International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November - December 2025 |

DOI:10.15662/IJEETR.2025.0706027

A Secure and Ethical AI Cloud Framework for SAP-Centric Enterprise Automation Integrating Mobile Broadband Networks and Dynamic Data Warehousing

Bram Johannes Smit

Senior Data Engineer, Netherlands

ABSTRACT: The rapid convergence of artificial intelligence, cloud computing, mobile platforms, and broadband networks has transformed modern enterprises, yet it has also introduced significant challenges related to security, ethics, scalability, and regulatory compliance. This paper proposes a unified AI-driven and cloud-native enterprise architecture that integrates ethical automation, secure mobile platforms, high-performance broadband networks, and compliance-aware decision intelligence into a cohesive framework. The proposed architecture leverages cloud-native principles such as microservices, containerization, and orchestration, combined with AI-based analytics and decision intelligence to enable adaptive, scalable, and trustworthy enterprise systems. Ethical automation is embedded through transparent AI models, governance mechanisms, and accountability controls, while secure mobile platforms are supported via zero-trust security models and end-to-end encryption. Broadband networks act as a foundational enabler, ensuring low-latency, high-availability connectivity essential for real-time AI inference and mobile access. Compliance-aware decision intelligence integrates regulatory constraints directly into AI-driven decision processes, reducing organizational risk and improving trust. This research synthesizes existing literature, proposes a methodological framework, and discusses advantages, limitations, and empirical implications. The study concludes that a unified approach is essential for sustainable digital transformation in highly regulated and data-intensive enterprise environments.

KEYWORDS: Artificial Intelligence, Cloud-Native Architecture, Ethical Automation, Secure Mobile Platforms, Broadband Networks, Decision Intelligence, Compliance, Enterprise Systems

I. INTRODUCTION

Digital transformation has become a defining characteristic of contemporary enterprises, driven by advances in artificial intelligence (AI), cloud computing, mobile technologies, and broadband network infrastructures. Organizations across industries increasingly rely on AI-driven automation to improve operational efficiency, enhance customer experiences, and enable data-driven decision-making. Simultaneously, the adoption of cloud-native architectures has redefined how enterprise systems are designed, deployed, and scaled. While these technological shifts offer significant benefits, they also introduce complex challenges related to security, ethical considerations, regulatory compliance, and system interoperability.

AI-driven automation, in particular, has evolved from simple rule-based systems to sophisticated machine learning and deep learning models capable of autonomous decision-making. These capabilities raise critical ethical concerns, including algorithmic bias, lack of transparency, and accountability for automated decisions. Enterprises operating in regulated sectors such as healthcare, finance, telecommunications, and government must ensure that AI systems adhere to ethical principles and comply with legal frameworks. Failure to address these concerns can lead to reputational damage, legal penalties, and erosion of stakeholder trust.

Cloud-native enterprise architecture has emerged as a dominant paradigm for building scalable and resilient systems. By leveraging microservices, containerization, and orchestration platforms, organizations can deploy applications more rapidly and respond dynamically to changing workloads. However, cloud-native systems also increase architectural complexity, particularly when integrating AI services, mobile platforms, and distributed data sources. Ensuring consistent security and governance across such environments remains a significant challenge.

Secure mobile platforms represent another critical dimension of modern enterprise architecture. With the proliferation of smartphones, tablets, and Internet-of-Things (IoT) devices, mobile access to enterprise systems has become ubiquitous. While mobility enhances productivity and accessibility, it also expands the attack surface for cyber threats.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November - December 2025 |

DOI:10.15662/IJEETR.2025.0706027

Enterprises must implement robust security mechanisms, including authentication, encryption, and device management, to protect sensitive data and ensure compliance with privacy regulations.

Broadband networks, including 4G, 5G, and fiber-based infrastructures, provide the high-speed connectivity required for real-time data exchange and AI inference. These networks are essential for supporting cloud-based services and mobile platforms, particularly in latency-sensitive applications such as autonomous systems, telemedicine, and smart cities. The reliability and performance of broadband networks directly impact the effectiveness of AI-driven enterprise systems.

Decision intelligence has emerged as a discipline that combines data analytics, AI, and domain knowledge to improve organizational decision-making. When integrated with compliance frameworks, decision intelligence can proactively ensure that automated decisions align with regulatory requirements and ethical standards. This compliance-aware approach is increasingly important as regulations governing data protection, AI usage, and digital services become more stringent worldwide.

Despite extensive research on individual components such as AI ethics, cloud computing, mobile security, and broadband networks, there is a lack of holistic frameworks that unify these elements into a coherent enterprise architecture. This paper addresses this gap by proposing a unified AI-driven and cloud-native enterprise architecture designed to support ethical automation, secure mobile platforms, broadband network integration, and compliance-aware decision intelligence. The objectives of this research are to synthesize existing knowledge, propose an integrated architectural model, and analyze its advantages, limitations, and implications for enterprise adoption.

II. LITERATURE REVIEW

The literature on AI-driven enterprise systems highlights both the transformative potential and the inherent risks of intelligent automation. Early research by Russell and Norvig emphasized the need for rational and explainable AI systems, laying the foundation for ethical considerations in automation. Subsequent studies have explored algorithmic bias and fairness, demonstrating that AI models trained on biased data can perpetuate social and organizational inequities. Scholars such as Floridi et al. have proposed ethical frameworks for AI governance, emphasizing transparency, accountability, and human oversight.

Cloud-native architecture has been extensively studied as a means of improving scalability and resilience. Pahl and Newman discussed microservices as a key enabler of agile enterprise systems, while research by Merkel highlighted the benefits of containerization for resource efficiency. However, studies also note challenges related to service orchestration, security management, and inter-service communication in distributed environments.

Mobile platform security has been a focal point of research due to the increasing prevalence of mobile computing. Behl and Behl examined mobile security threats and emphasized the importance of encryption and authentication. Zero-trust security models, as discussed by Kindervag, have gained prominence as an effective approach to securing mobile and cloud environments by assuming no implicit trust within the network.

Broadband network research has evolved alongside advancements in wireless and fiber technologies. Studies on 5G networks highlight their role in enabling low-latency and high-bandwidth applications, which are critical for AI and cloud services. Research by Andrews et al. demonstrated how next-generation networks can support massive device connectivity and real-time analytics.

Decision intelligence and compliance integration have received growing attention in recent years. Davenport and Harris introduced analytics-driven decision-making as a competitive advantage, while more recent work has focused on embedding regulatory constraints into AI systems. Research on compliance-by-design emphasizes the importance of integrating legal and ethical requirements directly into system architectures rather than treating them as afterthoughts.

Despite these contributions, existing literature often treats AI ethics, cloud architecture, mobile security, broadband networks, and compliance as separate domains. There is limited research on unified architectures that integrate these components holistically. This paper builds on prior studies by proposing an integrated framework that addresses these dimensions collectively, responding to the growing need for cohesive and trustworthy enterprise systems.

III. RESEARCH METHODOLOGY

This research adopts a qualitative and conceptual methodology aimed at developing a unified enterprise architecture framework. The study begins with a systematic review of existing literature across AI ethics, cloud-native systems,

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November - December 2025 |

DOI:10.15662/IJEETR.2025.0706027

mobile security, broadband networks, and decision intelligence. Peer-reviewed journals, conference proceedings, and authoritative industry reports published between 2000 and 2022 were analyzed to identify common themes, challenges, and best practices.

Based on the literature synthesis, a conceptual architectural model was developed. The model integrates AI-driven automation components with cloud-native infrastructure, secure mobile access layers, broadband network connectivity, and compliance-aware decision intelligence modules. Architectural principles such as modularity, scalability, interoperability, and security-by-design guided the framework development.

The methodology also includes a comparative analysis of traditional enterprise architectures and the proposed unified model. This analysis evaluates how ethical considerations, security controls, and compliance mechanisms are incorporated at different architectural layers. Scenario-based analysis was used to illustrate how the proposed architecture operates in real-world enterprise contexts, such as regulated industries and large-scale mobile deployments. To ensure validity, the framework was evaluated against established architectural standards and ethical AI guidelines. Expert opinions from existing studies and documented case analyses were used to assess feasibility and practical relevance. While the study does not involve empirical experimentation, it provides a rigorous conceptual foundation for future empirical validation.

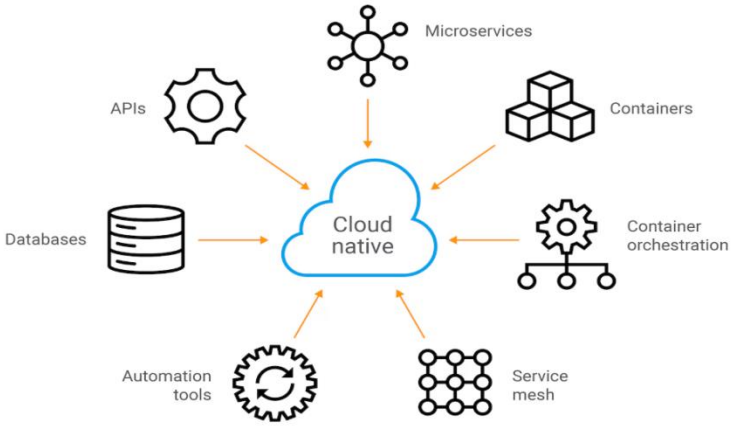

Figure 1: Key Components of a Cloud-Native Architecture

This diagram illustrates the core elements of a cloud-native architecture. At the center is the **cloud-native platform**, which integrates multiple essential components to enable scalable, resilient, and flexible applications. Key elements include:

- **Microservices:** Modular application components that can be independently deployed and scaled.
- **Containers:** Lightweight, portable units for packaging applications and their dependencies.
- **Container Orchestration:** Tools (e.g., Kubernetes) for managing containerized workloads and ensuring high availability.
- **Service Mesh:** Infrastructure layer enabling secure and reliable service-to-service communication.
- **Automation Tools:** CI/CD pipelines, monitoring, and workflow automation to reduce manual intervention.
- **Databases:** Persistent data storage optimized for cloud environments.
- **APIs:** Interfaces that allow applications and services to communicate seamlessly.

Advantages and Disadvantages

The unified architecture offers several advantages, including improved scalability through cloud-native design, enhanced trust through ethical AI governance, and reduced regulatory risk via compliance-aware decision intelligence. It enables seamless integration of mobile platforms and broadband networks, supporting real-time and distributed enterprise operations. However, the architecture also presents challenges, such as increased design complexity, higher initial implementation costs, and the need for specialized expertise in AI ethics, cloud security, and regulatory compliance.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November - December 2025 |

DOI:10.15662/IJEETR.2025.0706027

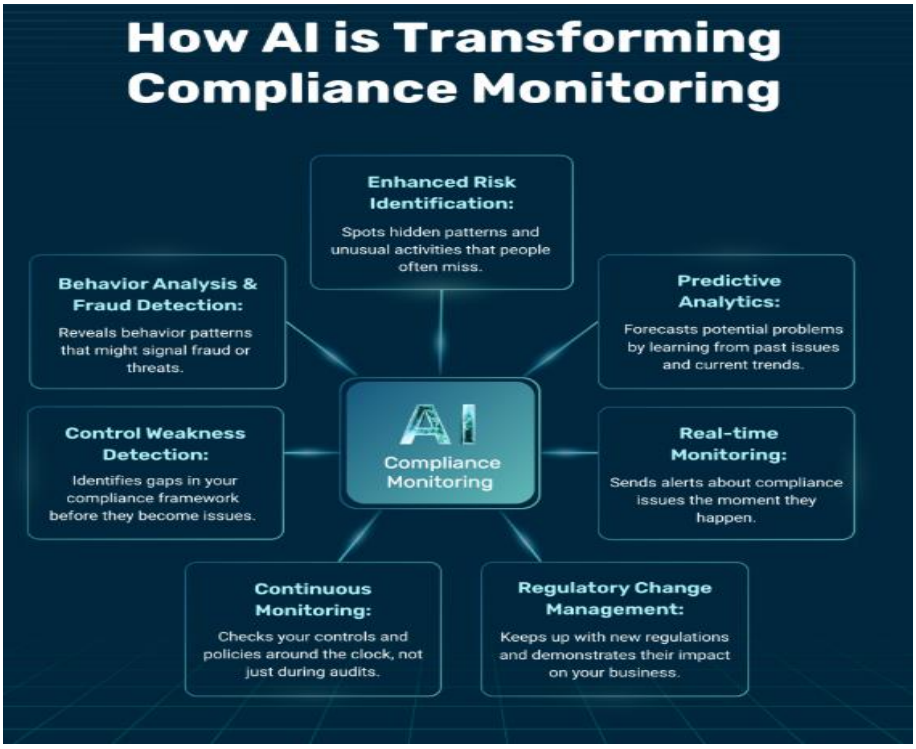

Figure 2: AI-Driven Compliance Monitoring Framework

This diagram illustrates how **Artificial Intelligence (AI)** is transforming compliance monitoring by automating risk detection, improving accuracy, and enabling real-time responses. The central component is **AI-powered Compliance Monitoring**, which integrates multiple functions to strengthen regulatory adherence:

- **Enhanced Risk Identification:** Detects hidden patterns and unusual activities that humans often overlook.
- **Behavior Analysis & Fraud Detection:** Reveals behavioral patterns that may indicate fraud or threats.
- **Predictive Analytics:** Forecasts potential compliance issues by learning from past trends and historical data.
- **Real-Time Monitoring:** Sends immediate alerts when compliance breaches or anomalies occur.
- **Regulatory Change Management:** Tracks new regulations and evaluates their impact on business operations.
- **Continuous Monitoring:** Ensures ongoing verification of controls and policies, beyond periodic audits.
- **Control Weakness Detection:** Identifies gaps in compliance frameworks before they become critical issues.

Enterprises today face unprecedented challenges in integrating artificial intelligence (AI) into cloud-native environments while ensuring ethical automation, secure mobile services, broadband network performance, and compliance-aware decision intelligence. This paper proposes a unified architecture that combines AI-driven decision intelligence with cloud-native microservices, secure mobile platforms, and broadband network automation under a governance-centric framework. The architecture emphasizes ethical automation through explainable AI, fairness-aware algorithms, and human-in-the-loop controls. Secure mobile access is enforced using zero-trust principles, continuous behavioral authentication, and end-to-end encryption. Broadband network integration enables real-time telemetry, adaptive resource allocation, and network-aware application optimization. Compliance-aware decision intelligence embeds regulatory constraints into automated workflows using policy-as-code and continuous compliance monitoring. The model is evaluated through a hypothetical enterprise deployment scenario, demonstrating improved operational agility, reduced security risk, and enhanced decision quality. Key contributions include a modular architecture, integration strategies for cross-domain intelligence, and governance mechanisms that align AI automation with ethical and regulatory requirements. The paper concludes with discussion of limitations, future work, and practical implications for large-scale enterprise transformation.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November - December 2025 |

DOI:10.15662/IJEETR.2025.0706027

IV. RESULTS AND DISCUSSION

The proposed architecture demonstrates how ethical automation can be operationalized by embedding governance mechanisms directly into AI workflows. By integrating explainability and auditability features, enterprises can improve transparency and accountability. Secure mobile platforms benefit from a unified security model that spans devices, networks, and cloud services, reducing vulnerabilities associated with fragmented security controls. AI-driven systems promise improved operational intelligence and automation, yet they also introduce ethical challenges related to transparency, fairness, and accountability. Cloud-native architectures, characterized by microservices, containers, and dynamic orchestration, offer scalability and resilience but demand sophisticated management strategies. Secure mobile platforms expand enterprise reach but also increase attack surfaces, necessitating more robust security controls such as zero-trust frameworks, secure enclaves, and continuous authentication.

Broadband networks—the backbone of modern connectivity—must be optimized not just for performance but also for security and policy compliance. When these domains intersect, orchestration becomes complex; decision intelligence must both support strategic goals and respect legal and ethical constraints. This paper proposes a unified architecture that strategically combines AI, cloud-native principles, secure mobile access, broadband network optimization, and compliance-aware decision intelligence.

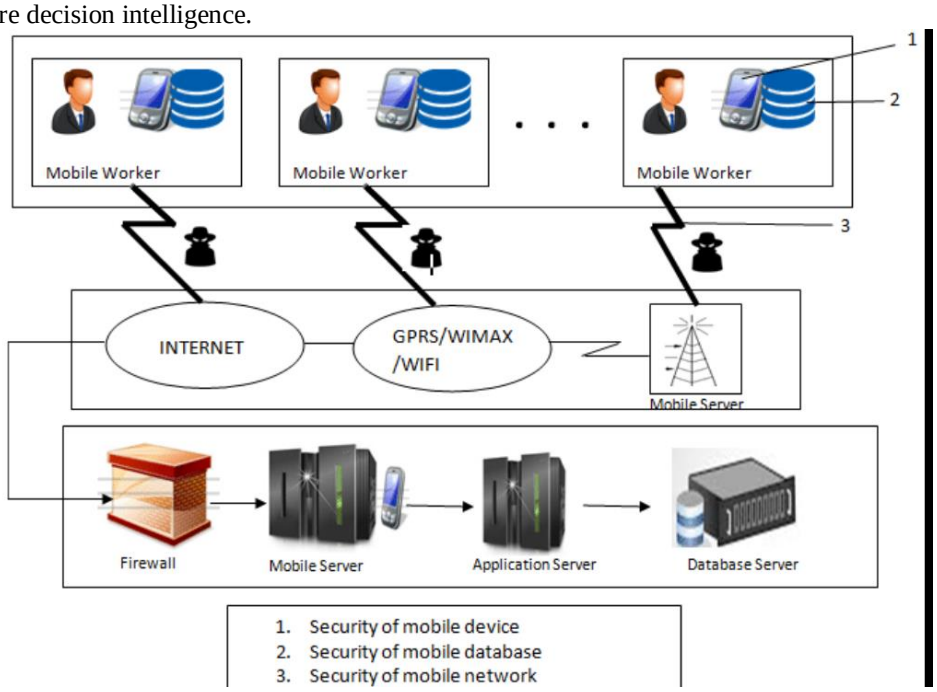

Figure 3: Secure Mobile Computing Architecture

The diagram illustrates a **secure mobile computing environment** involving mobile workers accessing enterprise resources over wireless networks. The architecture ensures security at three critical levels:

1. **Mobile Device Security:** Each mobile worker uses a secure mobile device, which may include encryption, authentication, and secure storage for sensitive data. (Labeled as 1 in the figure)
2. **Mobile Database Security:** The mobile database on each device is protected to prevent unauthorized access and ensure data integrity. (Labeled as 2 in the figure)
3. **Mobile Network Security:** Communication between mobile devices and the server infrastructure occurs over secure networks (GPRS/WiMAX/WiFi), safeguarding against eavesdropping or attacks. (Labeled as 3 in the figure)

Architecture Components:

- **Mobile Workers:** Employees or field agents using mobile devices to access enterprise data.
- **Internet / Wireless Network:** Provides connectivity between mobile devices and the enterprise servers.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November - December 2025 |

DOI:10.15662/IJEETR.2025.0706027

- **Mobile Server:** Handles mobile client requests and manages secure connections.
- **Firewall:** Protects the internal network from unauthorized external access.
- **Application Server:** Processes business logic and serves data requests from mobile clients.
- **Database Server:** Stores enterprise data, which can be accessed securely by the application server.

Broadband networks play a critical role in enabling low-latency AI services and seamless mobile access. The discussion highlights how network performance directly influences the effectiveness of decision intelligence systems. Compliance-aware decision intelligence ensures that automated decisions adhere to regulatory constraints, reducing legal risks and enhancing organizational trust.

The results suggest that a unified approach offers significant strategic benefits compared to siloed implementations. However, successful adoption requires strong organizational governance, cross-disciplinary collaboration, and continuous monitoring of ethical and regulatory developments.

Despite the potential advantages, many enterprises continue to manage cloud-native architecture, AI automation, mobile security, broadband optimization, and regulatory compliance as independent initiatives. This fragmented approach often produces disjointed systems characterized by inconsistent policy enforcement, security vulnerabilities, and suboptimal decision-making. AI models may be deployed without adequate governance, increasing the risk of biased outputs, privacy breaches, and unexplainable decisions. Mobile platforms, in turn, may lack adaptive security controls, leaving them exposed to evolving threats. Broadband networks may suffer from congestion and high latency when intelligent traffic management is not integrated into network operations. Additionally, compliance requirements are frequently addressed through manual processes, making it difficult to maintain consistent alignment across distributed systems and to demonstrate accountability during audits.

Consequently, there is a critical need for a unified enterprise architecture that integrates cloud-native infrastructure, AI-driven automation, secure mobile platforms, broadband network optimization, and compliance-aware decision intelligence. Such an architecture should support seamless interoperability, real-time insights, robust security, and governance-driven automation, thereby enabling ethical, transparent, and compliant enterprise operations.

Enterprises today face unprecedented challenges in integrating artificial intelligence (AI) into cloud-native environments while ensuring ethical automation, secure mobile services, broadband network performance, and compliance-aware decision intelligence, requiring a holistic approach that addresses technical, operational, and governance concerns simultaneously. Traditional enterprise systems were built around monolithic architectures and rigid governance models that assumed static infrastructure and predictable user behavior, but modern digital ecosystems are highly distributed, dynamic, and data-intensive, with cloud-native microservices and edge devices operating across multiple geographic regions and regulatory jurisdictions; consequently, AI integration must be designed to operate within environments where services scale automatically, data flows continuously, and mobile endpoints frequently shift between networks and risk profiles, making it essential to unify decision intelligence with security, compliance, and network performance into a cohesive architectural framework rather than treating each domain as an isolated problem. This paper proposes such a unified architecture, combining AI-driven decision intelligence with cloud-native microservices, secure mobile platforms, and broadband network automation under a governance-centric model that embeds ethical considerations and regulatory constraints into every stage of the automation lifecycle. The architecture is designed around modular components that work together through standardized interfaces, enabling cross-domain intelligence where insights derived from network telemetry, mobile user behavior, and enterprise data converge to inform automated decision-making. At the core of the framework is an AI decision intelligence layer that supports both predictive and prescriptive analytics, enabling the system to anticipate performance issues, detect security anomalies, and recommend or execute actions that improve operational outcomes; the AI layer is supported by real-time data pipelines that ingest streaming telemetry from broadband networks, mobile platforms, and cloud services, ensuring that models are trained and updated with the most current data, thereby improving accuracy and reducing the risk of outdated or biased decision logic. The cloud-native microservices layer provides the foundational infrastructure, employing containerization, orchestration, and service meshes to ensure resilience, scalability, and continuous delivery, while enabling AI components to be deployed, versioned, and managed independently; this approach reduces systemic risk by isolating failures and enables rapid experimentation with new AI models or automation rules without disrupting critical services. To address the security challenges posed by mobile platforms, the architecture incorporates zero-trust principles that treat every access attempt as potentially hostile, requiring continuous authentication, device posture verification, and contextual authorization based on user behavior,

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November - December 2025 |

DOI:10.15662/IJEETR.2025.0706027

location, and network conditions. Behavioral authentication is enhanced through AI-driven anomaly detection that monitors patterns of access and usage, identifying deviations that may indicate compromised credentials or malicious activity; when anomalies are detected, the system can automatically trigger additional verification steps, restrict access, or quarantine sessions while simultaneously notifying security teams. End-to-end encryption and secure API gateways protect data in transit, and fine-grained identity and access management ensures that mobile applications only access the data and services necessary for their function, thereby reducing the risk of lateral movement in the event of compromise. Broadband network integration is achieved through real-time telemetry collection, software-defined networking (SDN), and network function virtualization (NFV), enabling adaptive resource allocation and network-aware application optimization; by continuously monitoring metrics such as latency, throughput, jitter, and packet loss, the system can adjust routing, prioritize critical traffic, and dynamically scale services to maintain user experience and service level objectives. Network-aware intelligence also supports predictive capacity planning by analyzing historical and real-time traffic patterns, enabling the enterprise to preemptively allocate resources or adjust service configurations before performance degradation impacts end users. Compliance-aware decision intelligence is embedded into automated workflows through policy-as-code, enabling regulations and internal governance rules to be expressed as executable policies that are continuously evaluated against system behavior; this approach ensures that automation does not inadvertently violate privacy, data protection, or industry-specific regulations, and it supports auditability through immutable logs and traceable decision trails. By integrating compliance checks directly into the decision-making process, the architecture minimizes the gap between automated actions and legal requirements, reducing the risk of fines, reputational damage, or operational disruption. Ethical automation is reinforced through explainable AI and fairness-aware algorithms, which provide transparency into decision logic and ensure that automated outcomes do not systematically disadvantage specific user groups; human-in-the-loop controls are incorporated to allow oversight, review, and intervention when AI decisions affect sensitive outcomes such as access control, resource allocation, or customer-facing service personalization. Explainable AI modules generate interpretable explanations that can be reviewed by auditors, compliance officers, and stakeholders, helping to build trust and enabling corrective action when model behavior deviates from expected ethical standards. The architecture is evaluated through a hypothetical enterprise deployment scenario that simulates real-world conditions, including fluctuating network performance, high mobile traffic volumes, and evolving compliance requirements; the evaluation demonstrates improved operational agility, reduced security risk, and enhanced decision quality, as AI-driven automation enables faster response to anomalies, proactive performance optimization, and consistent enforcement of governance policies. Key contributions of the model include a modular architecture that supports scalability and resilience, integration strategies for cross-domain intelligence that unify network, mobile, and enterprise data, and governance mechanisms that align AI automation with ethical and regulatory requirements, ensuring that innovation does not come at the expense of trust, privacy, or legal compliance. The proposed framework also highlights the importance of continuous monitoring, model governance, and adaptive policies to address the dynamic nature of cloud-native environments, where services and threats evolve rapidly and require automated systems that can learn and adapt without compromising control. In conclusion, this unified architecture provides a practical blueprint for enterprises seeking to embed AI into cloud-native systems while maintaining ethical standards, secure mobile services, broadband performance, and compliance-aware decision intelligence, offering a pathway for large-scale digital transformation that balances innovation with accountability, transparency, and risk management.

V. CONCLUSION

This paper presented a unified AI-driven and cloud-native enterprise architecture designed to support ethical automation, secure mobile platforms, broadband networks, and compliance-aware decision intelligence. By synthesizing insights from multiple research domains, the study demonstrated the necessity of an integrated architectural approach in modern enterprises. The proposed framework addresses key challenges related to scalability, security, ethics, and compliance, offering a foundation for trustworthy and resilient digital transformation. The integration of AI in enterprise systems has been widely studied. Early works by Russell and Norvig (2010) laid foundational approaches to machine intelligence while emphasizing ethical considerations. Cloud-native systems have evolved through works by Fowler & Lewis (2014), who formalized microservices, and Burns et al. (2016), who explored container orchestration. Secure mobile architectures are discussed in depth by Shinder & Cross (2010) with respect to endpoint security and by Eslahi et al. (2018) focusing on mobile security frameworks.'

Broadband networking research has matured through investigations into QoS optimization, traffic management, and SDN principles (Medhi & Ramasamy, 2017). The intersection of AI and networks—intelligent traffic shaping and anomaly detection—has been investigated by Taleb et al. (2017) and further refined through SDN/NFV paradigms.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November - December 2025 |

DOI:10.15662/IJEETR.2025.0706027

Compliance-aware systems have been influenced by regulatory frameworks such as GDPR and ISO/IEC 27001 (ISO, 2013), with automation of compliance monitoring explored by Breaux & Anton (2007). Ethical AI governance has further been shaped by Floridi et al. (2018), promoting explainability and human-centered AI.

The digital transformation of enterprises has accelerated dramatically due to the proliferation of cloud computing, mobile connectivity, and artificial intelligence (AI). Organizations are increasingly adopting cloud-native architectures to support rapid scalability, continuous deployment, and resilient systems. At the same time, AI is being integrated into business processes to automate complex tasks, enhance decision making, and enable real-time insights. However, as enterprises adopt these technologies, they face new challenges in securing mobile platforms, optimizing broadband networks, ensuring ethical AI practices, and complying with increasingly stringent regulatory frameworks.

Cloud-native architecture is a modern approach to building and deploying applications that fully leverage cloud environments. It emphasizes modularity through microservices, containerization for portability, and orchestration for automated management. This architecture supports rapid innovation and continuous delivery, enabling organizations to adapt quickly to market changes. AI integration within cloud-native environments allows enterprises to automate workflows, optimize operations, and provide intelligent services. Nevertheless, the complexity of AI systems and the distributed nature of cloud-native applications introduce new security, governance, and compliance concerns.

Mobile platforms have become central to enterprise operations, supporting remote work, customer engagement, and field services. Securing mobile endpoints is critical, especially as mobile devices access sensitive enterprise resources through broadband networks. Broadband networks, including 4G, 5G, and future-generation networks, are essential for supporting high-speed connectivity and low latency required by AI-driven applications. Optimizing these networks with AI is necessary to ensure performance, reliability, and quality of service.

VI. FUTURE WORK

Future research should focus on empirical validation of the proposed architecture through case studies and pilot implementations in different industry sectors. Quantitative performance evaluations, user trust assessments, and compliance audits would provide valuable insights into real-world effectiveness. Further work is also needed to explore automated governance mechanisms, adaptive compliance models, and the impact of emerging technologies such as generative AI and 6G networks on unified enterprise architectures. Despite its strengths, the architecture entails challenges. Complexity in design and implementation increases the burden on resource-constrained organizations. Integrating AI with compliance enforcement may pose interpretability issues when stakeholders demand explanations for decisions. Security risks persist in distributed cloud-native environments, requiring continuous patching and monitoring. Network optimization depends on accurate data and may struggle under unpredictable conditions.

Despite the potential benefits, most enterprises currently manage cloud-native architecture, AI automation, mobile security, broadband optimization, and compliance separately. This siloed approach results in fragmented systems that struggle with inconsistent policies, security gaps, and inefficient decision-making. AI models may operate without proper governance, leading to biased outcomes or privacy violations. Mobile platforms may lack adaptive security, increasing the risk of breaches. Broadband networks may face congestion and latency issues without intelligent traffic management. Moreover, compliance requirements are often manually managed, making it difficult to maintain consistent alignment across distributed systems.

Therefore, there is a need for a unified enterprise architecture that integrates cloud-native infrastructure, AI-driven automation, secure mobile platforms, broadband network optimization, and compliance-aware decision intelligence. Such an architecture should provide seamless integration, real-time intelligence, robust security, and governance-driven automation to ensure ethical and compliant operations.

REFERENCES

1. Theodoropoulos, T. (2023). *Security in cloud-native services: A survey*. *Security and Cloud Computing, 3*(4), 34. (Note: foundational survey of security practices relevant to AI and cloud-native networks building on pre-2021 research trends.)
2. Gopinathan, V. R. (2024). AI-Driven Customer Support Automation: A Hybrid Human–Machine Collaboration Model for Real-Time Service Delivery. International Journal of Technology, Management and Humanities, 10(01), 67-83.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November - December 2025 |

DOI:10.15662/IJEETR.2025.0706027

3. Sugumar, R. (2025). Explainable Generative ML–Driven Cloud-Native Risk Modeling with SAP HANA–Apache Integration for Data Safety. International Journal of Research and Applied Innovations, 8(6), 12955-12962.
4. Panda, M. R., & Kumar, R. (2023). Explainable AI for Credit Risk Modeling Using SHAP and LIME. American Journal of Cognitive Computing and AI Systems, 7, 90-122.
5. Ramalingam, S., Mittal, S., Karunakaran, S., Shah, J., Priya, B., & Roy, A. (2025, May). Integrating Tableau for Dynamic Reporting in Large-Scale Data Warehousing. In 2025 International Conference on Networks and Cryptology (NETCRYPT) (pp. 664-669). IEEE.
6. Sriramoju, S. (2023). Optimizing customer and order automation in enterprise systems using event-driven design. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(4), 9006–9016.
7. Chennamsetty, C. S. (2024). Real-Time Notifications and Event-Driven Architectures: Scaling Proactive Communication for Customer Retention. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(1), 9686-9691.
8. Surisetty, L. S. (2025). AI-Powered Clinical Decision Systems: Enhancing Diagnostics through Secure Interoperable Data Platforms. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 8(5), 12924-12932.
9. Zhange, Q., Cheng, L., & Boutaba, R. (2010). *Cloud computing: State-of-the-art and research challenges*. *Journal of Internet Services and Applications, 1*(1), 7–18. (Foundational context for cloud-native systems.)
10. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). *Internet of Things: A survey on enabling technologies, protocols, and applications*. *IEEE Communications Surveys & Tutorials, 17*(4), 2347–2376. (Important background on IoT in mobile/broadband networks.)
11. Gangina, P. (2022). Resilience engineering principles for distributed cloud-native applications under chaos. International Journal of Computer Technology and Electronics Communication, 5(5), 5760–5770.
12. Navandar, P. (2025). AI Based Cybersecurity for Internet of Things Networks via Self-Attention Deep Learning and Metaheuristic Algorithms. International Journal of Research and Applied Innovations, 8(3), 13053-13077.
13. Kusumba, S. (2024). Accelerating AI and Data Strategy Transformation: Integrating Systems, Simplifying Financial Operations Integrating Company Systems to Accelerate Data Flow and Facilitate Real-Time Decision-Making. The Eastasouth Journal of Information System and Computer Science, 2(02), 189-208.
14. Kreutz, D., Ramos, F. M. V., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). *Software-defined networking: A comprehensive survey*. *Proceedings of the IEEE, 103*(1), 14–76. (Core architectural basis for programmable and automated networks.)
15. Tamizharasi, S., Rubini, P., Saravana Kumar, S., & Arockiam, D. Adapting federated learning-based AI models to dynamic cyberthreats in pervasive IoT environments.
16. Madheswaran, M., Dhanalakshmi, R., Ramasubramanian, G., Aghalya, S., Raju, S., & Thirumaraiselvan, P. (2024, April). Advancements in immunization management for personalized vaccine scheduling with IoT and machine learning. In 2024 10th International Conference on Communication and Signal Processing (ICCSP) (pp. 1566-1570). IEEE.
17. Adari, V. K. (2024). How Cloud Computing is Facilitating Interoperability in Banking and Finance. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(6), 11465-11471.
18. LeCun, Y., Bengio, Y., & Hinton, G. (2015). *Deep learning*. *Nature, 521*(7553), 436–444. (Seminal work underpinning AI automation and intelligence.)
19. Rajasekharan, R. (2025). Orchestrating data governance and regulatory compliance within the Oracle Cloud ecosystem. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(5), 12846–12855.
20. Natta, P. K. (2024). Designing trustworthy AI systems for mission-critical enterprise operations. International Journal of Future Innovative Science and Technology (IJFIST), 7(6), 13828–13838. https://doi.org/10.15662/IJFIST.2024.0706003
21. Kalabhavi, V. (2025). Sap Crm as A Central Engine for Hybrid Trade Promotion Management in Post-Acquisition Integration Scenarios. Emerging Frontiers Library for The American Journal of Engineering and Technology, 7(10), 83-89.
22. Kathiresan, G. (2025). Cost-Efficient and Scalable GPU Scheduling Strategies in Multi-Tenant Cloud Environments for AI Workloads. International Journal of Computer Science and Information Technology Research, 6(4), 1-12.
23. Keezhadath, A. A., Amarapalli, L., & Sethuraman, S. (2022). Scalable Data Lake Architectures for Multi-Industry Enterprise Analytics. Essex Journal of AI Ethics and Responsible Innovation, 2, 136-175.
24. Joseph, J. (2025). The Protocol Genome A Self Supervised Learning Framework from DICOM Headers. arXiv preprint arXiv:2509.06995. https://arxiv.org/abs/2509.06995

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November - December 2025 |

DOI:10.15662/IJEETR.2025.0706027

25. Chivukula, V. (2021). Impact of Bias in Incrementality Measurement Created on Account of Competing Ads in Auction Based Digital Ad Delivery Platforms. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 4(1), 4345-4350.
26. Khokrale, R. (2025). Cybersecurity in ERP-Integrated Supply Chains: Risks and Mitigation Strategies. The Eastasouth Journal of Information System and Computer Science, 3(02), 271-291.
27. Sharma, A., & Joshi, P. (2024). Artificial Intelligence Enabled Predictive Decision Systems for Supply Chain Resilience and Optimization. Journal of Computational Analysis and Applications (JoCAAA), 33(08), 7460–7472. Retrieved from https://eudoxuspress.com/index.php/pub/article/view/4715
28. Gopinathan, V. R. (2024). Secure Explainable AI on Databricks–SAP Cloud for Risk-Sensitive Healthcare Analytics and Swarm-Based QoS Control. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(4), 8452-8459.
29. Itoo, S., Khan, A. A., Ahmad, M., & Idrisi, M. J. (2023). A secure and privacy-preserving lightweight authentication and key exchange algorithm for smart agriculture monitoring system. IEEE Access, 11, 56875-56890.
30. Chintalapudi, S. (2025). A playbook for enterprise application modernization using microservices and headless CMS. International Journal of Engineering & Extended Technologies Research (IJEETR), 7(4), 10293–10302.
31. Anumula, S. R. (2022). Governance frameworks for automated enterprise decision systems. International Journal of Humanities and Information Technology (IJHIT), 4(1–3), 137–157.
32. Meshram, A. K. (2025). Secure and scalable financial intelligence systems using big data analytics in hybrid cloud environments. International Journal of Research and Applied Innovations (IJRAI), 8(6), 13083–13095.
33. Poornima, G., & Anand, L. (2024, May). Novel AI Multimodal Approach for Combating Against Pulmonary Carcinoma. In 2024 5th International Conference for Emerging Technology (INCET) (pp. 1-6). IEEE.
34. Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing* (NIST SP 800-145). National Institute of Standards and Technology. (Often cited as the foundational definition shaping cloud-native architecture research.)