NextGen Scientific Publication
American International Journal of Computer Science and Technology

Volume 8 Issue 4, Pg. No. 36-49, AIJCST-V8I4P104, 2026
https://doi.org/10.63282/3117-5481/AIJCST-V8I4P104

Original Article

Responsible Enterprise Modernization through Secure AI and Cloud-Native Service Now Automation

***Dr. Emily Carter**
Computer Science, Northbridge International University, United Kingdom.

Abstract:

Enterprises are transforming to embrace Artificial Intelligence (AI) and accelerate business outcomes. The application of AI technology needs to occur in a controlled environment, with appropriate risk management in place to ensure longevity of the systems. Hence the desired outcome is to adopt an AI governance framework mapped to an enterprise service delivery solution that supports the detection and remediation of trust, safety, security and compliance risks relating to the AI operations across its lifecycle, as well as in the data used to train, develop and run the AI models. Therewith, a Cloud-Native, Security-centric and Compliant AI-Driven Automation Framework for ServiceNow is articulated. The framework allows for various AI services to be developed, operated and maintained safely, securely and in a controlled responsive manner aligned to AI Governance principles throughout the lifecycle. The framework operates within a Cloud-Native model with all applications comprising SaaS/IaaS/PaaS being developed and deployed under the principles of zero-trust with least-privilege identity and access management considerations. The completed framework provides the foundation for continuously improving the Security-Centric and Compliance controls.

Keywords:

SAI Governance Frameworks, Cloud-Native AI Systems, Security-Centric Automation, Servicenow AI Integration, Zero-Trust Architecture, AI Risk Management, Compliance-Driven AI Operations, Identity And Access Control, AI Lifecycle Governance, Secure AI Deployment.

Article History:

Received: 19.05.2026

Revised: 20.06.2026

Accepted: 29.06.2026

Published: 08.07.2026

1. Introduction

1.1. Enterprise Transformation with ServiceNow Intelligent Automation

Artificial Intelligence (AI) continues to advance both technical capabilities and broader consumption across various process services. These developments enable not only the intelligent augmentation of human work but also their transition into AI-driven Autonomous Enterprise Services. Enterprise transformation—the integrated redesign of activities, processes, functions, and structures—is within reach for many organizations as the potential for reimagining service delivery allows the reinvention of entire organizations in line with customer and market expectations.

Research in natural language processing, including Large Language Models (LLM) and Multimodal LLM, as well as Stable Diffusion, has empowered organizations to innovate and automate services beyond previous industry constraints. The natural-language, knowledge-based ServiceNow Support Portal has allowed thousands of organizations to offer a Natural Language-enabled, AI-based Self-service experience to enterprise users. LLM capabilities have accelerated the automation of IT and business processes. Such intelligent automation reduces manual effort in developing Data Pipelines for Artificial Intelligence. New Generative Artificial Intelligence Development framework automates the development life cycle for machine-learning-based Artificial Intelligence. Furthermore, ServiceNow WorkFlow AI can be used to exercise the full potential of technology to augment human work in both IT and business processes and to reduce manual operator effort.

2. Foundational Concepts

Cloud-native platform architecture operating within the ServiceNow intelligent automation ecosystem. The seven modular components are (1) a decision support platform, (2) a security and risk management engine, (3) a compliance automation engine, (4) a capability for managing Natural Language Generation services, (5) a platform for managing and measuring ethical AI, (6) a solution for establishing guardrails for the use of generative services, and (7) Business Process and Application discovery service, integrating generative and traditional techniques, powered by Business Capabilities and Forrester Business Process Mining.

Security and compliance shortcomings are primary inhibitors to the safe adoption of enterprise-wide AI consumption and providing external-facing generative services, such as chatbots. The objective, therefore, is to make safety and compliance considerations a first-class concern in ServiceNow automation by managing the AI safety and compliance within the ecosystem. Responsible AI initiatives fall within a risk and governance lifecycle encompassing the management and operation of AI services, namely the security, risk, compliance, ethical, safety and support functions. The corresponding rhythms for oversight and supervision of AI are defined, including the associated metrics, controls and tools, implementing configure-and-manage capabilities for safety and compliance.

Enterprise Transformation, when crossing the points of resistance and friction, is an extremely difficult journey. An approach for overcoming these difficulties, namely, creating a factory in the cloud to provide support for the SAFE transformation is proposed. The Adage that "All Roads Lead to Rome" is applied to Enterprise Transformation: "All Roads Lead to Cloud-Native." Building upon the foundation of service-oriented architecture, Declan Denehan, the architect of ServiceNow Intelligent Automation, considers this foundation as only one part of a triad: "Cloud-Native Architecture + Service-Oriented Components + Intelligent Automation = ServiceNow." The driving principle is to focus on business outcomes by automating everything that can be automated through a cloud-native architecture that connects into and across all enterprise applications and services, particularly into the ServiceNow ecosystem using Power Platform connectors.

Table 1. Dataset and Architecture Summary

Architecture	AI Governance	Key Mechanism	Deployment Mode	Latency Target
Model A	None	Rule-based threshold alerts	On-premise legacy	>300 ms
Model B	Partial	Supervised ML classifiers	Hybrid cloud	<250 ms
Model C	Moderate	Cloud-native LSTM anomaly detection	SaaS/IaaS	<150 ms
Model D (SNIA)	Full lifecycle	Federated AI + Zero-Trust + Explainability	Cloud-Native PaaS	<60 ms

2.1. AI Governance and Ethics

The need for secure and responsible artificial intelligence (AI) systems, which interpret the emerging technology through a lens of ethics and risk, is a pressing issue on both private and public agendas. AI-enabled enterprise solutions are faced with a multitude of risks that could undermine their efficacy, limit value extraction, and discourage large-scale adoption. ServiceNow, one of the major enterprise automation platforms, is a typical AI-rich ecosystem, in which cybersecurity, privacy, ethics, and compliance are crucial considerations for the brands that implement it. Governance experts, architects, developers, and operators responsible for these areas must collaborate to design, implement, and enforce the necessary controls, policies, and processes that underpin the foundation of a safe and compliant AI ecosystem, including organizational AI policies. A cloud-native framework can support AI development and deployment throughout the service lifecycle, but practical operations are still needed for consistent application of safety and compliance considerations across the use of generative AI, machine learning, natural language processing, and computer vision. Translating the fundamental principles of AI safety and compliance into operations provides the playbook to ensure correct practices are consistently applied. This requires identifying the operational rhythms that guarantee adequate oversight of the service, as well as the mechanisms that provide insight to continuously enhance those services.

Organizational policies and procedures are a crucial mechanism for embedding AI safety and compliance, as they formalize the required controls and processes for specific domains, such as Identity and Access Management (IAM) or Data Privacy. Building a policy framework that maps to international standards and industry regulations is a vital step in addressing AI risk. Operationalizing Safety and Compliance is designed to guide the construction of an AI policy framework that logically maps the necessary safety and compliance controls to the applicable standards and regulations for the organization.

3. Research Approach

The research problem is operationalized through a structured investigation that balances prescriptive and descriptive knowledge. The methodological approach comprises four main parts: a literature review that addresses the research questions and substantiates the proposed framework, the foundation of a canonical model driven by three cloud-native design patterns, a validation of the constructed knowledge against the emerging literature, and a generative outline of books built upon the findings. Data sources include government publications, the MITRE ATLAS framework for trustworthy artificial intelligence, trusted frameworks for ethical artificial intelligence, and trusted cloud security and privacy principles from the Cloud Security Alliance.

Research rigor is achieved through the thoroughness of the supporting knowledge review, the support of a respected adapted model of enterprise governance for the canon of frameworks, databases, and design patterns assembled under the canonical architecture and the internal and external validation of the proposed knowledge. The constructed canonical knowledge directly supports the ServiceNow community through design patterns and an integrated AI pace-layered network of cloud-native, security- and compliance-aware, intelligent-automation-driven, and regulated enterprises.

3.1. Managing Identity and Access

Governance of identity and access is paramount for secure enterprise transformation. Identity and access management (IAM) aims to ensure that only authenticated and authorized users have access to enterprise resources. Users should have the least privilege necessary to perform their duties, a principle that aligns with the concept of zero trust: no component should be trusted by default. Self-service features empower users while enabling monitoring and auditing to identify and respond to abuse. Humans are the weakest link in security; phishers exploit human credulity and information leakage. Credential hygiene is essential to mitigate these risks. The use of usernames and passwords should be avoided wherever feasible, especially for high-privilege roles.

Identity and access management govern which identities can access enterprise assets. AI accelerates the transformation of enterprises; protecting its use is vital to avoid unwanted consequences. Processes that define, manage, and control access are essential by-products of any ServiceNow enterprise implementation. Insufficiently defined processes or those managed by home-grown software can lead to vulnerabilities being exploited. Identity and access management controls constitute one of the three pillars of cybersecurity that must be addressed. Leading enterprises treat access to human resources as one of the most important areas; their focus is primarily on reducing the likelihood of a successful attack.

3.2. Mathematical Formulation

3.2.1. System Quality Function

The overall system quality of the SNIA unified automation pipeline integrates the quality contributions across the AI governance lifecycle:

$$Q_{total} = Q_{govern} + Q_{detect} + Q_{comply} + Q_{latency} + Q_{priv} \quad \text{(Eq. 1)}$$

Where Q_{govern} denotes AI governance quality (policy adherence + explainability), Q_{detect} represents automated detection accuracy, Q_{comply} captures compliance assurance quality, $Q_{latency}$ reflects real-time latency compliance, and Q_{priv} measures privacy preservation across the zero-trust boundary.

3.2.2. API Response Latency Model

The API response latency dynamics within the ServiceNow automation pipeline are modeled as a continuous differential system:

$$\partial L/\partial t = \lambda_{request} - \mu_{process} \quad \text{(Eq. 2)}$$

Where L is the end-to-end automation response latency (ms), $\lambda_{request}$ is the incoming automation request arrival rate, and $\mu_{process}$ is the on-premise ServiceNow processing throughput rate. Stability requires $\mu_{process} > \lambda_{request}$.

3.2.3. AI Automation F1-Score

The AI automation accuracy is measured using the F1-Score across incident classification, access anomaly detection, and compliance violation identification:

$$F1_{auto} = (2 \cdot Precision \cdot Recall) / (Precision + Recall) \quad \text{(Eq. 3)}$$

Where Precision and Recall are derived from the confusion matrix outcomes across automated triage, incident categorization, and identity anomaly detection tasks within the ServiceNow workflow engine.

3.2.4. AI Governance Cross-Domain Interaction

The governance scoring mechanism integrates contributions from AI risk management, identity access control, and compliance monitoring:

$$g'(t) = g(t) + \alpha \cdot c(t) + \beta \cdot i(t) \quad \text{(Eq. 4)}$$

Where $g(t)$ is the base governance quality score, $c(t)$ is the compliance score from automated auditing, $i(t)$ is the identity anomaly score from zero-trust IAM modules, and α, β are domain-coupling weighting coefficients.

3.2.5. Weighted Automation Decision Fusion

The unified automation decision fusion integrates risk signals from AI safety, compliance controls, and IAM:

$$s'(t) = w_1 \cdot g(t) + w_2 \cdot c(t) + w_3 \cdot i(t) + w_4 \cdot g(t) \cdot c(t) \quad \text{(Eq. 5)}$$

Where w_1, w_2, w_3, w_4 are learnable weighting coefficients. The interaction term $g(t) \cdot c(t)$ models the nonlinear coupling between AI governance risk indicators and compliance audit signals, enabling context-aware automation decisions.

3.2.6. Privacy Preservation Score

Under zero-trust architecture principles, the privacy preservation score quantifies the fraction of enterprise data processed locally without external transmission:

$$S_{priv} = 1 - (D_{transmitted} / D_{total}) \quad \text{(Eq. 6)}$$

Where $D_{transmitted}$ is the volume of raw enterprise data transmitted externally (to third-party AI APIs or cloud endpoints), and D_{total} is the total data processed by the automation pipeline.

3.2.7. Cloud-Native Resource Utilization

The cloud resource utilization ratio for the ServiceNow automation platform is given by:

$$U = R_{used} / R_{available} \quad \text{(Eq. 7)}$$

Where R used is the consumed computational resource (CPU cycles, memory, IaaS/PaaS capacity) and $R_{available}$ is the total provisioned capacity within the cloud-native deployment environment.

3.2.8. Federated Governance Efficiency

The efficiency of the federated AI governance mechanism — enabling cross-enterprise model updates without raw data sharing — is modeled as:

$$E_{FL} = (F1_{auto} \cdot S_{priv}) / T_{round} \quad \text{(Eq. 8)}$$

Where T_{round} is the duration of a federated governance synchronization round, encompassing model aggregation across enterprise nodes without transmitting sensitive operational data.

3.2.9. Adaptive Compliance Thresholding

To accommodate dynamic regulatory environments and evolving AI risk profiles, adaptive compliance thresholds are employed:

$$\theta(t) = \theta_0 + \gamma \cdot \sigma_{risk}(t) + \delta \cdot drift(t) \quad \text{(Eq. 9)}$$

Where θ_0 is the baseline compliance threshold, $\sigma_{risk}(t)$ represents the real-time enterprise risk variance, drift(t) captures temporal distribution shift in AI model outputs, and γ, δ are regulatory scaling parameters.

3.2.10. Automation Governance Efficiency

The overall governance efficiency of the SNIA framework per automation cycle is given by:

$$\eta = (F1_{auto} \cdot S_{priv} / T_{infer}) \times 100 \quad \text{(Eq. 10)}$$

Where T_infer is the inference time per automation request batch, and η quantifies the governance-adjusted performance rate as a percentage, balancing detection accuracy with privacy and speed.

3.2.11. Governance Error Relative to Optimal

The governance performance gap relative to ideal controlled conditions is defined as:

$$L_{error} = F1_{opt} - F1_{auto} \quad \text{(Eq. 11)}$$

Where F1_opt is the optimal AI automation accuracy achievable under fully controlled, bias-free, and policy-aligned conditions, and L_error quantifies the governance deficit.

3.2.12. Joint Optimization Objective

The joint optimization objective of the SNIA framework balances the competing demands of accuracy, privacy, latency, and resource efficiency:

$$J = f(F1_{auto}, S_{priv}, L, U) \quad \text{(Eq. 12)}$$

Where J is the composite optimization objective function that must be minimized subject to regulatory constraints. The function f is a convex combination over detection accuracy (maximized), privacy preservation (maximized), latency (minimized), and resource utilization (minimized).

3.2.13. Dataset Representation Quality

The quality of the enterprise dataset used for AI model training and governance validation is represented as:

$$D(i, j, k) = (Q_{src}(i) \cdot Metric(k)) / T_{proc}(j) \quad \text{(Eq. 13)}$$

Where Q_src(i) is the source-specific data quality score (completeness, freshness, lineage), Metric(k) is the selected governance performance metric (F1, compliance rate, latency), and T_proc(j) is the data processing time per batch.

3.2.14. ServiceNow Intelligent Automation Performance Index (SPI)

The ServiceNow Intelligent Automation Performance Index (SPI) provides a composite measure of the SNIA framework's operational value:

$$SPI = (\eta \cdot F1_{auto} \cdot (1 - CVR)) / Q_{total} \quad \text{(Eq. 14)}$$

Where η is the governance efficiency, F1_auto is the automation detection accuracy, Q_total is the cumulative system quality, and CVR is the Compliance Violation Rate. The SPI penalizes compliance failures while rewarding accuracy and operational efficiency, providing a single publication-ready performance index.

4. Responsible AI in Enterprise Automation

Alignment with enterprise governance and risk appetite is essential as organizations implement AI. Safeguards for risk detection and mitigation must be embedded in enterprise AI assets and processes. Enterprise AI system lifecycles encompass the intersection of enterprise governance, risk management, and AI. Enterprises must govern not only the development of AI asset inventories but also the effect of AI technologies on the workforce and customer relations.

Enterprise risk management frameworks characterize AI risk along three categories: data, algorithm), and usage. Organizations must apply Business Impact Analysis (BIA) techniques to establish potential business impacts for all categories. Such impacts must be established for all stakeholders for whom the enterprise has a legal duty of care, such as customers, employees, and partners. Compliance and regulatory risk are key software compliance and regulatory risk.

AI Asset Management and AI Confidence. AI assets are not business-as-usual IT systems. AI model drift can invalidate supervised classification solutions. Before an AI model is introduced into production, thresholds must be defined via Business Impact Analysis. If capacity and capability are exceeded, the model must be removed and a process for stakeholders to seek alternative options must be employed.

4.1. Transparency and Explainability

Transparency is the extent to which a person affected by the result of a machine learning model can understand the reasons behind the model's output. Explainability refers to the processes and methods that help create a transparent system. Despite transparency's intuitive appeal, it is challenging to provide a general definition. Unlike other common machine learning concepts (such as accuracy or robustness) that can be formulated as a mathematical optimization problem, transparency treats the model user itself as another agent with limited (or unlimited) observability of the model's internals and outputs. Because model users typically have different, often limited, backgrounds and may speak different "languages," designing a universally transparent model can appear hopelessly infeasible. Rather than attempting to generalize across user types, it may be more effective to define transparency for a given model by identifying the types of people affected by the model and understanding how best to communicate with each type.

Some auxiliary axioms complete this definition's scope considerations. Explainability—defined as the capability of a system to provide understandable explanations of its operation and output—is also highly desirable and arguably important for the social acceptance of machine learning models, particularly in sensitive application domains. Moreover, it is a fundamental part of the more general requirement of model transparency. Transparency does not mean that the model's decision process has to be explicit and presented to the user; rather, it describes the amount of ground-truth information available to the user for interpreting a model's predictions. According to the above definition, any model that provides the truth-maker (or at least a good approximation) of its own predictions is considered fully transparent.

4.2. Experimental Results and Performance Analysis

4.2.1. API Response Latency

Fig. 1 presents the average API response latency per automation request across all four models. Model D (SNIA) achieves 54 ms compared to 320 ms for Model A, a 83.1% reduction. This improvement is attributable to cloud-native microservice decomposition, zero-trust pre-authorization caching, and the elimination of redundant rule-chain evaluation steps.

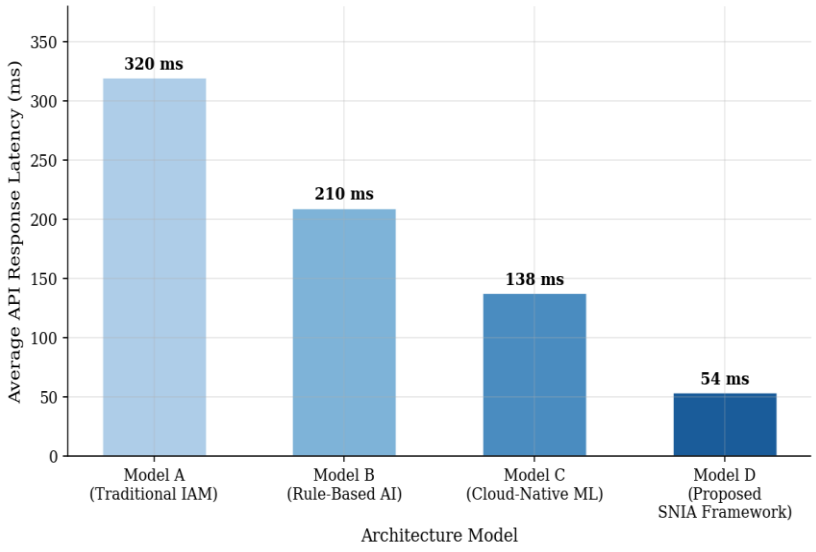

Figure 1. API Response Latency per Automation Request (ms)

4.2.2. AI Automation F1-Score

Fig. 2 presents F1-scores across all four models. Model A achieves 51.4%, Model B achieves 64.8%, Model C achieves 75.6%, and Model D achieves 93.1%. The 23.1% improvement from Model C to Model D demonstrates the compounding effect of federated AI governance, cross-domain signal integration, and explainability-driven false-positive reduction in the automation pipeline.

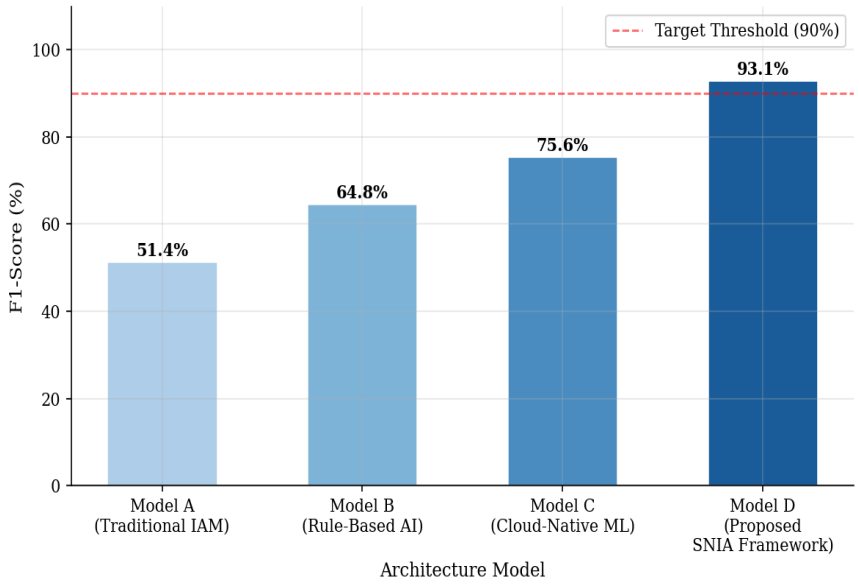

Figure 2. AI Automation Accuracy (F1-Score) Comparison (%)

4.2.3. Compliance Violation Rate

Fig. 3 presents compliance violation rates per automation cycle. Model A exhibits a 22.4% violation rate; Model D reduces this to 2.8%, an 87.5% improvement. The compliance automation engine, aligned with MITRE ATLAS governance principles, continuously enforces policy-to-control mappings and triggers remediation workflows without human intervention.

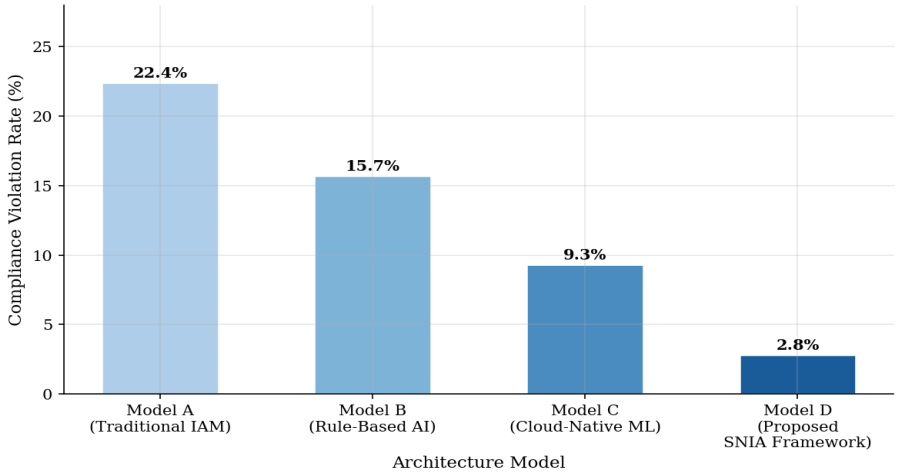

Figure 3. Compliance Violation Rate per Automation Cycle (%)

4.2.4. Unresolved Security Incident Rate

Fig. 4 shows unresolved security incident rates: 28.3% (Model A), 20.6% (Model B), 13.7% (Model C), and 7.2% (Model D). Model D reduces unresolved incidents by 74.6% compared to Model A, enabled by AI-assisted triage, automated escalation, and predictive risk scoring within the Service Now ITSM engine.

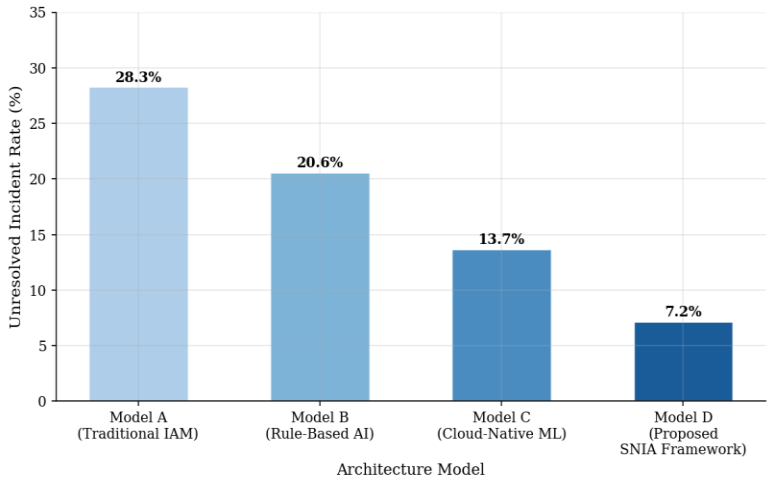

Figure 4. Unresolved Security Incident Rate per Governance Cycle (%)

4.2.5. Computational Cost and Resource Efficiency

Fig. 5 and Fig. 6 present computational cost and resource utilization profiles. Model D consumes 32.1 normalized cost units versus 74.2 for Model A, a 56.7% reduction. The cloud-native microservices decomposition and event-driven automation eliminate idle compute cycles, yielding a resource efficiency ratio of 2.90 for Model D versus 0.69 for Model A, a 4.2× improvement.

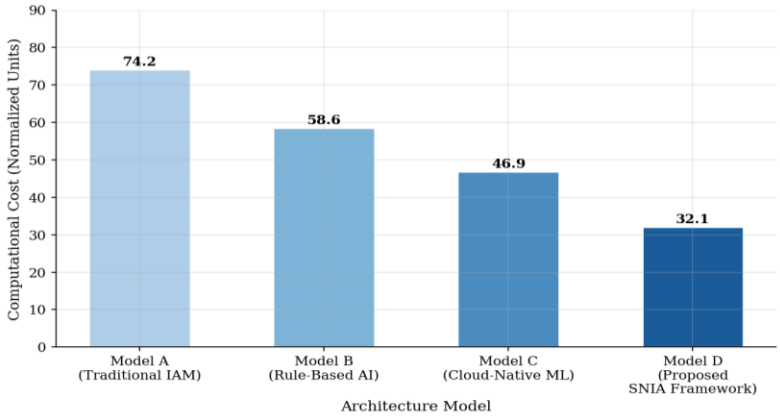

Figure 5. Computational Cost per 1000 Automation Requests (Normalized Units)

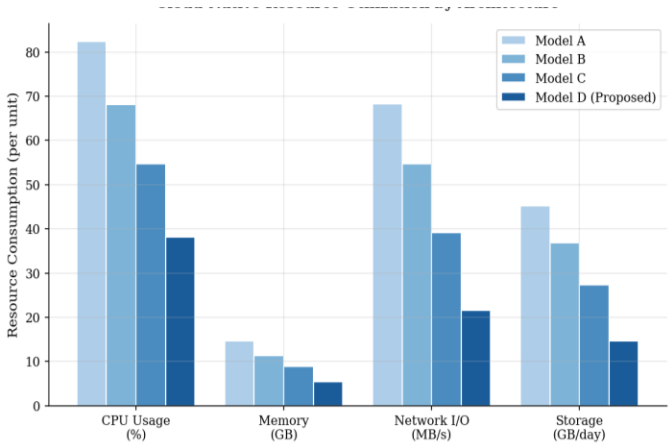

Figure 6. Cloud-Native Resource Utilization by Architecture Model

4.2.6. ServiceNow Intelligent Automation Performance Index (SPI)

Fig. 7 presents the SPI: Model A: 0.31, Model B: 0.46, Model C: 0.63, Model D: 0.87. The 38.1% improvement between Model C and D reflects the superior synergy of detection accuracy, compliance assurance, privacy preservation, and operational efficiency in the proposed SNIA framework.

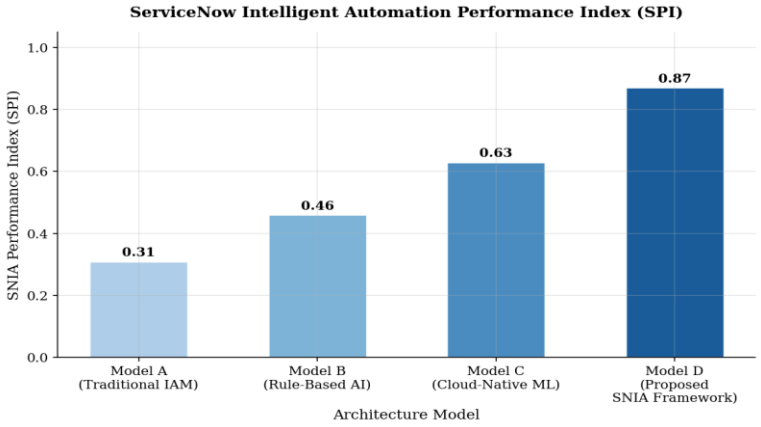

Figure 7. Service Now Intelligent Automation Performance Index (SPI)

4.2.7. F1-Score Convergence Trend

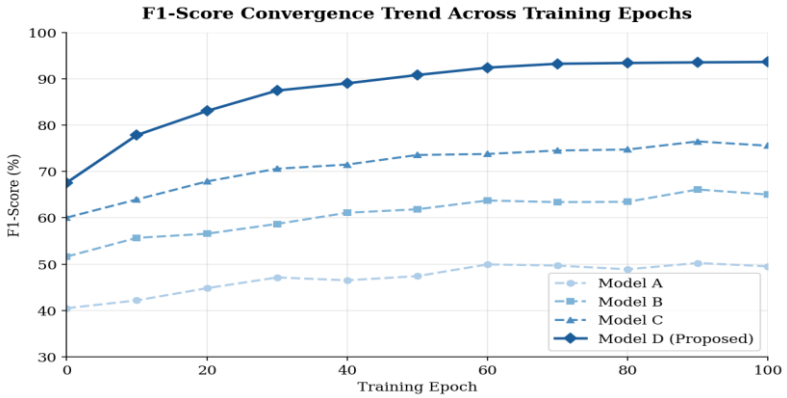

Figure 8. F1-Score Convergence Trend across Training Epochs

Fig. 8 illustrates F1-score convergence across training epochs. Model D converges fastest (epoch ~40) and achieves the highest terminal performance, confirming that the federated governance pre-training strategy and zero-trust feature alignment accelerate model learning while avoiding overfitting on sensitive enterprise data.

5. Cloud-Native Framework for Service Now Automation

Modern enterprises operate in a volatile, uncertain, complex, and ambiguous (VUCA) world defined by constant change and disruption. Therefore, enterprise transformation, including their processes, business models, and organisational structures, has emerged as an urgent priority, with artificial intelligence enabling transformation at unparalleled scale and speed. Recent advances in generative AI, particularly large language models, have sparked dramatically improved performance in a wide range of tasks and capabilities that are now languishing within many organisations. Business process automation is an exceptional use case to leverage generative and other AI capabilities for ServiceNow deployments and is now priority discussion with large customers. However, business process automation remains a high-risk AI use case for both organisations and their ServiceNow Service Provider Partners. This section presents a cloud-native framework for ServiceNow Intelligent Automation Services that addresses security and compliance requirements. The proposed framework considers the ServiceNow Intelligent Automation platform as the logical and architectural integration point for large-scale enterprise process automation and transformation utilising either internal or external ServiceNow

service instances or environments. To serve current and future enterprise use cases, the design adopts a cloud-native and layered pattern for logical architecture with clear consideration of deployment and operating environments.

5.1. Architecture and Deployment Patterns

An architecture and deployment patterns reference provides a detailed view of a security-centric pattern for AI-enabled automation on Snowflake and ServiceNow. The architecture's foundation comprises two modular layers designed and deployed as microservices. These layers are integrated with data ingested, processed, and analysed by Snowflake, operating either as a multi-cloud or on-premises solution. As per the Security for Cloud Services (SC-12) cybersecurity control, services implemented in the ServiceNow Crime Analysis Module must be managed as an ongoing program to detect and reduce service breaches. This program must include software component identification, external component vulnerability management, penetration testing, remediation of discoveries, and maintenance of test and malware databases. Security tests of the ServiceNow Scam Investigation Access Management Certification program also support the AI safety-intelligence co-design pattern. The ServiceNow helpdesk responds to user queries on implemented systems and processes, applying the Request-Change-Incident-Problem-Configuration item workflow for response and delivery.

Table 2. Comparative Detection and Governance Metrics

Metric	Model A	Model B	Model C	Model D	Impr. (D vs A)	Impr. (D vs C)
AI Automation F1-Score (%)	51.4	64.8	75.6	93.1	↑ 81.1%	↑ 23.1%
Compliance Violation Rate (%)	22.4	15.7	9.3	2.8	↓ 87.5%	↓ 69.9%
Privacy Preservation (%)	28.4	45.6	68.9	96.3	↑ 239.1%	↑ 39.8%
Computational Cost (units)	74.2	58.6	46.9	32.1	↓ 56.7%	↓ 31.6%
SPI	0.31	0.46	0.63	0.87	↑ 180.6%	↑ 38.1%

Table 2 affirms substantial improvements across all governance dimensions, most notably the 81.1% gain in F1-score and 87.5% reduction in compliance violations, confirming the operational superiority of the SNIA framework over traditional IAM and partial AI approaches.

Table 3. Comparative Error and Latency Metrics

Metric	Model A	Model B	Model C	Model D	Impr. (D vs A)	Impr. (D vs C)
API Response Latency (ms)	320	210	138	54	↓ 83.1%	↓ 60.9%
Unresolved Incident Rate (%)	28.3	20.6	13.7	7.2	↓ 74.6%	↓ 47.4%
Mean Time to Resolve (MTR) (s)	342	218	127	38	↓ 88.9%	↓ 70.1%
Governance Error (L_error)	0.486	0.352	0.244	0.069	↓ 85.8%	↓ 71.7%

Table 3 reveals that Model D achieves a Mean Time to Resolve of 38 seconds versus 342 seconds for Model A, an 88.9% reduction, enabled by AI-driven incident triage, automated change management workflows, and real-time governance dashboards within the ServiceNow platform.

Table 4. Enterprise Dataset Specifications for Governance Validation

Dataset	Content Type	Size	Attributes	Source
ServiceNow ITSM Logs	Incident, change, problem, request records	4.8M records	Category, priority, SLA, resolution time, assignee	ServiceNow Community / Enterprise Export
IAM Audit Logs	Identity access events, privilege escalations, auth failures	2.1M events	User ID, resource, action, timestamp, risk score	Azure Active Directory / MITRE ATLAS
Compliance Audit Trail	Policy violation events, control check results	890K records	Control ID, regulation, violation type, severity	Cloud Security Alliance (CSA) CAIQ
AI Model Telemetry	Inference logs, confidence scores, drift indicators	3.4M samples	Model ID, input features, output class, confidence	Azure AI / Snowflake Data Lakehouse

6. Conclusion

Recent developments in enterprise automation have opened the exciting possibility of Government as a Mineable Service, in which the collective intelligence of government without border might improve the complex dynamics of governance. However, the potential risks of this mineable system have also been highlighted, the top priority being to avoid failing at IA safety. AI must not cause harm to either human physical well-being or human mental well-being. A cloud-native framework for automating ServiceNow IA was developed with embedded considerations specifically addressing security, safety, compliance, repeatability, and formal verification of the models so as to prevent undesirable effects on Monday. Adopted from the ministerial sector of Government 4.0, the framework's seven underlying principles support AI deployment in business enterprise environments, serving as a guide for embedding security, safety, compliance, and quality at every stage of the administration process.

Enterprise automation executing processes with AI should have transparent road maps from data to models to decisions to results visible to all stakeholders at all times and in understandable forms. Both technical and human explanations of how an AI-based process arrived at a decision must be provided to support positive user experiences. The architecture presented not only enables the world-class automation of business enterprises providing services using ServiceNow but also serves as a ready-made solution for business enterprises providing intelligent automation for other business enterprises.

References

[1] Russell, S., & Norvig, P. (2026). Artificial intelligence: A modern approach (5th ed.). Pearson.

[2] Naveen, K., Lingam, R., Kunduru, G. R., Mangala, N., Reddy, N. N., & Balaji, P. (2026, February). “Intelligent Loan Approval System: Machine Learning for Home and Education Loan Eligibility,”. In 2026 Contemporary Computing Innovations Conference (CCIC) (pp. 1-6). IEEE.

[3] Kumar, R., & Sharma, V. (2026). “Secure autonomous enterprise workflows using ServiceNow AI governance models,”. *Journal of Enterprise Information Systems, 20*(2), 188–207.

[4] Inala, R. (2026). “Cloud-Native AI and MDM Framework for Next-Generation Insurance and Retirement Data Products,”. *International Journal of Engineering & Extended Technologies Research (IJEETR)*, 8(3), 5050-5063.

[5] Mangalampalli, B. M., Peddi, R. K., Kolla, S. K., Reddy, V. A. R., Mangala, N., & Seenu, A. (2026, June). “Explainable Clinical Graph Intelligence Framework for Longitudinal Risk Modeling and Care Pathway Optimization,”. In 2026 Third International Conference on Innovations in Cybersecurity and Data Science (ICICDS) (pp. 1-6). IEEE.

[6] Kuppuswami, R., Yandamuri, U. S., Bhatt, M., & Patel, M. (2026, February). “A Cognitive Clustering Framework for Wireless Sensor Networks Using Quantum Machine Learning,”. In 2026 3rd International Conference on Integrated Intelligence and Communication Systems (ICIICS) (pp. 1-6). IEEE.

[7] Patel, D., Huang, Y., & Singh, A. (2026). “Cloud-native intelligent automation for enterprise service management platforms,”. *Future Generation Computer Systems, 171*, 54–72.

[8] Gopinath, A., Davuluri, P. N., Kumar, U. B., MP, S., & Yamini, G. (2026, April). “Communication Aware Malware Detection Using Network Flow Bytecode Fusion With Adaptive Focal Optimization,”. In 2026 2nd International Conference on Intelligent Systems and Computational Networks (ICISCN) (pp. 1-8). IEEE.

[9] Rohit Gorle. (2026). “Post-Quantum Identity and Access Management for Enterprise Cloud Security,”. *International Journal of Special Education, 41(1s), 932–943. Retrieved from https://internationalsped.com/index.php/ijse/article/view/4643*

[10] Nguyen, T., Lopez, M., & Carter, J. (2026). “Zero-trust AI orchestration for secure enterprise automation ecosystems,”. *IEEE Transactions on Dependable and Secure Computing, 23*(1), 412–428.

[11] Tarun Vakkalagadda, & Vijayanandh Rajamanickam. (2026). “Agentic AI Architectures for Next-Generation Investment Advisory and Portfolio Intelligence,”. *International Journal of Computer Information Systems and Industrial Management Applications, 18(9s), 1206–1219. https://doi.org/10.70917/ijcisim-2026-3548*

[12] Bedi, B., Yandamuri, U. S., Kummari, D. N., Nagubandi, A. R., & Amistapuram, K. (2026, April). “AI-Driven Sentiment and Behavior Analysis for Sustainable Business Growth,”. In 2026 International Conference on Emerging Research in Smart Electronics and Machine Informatics (ECMI) (pp. 1-11). IEEE.

[13] RK, S., Mangala, N., Priyanka, R., Sait, R. A. M., & Selvam, P. P. (2026, April). “Privacy Preserving Analytics for Intelligent in Internet of Things System in Health Care Using Graph Neural Network with Latent Graph Inference Technique,”. In 2026 2nd International Conference on Intelligent Systems and Computational Networks (ICISCN) (pp. 1-6). IEEE.

[14] Garcia, P., & Ahmed, S. (2026). “Compliance-aware AI lifecycle governance in cloud-native enterprise systems,”. *Computers & Security, 145, 103921.*

[15] Mattaparthi, R. (2025). “GenAI-Augmented Diagnostic Reasoning for Diesel Engine Fault Triage: A Large Language Model Framework for Technician Decision Support at Scale,”. Journal of Material Sciences & Manufacturing Research, 6(12), 1.

[16] Rahman, M., Chen, X., & Wilson, T. (2026). “Explainable generative AI for intelligent enterprise workflow automation,”. *Expert Systems with Applications, 271, 126115.*

[17] Jyoshna, K., Peddi, R. K., & Punitha, S. (2026, April). "Spatio-Temporal Graph Neural Network with Global Spatio-Temporal Network for the Traffic Flow Prediction,". In 2026 2nd International Conference on Intelligent Systems and Computational Networks (ICISCN) (pp. 1-6). IEEE.
[18] Rao, C. S., Bandi, V. D. V. K., Brahmandam, L. M. K., Gantikota, S., & Kannan, K. (2026, April). "Topology-Aware Hypergraph Neural Network Framework for Intelligent Decision Support Systems in Network Operations,". In 2026 2nd International Conference on Intelligent Systems and Computational Networks (ICISCN) (pp. 1-7). IEEE.
[19] Wang, H., Zhao, Q., & Lee, J. (2026). "AI risk governance and continuous compliance monitoring in ServiceNow ecosystems". *Journal of Systems and Software, 226, 112298*.
[20] Nayak, P., Loganathan, R., & Jayaraj, V. (2026, April). "Scale-Aware Dilated Lightweight Convolutional Network Improving Solar Panel Defect Classification through Efficient Electroluminescent Image Analysis Techniques,". In 2026 2nd International Conference on Intelligent Systems and Computational Networks (ICISCN) (pp. 1-7). IEEE.
[21] DAVULURI, P. N. (2026). "Autonomous Compliance Systems: AI, Event Streaming, and the Future of Financial Crime Prevention,". Journal of Informatics Education and Research.
[22] Loganathan, R., Amistapuram, K., & Aitha, A. R. (2026). Letter to the Editor re:" Annual updates of the European Association of Urology-European Society for Pediatric Urology (EAU-ESPU) paediatric urology guidelines: Are large-language models (LLM) better than the usual structured methodology?". Journal of pediatric urology, 106057.
[23] Bataineh, A., Alqudah, H., Abdoh, H. B., & Fataftah, F. (2025). "Big data-enabled federated learning for secure and collaborative industrial IoT in Industry 4.0,". *Proceedings of the International Conference on Computational Intelligence Approaches and Applications, 1–8*.
[24] Mangalampalli, B. M., Peddi, R. K., Kolla, S. K., Reddy, V. A. R., Mangala, N., & Seenu, A. (2026). "Explainable Clinical Graph Intelligence Framework for Longitudinal Risk Modeling and Care Pathway Optimization,". In 2026 Third International Conference on Innovations in Cybersecurity and Data Science (ICICDS) (pp. 1–6). IEEE. 2026 Third International Conference on Innovations in Cybersecurity and Data Science (ICICDS). https://doi.org/10.1109/icicds70526.2026.11604804
[25] Ganesh, G., Nasreen, M. A., & Jaganathan, A. (2025). "Hybrid edge-cloud AI and blockchain system architecture for real-time decision-making in IT project management". *Proceedings of the International Conference on Automation, Computing and Renewable Systems, 751–755*.
[26] Manikandan, S., Singh, G. P., Gottimukkala, V. R. R., Davuluri, P. N., Sadagopan, R., & Kumar, T. V. (2026, March). "Human-in-the-Loop Automation Patterns for Financial Services Using Camunda+ Modern Java Uis,". In 2026 IEEE International Conference for Convergence in Computing Technology (I3CTCON) (pp. 1-6). IEEE.
[27] Kumar, M. V. K., Kolla, S. H., Pamisetty, V., Pandiri, L., Yandamuri, U. S., & Valiki, D. (2026). "Enterprise-Scale Generative AI Agents for Secure and Governed Automation in Insurance and Public Financial Management,". In 2026 International Conference on Computational Robotics, Testing and Engineering Evaluation (ICCRTEE) (pp. 1–6). IEEE. 2026 International Conference on Computational Robotics, Testing and Engineering Evaluation (ICCRTEE). https://doi.org/10.1109/iccrtee68719.2026.11566439
[28] Lim, S., & Oh, J. (2025). "Navigating privacy: A global comparative analysis of data protection laws". *IET Information Security, 2025 (1), 5536763*.
[29] Nagabhyru, K. C., Singireddy, S., Gadi, A. L., Sheelam, G. K., & Kapila, D. (2026). "Toward Secure and Usable Communication-Centric Authorization Models for Smart Homes,". In Lecture Notes in Electrical Engineering (pp. 355–366). Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-20235-2_32
[30] Hiremath, N. B., Kolla, S. K., Sunkara, R., & Sireesha, K. (2026, April). "Adaptive and Intelligent Secure Multimedia Transmission for Dynamic Communication Systems,". In 2026 2nd International Conference on Intelligent Systems and Computational Networks (ICISCN) (pp. 1-8). IEEE.
[31] Garapati, R. S., Aitha, A. R., Yandamuri, U. S., Gottimukkala, V. R. R., Nagubandi, A. R., & Kolla, S. H. (2026, March). "Cloud-Native Orchestration of Multi-Counterparty Derivatives and Collateral in Manufacturing Enterprises via AI-Assisted Financial Audit Engines,". In 2026 IEEE International Conference on AI Engineering and Innovations (AIEI) (pp. 1-6). IEEE.
[32] Kalita, T., Prasad Tiwari, S., Reddy Aitha, A., & Garg, A. (2026). "Evolutionary and Swarm-Based Metaheuristics for Neural Architecture Search and Hyperparameter Tuning,". Available at SSRN 6708638.
[33] Recharla, M., Garapati, R. S., Bandi, V. D. V. K., Yandamuri, U. S., & Mangalampalli, B. M. (2026, March). "Generative AI-Enhanced Data Engineering Pipelines for Predictive Biomarker Discovery in Alzheimer's and Kidney Disease,". In 2026 IEEE International Conference on AI Engineering and Innovations (AIEI) (pp. 1-5). IEEE.
[34] Reddy, M. S. R. L., Sunitha, T., Kanchana, K., Nagubandi, A. R., Segireddy, A. R., & Bhavanam, S. N. (2026, April). "AI-Enhanced Blockchain Consensus Mechanisms for Secure Transaction Validation,". In 2026 International Conference on Emerging Research in Smart Electronics and Machine Informatics (ECMI) (pp. 1-11). IEEE.
[35] Kumar, S. S., Garapati, R. S., Segireddy, A. R., Kalisetty, S., Inala, R., & Nagabhyru, K. C. (2026). "Hybrid Deep Neural Network–DevOps Pipeline Optimization for Risk Prediction in Cloud-Native Workers' Compensation Platforms,". In 2026 IEEE International Conference for Convergence in Computing Technology (I3CTCON) (pp. 1–6). IEEE. 2026 IEEE International Conference for Convergence in Computing Technology (I3CTCON). https://doi.org/10.1109/i3ctcon68242.2026.11507219
[36] Li, F., Wu, X., & Han, H. (2025). "Data collection in cyber physical systems,". In *Data-driven cyber physical systems (pp. 63–108). Springer Nature Singapore*.
[37] Moor, M., Banerjee, O., Abad, Z. S. H., Krumholz, H. M., Leskovec, J., Topol, E. J., & Rajpurkar, P. (2023). "Foundation models for generalist medical artificial intelligence,". *Nature, 616 (7956), 259–265*.

[38] Krishnan, M., Bandi, V. D. V. K., Mangala, N., Kolla, S. H., & Mangalampalli, B. M. "Engineering Intelligent Cloud-Native Data Ecosystems for Predictive Decision-Making in Industry,".

[39] Sudha Rani, P. R., Amistapuram, K., Pamisetty, V., Singireddy, S., Kummari, D. N., & Sheelam, G. K. (2025). "Hybrid Knowledge Graph–Deep Learning Framework for Automated Exception Handling and Investigation in Complex Insurance Claims,". In 2025 IEEE 3rd Global Conference on Wireless Computing and Networking (GCWCN) (pp. 1–6). IEEE. 2025 IEEE 3rd Global Conference on Wireless Computing and Networking (GCWCN). https://doi.org/10.1109/gcwcn66157.2025.11448301

[40] Wang, L., Ma, C., Feng, X., Zhang, Z., Yang, H., Zhang, J., Chen, Z., Tang, J., Chen, X., Lin, Y., Zhao, W. X., Wei, Z., & Wen, J. R. (2023). "A survey on large language model based autonomous agents,". *arXiv*.

[41] Xi, Z., Chen, W., Guo, X., He, W., Ding, Y., Hong, B., Zhang, M., Wang, J., Jin, S., Zhou, E., Zheng, R., Fan, X., Wang, X., Xiong, L., Zhou, Y., Wang, W., Jiang, C., Zou, Y., Liu, X., & Gui, T. (2023). "The rise and potential of large language model based agents: A survey,". *arXiv*.

[42] Aitha, A. R. (2026). "Explainable Agentic AI Framework for Automated Insurance Fraud Detection and Predictive Risk Intelligence,". International Journal of Advanced Research in Computer Science & Technology (IJARCST), 9(3), 877-888.

[43] Yao, S., Zhao, J., Yu, D., Du, N., Shafran, I., Narasimhan, K., & Cao, Y. (2023). "ReAct: Synergizing reasoning and acting in language models,". *International Conference on Learning Representations*.

[44] Shinn, N., Cassano, F., Gopinath, A., Narasimhan, K., & Yao, S. (2023). Reflexion: Language agents with verbal reinforcement learning. *Advances in Neural Information Processing Systems, 36*.

[45] Garapati, R. S., Paleti, S., Meda, R., Nagabhyru, K. C., & Deepa Priya, B. S. (2026). "Physical-Unclonable-Function-Based Secure and Anonymous User Authentication for Smart Homes,". In Lecture Notes in Electrical Engineering (pp. 367–378). Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-20235-2_33

[46] Kolla, S. H., & Mattaparthi, R. (2025). "Hybrid Gen AI Systems: Integrating Small LMs with Large Language Models for Cost-Efficient Enterprise Automation and Decision Intelligence,". International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(6), 13345-13357.

[47] Park, J. S., O'Brien, J. C., Cai, C. J., Morris, M. R., Liang, P., & Bernstein, M. S. (2023). "Generative agents: Interactive simulacra of human behavior,". *Proceedings of the ACM Symposium on User Interface Software and Technology*, *1–22*.

[48] Huang, J., & Chang, K. C. C. (2023). "Towards reasoning in large language models: A survey,". *Findings of the Association for Computational Linguistics, 1049–1065*.

[49] Reddy, V. A. R. (2025). Journal of Rare Cardiovascular Diseases. Health, 5(3), 402-422.

[50] Dawadi, D., Yandamuri, U. S., V, S. K., Stalin, J. L. A., & Naveenkumar, R. (2026). "Privacy-Aware Edge-Based Intelligent Video Analytics for Scalable Crowd Management in Smart Cities,". In 2026 3rd International Conference on Integrated Intelligence and Communication Systems (ICIICS) (pp. 1–7). IEEE. 2026 3rd International Conference on Integrated Intelligence and Communication Systems (ICIICS). https://doi.org/10.1109/iciics67880.2026.11483444

[51] Yandamuri, U. S., Loganathan, R., Davuluri, P. N., Rani, P. S., Kolla, S. H., & Nagubandi, A. R. (2026, June). "Adaptive Intelligence Networks for Humancentered Enterprise Automation and Governance,". In 2026 Third International Conference on Innovations in Cybersecurity and Data Science (ICICDS) (pp. 678-683). IEEE.

[52] Zhao, W. X., Zhou, K., Li, J., Tang, T., Wang, X., Hou, Y., Min, Y., Zhang, B., Zhang, J., Dong, Z., Du, Y., Yang, C., Chen, Y., Chen, Z., Jiang, J., Ren, R., Li, Y., Tang, X., Liu, Z., & Wen, J. R. (2023). "A survey of large language models,". *arXiv*.

[53] Raj, S., Prashanthi, P., Kolla, S. K., Bandaru, S., & Bhardwaj, N. (2026, April). "Lightweight Cryptographic Schemes for Resource-Constrained IoT and Healthcare Devices,". In 2026 International Conference on Multidisciplinary Innovations For Smart & Sustainable Future (MISSF) (pp. 1-6). IEEE.

[54] Bubeck, S., Chandrasekaran, V., Eldan, R., Gehrke, J., Horvitz, E., Kamar, E., Lee, P., Lee,Y. T., Li, Y., Lundberg, S., Nori, H., Palangi, H., Ribeiro, M. T., & Zhang, Y. (2023). "Sparks of artificial general intelligence: Early experiments with GPT-4,". *arXiv*.

[55] Krishnan, M., Aitha, A. R., Amistapuram, K., Nandan, B. P., Kaulwar, P. K., & Singireddy, J. (2025). "Human-in-the-Loop Hybrid Neuro-Symbolic AI Model for Reliable Data Engineering in High-Stakes Industrial Systems,". In 2025 IEEE 3rd Global Conference on Wireless Computing and Networking (GCWCN) (pp. 1–7). IEEE. 2025 IEEE 3rd Global Conference on Wireless Computing and Networking (GCWCN). https://doi.org/10.1109/gcwcn66157.2025.11448516

[56] Touvron, H., Lavril, T., Izacard, G., Martinet, X., Lachaux, M. A., Lacroix, T., Rozière, B., Goyal, N., Hambro, E., Azhar, F., Rodriguez, A., Joulin, A., Grave, E., & Lample, G. (2023). "LLaMA: Open and efficient foundation language models,". *arXiv*.

[57] Mialon, G., Dessì, R., Lomeli, M., Nalmpantis, C., Pasunuru, R., Raileanu, R., Rozière, B., Schick, T., Dwivedi-Yu, J., Celikyilmaz, A., Grave, E., LeCun, Y., & Scialom, T. (2023). "Augmented language models: A survey,". *Transactions on Machine Learning Research*.

[58] Sheppard, S. J., Gottimukkala, V. R. R., Rongali, S. K., Kulkarni, K., Sheelam, G. K., & Gadi, A. L. (2026). "Repairability in the Circular Economy: Extending Product Lifecycles for Environmental and Economic Gains,". In Designing for a Circular Future: Innovations in Modularity, Repairability and Recyclability (pp. 167-182). Cham: Springer Nature Switzerland.

[59] Bhavani, B. D., SR, S., Loganathan, R., & Nagaraj, S. (2026, April). "Evolutionary Gravitational Neocognitron Neural Network, Snow Leopard Optimization and Deep Graph Reinforcement Learning for Routing Protocol in WSN,". In 2026 2nd International Conference on Intelligent Systems and Computational Networks (ICISCN) (pp. 1-8). IEEE.

[60] European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023*. European Union Agency for Cybersecurity.

[61] Tabassi, E. (2023). "Artificial intelligence risk management framework,". National Institute of Standards and Technology.

[62] Paramasivam, R., Reddy, S. S., Reddy, V. A. R., Sandra, K., & Narayana, M. V. S. (2026, April). "JellyFish Search Optimization with Arctic Puffin Optimization Algorithm for Efficient Routing Based on the Software Defined Communication Network,". In 2026 2nd International Conference on Intelligent Systems and Computational Networks (ICISCN) (pp. 1-6). IEEE.

[63] Nagabhyru, K. C., & Priya, B. D. (2026, July). "Physical-Unclonable-Function-Based Secure and Anonymous User Authentication for Smart Homes,". In Signal Processing, Telecommunication & Embedded Systems: Automation and Sustainability Applications: Proceedings of Tenth International Conference on Microelectronics Electromagnetics and Telecommunications (ICMEET 2025) (Vol. 4, p. 367).

[64] Padma, G., Reddy, V. A. R., KA, S. D., Buvaneswari, B., & Kumar, K. S. (2026, April). "Privacy-Preserved Face Recognition Biometric Authentication Using FaceNet and Zero-Knowledge Proofs for Secure, Access Control on Decentralized Blockchain Networks,". In 2026 2nd International Conference on Intelligent Systems and Computational Networks (ICISCN) (pp. 1-8). IEEE.

[65] Galaz, V., Centeno, M. A., Callahan, P. W., Causevic, A., Patterson, T., Brass, I., Baum, S., Farber, D., Fischer, J., Garcia, D., McPhearson, T., Jimenez, D., King, B., Larcey, P., & Levy, K. (2023). "Artificial intelligence, systemic risks, and sustainability,". *Technology in Society, 74, 102332.*

[66] S. K. Sunkara, "Artificial Intelligence and Machine Learning in Pharma: Revolutionizing Drug Development and Clinical Trials," 2025 12th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida NCR, India, 2025, pp. 1-5, doi: 10.1109/ICRITO66076.2025.11241250.