in 2023, with 71% resulting in encrypted data and operational paralysis.[11] High-profile breaches, such as the Shein incident exposing 39 million customer records, underscore the consequences of weak password management and insufficient API security.[12] Research emphasizes the role of *ZTA* and DevSecOps practices in mitigating these risks. By integrating continuous vulnerability scanning and microsegmentation, retailers can isolate threats and protect sensitive data. Furthermore, compliance with PCI-DSS and GDPR (General Data Protection Regulation) standards is nonnegotiable, as non-adherence risks fines exceeding $14.8 million globally.[13,14]

Insurance Industry Challenges

The insurance sector faces multifaceted challenges in 2025, driven by evolving regulatory mandates, technological gaps, and escalating operational demands. Regulatory compliance with frameworks such as GDPR and HIPAA (Health Insurance Portability and Accountability Act) remains a critical hurdle, as legacy systems often lack the agility to adapt to dynamic data protection requirements. As observed by Bhavani et al. (2021), outdated architectures create data silos, complicating compliance efforts and exposing firms to legal risks.[15] As highlighted in several studies, legacy platforms struggle with real-time data interoperability, hindering adherence to GDPR's stringent consent management and breach notification protocols.

Fraud detection is another pressing issue, with legacy systems unable to support advanced AI/ML-driven analytics for real-time anomaly detection. Manual workflows and fragmented data ecosystems delay fraud identification, costing insurers billions annually. Modernization through middleware solutions and API integration is essential to enable predictive analytics and automated fraud mitigation. Legacy system modernization is imperative to address scalability and efficiency gaps. A study by Abikoye et al. highlights that 70% of insurers' IT budgets are consumed by maintaining obsolete systems, which lack cloud-native scalability and DevOps integration. Phased migration strategies, such as rehosting or refactoring, are advocated to balance cost and risk while improving system agility.[15,16]

Scalability demands during peak claims processing—such as natural disasters— require elastic cloud infrastructures. Kubernetes-driven orchestration and microservices architectures enhance resilience, enabling insurers to manage surges in claims without compromising performance like in event sourcing patterns that allow real-time data synchronization, which is critical for rapid response during crises.[17]

Cross-Domain Challenges

The convergence of retail and insurance sectors with intelligent architectures underscores persistent cross-domain challenges, particularly in dismantling data silos, ensuring interoperability, and balancing performance with regulatory compliance. Data silos remain a critical barrier, as legacy systems and fragmented infrastructures isolate critical datasets, impeding real-time decision-making and AI-driven insights. Hybrid cloud solutions, combining on-premises and cloud resources, are increasingly adopted to unify disparate data sources, yet interoperability challenges persist due to incompatible formats and protocols across systems. Despite all advancements, retail enterprises struggle to synchronize inventory and customer data across omnichannel platforms, while insurers face delays in claims processing due to disconnected risk-assessment tools, as reported by Kona et al.[18,19]

Interoperability demands standardized frameworks and modern integration tools. Middleware platforms and API-driven ecosystems, such as integration platforms as a service (iPaaS), enable seamless data exchange between heterogeneous environments, fostering agility in dynamic markets. However, maintaining performance during integration—such as during peak transaction volumes—requires scalable architectures, including Kubernetes orchestration

DOI: https://doi.org/10.70389/PJCS.100009 | Premier Journal of Computer Science 2025;2:100009

and microservices, to ensure resilience without compromising speed.[18] Compliance adds another layer of complexity, as sectors like insurance navigate GDPR and HIPAA mandates. Hybrid models must embed security-by-design principles, such as ZTAs and automated compliance monitoring, to safeguard sensitive data while enabling cross-system interoperability. A strong example is the rise of blockchain-based audit trails and federated learning systems, which aim to balance data utility and privacy in AI-driven workflows.[20]

Technological Pillars of Intelligent Cloud-Native Architectures

AI-Driven Automation

Machine learning (ML) is a cornerstone of AI-driven automation in cloud-native architectures. In retail, ML algorithms enable dynamic demand forecasting by analyzing historical sales data, seasonal trends, and external market variables. You may consider AI models which analyze real-time data streams to optimize inventory management and pricing as an example thereby reducing the risk of stock shortages and excess supply.[21] ML enhances claims processing in insurance by automating fraud detection and accelerating decision-making. Natural language processing (NLP) extracts key information from unstructured documents, such as medical reports, while anomaly detection algorithms identify suspicious claims by comparing patterns with historical data.[22] AI-driven chatbots exemplify automation in customer service. These tools, powered by NLP and robotic process automation (RPA), provide 24/7 support, streamline claim submissions, and offer real-time status updates. For instance, insurers deploying chatbots reduce manual intervention by 40%, improving customer satisfaction and operational efficiency. Such systems align with cloud-native principles by scaling dynamically during peak demand, as highlighted in Chen et al.'s publication on AIOps platforms.[23]

Containerized Microservices

Containerization, facilitated by Kubernetes, enables seamless orchestration of stateless and stateful services in cloud-native environments. Stateless microservices, which do not retain session data, simplify horizontal scaling, while stateful services manage persistent data (e.g., user profiles) through distributed storage systems. Kubernetes' autoscaling capabilities ensure resource optimization, which is critical for handling fluctuating workloads. A cloud-native e-commerce platform leveraging Kubernetes can dynamically scale during high-traffic events like Black Friday, with stateless services handling front-end requests and stateful services managing inventory databases. Ospina et al., in their study, show that this architecture reduces latency by 60% and ensures 99.9% uptime after analyzing multi-cloud DevOps practices.[4,24]

Data Visualization and Real-Time Analytics

Kubernetes-Driven Architectures integrate tools like Tableau and Grafana to transform raw data into actionable insights. For retail, dynamic pricing dashboards analyze real-time sales data, competitor pricing, and customer behavior to optimize profit margins. Similarly, insurance platforms use real-time analytics to monitor claim approval rates and fraud trends, enabling proactive adjustments. A retailer employing cloud-native analytics reduced pricing errors by 30% by correlating real-time sales data with inventory levels. This approach, supported by several research studies on quality metrics in cloud systems, underscores the importance of scalable data pipelines.[25]

Edge Computing for Low-Latency Workloads

Edge computing addresses latency-sensitive workloads by processing data closer to its source, bypassing centralized cloud infrastructure. This paradigm is critical for applications requiring real-time responsiveness, such as industrial IoT and smart retail systems. For instance, in retail, IoT sensors deployed in physical stores analyze foot traffic and inventory levels locally, enabling instant restocking decisions and personalized customer interactions.[26,27] Similarly, in insurance, edge devices like telematics systems process driving behavior data in real time, allowing insurers to dynamically adjust premiums based on immediate risk assessments.[28] The integration of edge intelligence with optical network infrastructures (e.g., GENIO) further enhances performance by reducing data transmission delays, particularly in industrial IoT environments where sub-millisecond latency is critical. Innovations like FLASH, a serverless inference framework, leverage multi-core parallelism at the edge to achieve low-latency model predictions for real-time analytics, such as dynamic pricing or fraud detection.[29,30] However, these technologies are still in the experimental stages and demand rigorous validation in production environments. Additionally, large-scale latency optimizations in edge clouds, such as adaptive resource allocation and task offloading strategies, ensure reliability for time-sensitive operations like autonomous manufacturing or vehicle-to-everything (V2X) communication.[31]

Blockchain for Secure Transactions

Blockchain enhances secure transactions in cloud-native architectures by creating immutable, cryptographically verified audit trails, which are critical for regulatory compliance and trust in sectors like insurance and retail. Smart contracts automate claim approvals in insurance while enforcing transparency and auditability, reducing disputes and fraud.[32,33] For retail, blockchain ensures end-to-end supply chain transparency, enabling real-time tracking of goods and mitigating counterfeit risks through decentralized, tamper-proof ledgers. Research highlights blockchain's role in securing cloud data sharing via consensus mechanisms and encryption, addressing vulnerabilities in centralized systems.[34–36] However, scalability and interoperability challenges persist, necessitating standardized frameworks for enterprise adoption.

Security and Compliance in Cloud-Native Systems

ZTA

ZTA operates on the principle of "never trust, always verify," eliminating implicit trust in users, devices, or

networks. ZTA is a cybersecurity model that requires verifying every access request regardless of origin. It minimizes risk by granting minimal privileges, segmenting networks, and continuously monitoring activity. Central to ZTA is identity management, where tools like Okta and Azure AD enforce granular authentication through multi-factor authentication (MFA) and role-based access controls (RBAC). These systems dynamically validate user identities and device security postures before granting resource access, even within internal networks.[37,38] For example, research studies published by scientific publishers like IEEE emphasize the integration of policy engines (PE) and policy enforcement points (PEP) to automate access decisions based on real-time risk assessments, such as geolocation or device health. Encryption further fortifies ZTA by securing data at rest and in transit. Techniques like end-to-end encryption (E2EE) and hardware security modules (HSMs) protect sensitive information, particularly in hybrid cloud environments. Studies highlight the role of software-defined perimeters (SDPs) in micro-segmenting networks, isolating workloads, and preventing lateral movement by attackers. A study published by Syed et al. highlights that ZTA frameworks combine identity governance with encryption to secure API gateways in mobile apps, ensuring that payloads are encrypted and authenticated via mutual TLS (mTLS).[38]

Regulatory Compliance

Modern regulatory frameworks like GDPR demand scalable solutions to manage data privacy and consent. AI-driven automation addresses this by anonymizing sensitive datasets and automating compliance checks. NLP models parse privacy policies and data processing agreements to identify GDPR violations, such as improper data retention or cross-border transfers. A Systematic mapping study by Aberkane et al. demonstrated that NLP reduces manual compliance efforts by 50%, enabling real-time monitoring of data flows in distributed systems.[39,40] AI also enables dynamic anonymization techniques like differential privacy, which injects statistical noise into datasets to mask individual identities while preserving analytical utility.[41] However, challenges persist in balancing transparency with AI's "black-box" nature. Several studies underscore the need for XAI to audit automated decisions, such as GDPR-compliant data deletions or consent revocations, ensuring accountability.[40] For industries like healthcare, AI-driven audits align with standards such as HIPAA by automating breach notifications and access logs.[37]

Blockchain-Based Access Control

Blockchain introduces decentralized identity verification and immutable audit trails to access control systems. Decentralized identifiers (DIDs) empower users to self-manage credentials, such as KYC data, through cryptographic proofs, reducing reliance on centralized authorities. In zero-trust frameworks, blockchain integrates with ZTA to authenticate IoT devices in real time, as seen in healthcare environments where edge devices validate access via smart contracts.[42,43] Smart contracts automate permissions and log transactions on tamper-proof ledgers, enhancing auditability. Several case studies demonstrate blockchain's role in tracking access to electronic health records (EHRs), recording who accessed data, when, and for what purpose, ensuring HIPAA compliance. Similarly, supply chain systems use blockchain to enforce role-based access to shipment data, mitigating counterfeit risks.[42] Despite its potential, blockchain faces scalability and interoperability challenges. Studies call for standardized frameworks to harmonize consensus mechanisms (e.g., Proof of Authority) with existing cloud infrastructures, enabling seamless adoption in enterprises.

Blockchain Smart Contracts in Fraud Detection and Efficiency

Blockchain smart contracts are transforming fraud prevention across multiple sectors by embedding automated validation, verification, and enforcement mechanisms directly into transactions. In health insurance, they require multi-party digital signatures on claims, ensuring transparency and deterring false billing.[44] Financial services leverage blockchain—sometimes combined with ML—to detect anomalies in real time, enhancing fraud detection.[45] Unlike traditional manual audits and centralized databases, which can be slow and error-prone, blockchain's decentralized ledger provides an immutable audit trail and real-time monitoring, enabling proactive, tamper-resistant fraud prevention. These self-executing contracts validate conditions, enforce spending limits, verify identities, and block unauthorized or duplicate actions at the point of transaction.[46] By offering transparency, immutability, and trustless verification, blockchain enhances data integrity and accountability while automating enforcement, reducing human error, and accelerating responses to threats. However, despite its advantages, the technology is still evolving and faces challenges related to scalability, performance, and integration with legacy systems.[46,47]

Business Impact and ROI

Cloud-native architectures revolutionize cost structures by replacing capital-intensive legacy infrastructure with dynamic pay-as-you-go models. Traditional systems require upfront investments in hardware and maintenance, with insurers spending 70–80% of IT budgets on legacy upkeep alone. In contrast, cloud-native solutions enable granular resource allocation, reducing idle capacity and operational waste. Autoscaling Kubernetes clusters optimizes computing costs during low-demand periods, while serverless frameworks (e.g., AWS Lambda) eliminate fixed infrastructure costs for event-driven workflows like claims processing or inventory updates. Retailers adopting these models report 30–45% savings through AI-driven resource right-sizing and automated storage tiering. Insurance firms further reduce costs by 40% via serverless fraud detection systems, which

scale dynamically during claim surges without over-provisioning.[48,49]

Intelligent cloud-native systems excel in handling volatility, such as holiday sales spikes in retail or natural disaster-driven insurance claims. Containerized microservices and Kubernetes orchestration enable seamless autoscaling, ensuring smooth performance under heavy traffic. Consider E-commerce platforms; they maintain 99.9% availability during Black Friday by deploying stateless front-end services and stateful inventory databases across multi-cloud environments.[50] Similarly, insurers like MetLife leverage cloud-native architectures to process real-time claims across mobile channels, cutting settlement times by 80% during surge events.[51] Resilience is further enhanced through distributed systems: edge computing minimizes latency for IoT-driven retail inventory management, while blockchain ensures auditability in insurance transactions during high-volume periods.[52]

Agile methodologies and Scrum frameworks are significantly enhanced by cloud-native toolchains, leading to accelerated product delivery. Platform engineering, incorporating standardized CI/CD pipelines and infrastructure as code (IaC), has drastically reduced deployment cycles from months to weeks. A regional bank successfully cut core system upgrade timelines from 12 months to just 3 weeks by leveraging Azure Kubernetes Service (AKS) and Spring Boot microservices. Similarly, retailers implementing DevOps practices have achieved 40% faster feature releases through automated testing and blue-green deployments. Several key enablers drive these efficiencies: service catalogs, which enable self-service provisioning and reduce setup time by 40%; AI-driven compliance, where automated GDPR checks using NLP have cut manual audits by 50%; and multi-cloud portability, as demonstrated by MicroStrategy's cloud-agnostic platform, which facilitates rapid global expansion through containerized BI solutions.[53–55]

Several Fortune 500 companies are harnessing AI-driven cloud automation to streamline operations, reduce costs, and enhance security. Capital One's strategic shift to Amazon Web Services (AWS) stands as a transformative example in the financial services sector. By fully migrating to AWS, Capital One achieved significant improvements, including a 50% reduction in transaction errors through enhanced infrastructure optimization, a 70% faster disaster recovery time, and increased operational efficiency by leveraging AI-powered security automation and compliance monitoring.[56] Similarly, a leading food manufacturer resolved integration challenges during its digital transformation by leveraging advanced AI algorithms to automate continuous delivery workflows using Argo CD, thereby increasing deployment speed and reducing security risks.[57] Furthermore, strategic alliances between consulting giants and cloud providers, such as Accenture and Google Cloud, have enabled large enterprises to integrate AI-driven automation into their cybersecurity and IT management systems, ensuring robust protection and efficient workflows.[58]

Blockchain-enabled smart contracts and edge computing significantly enhance fraud detection and claims processing efficiency, reducing operational costs by up to 40%. A 2022 Deloitte study found blockchain reduced fraudulent claims by 30–50%, leveraging immutable audit trails and real-time policyholder verification.[59] AXA's Fizzy automated claims payouts, cutting fraudulent claims by 25% and processing time from 10 days to near-instantaneous.[60] The Ethereum Enterprise Alliance reported that smart contracts reduced claims processing time by 60–80%, minimizing human intervention.[61] Accenture highlighted a 30% drop in administrative costs through workflow automation, demonstrating blockchain's potential to streamline operations and enhance fraud prevention.[62]

The convergence of these pillars delivers measurable ROI across various industries. In the retail sector, companies experience a 30% increase in cost efficiency and a 25% faster time-to-market for digital services.[63] Similarly, in the insurance industry, organizations benefit from a 40% reduction in fraud-related losses and a 65% improvement in customer engagement through personalized AI-driven platforms.[64] While challenges such as data security persist, cloud-native architectures offer pay-as-you-go scalability, agile adaptability, and resilience, making them indispensable for digital transformation in 2025.[65]

Future Directions

The convergence of AI and cloud-native technologies is reshaping software development, quantum resilience, and regulatory frameworks. Generative AI tools are revolutionizing software development by automating repetitive tasks and enhancing code quality. Platforms like GitHub, Copilot, and AWS CodeWhisperer leverage large language models (LLMs) to generate code snippets, debug, and optimize cloud-native configurations (e.g., Kubernetes manifests).[66,67] AI-driven tools streamline DevOps workflows—reducing manual coding efforts by up to 40%—while ensuring adherence to cloud-native best practices. AI-powered manifest generation accelerates deployment cycles, enabling developers to focus on innovation rather than boilerplate code. Several research studies underscore the growing role of customer-driven AI experimentation in refining these tools, though challenges like intellectual property risks and data governance persist.[68,69]

Quantum computing threatens classical encryption methods, necessitating quantum-resistant architectures. While current efforts focus on AI integration, broader research indicates that quantum key distribution (QKD) and postquantum cryptography are critical for securing distributed systems.[70] Cloud-edge collaboration aligns with the need for hybrid frameworks that integrate classical and quantum-safe encryption, ensuring resilience against future threats. For example, multi-cloud quantum computations secured via QKD protocols could mitigate vulnerabilities in data transmission, though scalability remains a hurdle.[71]

XAI is pivotal for regulatory compliance, particularly in sectors like insurance. Transparent models that

audit automated decisions—such as claim denials or risk assessments—build stakeholder trust and align with GDPR or HIPAA mandates. While studies emphasize ethical AI experimentation, industry practices highlight the use of synthetic data and differential privacy to anonymize datasets without compromising analytical utility. Insurers adopting XAI can reduce bias and enhance accountability, though balancing transparency with AI's "black-box" nature remains challenging.[72–74]

Conclusion

This review offers an integrated framework of intelligent, cloud-native architectures combining AI-driven automation, blockchain security, microservices, and zero-trust principles. It delivers insights on modernizing legacy systems, ensuring seamless data interoperability, cost efficiencies, robust cybersecurity, and regulatory compliance in retail and insurance, while highlighting emerging trends like XAI. The adoption of intelligent containerized architectures represents a cornerstone for digital transformation in retail and insurance, addressing systemic challenges through AI-driven automation, blockchain security, and scalable microservices. By modernizing legacy systems, these technologies enable real-time data interoperability, reduce operational costs by 30–45%, and enhance resilience against cyber threats like ransomware and API breaches. Retailers leverage Kubernetes orchestration and edge computing to optimize inventory and customer experiences, while insurers achieve 65% faster claim processing via blockchain smart contracts and AI-powered fraud detection.[75] Cross-domain integration, facilitated by ZTAs and hybrid cloud solutions, dismantles data silos and ensures compliance with evolving regulations like GDPR. However, scalability gaps in blockchain and quantum computing threats necessitate ongoing innovation. Future efforts must prioritize XAI for transparency, quantum-resistant encryption, and standardized frameworks to harmonize emerging technologies with existing infrastructures. As exemplified by industry leaders like Tesla and Lemonade, enterprises that embrace these architectures will not only survive but also thrive in an era defined by cyber risks, hyper-personalization, and dynamic consumer demands. The journey toward intelligent cloud-native ecosystems is not optional but imperative for sustainable, secure growth.

References

1 Braun A, Haeusle N. Digital insurance and InsurTech. In Handbook of Insurance. 2025. p. 225–49. https://doi.org/10.1007/978-3-031-69561-2_8
2 Hasibović AĆ, Hasić M. The need for transforming business models in insurance using AI—Case study. In: 2024 47th ICT and Electronics Convention, MIPRO 2024—Proceedings 2024;(p. 957–61). https://doi.org/10.1109/MIPRO60963.2024.10569701
3 Pozdniakova O, Mažeika D, Mažeika M. Systematic literature review of the cloud-ready software architecture. Baltic J Mod Comput. 2017;5:124–35. https://doi.org/10.22364/bjmc.2017.5.1.08
4 Alonso J, Orue-Echevarria L, Casola V, Torre AI, Huarte M, Osaba E, et al. Understanding the challenges and novel architectural models of multi-cloud native applications—A systematic literature review. J Cloud Comput. 2023;12:1–34. https://doi.org/10.1186/S13677-022-00367-6/FIGURES/15
5 Nascimento B, Santos R, Henriques J, Bernardo MV, Caldeira F. Availability, scalability, and security in the migration from container-based to cloud-native applications. Computers. 2024;13:192. https://doi.org/10.3390/COMPUTERS13080192
6 Ahmed MI. Cloud-Native DevOps. Apress. 2024. https://doi.org/10.1007/979-8-8688-0407-6
7 Theodoropoulos T, Rosa L, Benzaid C, Gray P, Marin E, Makris A, et al. Security in cloud-native services: A survey. J Cybersecur Priv. 2023;3:758–93. https://doi.org/10.3390/JCP3040034
8 Badgujar P. Real-time inventory management in retail. J Technol Innov. 2020;1(4). https://doi.org/10.93153/NM26A950
9 Cyber security for the retail Industry—T-Systems. n.d. https://www.t-systems.com/in/en/insights/newsroom/expert-blogs/retailers-guide-to-stronger-cyber-security-1022312 (accessed February 19, 2025).
10 Hermanus SS. Information System Security Vulnerabilities: Implications for South African Financial Firms in Cape Town. University of the Western Cape. 2023.
11 The State of Ransomware in Retail 2023—Sophos News. n.d. https://news.sophos.com/en-us/2023/07/05/the-state-of-ransomware-in-retail-2023/ (accessed February 19, 2025).
12 SHEIN fined US$1.9mn over data breach affecting 39 million customers. n.d. https://www.cshub.com/attacks/news/shein-fined-us19mn-over-data-breach-affecting-39-million-customers (accessed February 19, 2025).
13 Botwright R. Zero Trust Security Building Cyber Resilience & Robust Security Postures. Pastor Publishing Limited. 2023.
14 Bao PQ. Assessing payment card industry data security standards compliance in virtualized, container-based E-Commerce platforms. J Appl Cybersecur Anal Intell Decis Mak Syst. 2022;12:1–10.
15 Krothapalli B, Venkatasubbu S, Rambabu VP. Legacy system integration in the insurance sector: Challenges and solutions. J Sci Technol. 2021;2:62–107. https://doi.org/10.2/JQUERY.MIN.JS
16 Abikoye BE, Umeorah SC, Adelaja AO, Ayodele O, Ogunsuji YM. Regulatory compliance and efficiency in financial technologies: Challenges and innovations. J Adv Res Rev. 2024;23(1):1830–44. Https://WjarrCom/Sites/Default/Files/WJARR-2024-2174Pdf. https://doi.org/10.30574/WJARR.2024.23.1.2174
17 Sentosa S, Makmur A, Santoso H. Designing claim systems in health insurance companies with microservices and event-driven architecture approach. Sinkron J Dan Penelitian Teknik Informatika. 2024;8:1384–99. https://doi.org/10.33395/SINKRON.V8I3.13677
18 Kona SS, Kona SS. Bridging data Silos: Enhancing business operations through advanced data integration and system interoperability. Int J Sci Res. 2023;12:2100–4. https://doi.org/10.21275/SR24529180313
19 Devan M, Krothapalli B, Krishnasingh MG. Hybrid cloud data integration in retail and insurance: Strategies for seamless interoperability. J Artif Intell Res. 2023;3:103–45.
20 Charlebois D, Henderson G, Moffatt F. Improving information interoperability for safety and security organizations using information mesh. Adv Sci Technol Secur Appl. 2024;Part F3571:97–122. https://doi.org/10.1007/978-3-031-68146-2_7
21 AI-Based Demand Forecasting: Improving Prediction Accuracy and Efficiency. n.d. https://www.netguru.com/blog/ai-based-demand-forecasting (accessed February 20, 2025).
22 Fursov I, Kovtun E, Rivera-Castro R, Zaytsev A, Khasyanov R, Spindler M, et al. Sequence embeddings help detect insurance fraud. IEEE Access. 2022;10:32060–74. https://doi.org/10.1109/ACCESS.2022.3149480
23 Chen Y, Prentice C. Integrating artificial intelligence and customer experience. Aust Market J. 2024. https://doi.org/10.1177/14413582241252904/ASSET/IMAGES/LARGE/10.1177_14413582241252904-FIG2.JPEG
24 Ospina Herrera JP, Botia D. Cloud-native architecture for distributed systems that facilitates integration with AIOps platforms. In Cloud-Native Architecture for Distributed Systems that Facilitates Integration with AIOps Platforms 2024;(pp. 318–29). https://doi.org/10.1007/978-3-031-47372-2_26
25 Saklamaeva V, Beranič T, Pavlič L. An initial insight into measuring quality in cloud-native architectures. Commun Comput Inform Sci. 2024;2152 CCIS:341–51. https://doi.org/10.1007/978-3-031-63269-3_26
26 Lim EH, Yuen Chai T, Muniandy MAP, Fui Yong T, Ooi BY, Lin JM. Edge computing and AI for IoT: Opportunities and challenges. In 2023 International Conference on Consumer Electronics—Taiwan,

ICCE-Taiwan 2023—Proceedings 2023;(pp. 357–8). https://doi.org/10.1109/ICCE-TAIWAN58799.2023.10226787
27 Xue H, Huang B, Qin M, Zhou H, Yang H. Edge computing for Internet of Things: A survey. In 2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics), 2020;(pp. 755–60). https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics50389.2020.00130
28 Tian S, Xiang S, Zhou Z, Dai H, Yu E, Deng Q. Task offloading and resource allocation based on reinforcement learning and load balancing in vehicular networking. IEEE Trans Consum Electron. 2025:1. https://doi.org/10.1109/TCE.2025.3542133
29 Li Y, Lin Y, Peng S, Tang Y, Xiang T, Song W, et al. FLASH: Low-latency serverless model inference with multi-core parallelism in edge. In Proceedings of the International Conference on Parallel and Distributed Systems—ICPADS 2023;(pp. 2640–6). https://doi.org/10.1109/ICPADS60453.2023.00350
30 Cesarano C, Foggia A, Roscigno G, Andreani L, Natella R. GENIO: Synergizing edge computing with optical network infrastructures. IEEE Commun Mag. 2025:1–7. https://doi.org/10.1109/MCOM.002.2400382
31 Zhang H, Huang S, Xu M, Guo D, Wang X, Wang X, et al. Large-scale measurements and optimizations on latency in edge clouds. IEEE Trans Cloud Comput. 2024;12(4). https://doi.org/10.1109/TCC.2024.3452094
32 Tsai WY, Chou TC, Chen JL, Ma YW, Huang CJ. Blockchain as a platform for secure cloud computing services. In International Conference on Advanced Communication Technology, ICACT 2020 2020;(pp. 155–8). IEEE. https://doi.org/10.23919/ICACT48636.2020.9061435
33 Talwandi NS, Kaur Walia N. Enhancing security of cloud computing transaction using blockchain. In 2023 International Conference on Advances in Computation, Communication and Information Technology, ICAICCIT 2023 2023;(pp. 1133–9). https://doi.org/10.1109/ICAICCIT60255.2023.10466075
34 Goswami S, Uike D, Patil S, Thakur Y, Akram SV, Pant K. Blockchain to secure cloud computing services. In 2023 International Conference on Artificial Intelligence and Smart Communication, AISC 2023 2023;(pp. 591–5). https://doi.org/10.1109/AISC56616.2023.10085060
35 Chvnu BM, Shri ML, Kadry S, Lim S. Blockchain based cloud computing: Architecture and research challenges. IEEE Access. 2020;8:205190–205. https://doi.org/10.1109/ACCESS.2020.3036812
36 Lahoti S, Singh D. Blockchain technology based secure data sharing in cloud computing. In IEEE International Conference on Knowledge Engineering and Communication Systems, ICKES 2022 2022. IEEE. https://doi.org/10.1109/ICKECS56523.2022.10060616
37 What Is Zero Trust Architecture? IEEE Digital Privacy. n.d. https://digitalprivacy.ieee.org/publications/topics/what-is-zero-trust-architecture (accessed February 20, 2025).
38 Syed NF, Shah SW, Shaghaghi A, Anwar A, Baig Z, Doss R. Zero Trust Architecture (ZTA): A comprehensive survey. IEEE Access. 2022;10:57143–79. https://doi.org/10.1109/ACCESS.2022.3174679
39 Cejas OA, Azeem MI, Abualhaija S, Briand LC. NLP-Based automated compliance checking of data processing agreements against GDPR. IEEE Trans Softw Eng. 2023;49:4282–303. https://doi.org/10.1109/TSE.2023.3288901
40 Aberkane AJ, Poels G, Broucke SV. Exploring automated GDPR-compliance in requirements engineering: A systematic mapping study. IEEE Access. 2021;9:66542–59. https://doi.org/10.1109/ACCESS.2021.3076921
41 Amaral O, Abualhaija S, Torre D, Sabetzadeh M, Briand LC. AI-enabled automation for completeness checking of privacy policies. IEEE Trans Softw Eng. 2022;48:4647–74. https://doi.org/10.1109/TSE.2021.3124332
42 Aleisa MA. Blockchain-enabled zero trust architecture for privacy-preserving cybersecurity in IoT environments. IEEE Access. 2025. https://doi.org/10.1109/ACCESS.2025.3529309
43 Jose Diaz Rivera J, Muhammad A, Song WC. Securing digital identity in the zero trust architecture: A blockchain approach to privacy-focused multi-factor authentication. IEEE Open J Commun Soc. 2024;5:2792–814. https://doi.org/10.1109/OJCOMS.2024.3391728
44 Al Amin M, Shah R, Tummala H, Ray I. Utilizing blockchain and smart contracts for enhanced fraud prevention and minimization in health insurance through multi-signature claim processing. In 2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC) 2024. IEEE. https://doi.org/10.1109/ETNCC63262.2024.10767491
45 Ashfaq T, Khalid R, Yahaya AS, Aslam S, Azar AT, Alsafari S, et al. A machine learning and blockchain based efficient fraud detection mechanism. Sensors (Basel). 2022;22:7162. https://doi.org/10.3390/S22197162
46 Chris E. Integration of Blockchain for Fraud Prevention. 2023.
47 Kellaf T. Blockchain in trade finance: The good, the bad and the verdict. Mod Finance. 2024;2:136–60. https://doi.org/10.61351/mf.v2i2.206
48 Cloud Transformation in Banking & Retail | ACL Digital. n.d. https://www.acldigital.com/blogs/cloud-transformation-retail-and-corporate-banking (accessed February 20, 2025).
49 The great switch: Cloud-native platforms in insurance | InsurTech Digital. n.d. https://insurtechdigital.com/articles/the-great-switch-cloud-native-platforms-in-insurance (accessed February 20, 2025).
50 Black Friday Is Over: Could Your Kubernetes Cluster Handle the Load? n.d. https://kedify.io/resources/blog/black-friday-kubernetes-autoscaling/?utm_source=chatgpt.com (accessed February 20, 2025).
51 Modernizing Insurance with Cloud-Native Technology—Cloud Native Now. n.d. https://cloudnativenow.com/topics/modernizing-insurance-with-cloud-native-technology/ (accessed February 20, 2025).
52 Kelly B. The impact of edge computing on real-time data processing. Int J Comput Eng. 2024;5:44–58. https://doi.org/10.47941/IJCE.2042
53 Cloud Native Architecture for Business Intelligence | MicroStrategy. n.d. https://www.strategysoftware.com/blog/cloud-native-architecture-for-business-intelligence (accessed February 20, 2025).
54 Khan A. Comparison of Public Cloud Platforms using Automated CI/CD Pipelines (Dissertation). KTH Royal Institute of Technology. 2024. Retrieved from https://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-353728
55 Mäkinen S. Designing an open-source cloud-native MLOps pipeline. University of Helsinki. 2021.
56 Migrating from Data Centers to AWS | Capital One Case Study | AWS, n.d. https://aws.amazon.com/solutions/case-studies/capital-one-all-in-on-aws/ (accessed March 5, 2025).
57 How CloudRaft Helped a Fortune 500 Company Overcome Argo CD Challenges? n.d. https://www.cloudraft.io/casestudy/how-we-unblocked-a-fortune-500-with-argo-cd-consulting (accessed March 5, 2025).
58 Accenture and Google Cloud Advance AI Adoption and Cybersecurity with Fortune 500 Companies. n.d. https://newsroom.accenture.com/news/2024/accenture-and-google-cloud-advance-ai-adoption-and-cybersecurity-with-fortune-500-companies (accessed March 5, 2025).
59 Bible W, Raphael J, Taylor P, Valiente IO. Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession. Deloitte Development LLC. 2017.
60 Sedkaoui S, Chicha N. Blockchain-based smart contract technology application in the insurance industry: The case of 'Fizzy'. MJBS, vol. 2, 2021.
61 Nevile C. Enterprise Ethereum Alliance Permissioned Blockchains Specification v3. Enterprise Ethereum Alliance. 2022.
62 Blockchain Technology Could Reduce Investment Banks' Infrastructure Costs by 30 Percent, According to Accenture Report. n.d. https://newsroom.accenture.com/news/2017/blockchain-technology-could-reduce-investment-banks-infrastructure-costs-by-30-percent-according-to-accenture-report (accessed March 5, 2025).
63 Giménez JF. Customer-Centricity: The New Path to Product Innovation and Profitability. Cambridge Scholars Publishing. 2018. p. 150.
64 Pingili R. The role of AI in personalizing insurance policies. Int J Sci Res Comput Sci Eng Inform Technol. 2024. https://doi.org/10.32628/CSEIT24106194

65 Christoforidis C. Revolutionizing Enterprise IT: Exploring the Transformative Impact of Cloud and SaaS Solutions on Business Operations. THESEUS. 2024.
66 Amazon CodeWhisperer vs. Copilot: Which Is Right for You? n.d. https://www.missioncloud.com/blog/github-copilot-vs-amazon-codewhisperer?utm_source=chatgpt.com (accessed February 20, 2025).
67 Generative AI and ScienceDirect. n.d. https://www.elsevier.com/promotions/ai-on-sciencedirect (accessed February 20, 2025).
68 Alenezi M, Akour M. AI-driven innovations in software engineering: A review of current practices and future directions. Appl Sci. 2025;15:1344. https://doi.org/10.3390/APP15031344
69 Ugwueze V, Ugwueze VU, Chukwunweike JN. Continuous integration and deployment strategies for streamlined DevOps in software engineering and application delivery. Int J Comput Appl Technol Res. 2024;14:1. https://doi.org/10.7753/IJCATR1401.1001
70 Chawla D, Mehra PS. A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions. Internet of Things. 2023;24:100950. https://doi.org/10.1016/J.IOT.2023.100950
71 Goel PK, Pandey HM, Singhal A, Agarwal S, editors. Analyzing and Mitigating Security Risks in Cloud Computing. IGI Global. 2024. https://doi.org/10.4018/979-8-3693- 3249-8
72 Bouderhem R. A comprehensive framework for transparent and explainable AI sensors in healthcare. Eng Proc. 2024;82:49. https://doi.org/10.3390/ECSA-11-20524
73 Cairo M. Synthetic data and GDPR compliance: How artificial intelligence might resolve the privacy-utility tradeoff. J Technol Law Policy. 2023;28:71.
74 Jadon A, Kumar S. Leveraging generative AI models for synthetic data generation in healthcare: Balancing research and privacy. In 2023 International Conference on Smart Applications, Communications and Networking, SmartNets 2023 2023. https://doi.org/10.1109/SMARTNETS58706.2023.10215825
75 Oliveira M, Müller H, Nowak M. Blockchain in insurance claims processing: A review of transparency and fraud prevention. Business Market Finance Open. 2024;1:65–76.