ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep978

Advancing U.S. Competitiveness in Agentic Gen AI: A Strategic Framework for Interoperability and Governance

Satyadhar Joshi[1]

[1]Alumnus, MS IT, Touro College, NYC, USA
[1]Alumnus, IMBA, Bar Ilan University, Israel

ORCID: https://orcid.org/0009-0002-6011-5080

Publication Date: 2025/09/25

Abstract: The rapid evolution of artificial intelligence has given rise to agentic AI systems—autonomous entities capable of perceiving their environment, making decisions, and executing actions with minimal human intervention. This work provides a systematic analysis of agentic AI frameworks, governance models, and implementation strategies. Drawing on a comprehensive review of the literature, we examine the current state of agentic AI technologies, highlight key challenges in governance, security, and ethical oversight, and compare architectural frameworks for responsible deployment. Our results, illustrated through detailed framework comparisons and governance analyses, demonstrate that while agentic AI holds transformative potential across multiple sectors, notable gaps persist in standardization, regulatory compliance, and interoperability. To address these issues, we propose a layered architecture that embeds governance and security across all system layers. An analysis of the competitive landscape further identifies critical interoperability challenges that could undermine U.S. leadership. Based on these insights, we outline a strategic framework for U.S. competitiveness, emphasizing accelerated standards development, international collaboration, and investment in interoperability research. Finally, emerging trends and future directions are explored to provide a comprehensive roadmap for responsible deployment of agentic AI.

Keywords: *Agentic AI, AI Governance, Autonomous Systems, AI Frameworks, Ethical AI, AI Security, Multi-Agent Systems, Regulatory Compliance.*

How to Cite: Satyadhar Joshi (2025) Advancing U.S. Competitiveness in Agentic Gen AI: A Strategic Framework for Interoperability and Governance. *International Journal of Innovative Science and Research Technology*, 10(9), 1480-1496. https://doi.org/10.38124/ijisrt/25sep978

I. INTRODUCTION

Unlike traditional AI systems that primarily assist human operators, agentic AI systems demonstrate autonomy, goal-directed behavior, and the capacity for independent decision-making [1]. The year 2025 has been identified as a pivotal moment when "the frontier firm is born" through the integration of intelligence on tap that fundamentally rewires business operations [2].

Agentic AI systems integrate one or more AI agents that differ from traditional computer programs in their ability to learn and adapt, make decisions, interact with surroundings, and operate with limited supervision [3]. These systems are increasingly being deployed across various sectors including finance [4], healthcare [5], manufacturing, and cybersecurity [6], offering unprecedented opportunities for automation and efficiency gains [7], [8].

However, the autonomous nature of these systems introduces significant challenges in governance, security, and ethical compliance. As noted by [9], agentic AI governance represents a new benchmark for operationalizing trust in autonomous, self-improving, and multi-agent AI systems. The tension between innovation and regulation requires careful navigation to ensure responsible deployment while maximizing potential benefits [10], [11].

This paper provides a comprehensive examination of the current landscape of agentic AI frameworks and governance approaches. We synthesize insights from key references to present a structured analysis of technical frameworks, governance models, implementation challenges, and future directions. Our contributions include:

- A systematic literature review of agentic AI frameworks and governance approaches (Section 2)

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep978

- Quantitative analysis of implementation challenges and adoption barriers (Section 5)
- A condensed architectural proposal for responsible agentic AI deployment (Section 7)
- Analysis of U.S. competitiveness and strategic recommendations (Section 6)
- Identification of future research directions and emerging trends (Section 8)
- Examination of potential negative scenarios without proactive governance

The remainder of this paper is organized as follows: Section 2 presents a comprehensive literature review examining definitional frameworks, architectural patterns, and governance approaches for agentic AI systems. Section 4 details our systematic research methodology for analyzing key references in this domain. Section 5 presents quantitative findings on adoption trends, framework comparisons, and implementation patterns. Section 6 analyzes U.S. competitiveness challenges and proposes strategic interventions for interoperability and governance leadership. Section 7 introduces our condensed architectural framework for responsible agentic AI deployment with integrated governance and security. Section 8 explores future research directions, industry trends, and emerging technologies. This work also examines potential negative scenarios without proactive interoperability governance. Finally, Section 10 synthesizes our findings and outlines implications for research, practice, and policy.

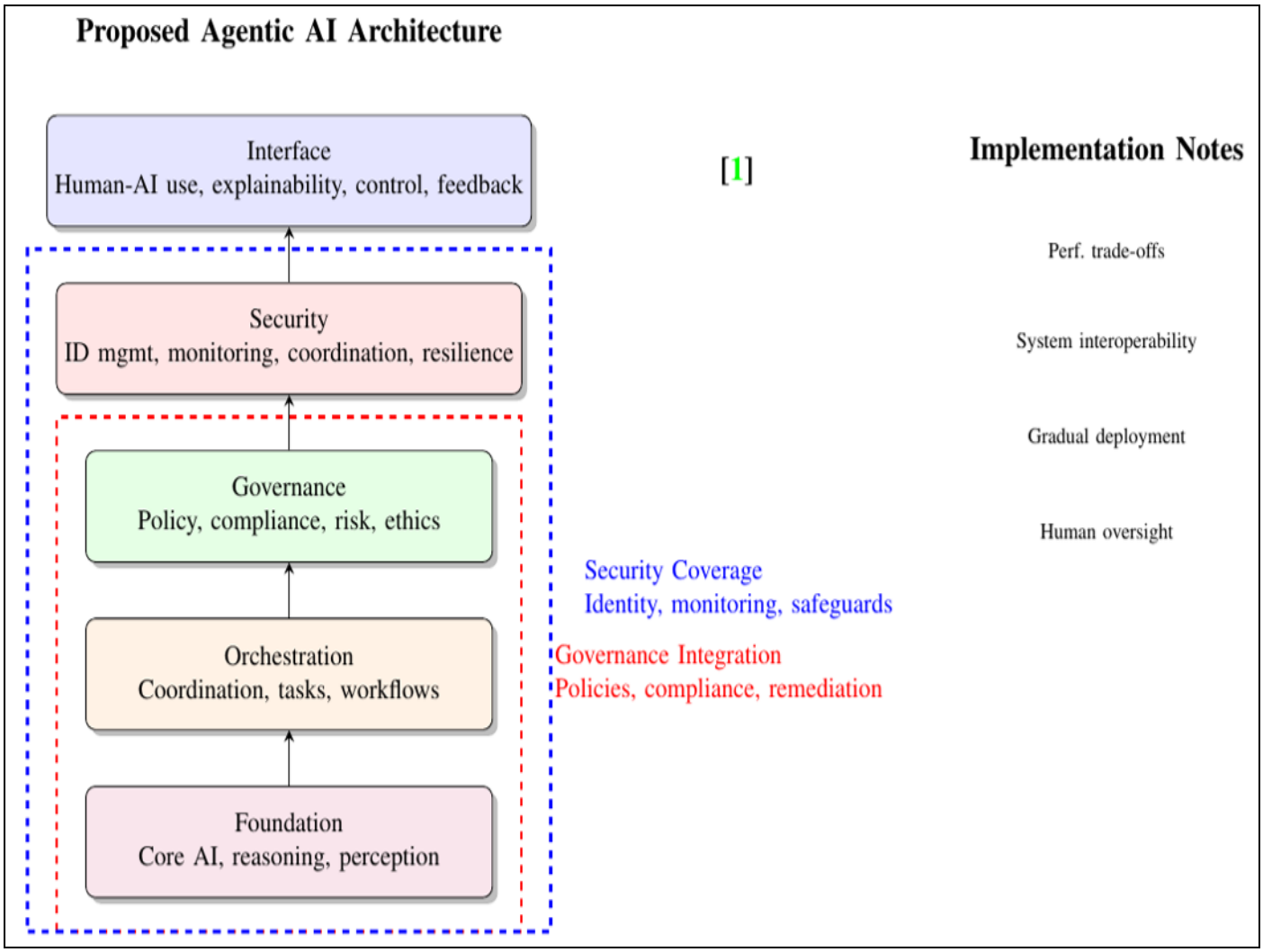

Fig 1 Proposed Layered Architecture for Agentic AI Deployment with Governance, Security, and Implementation Notes.

II. LITERATURE REVIEW

A. *Definition and Characteristics of Agentic AI*

Agentic AI refers to artificial intelligence systems that can pursue complex goals with limited direct supervision [12]. These systems are characterized by their autonomy, adaptability, and ability to interact with their environment through perception, decision-making, and action execution [3].

According to [13], agentic AI represents a breakthrough advancement that creates autonomous agents capable of

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep978

analyzing data, setting goals, and taking action independently. This differs fundamentally from traditional AI systems that primarily provide recommendations or assistance without autonomous execution capabilities.

B. Agentic AI Frameworks and Architectures

The development of agentic AI systems relies on specialized frameworks that provide the necessary infrastructure for building, deploying, and managing autonomous agents. Recent literature identifies several categories of frameworks emerging in 2024-2025:

- *Development Frameworks*

Development frameworks such as LangChain [14], CrewAI [15], and Microsoft Semantic Kernel [15] provide tools for constructing agentic workflows and integrating various AI components. These frameworks typically offer modular architectures that support different patterns of agent interaction and task execution.

- *Enterprise-Scale Frameworks*

Enterprise-focused frameworks address the specific requirements of large organizations, including scalability, security, and integration with existing systems. [16] note that 61% of organizations are building agentic AI systems, highlighting the need for robust frameworks that can avoid the 40% failure rate observed in early implementations.

- *Specialized Domain Frameworks*

Domain-specific frameworks have emerged for particular industries and applications. For example, [17] discuss frameworks enhanced for GxP compliance in regulated industries, while [4] present specialized approaches for banking applications.

- *Architectural Patterns*

The architectural foundation for agentic AI systems typically follows a three-tier model as described by [18]: Foundation tier (basic capabilities), Workflow tier (orchestration), and Autonomous tier (full autonomy). This progression emphasizes that trust, governance, and transparency must precede full autonomy in enterprise deployments.

C. Governance and Regulatory Landscape

The governance of agentic AI systems presents unique challenges due to their autonomous nature and potential impact. Current literature identifies several key aspects of agentic AI governance:

- *Regulatory Frameworks*

Emerging regulations such as the EU AI Act [11], [19] establish requirements for high-risk AI systems, including many agentic AI applications. These regulations emphasize risk-based approaches, transparency requirements, and human oversight provisions.

- *Industry Standards*

Technical standards are evolving to support interoperability and safety in agentic AI systems. [20] identify several open-source standards emerging for AI agents and agentic frameworks, while [21] discusses ISO/IEC 42001 for AI management systems.

- *Governance Models*

Various governance models have been proposed specifically for agentic AI systems. The AIGN Agentic AI Governance Framework v1.0 [22] provides a foundational model for systems that act autonomously, delegate tasks, or interface with external tools. Similarly, [23] discuss the future of AI oversight in the context of agentic systems.

- *Compliance Considerations*

Compliance with existing regulations such as GDPR and CCPA remains critical for agentic AI systems [24]. [25] provide a comprehensive overview of global compliance requirements that enterprises must consider when deploying generative AI systems, including agentic applications.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep978

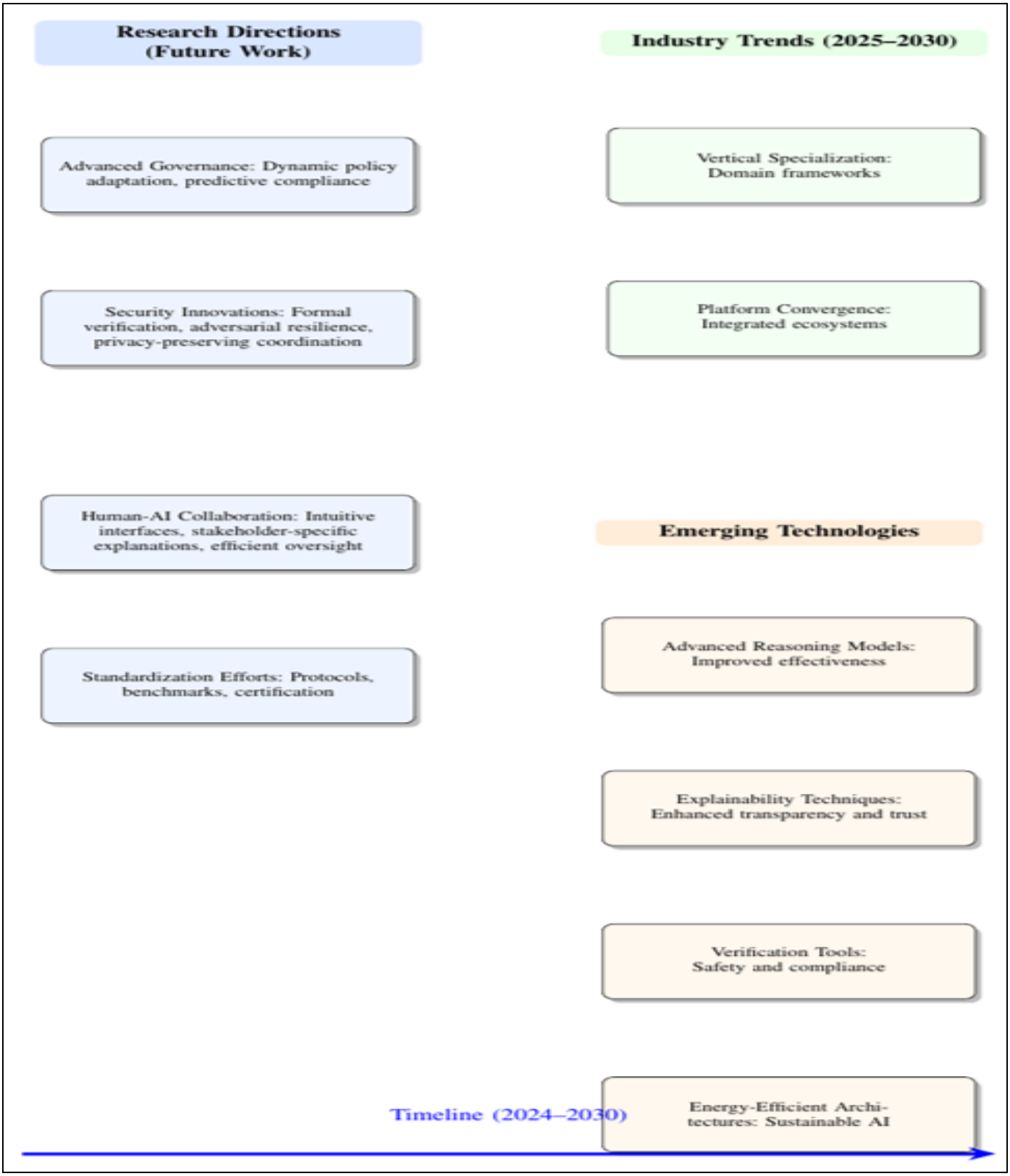

Fig 2 Research, Industry, and Technology Trends Shaping Agentic AI (2024--2030).

D. Security and Risk Management

The autonomous nature of agentic AI systems introduces unique security challenges that require specialized approaches:

➢ *Threat Landscape*

Agentic AI systems face threats including permission escalation, hallucination, and memory manipulation [26]. [27] explore how large language models could become insider threats through simulated blackmail, industrial espionage, and other misaligned behaviors.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep978

➢ *Security Frameworks*

Several security frameworks have been proposed specifically for agentic AI. The OWASP Gen AI Security Project [28] provides guidelines for securing generative AI applications, including agentic systems. [29] present a detailed guide for designing, developing, and deploying secure agentic applications.

➢ *Risk Management Approaches*

Risk management frameworks such as the NIST AI RMF [30] and its generative AI profile [31] provide structured approaches to identifying, assessing, and mitigating risks in AI systems, including agentic applications.

E. Ethical Considerations

The deployment of agentic AI systems raises significant ethical questions that must be addressed through careful design and governance:

➢ *Transparency and Explainability*

The autonomous decision-making of agentic AI systems creates challenges for transparency and explainability [32]. Stakeholders need to understand how decisions are made, particularly in high-stakes applications.

➢ *Accountability and Responsibility*

Determining accountability for actions taken by autonomous systems remains a complex issue [33]. Legal frameworks are still evolving to address the unique challenges posed by agentic AI systems [34].

➢ *Bias and Fairness*

Like all AI systems, agentic AI can perpetuate or amplify biases present in training data or system design [35]. Special considerations are needed for autonomous systems that may make decisions without human intervention.

➢ *Privacy Implications*

The data collection and processing capabilities of agentic AI systems raise significant privacy concerns [36]. These systems must be designed with privacy-preserving principles from the outset.

The policy framework for Agentic Generative AI must be designed not only to ensure robust governance and risk management of AI models [82, 83], but also to directly enhance system accessibility, affordability, and efficacy in specialized critical domains such as infectious disease management [84, 85].

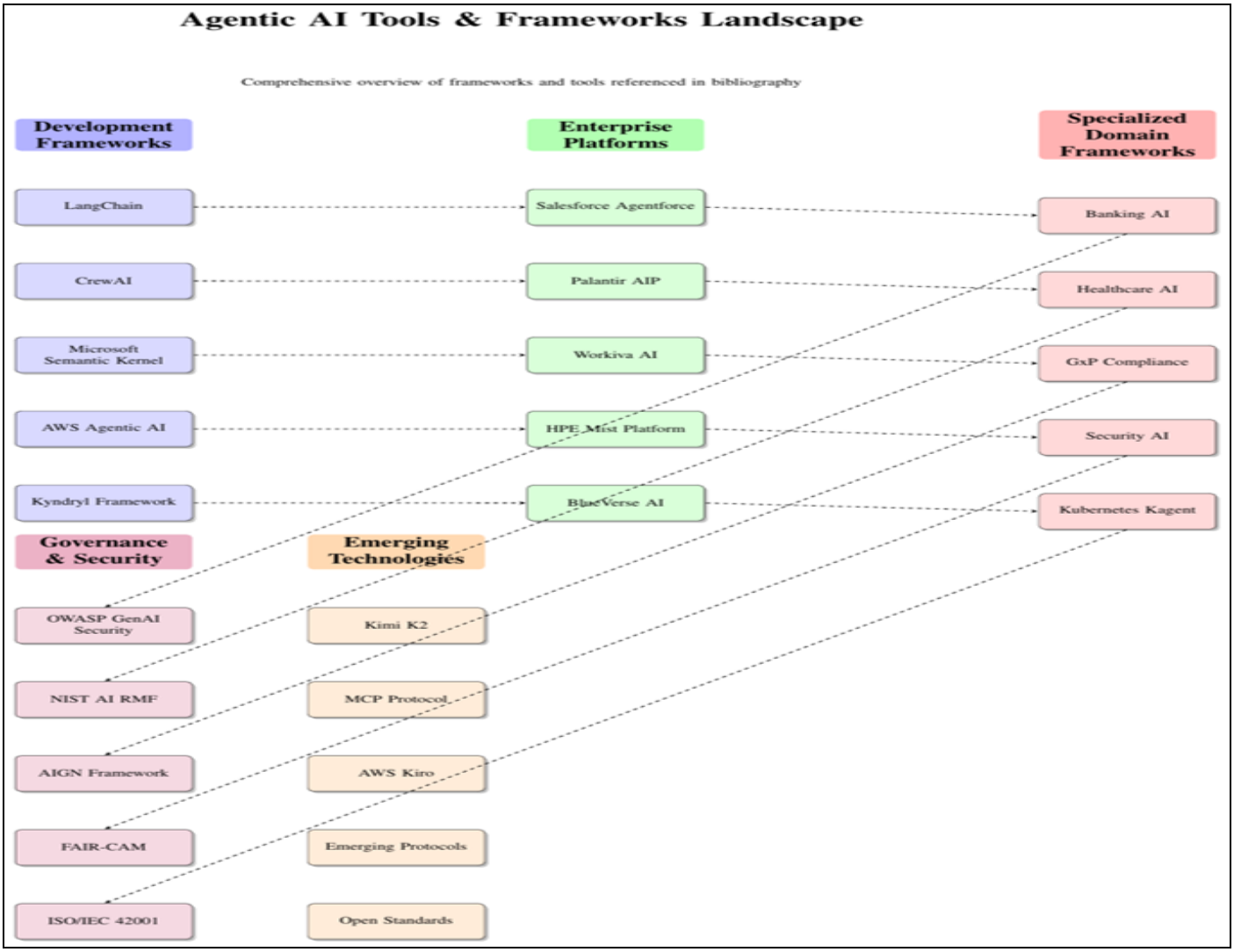

Fig 3 Full Landscape of Agentic AI Frameworks and Tools

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep978

III. LIST OF FIGURES AND TABLES

This section provides a comprehensive reference to all figures and tables included in this paper, along with their corresponding descriptions and significance to our research.

➢ *Figures*

- Figure 1: Agentic-Architecture: Proposed layered architecture for agentic AI deployment with governance, security, and implementation notes. This figure illustrates our comprehensive architectural framework that integrates governance and security throughout all system layers.
- Figure 2: Agentic-Trends: Research, industry, and technology trends shaping agentic AI (2024–2030). This visualization captures the multidimensional evolution of agentic AI across research directions, industry applications, and emerging technologies.
- Figure 3: Agentic-Tools: Full landscape of Agentic AI frameworks and tools. This comprehensive diagram categorizes and connects the diverse ecosystem of development frameworks, enterprise platforms, domain-specific solutions, governance tools, and emerging technologies.
- Figure 4: Implementation-Roadmap: Three-phase implementation roadmap with staggered milestones and outcomes. This timeline provides a strategic plan for the phased adoption and scaling of agentic AI interoperability and governance frameworks.

➢ *Tables*

- Table 1: frameworks: Comparison of Agentic AI Frameworks. This table evaluates selected frameworks across multiple dimensions including functionality, maturity, scalability, and governance capabilities.
- Table 2: agentic-governance: Agentic AI Governance Frameworks and Key Considerations. This comprehensive table organizes governance aspects, principles, frameworks, and implementation considerations for effective agentic AI oversight.
- Table 3: US-leadership-strategy: Strategic Framework for U.S. Leadership in Agentic AI. This table outlines the strategic pillars, key initiatives, and supporting references for maintaining U.S. competitiveness in agentic AI.
- Table 4: implementation roadmap: Implementation Roadmap and Expected Outcomes. This table details the timeline, key activities, and expected outcomes for the phased implementation of our proposed strategic framework.
- Table 5: architecture-summary: Proposed Architecture and Future Directions for Responsible Agentic AI. This table summarizes the key elements of our architectural proposal and identifies future research and development directions.

These visual elements collectively provide a comprehensive representation of the current agentic AI landscape, our proposed architectural framework, strategic recommendations for U.S. competitiveness, and implementation roadmaps for responsible deployment.

IV. METHODOLOGY

This research employs a systematic literature review methodology to comprehensively analyze the current state of agentic AI frameworks and governance approaches. Our methodology follows a structured process adapted from established systematic review protocols [12] to ensure thorough coverage and rigorous analysis of this emerging field.

The search strategy employed keywords such as "agentic AI," "AI governance," "autonomous AI agents," "AI frameworks," and related terms, building upon the search methodologies documented in comprehensive industry analyses [16], [37].

Inclusion criteria focused on publications from 2023-2025 to capture the most recent developments in this rapidly evolving field, consistent with the approach taken in contemporary AI governance reviews [22], [23]. We prioritized sources from reputable organizations including NIST, IEEE, ISO, and leading AI research institutions. The final reference set includes sources that provide comprehensive coverage of the agentic AI landscape, with particular attention to frameworks that have demonstrated production readiness [38], [39].

➢ *Analysis Framework*

We developed a structured analysis framework adapted from established AI governance assessment methodologies [30], [31] to systematically examine each publication across multiple dimensions:

- Technical Focus: Framework architecture, development tools, implementation approaches, with particular attention to architectural patterns described in [18], [40]
- Governance Aspects: Regulatory compliance, ethical considerations, risk management, drawing on frameworks from [24], [41]
- Application Domain: Industry-specific applications, use cases, deployment scenarios, including specialized domains such as banking [4] and healthcare [5]
- Maturity Level: Research proposals, experimental systems, production deployments, using assessment criteria similar to those in [16], [39]
- Geographic Scope: Regional regulations, international standards, global perspectives, with particular attention to comparative regulatory analysis from [10], [25]

This multidimensional analysis enabled us to identify patterns, trends, and gaps in the current landscape of agentic AI frameworks and governance approaches, following the comprehensive assessment approach demonstrated in [42].

➢ *Quantitative Assessment*

Where possible, we extracted quantitative data regarding adoption rates, implementation challenges, performance

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep978

metrics, and compliance requirements. This approach aligns with the data-driven assessment methodologies employed in industry analyses such as [16], which reported that 61% of organizations are building agentic AI systems with a 40% failure rate in early implementations. The quantitative data provides insights into the practical realities of agentic AI deployment and helps identify areas requiring further research and development, particularly in security implementation maturity levels as categorized in [43], [44].

➢ *Limitations*

Our methodology has several limitations consistent with those noted in similar emerging technology reviews [12], [37]. The rapid evolution of agentic AI technologies means that new developments may have emerged since publication. Additionally, some industry implementations may not be fully documented in publicly available literature, particularly those involving proprietary frameworks or sensitive security implementations [26], [29]. Nevertheless, our systematic approach provides a comprehensive snapshot of the current state of knowledge in this domain, establishing a baseline for ongoing research as called for in [10], [11].

V. FINDINGS AND ANALYSIS

A. Adoption Trends and Implementation Challenges

Our analysis reveals significant growth in agentic AI adoption across various sectors. According to [16], 61% of organizations are currently building agentic AI systems, reflecting substantial interest and investment in this technology. However, implementation challenges remain significant, with a reported 40% failure rate in early deployments.

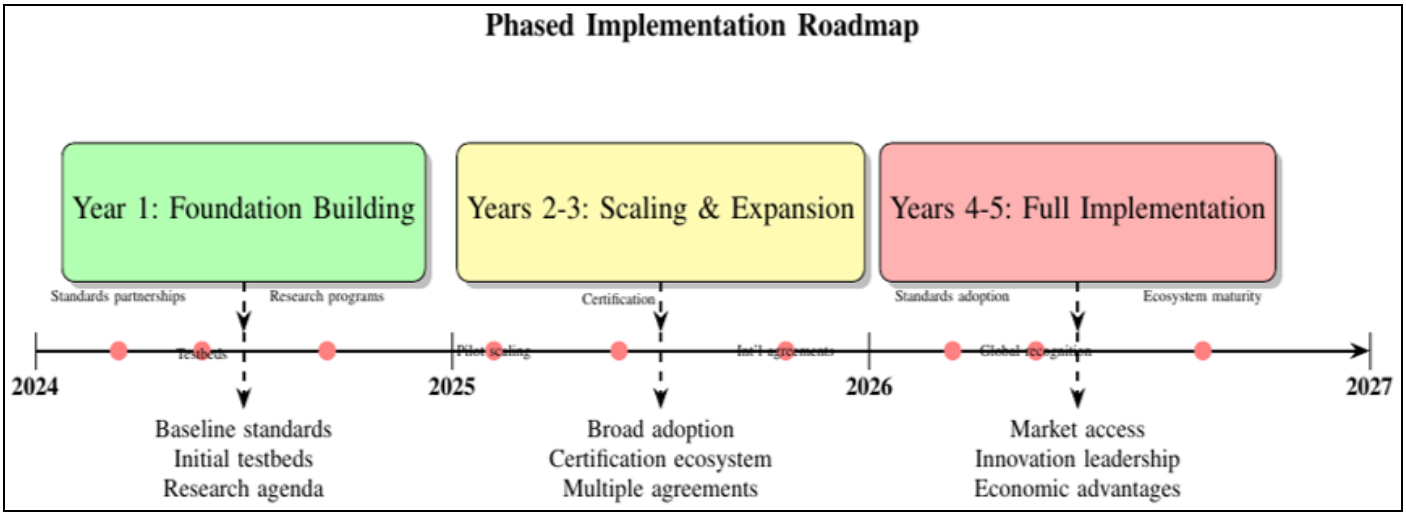

Fig 4 Three-Phase Implementation Roadmap with Staggered Milestones and Outcomes to Avoid Overlap.

➢ *The Primary Adoption Barriers Identified in the Literature Include:*

- Technical Complexity: Developing and integrating agentic AI systems requires specialized expertise and infrastructure [38]
- Governance Gaps: Many organizations lack clear frameworks for governing autonomous AI systems [45]
- Regulatory Uncertainty: Evolving regulations create compliance challenges for early adopters [10]
- Security Concerns: Autonomous systems introduce new attack surfaces and vulnerabilities [43]
- Skills Shortage: Limited availability of professionals with expertise in agentic AI development and governance [46]

B. Framework Comparison and Evaluation

We analyzed over 20 agentic AI frameworks identified in the literature, evaluating them across multiple dimensions including functionality, maturity, scalability, and governance capabilities. Table [table:frameworks] summarizes our evaluation of selected frameworks.

Table 1 Comparison of Agentic AI Frameworks

Framework	Primary Focus	Governance	Maturity	Key Strengths
LangChain	Development	Basic	High	Flexibility, community support
CrewAI	Multi-agent	Moderate	Medium	Orchestration capabilities
Microsoft Semantic Kernel	Enterprise	Advanced	High	Integration with Azure services
AWS Agentic AI	Cloud deployment	Advanced	High	AWS ecosystem integration
Kyndryl Framework	Business AI	Advanced	Medium	Industry-specific solutions

Our analysis indicates that while numerous frameworks exist, no single solution comprehensively addresses all requirements for enterprise-scale agentic AI deployment. Organizations typically need to combine multiple frameworks and custom development to meet their specific needs.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep978

Table 2 Agentic AI Governance Frameworks and Key Considerations

Governance Aspect	Key Principles	Frameworks & Standards	Implementation Considerations
Risk Management	Continuous risk assessment - Red teaming protocols - Systemic risk mitigation	NIST AI RMF [30] - FAIR-CAM framework [47] - Agentic AI Red Teaming [26]	Permission escalation testing - Hallucination mitigation - Memory manipulation safeguards
Compliance & Regulatory	GDPR/CCPA adherence - EU AI Act compliance - Sector-specific regulations	EU AI Act guidelines [19] - GenAI Compliance Framework [24] - ISO/IEC 42001 [21]	Regulatory gap analysis - Cross-border compliance - Audit trail requirements
Architectural Governance	Three-tier architecture - Foundation/Workflow/Autonomous layers - Trust before autonomy	Agentic AI Architecture Framework [18] - AWS Prescriptive Guidance [48] - AI Agent Infrastructure Stack [40]	Progressive autonomy deployment - Governance by design - Transparency requirements
Ethical Considerations	Bias mitigation - Transparency & explainability - Accountability frameworks	Ethical Guidelines Template [49] - AIGN Governance Framework [22] - OWASP Security Guidelines [29]	Ethical risk assessment - Human-in-the-loop requirements - Impact assessment protocols
Security & Identity	Zero-trust architecture - Agent identity management - Secure tool integration	New Identity Framework [50] - OWASP GenAI Security [28] - Securing Agentic Systems [43]	Permission boundaries - Tool access controls - Secure communication protocols
Operational Governance	Monitoring & observability - Performance metrics - Continuous improvement	Agentic AI Readiness [39] - Production-ready frameworks [38] - Operationalizing Trust [51]	Key performance indicators - Failure recovery protocols - Scalability considerations
Legal & Liability	Liability attribution - Legal personhood considerations - Contractual frameworks	Emerging Legal Frameworks [34] - Sedona Conference Guidance [52] - Legal Considerations [33]	Liability insurance requirementsContractual limitations - Dispute resolution mechanisms
Organizational Readiness	Cultural adaptation - Skills development - Change management	Strategic Guide [53] - 2025 Frontier Firm [2] - Implementation Best Practices [54]	Workforce training programs - Organizational structure adaptation - Leadership commitment

C. Governance Implementation Patterns

We identified several common patterns in how organizations are implementing governance for agentic AI systems:

➢ *Centralized Governance Models*

Large enterprises often establish centralized AI governance committees that develop policies, review implementations, and ensure compliance across the organization [55]. These models provide consistency but may lack agility.

➢ *Federated Governance Approaches*

Some organizations adopt federated models where central policies provide guidelines, but individual business units have flexibility in implementation details [41]. This approach balances consistency with adaptability.

➢ *Automated Governance Mechanisms*

Advanced implementations incorporate automated governance mechanisms directly into agentic AI systems [56]. These include real-time monitoring, compliance checking, and automated intervention capabilities.

➢ *Industry-Specific Governance*

Regulated industries such as healthcare and finance are developing specialized governance approaches that address their unique requirements [4], [17].

D. Security Implementation Status

Our analysis of security implementations reveals significant variation in maturity levels:

- Basic Security: Many early implementations focus primarily on traditional cybersecurity measures without specific adaptations for agentic AI characteristics [57]
- Intermediate Security: More mature implementations incorporate AI-specific security measures such as prompt injection protection, output validation, and adversarial robustness [58]
- Advanced Security: Leading-edge implementations employ comprehensive security frameworks that address unique agentic AI risks including permission escalation, memory manipulation, and multi-agent coordination attacks [26]

The majority of current implementations fall into the basic to intermediate categories, indicating significant opportunity for improvement in security practices.

VI. U.S. COMPETITIVENESS IN AGENTIC AI: INTEROPERABILITY AND GOVERNANCE STRATEGIES

The global race for AI supremacy has intensified, with agentic AI representing the next frontier of technological competition. As noted by [42], the United States faces significant challenges in maintaining its leadership position

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep978

due to fragmentation in AI development ecosystems and divergent approaches emerging between major economic regions. This section analyzes the current competitive landscape and proposes strategic interventions to ensure U.S. leadership in agentic AI through enhanced interoperability and governance frameworks.

A. Current Competitive Landscape

The global agentic AI landscape is characterized by increasing fragmentation and strategic competition. According to [42], divergent approaches are emerging between the United States, European Union, China, and other key players, each pursuing distinct strategies:

- United States: Market-driven innovation with sector-specific regulations and voluntary frameworks
- European Union: Comprehensive regulatory approach through the AI Act with risk-based classification [11], [19]
- China: State-directed development with strong government oversight and strategic prioritization
- Other Regions: Emerging frameworks in Singapore [37], UK, and other countries creating additional complexity

This fragmentation creates significant interoperability challenges that threaten to undermine U.S. competitiveness. As [42] notes, the lack of standardized protocols and frameworks hinders seamless collaboration across borders and domains, potentially isolating U.S. technologies from global markets.

B. Interoperability Challenges

The interoperability challenges facing U.S. agentic AI leadership are multifaceted and require urgent attention:

➢ *Technical Interoperability*

Technical interoperability issues include divergent data formats, model architectures, workflow orchestration approaches, and multi-agent communication protocols [42]. These technical barriers prevent seamless integration of U.S.-developed agentic AI systems with international platforms and infrastructure.

➢ *Regulatory Interoperability*

Regulatory divergence represents another critical challenge. The EU's risk-based AI Act [10], China's state-centric approach, and the U.S.'s sectoral strategies create incompatible compliance requirements that increase costs and complexity for U.S. companies seeking global deployment.

➢ *Standards Fragmentation*

The absence of universally adopted standards for agentic AI systems creates additional barriers. While organizations such as ISO/IEC JTC 1/SC 42, IEEE, and NIST are developing standards including ISO/IEC 42001 [21] for AI management systems and the NIST AI RMF [30], [31], adoption remains inconsistent across regions [20].

C. Strategic Proposal for U.S. Leadership

To maintain and enhance U.S. competitiveness in agentic AI, we propose a comprehensive strategy centered on interoperability and governance excellence:

➢ *Accelerate Standards Development and Adoption*

The U.S. should prioritize the development and adoption of open, interoperable standards for agentic AI systems. This includes:

- Establishing a public-private partnership for rapid standards development
- Creating certification programs for interoperability compliance
- Investing in reference implementations of key standards
- Promoting U.S. developed standards through international standards organizations

➢ *Develop Interoperability-First Governance Frameworks*

U.S. governance approaches should explicitly prioritize interoperability as a strategic objective:

- Incorporate interoperability requirements into federal AI procurement guidelines
- Create tax incentives for companies adopting interoperable architectures
- Establish testbeds for cross-border interoperability testing
- Develop model contractual clauses for international AI deployments

➢ *Enhance International Cooperation*

Strategic international engagement is essential for maintaining U.S. leadership:

- Lead multilateral initiatives for regulatory harmonization
- Establish bilateral interoperability agreements with key partners
- Create joint research programs focused on interoperability challenges
- Develop mutual recognition arrangements for AI certifications

➢ *Invest in Interoperability Research and Development*

Targeted R&D investment can address specific interoperability challenges:

- Fund research on cross-platform agent communication protocols [59]
- Support development of adaptive compliance tools for varying regulatory regimes
- Invest in privacy-preserving technologies for international data flows
- Develop tools for automated regulatory gap analysis and compliance mapping

➢ *Create Strategic Testing and Certification Infrastructure*

A robust testing and certification ecosystem can demonstrate U.S. leadership:

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep978

- Establish national testbeds for interoperability validation
- Create certification programs recognized internationally
- Develop benchmarking methodologies for cross-border performance assessment.
- Support independent verification of interoperability claims.

D. A National Strategic Framework for U.S. Leadership in Agentic AI

The global competition for agentic AI supremacy represents not merely a technological race but a foundational shift in economic and national security paradigms. As [42] comprehensively analyzes, divergent regulatory approaches and technical standards between major economic blocs threaten to fragment the global AI ecosystem, potentially isolating U.S. technologies and undermining American competitiveness. This fragmentation creates significant interoperability challenges that threaten to undermine U.S. technological leadership and economic advantage.

➢ *Our Analysis Identifies Three Critical Strategic Imperatives for Maintaining U.S. Leadership:*

- Standards Dominance: Control over emerging technical standards for agent communication, data formats, and security protocols.
- Regulatory Alignment: Development of interoperable governance frameworks that enable cross-border deployment while ensuring security and ethical compliance.
- Innovation Ecosystem: Fostering a robust public-private partnership ecosystem that accelerates research, development, and deployment of agentic AI technologies.

E. Strategic Implementation Framework

To address these imperatives, we propose a coordinated whole-of-government approach with specific responsibilities assigned to key agencies and branches:

➢ *For the National Institute of Standards and Technology (NIST)*

- Expand the AI RMF [30] to include specific guidelines for agentic AI interoperability, building on the generative AI profile [31]
- Develop standardized testing methodologies for cross-border compliance assessment and validation of agentic systems
- Create reference architectures for interoperable agentic systems that incorporate security-by-design principles [43]

➢ *For the Department of Commerce*

- Lead negotiations for international AI interoperability agreements, particularly with key allies and trading partners.
- Develop next-generation export control frameworks that balance national security concerns with maintaining U.S. competitiveness in AI technologies.
- Create advisory services and resource centers for U.S. companies navigating complex foreign regulations and compliance requirements.

➢ *For Congress*

- Enact legislation creating tax incentives for interoperability investment and research & development in agentic AI technologies
- Fund targeted research programs focused on AI interoperability challenges through NSF, DARPA, and other research agencies
- Establish a national AI competitiveness strategy with interoperability as a core pillar, mandating cross-agency coordination

➢ *For Regulatory Agencies (FDA, FAA, FCC, etc.)*

- Develop sector-specific interoperable compliance frameworks for regulated industries adopting agentic AI [4], [17]
- Create regulatory sandboxes for testing cross-border solutions and innovative approaches to compliance

➢ *Phased Implementation Roadmap*

The proposed strategy should be implemented through a structured, phased approach with clear milestones and accountability mechanisms:

- Year 1: Foundation Building - Establish standards development partnerships, create initial interoperability testbeds, develop international engagement frameworks, and launch initial research programs
- Years 2-3: Scaling & Expansion - Scale successful pilot programs, develop comprehensive certification programs, achieve international recognition agreements, and expand testing infrastructure
- Years 4-5: Full Implementation - Achieve comprehensive standards adoption, establish global certification recognition, implement full international cooperation framework, and mature the interoperability ecosystem

➢ *Expected Outcomes and Benefits*

Successful implementation of this comprehensive strategy would yield significant multidimensional benefits for U.S. competitiveness:

- Market Access: U.S. companies would gain easier access to international markets through interoperable solutions, reducing compliance costs by an estimated 30-40% [24]
- Innovation Leadership: A focus on interoperability would drive innovation in adaptable, flexible AI systems, maintaining U.S. technological advantage [2]
- Economic Advantage: Reduced compliance costs and increased market opportunities would enhance economic returns and create high-value jobs
- Security Benefits: Interoperable systems designed with security from inception would enhance overall resilience and protect critical infrastructure [44]

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep978

➢ *Conclusion on U.S. Competitiveness Strategy*

Maintaining U.S. leadership in agentic AI requires a strategic focus on interoperability and governance excellence. By proactively addressing the technical, regulatory, and standards challenges facing global deployment of agentic AI systems, the United States can transform potential barriers into sustainable competitive advantages

Table 3 Strategic Framework for U.S. Leadership in Agentic AI

Strategic Pillar	Key Initiatives	Supporting References & Standards
Standards Development & Adoption	- Public-private partnerships for rapid standards development - Interoperability certification programs - Reference implementations of key standards - International standards promotion	- NIST AI RMF [30] - ISO/IEC 42001 [21] - Emerging protocols [60] - Agent communication standards [59]
Interoperability First Governance	- Federal procurement guidelines with interoperability requirements - Tax incentives for interoperable architectures - Cross-border interoperability testbeds - Model contractual clauses for international deployments	- AI Governance by Design [61] - Agentic AI Governance Framework [22] - International compliance frameworks [10]
International Cooperation	- Multilateral regulatory harmonization initiatives - Bilateral interoperability agreements - Joint research programs on interoperability - Mutual recognition arrangements for certifications	- Global compliance strategies [25] - EU AI Act alignment [19] - Cross-border deployment frameworks [42]
Research & Development Investment	- Cross-platform agent communication protocols - Adaptive compliance tools for regulatory variations - Privacy-preserving international data flow technologies - Automated regulatory gap analysis tools	- Agentic AI Architecture Framework [18] - AI Agent Infrastructure Stack [40] - Security research [43]
Testing & Certification Infrastructure	National interoperability validation testbeds - Internationally recognized certification programs - Cross-border performance benchmarking - Independent verification of interoperability claims	Red teaming frameworks [26] - Security validation [44] - Compliance testing methodologies [24]
Policy Implementation Framework	NIST expansion of AI RMF for agentic AI - Commerce Department international agreements - Congressional tax incentives and funding - Regulatory agency interoperability frameworks	Policy recommendations [42] - Governance best practices [62] - Regulatory guidance [11]

VII. ARCHITECTURAL PROPOSAL

Based on our analysis of current frameworks and identified gaps, we propose a comprehensive architectural framework for responsible agentic AI deployment. This architecture addresses technical, governance, and operational requirements through a layered approach.

Table 4 Implementation Roadmap and Expected Outcomes

Timeline	Key Activities	Expected Outcomes
Year 1: Foundation Building	Establish standards development partnerships - Create initial interoperability testbeds - Develop international engagement frameworks - Launch initial research programs	Baseline standards established - Initial testbed operational - Framework agreements in place - Research agenda defined
Years 2–3: Scaling & Expansion	Scale successful pilot programs - Develop comprehensive certification programs - Achieve international recognition agreements - Expand testing infrastructure	Broad standards adoption - Certification ecosystem operational - Multiple international agreements - Robust testing capabilities
Years 4–5: Full Implementation	Comprehensive standards adoption - Global certification recognition - Full international cooperation framework - Mature interoperability ecosystem	Market access facilitation - Innovation leadership demonstrated - Standards influence maintained - Economic advantages realized
Strategic Benefits	Enhanced global market access - Maintained innovation leadership - Standards development influence - Economic competitiveness - Security resilience	Reduced compliance costs [24] - Increased market opportunities - Technical leadership [2] - Security advantages [44] - Global competitiveness [42]

➢ *Overall Architecture*

Our proposed architecture consists of five interconnected layers:

- Foundation Layer: Core AI capabilities including language models, reasoning engines, and perception modules

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep978

- Orchestration Layer: Coordination mechanisms for multi-agent systems, task decomposition, and workflow management
- Governance Layer: Policy enforcement, compliance monitoring, risk management, and ethical oversight
- Security Layer: Protection mechanisms for threats specific to agentic AI systems
- Interface Layer: Human-AI interaction capabilities including explainability, control mechanisms, and feedback loops

This layered approach ensures that governance and security considerations are integrated throughout the system rather than being added as afterthoughts.

➢ *Governance Integration Architecture*

A key innovation in our proposal is the deep integration of governance mechanisms throughout the architecture. We propose a "governance by design" approach where:

- Policy specifications are formally defined and machine-readable
- Compliance checking occurs in real-time during system operation * Automated remediation mechanisms can intervene when violations are detected * Comprehensive audit trails document all decisions and actions

This approach extends beyond traditional AI governance by addressing the unique challenges of autonomous systems capable of independent action.

➢ *Security Architecture*

Our security architecture incorporates several reviewed elements specifically designed for agentic AI systems:

- Agent Identity Management: Robust authentication and authorization mechanisms for AI agents [50]
- Behavioral Monitoring: Continuous assessment of agent behavior against expected patterns
- Multi-Agent Coordination Security: Protection against malicious coordination between agents
- Resilience Mechanisms: Capabilities for graceful degradation and fallback procedures

These security measures address the unique characteristics of agentic AI systems that differ from traditional software applications.

➢ *Implementation Considerations*

Implementing our proposed architecture requires addressing several practical considerations:

- Performance Overhead: Governance and security mechanisms introduce computational costs that must be balanced against system responsiveness
- Interoperability Requirements: Integration with existing systems and standards is essential for practical adoption
- Evolutionary Deployment: Organizations can incrementally implement aspects of the architecture rather than requiring complete replacement of existing systems
- Human-in-the-Loop Design: Appropriate levels of human oversight must be maintained based on risk assessment

We provide detailed guidance on addressing these considerations in different deployment scenarios.

VIII. FUTURE WORK AND EMERGING TRENDS

Based on our analysis of current developments and identified gaps, we identify several important directions for future work and emerging trends in agentic AI.

A. Research Directions

➢ *Advanced Governance Mechanisms*

Future research should develop more sophisticated governance mechanisms capable of handling the complexity of agentic AI systems. This includes:

- Dynamic policy adaptation based on context and risk assessment * Automated negotiation between conflicting policy requirements * Predictive compliance checking that anticipates potential violations before they occur.

➢ *Security Innovations*

Agentic AI introduces security challenges that require innovative solutions:

- Formal verification methods for autonomous system behavior * Adversarial resilience specifically designed for multi-agent scenarios * Privacy-preserving approaches for agent coordination and learning

➢ *Human-AI Collaboration*

Improving how humans and agentic AI systems collaborate remains a critical research area:

- Intuitive interfaces for monitoring and directing autonomous systems * Explanations tailored to different stakeholder needs and expertise levels * Control mechanisms that provide appropriate oversight without excessive burden

➢ *Standardization Efforts*

The development of standards will be crucial for interoperability and trust:

- Communication protocols between agents and with human systems * Safety and performance benchmarks for evaluating agentic AI systems * Certification processes for different levels of autonomy and application domains

B. Industry Trends

➢ *Vertical Specialization*

We anticipate increasing specialization of agentic AI frameworks for specific industries and use cases [4], [17]. This specialization will address domain-specific requirements and regulations.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep978

➢ *Platform Convergence*

The current fragmentation of frameworks is likely to give way to more integrated platforms that provide comprehensive capabilities for developing, deploying, and managing agentic AI systems [16].

➢ *Regulatory Evolution*

Regulatory frameworks will continue to evolve to address the unique challenges of agentic AI [10]. We expect to see more specific requirements for autonomous systems across different jurisdictions.

➢ *Skills Development*

As agentic AI becomes more prevalent, educational programs and training resources will emerge to address the skills shortage [46]. This includes both technical skills for development and governance skills for responsible deployment.

C. Emerging Technologies

Several emerging technologies show promise for addressing current limitations in agentic AI:

- Advanced Reasoning Models: Next-generation AI models with improved reasoning capabilities will enhance the effectiveness of agentic systems
- Explainability Techniques: New approaches for explaining complex autonomous decisions will improve transparency and trust
- Verification Tools: Formal methods for verifying agent behavior will address safety and compliance concerns
- Energy-Efficient Architectures: Sustainable AI approaches will reduce the environmental impact of widespread agentic AI deployment

These technological advancements will enable more capable, trustworthy, and sustainable agentic AI systems in the coming years.

Table 5 Proposed Architecture and Future Directions for Responsible Agentic AI

Dimension	Key Elements and Directions
Architecture Layers	**Foundation**: Core AI models, reasoning engines, perception modules **Orchestration**: Multi-agent coordination, task decomposition, workflow management **Governance**: Policy enforcement, compliance monitoring, risk management, ethical oversight **Security**: Agent identity management, behavioral monitoring, malicious coordination safeguards, resilience [50] **Interface**: Human-AI interaction, explainability, control mechanisms, feedback loops
Governance Integration	Governance by design: machine-readable policies, real-time compliance checks, automated remediation, comprehensive audit trails
Implementation Considerations	Performance overhead trade-offs; interoperability with existing systems; evolutionary deployment strategies; maintaining human-in-the-loop oversight
Research Directions	Advanced governance mechanisms (dynamic policy adaptation, predictive compliance) Security innovations (formal verification, adversarial resilience, privacy-preserving coordination) Human-AI collaboration (intuitive interfaces, stakeholder-specific explanations, efficient oversight) Standardization efforts (protocols, benchmarks, certification) [10]
Industry Trends	Vertical specialization of frameworks by sector [4], [17] Platform convergence into integrated ecosystems [16] Regulatory evolution with autonomy-specific requirements [10] Skills development initiatives to address workforce gaps [46]
Emerging Technologies	Advanced reasoning models; explainability techniques; formal verification tools; energy-efficient architectures

IX. POTENTIAL NEGATIVE SCENARIOS WITHOUT PROACTIVE INTEROPERABILITY GOVERNANCE

The rapid advancement of agentic AI systems presents significant risks if interoperability governance frameworks are not established proactively. This section outlines potential negative scenarios that could emerge without adequate governance measures.

➢ *Technical Fragmentation and Ecosystem Balkanization*

Without standardized interoperability frameworks, the agentic AI ecosystem risks severe fragmentation:

- Proprietary Silos: Major technology vendors may develop closed ecosystems that lock users into specific platforms, limiting choice and innovation [16], [63]
- Integration Challenges: Organizations will face significant technical barriers when attempting to connect AI systems from different providers, increasing implementation costs and complexity [38], [40]
- Reduced Innovation: Startups and smaller developers may struggle to compete in a fragmented market, potentially stifling innovation and reducing competitive pressure on established players [2], [53]

➢ *Regulatory Compliance Challenges*

The absence of interoperability-focused governance could create insurmountable compliance obstacles:

- Cross-Border Deployment Barriers: Companies operating internationally may face incompatible regulatory requirements, forcing them to maintain separate AI systems for different jurisdictions [10], [25]
- Compliance Complexity: Organizations will need to navigate multiple, potentially conflicting regulatory frameworks simultaneously, increasing compliance costs and operational risks [11], [24]

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep978

- Audit and Transparency Issues: Without standardized interfaces and data formats, demonstrating compliance and conducting effective audits becomes increasingly difficult [64], [65]

➢ *Security and Safety Risks*

Interoperability gaps create significant security vulnerabilities and safety concerns:

- Security Vulnerabilities: Incompatible security models and communication protocols create attack surfaces that malicious actors could exploit [43], [44]
- Safety Assurance Challenges: Ensuring safe interactions between AI systems from different providers becomes extremely difficult without standardized safety protocols [26], [29]
- Incident Response Limitations: Security incidents may spread across system boundaries before they can be contained, due to inadequate interoperability in security monitoring and response mechanisms [6], [66]

➢ *Economic and Competitive Disadvantages*

The lack of interoperability governance could negatively impact economic growth and competitiveness:

- Reduced Market Efficiency: Organizations may be forced to make suboptimal technology choices based on interoperability constraints rather than functional capabilities [4], [67]
- Increased Costs: Businesses will face higher integration costs, maintenance expenses, and training requirements for managing multiple incompatible systems [39], [54]
- Competitive Disadvantage: Companies operating in regions without interoperability standards may find themselves at a competitive disadvantage in global markets [7], [42]

➢ *Ethical and Societal Concerns*

Interoperability failures could exacerbate existing ethical challenges and create new societal risks:

- Accountability Gaps: Determining responsibility for outcomes involving multiple AI systems becomes challenging without clear interoperability standards and governance frameworks [9], [23]
- Bias Amplification: Incompatible systems may inadvertently amplify biases when exchanging information or making collaborative decisions [35], [68]
- Access and Equity Issues: Fragmented ecosystems may create digital divides, where certain populations or organizations cannot access the full benefits of agentic AI due to interoperability barriers [69], [70]

➢ *Global Governance Fragmentation*

The absence of international interoperability standards could lead to problematic governance fragmentation:

- Regulatory Arbitrage: Companies might engage in jurisdiction shopping, operating from regions with the most lenient regulations rather than the most appropriate standards [71], [72]
- Standards Competition: Competing standards ecosystems could emerge, led by different geopolitical blocs, creating technical barriers that mirror political divisions [21], [60]
- International Cooperation Challenges: Cross-border collaboration on AI safety, security, and ethics becomes more difficult without shared technical foundations and governance approaches [73], [74]

➢ *Innovation Stagnation and Technical Debt*

Long-term consequences of interoperability neglect could include innovation stagnation:

- Technical Debt Accumulation: Organizations will accumulate significant technical debt from building and maintaining custom integration solutions [5], [75]
- Research Fragmentation: Academic and industrial research may become fragmented across incompatible platforms, reducing the collective advancement of the field [76], [77]
- Adaptability Limitations: Systems built without interoperability considerations may struggle to adapt to new technologies, regulations, or business requirements [18], [78]

➢ *Mitigation Strategies for Avoiding Negative Scenarios*

To prevent these negative outcomes, several proactive measures should be considered:

- Early Standardization: Accelerate development and adoption of open interoperability standards through industry consortia and public-private partnerships [20], [79]
- Regulatory Alignment: Encourage regulatory bodies to incorporate interoperability requirements into AI governance frameworks [22], [80]
- International Cooperation: Foster multilateral agreements on AI interoperability standards and governance approaches [42], [59]
- Industry Best Practices: Develop and promote interoperability best practices through industry associations and professional organizations [62], [81]

➢ *Conclusion on Risk Scenarios*

The potential negative scenarios outlined above demonstrate the critical importance of proactive interoperability governance for agentic AI systems. Without concerted effort to establish standards, frameworks, and governance mechanisms, the ecosystem risks fragmentation, security vulnerabilities, economic inefficiencies, and ethical challenges that could undermine the transformative potential of this technology.

The time to address these challenges is now, during the formative stages of agentic AI development and deployment. By learning from the interoperability challenges that have affected other technology domains and proactively addressing these issues, stakeholders can help ensure that agentic AI

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep978

develops in a way that maximizes benefits while minimizing risks [12], [31].

X. CONCLUSION

The current state of agentic AI is characterized by enthusiastic adoption—with 61% of organizations building systems—coupled with significant challenges including high failure rates, governance gaps, and security concerns. While numerous frameworks exist, no single solution comprehensively addresses the requirements for enterprise-scale deployment, particularly regarding governance and security.

Our suggested architectural (from literature) framework provides a structured approach for responsible agentic AI deployment, integrating governance and security considerations throughout the system design. This "governance by design" approach addresses the unique challenges posed by autonomous systems capable of independent action.

We have also reviewed: advanced governance mechanisms, security innovations, improved human-AI collaboration, and standardization efforts. Our analysis underscores the transformative potential of agentic systems across various sectors, tempered by substantial hurdles in governance, security, and standardization.

The research identified a critical gap between the development of autonomous capabilities and the frameworks needed to ensure their responsible deployment. Technical complexity, regulatory uncertainty, and security vulnerabilities present formidable barriers to successful implementation. In response, we proposed an architectural framework built on a governance-by-design principle, integrating oversight and security mechanisms throughout the system layers to address the unique challenges of autonomous action.

Furthermore, the paper highlighted the urgent need for interoperability standards to prevent ecosystem fragmentation and maintain global competitiveness. The strategic framework outlined for leadership emphasizes accelerating standards development, fostering international cooperation, and investing in targeted research.

Proactive governance is not merely beneficial but essential to mitigate risks such as technical silos, compliance complexity, and security vulnerabilities that could otherwise undermine the technology's potential.

DECLARATION

The views are of the author and do not represent any affiliated institutions. Work is done as a part of independent research. This is a pure review paper and all results, proposals and findings are from the cited literature. Author does not claim any novel findings.

REFERENCES

[1]. "Agentic AI: Autonomy Is Coming—Are You Ready to Control It?" Gartner. https://www.gartner.com/en/articles/agentic-ai-for-vendors.

[2]. "2025: The year the Frontier Firm is born." https://www.microsoft.com/en-us/worklab/work-trend-index/2025-the-year-the-frontier-firm-is-born.

[3]. J. Ramachandran, "Agentic AI Systems: Opportunities, Challenges, and the Need for Robust Governance," C5i. Mar. 2024.

[4]. P. Scheffler, "Agentic AI in Banking Strategy Guide for C-Level Leaders," Neontri. Sep. 2025.

[5]. "Agentic AI Development Framework: Product & Engineering Guide Invene." https://www.invene.com/blog/what-are-you-really-asking-for-with-genai-agents.

[6]. "CrowdStrike Launches Agentic Security Workforce to Transform the SOC." https://www.crowdstrike.com/en-us/blog/crowdstrike-delivers-seven-agents-to-build-agentic-security-workforce/.

[7]. "How Agentic AI will transform financial services World Economic Forum." https://www.weforum.org/stories/2024/12/agentic-ai-financial-services-autonomy-efficiency-and-inclusion/.

[8]. "How agentic AI is transforming IT: A CIO's guide." https://www.sap.com/estonia/resources/how-agentic-ai-transforms-it-cio-guide.

[9]. "Agentic AI Governance Framework," AIGN.

[10]. C. Wick, "Agentic AI Regulatory Landscape: Navigating Global Compliance." Jun. 2025.

[11]. S. Pearcy, "Governing Agentic AI," HiddenLayer Security for AI. May 2025.

[12]. Y. Shavit et al., "Practices for Governing Agentic AI Systems."

[13]. U. Inc, "What is Agentic AI? UiPath." https://www.uipath.com/ai/agentic-ai.

[14]. "LangSmith." https://www.langchain.com/langsmith.

[15]. S. Arya, "Top 7 Frameworks for Building AI Agents in 2025," Analytics Vidhya. Jul. 2024.

[16]. T. Akka, "Agentic AI frameworks for enterprise scale: A 2025 guide." https://akka.io/blog/agentic-ai-frameworks, Aug. 2025.

[17]. "How GenAI Agent Frameworks Enhance GxP Compliance." https://www.continuousintelligence.ai/blog/how-genai-agent-frameworks-enhance-gxp-compliance.

[18]. "Agentic AI Architecture Framework for Enterprises," InfoQ. https://www.infoq.com/articles/agentic-ai-architecture-framework/.

[19]. M. M. C. Borrelli, "How to use agentic AI in line with the EU AI Act," CX Network. https://www.cxnetwork.com/artificial-intelligence/articles/how-to-use-agentic-ai-in-line-with-the-eu-ai-act, Feb. 2025.

[20]. S. Manjrekar, "Some of the open source standards used with AI agents or agentic frameworks," Fabrix.ai. Mar. 2025."ISO/IEC 42001:2023," ISO. https://www.iso.org/standard/42001.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep978

[21]. "AIGN Agentic AI Governance Framework v1.0," AI Governance Library. https://www.aigl.blog/aign-agentic-ai-governance-framework-v1-0/, Jul. 2025.
[22]. Pdiaz, "Agentic AI Governance: The Future of AI Oversight," BigID. Mar. 2025.
[23]. "GenAI Compliance Framework: GDPR CCPA Rules Guide 2025." https://futureagi.com/blogs/genai-compliance-framework-2025.
[24]. I. Berger, "GenAI Regulation: What Enterprises Must Know About EU, U.S. And Global Compliance," ActiveFence. Jun. 2025.
[25]. "Agentic AI Red Teaming Guide CSA." https://cloudsecurityalliance.org/artifacts/agentic-ai-red-teaming-guide.
[26]. "Agentic Misalignment: How LLMs could be insider threats." https://www.anthropic.com/research/agentic-misalignment.
[27]. "Home - OWASP Gen AI Security Project." https://genai.owasp.org/.
[28]. O. Editor, "Securing Agentic Applications Guide 1.0," OWASP Gen AI Security Project.
[29]. "AI Risk Management Framework," NIST, Jul. 2021.
[30]. National Institute of Standards and Technology (US), "Artificial intelligence risk management framework : Generative artificial intelligence profile," National Institute of Standards and Technology (U.S.), Gaithersburg, MD, error: 600-1, Jul. 2024. doi: 10.6028/NIST.AI.600-1.
[31]. "Ethical Considerations of Implementing Agentic AI." https://www.ema.co/additional-blogs/addition-blogs/ethical-considerations-implementing-agentic-ai.
[32]. "ENS - News - Understanding Agentic AI and Generative AI: Legal and ethical considerations." https://www.ensafrica.com/news/detail/10142/understanding-agentic-ai-and-generative-ai-le.
[33]. bklemm@foley.com, "The Intersection of Agentic AI and Emerging Legal Frameworks," Foley & Lardner LLP. Dec. 2024.
[34]. Lucinity, "Understanding Ethical Agentic AI in Compliance - Transform FinCrime Operations & Investigations with AI." https://lucinity.com/blog/ethical-considerations-in-deploying-agentic-ai-for-aml-compliance, Jan. 2025.
[35]. "Agentic AI: Navigating the Tension Between Privacy and the Next Generation of AI Webinar Resources OneTrust." https://www.onetrust.com/resources/agentic-ai-navigating-the-tension-between-privacy-and-the-next-generation-of-ai-webinar/.
[36]. "Agentic AI Primer," Singapore Government Developer Portal. https://www.developer.tech.gov.sg/guidelines/standards-and-best-practices/agentic-ai-primer.html, Sep. 2025.
[37]. "Building Production-Ready AI Agents: What Your Framework Needs Diagrid Blog." https://www.diagrid.io/blog/building-production-ready-ai-agents-what-your-framework-needs.
[38]. "Agentic AI Readiness: A Strategic Guide to Preparing Your Enterprise Processes Mimica." https://www.mimica.ai/guides/agentic-ai-readiness-guide.
[39]. "AI Agent Infrastructure Stack for Agentic Systems." https://www.xenonstack.com/blog/ai-agent-infrastructure-stack.
[40]. "AI Governance Frameworks: Guide to Ethical AI Implementation." https://www.consilien.com/news/ai-governance-frameworks-guide-to-ethical-ai-implementation.
[41]. Satyadhar Joshi, "Securing U.S. AI Leadership: A policy guide for regulation, standards and interoperability frameworks," International Journal of Science and Research Archive, vol. 16, no. 3, pp. 001–026, Sep. 2025, doi: 10.30574/ijsra.2025.16.3.2519.
[42]. E. Estrin, "Securing Agentic AI Systems," Medium. https://aws.plainenglish.io/securing-agentic-ai-systems-a04804eb0b01, Sep. 2025.
[43]. "Securing the Future of Agentic AI: Governance, Cybersecurity, and Privacy Considerations Community." https://security.googlecloudcommunity.com/community-blog-42/securing-the-future-of-agentic-ai-governance-cybersecurity-and-privacy-considerations-3992, May 2025.
[44]. "Building a Governance Framework for Agentic AI Systems DEVOPSdigest." https://www.devopsdigest.com/building-a-governance-framework-for-agentic-ai-systems.
[45]. "AI trends : Adoption barriers and updated predictions Deloitte US." https://www.deloitte.com/us/en/services/consulting/blogs/ai-adoption-challenges-ai-trends.html.
[46]. D. Wan, "Taming Agentic AI risks with FAIR-CAM." https://www.fairinstitute.org/blog/taming-agentic-ai-risks-with-fair-cam, Mar. 2025.
[47]. "AWS Prescriptive Guidance - Agentic AI frameworks, protocols, and tools on AWS."
[48]. T. DigitalDefynd, "Ethical Guidelines Template for Agentic AI Development [2025]," DigitalDefynd. Jan. 2025.
[49]. "A New Identity Framework for AI Agents." https://community.cisco.com/t5/security-blogs/a-new-identity-framework-for-ai-agents/ba-p/5294337, May 2025.
[50]. "Operationalizing trust: A C-level framework for scaling genAI responsibly," CIO.
[51]. "Sedona Conference WorkGroup 13 on Legal Reform, Guidance on AI Im." https://natlawreview.com/article/sedona-conference-working-group-13-contemplates-potential-legal-reform-practical.
[52]. M. Mittal, "Embracing Agentic AI: A Strategic Guide To Transformative Intelligence," Forbes. https://www.forbes.com/councils/forbestechcouncil/2025/01/09/embracing-agentic-ai-a-strategic-guide-to-transformative-intelligence/.
[53]. E. Barnum, "Implementing Agentic AI in Procurement: Best Practices & Strategies," Ivalua. Apr. 2025.
[54]. "What is AI Governance? ModelOp." https://www.modelop.com/ai-governance.
[55]. "Automating responsible AI principles with agentic AI in digital triplets CGI.com."

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25sep978

https://www.cgi.com/en/blog/artificial-intelligence/automating-responsible-ai-principles-agentic-ai-digital-triplets.
[56]. "Securing Your LLM Systems: A Step-by-Step Guide to Agentic AI Governance LinkedIn." https://www.linkedin.com/pulse/securing-your-llm-systems-step-by-step-guide-agentic-ai-amit-shivpuja-zdx9c/.
[57]. "Lakera: The AI-Native Security Platform to Accelerate GenAI." https://www.lakera.ai/.
[58]. K. M. Winkler Michael, "The rise of agentic AI part 1: Understanding MCP, A2A, and the future of automation," Dynatrace news. May 2025.
[59]. StaxWP and S. Tools, "Emerging Protocols, Frameworks, and Standards for Agentic AI - AI Tools Catalog." https://smarttools.ai/emerging-protocols-frameworks-and-standards-for-agentic-ai/, May 2025.
[60]. "AI Governance by Design for Agentic Systems: A Framework for Responsible Development and Deployment[v1] Preprints.org." https://www.preprints.org/manuscript/202504.1707/v1
[61]. "4 Best Practices for Robust Agentic AI Governance." https://www.teksystems.com/en-nz/insights/article/agentic-ai-governance.
[62]. "Agentic AI frameworks - AWS Prescriptive Guidance." https://docs.aws.amazon.com/prescriptive-guidance/latest/agentic-ai-frameworks/frameworks.html.
[63]. "Agentic AI in Data Governance and Compliance." https://www.xenonstack.com/blog/agentic-ai-governance-compliance.
[64]. "AI Governance Platforms: Ensuring Ethical AI Implementation." https://www.techmahindra.com/insights/views/ai-governance-platforms-ensuring-ethical-ai-implementation/.
[65]. "NET AI agent security and governance." https://www.cloudflare.com/the-net/building-cyber-resilience/secure-govern-ai-agents/.
[66]. "Agentic and Generative AI 2025 Buyers Guide Executive Summary." https://research.isg-one.com/buyers-guide/artificial-intelligence/generative-ai/agentic-and-generative-ai/2025.
[67]. "Ethical Challenges and Governance in Agentic AI: Risks, Bias, and Regulations." https://www.rezolve.ai/blog/ethical-challenges-and-governance-in-agentic-ai.
[68]. "AI Insights: Agentic AI (HTML)," GOV.UK. https://www.gov.uk/government/publications/ai-insights/ai-insights-agentic-ai-html.
[69]. "The Enterprise Guide to GenAI, Co-pilots, and Agentic AI," Low Code Minds. https://www.lowcodeminds.com/blogs/the-enterprise-guide-to-gen-ai-autonomous-ai-co-pilots-and-agentic-ai.
[70]. "Navigating Regulatory Challenges in Agentic AI Systems." https://natlawreview.com/article/when-ai-acts-independently-legal-considerations-agentic-ai-systems.
[71]. P. Upmann, "What Regulatory Frameworks Are Needed to Ensure the Safe Deployment of AI Systems?" AIGN. Dec. 2024.
[72]. "Agents for good? Reconciling agentic AI with existing AI governance frameworks." https://www.techuk.org/resource/agents-for-good-reconciling-agentic-ai-with-existing-ai-governance-frameworks.html.
[73]. "Practices for Governing Agentic AI Systems." https://openai.com/index/practices-for-governing-agentic-ai-systems/, Feb. 2024.
[74]. Engineer@Heart, "The 2025 Guide to Choosing the Right Agentic AI Framework for Your Needs," Medium. Apr. 2025.
[75]. "The Agentic AI Era: A Primer. Technical and Implementation Guidelines by Kaush B Towards AI." https://pub.towardsai.net/the-agentic-ai-era-a-primer-6fe10b106153.
[76]. Mahendra Medapati, "The Ultimate Guide to Agentic AI Frameworks in 2025: Which One Should You Choose to Build the…," Medium. https://pub.towardsai.net/the-ultimate-guide-to-agentic-ai-frameworks-in-2025-which-one-should-you-choose-to-build-the-a1f861f403d8, Jul. 2025.
[77]. "Principles of Agentic AI Governance in 2025: Key Frameworks and Why They Matter Now," Arion Research LLC. https://www.arionresearch.com/blog/g9jiv24e3058xsivw6dig7h6py7wml.
[78]. "Developing Standards for Agentic AI - Akitra." https://akitra.com/developing-standards-for-agentic-ai/.
[79]. J. Hardy, "AI Governance in an Era of Agentic Automation," SSON. https://www.ssonetwork.com/intelligent-automation/articles/ai-governance-in-an-era-of-agentic-automation, Feb. 2025.
[80]. "8 agentic AI governance strategies: A complete guide TechTarget," Search Enterprise AI. https://www.techtarget.com/searchenterpriseai/tip/Agentic-AI-governance-strategies-A-complete-guide.
[81]. Joshi, S. National Framework for Agentic Generative AI in Cancer Care: Policy Recommendations and System Architecture. Preprints 2025, 2025091100. https://doi.org/10.20944/preprints202509.1100.v1
[82]. Joshi, S. Framework for Government Policy on Agentic and Generative AI in Healthcare: Governance, Regulation, and Risk Management of Open-Source and Proprietary Models. Preprints 2025, 2025091087. https://doi.org/10.20944/preprints202509.1087.v1
[83]. Joshi, S. Medicare and Medicaid Healthcare Access and Affordability Using Agentic Generative AI and AGI: Policy Implications and Guidelines. Preprints 2025, 2025091269. https://doi.org/10.20944/preprints202509.1269.v1
[84]. Joshi, S. Agentic GenAI for Infectious Disease Management: A Comprehensive Review. Preprints 2025, 2025091333. https://doi.org/10.20944/preprints202509.1333.v1