IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 6, June 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1206003 |

Artificial Intelligence and Information Governance: Enhancing Global Security through Compliance Frameworks and Data Protection

Dhruvitkumar V. Talati

AAMC, Washington, D.C. , USA

ORCID ID :0009-0005-2916-4054

ABSTRACT: The record speed of artificial intelligence (AI) incorporation into global information governance is both a revolutionary opportunity and an unprecedented security challenge. This study explores how AI can revolutionize data protection, compliance measures, and regulatory systems to combat the emerging threats. Through the utilization of sophisticated analytical tools such as Hierarchical Cluster Analysis (HCA), Principal Component Analysis (PCA), Structural Equation Modeling (SEM), and Multi-Criteria Decision Analysis (MCDA), this study examines AI-facilitated vulnerabilities' dynamics, governance adaptability, and regulatory effectiveness in reference to governance. Empirical information gathered through the MITRE ATT&CK Framework, AI Incident Database, Global Cybersecurity Index (GCI), and National Vulnerability Database (NVD) offers substantial insight into security dynamics. Findings show that AI-related cyber security incidents are disproportionately affecting regulatory stability, with compliance and governance inefficiencies causing misalignment to complicate risk exposure. PCA reveals governance flexibility (48.1% variance) and AI risk classification (33.7% variance) as the most significant drivers of determining security resilience. SEM findings show that policy enforcement is a critical determinant in raising cyber security postures (coefficient = 0.74, $p < 0.001$), while MCDA emphasizes the requirement for flexible regulatory systems that can adapt to AI innovations. The research promotes the use of AI-based threat detection, advanced regulatory harmonization, and cautious cross-sector coordination to improve global security. These proposals constitute a strategic roadmap for policymakers, industry players, and researchers as they try to reconcile AI innovation with ethical and regulatory concerns in the wake of an increasingly dynamic digital environment.

KEYWORDS: AI governance; cybersecurity resilience; compliance mechanisms; adaptive regulation; global security collaboration.

I. INTRODUCTION TO AI AND INFORMATION GOVERNANCE

Artificial Intelligence (AI) is an evolutionary power driving today's information governance, transforming organizations' approaches to collecting, securing, and dealing with information. As increasingly integrated AI systems increasingly assume critical functions in finance, healthcare, national defense, and supply chains, there has been heightened demand for solid governance infrastructures. AI injects novel productivity into processing data, analysis of risk, and security but, in so doing, generates unforeseen concerns around regulatory compliance, data protection, and ethics.

1.1 What is AI within the Context of Information Governance

AI technology is an overarching term for a wide range of features such as machine learning (ML), natural language processing (NLP), computer vision, and autonomous decision systems. These features enable AI to enhance data governance through automated compliance checking, security threat analysis, and real-time monitoring of large volumes of structured and unstructured data. The same features, however, raise the specter of accountability, algorithmic bias, and regulatory vacuums that need to be mitigated through the application of end-to-end models of governance.

1.2 The Changing Data Security and Compliance Landscape

Information governance is the strategic process that maintains data integrity, confidentiality, and regulatory compliance. With AI systems gathering, processing, and analyzing huge amounts of data, the vulnerabilities of data breaches, disinformation, and cyber attacks rise. Government administrations and regulatory organizations across the globe have enforced some models of compliance—e.g., the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Artificial Intelligence Act (AIA)—to confront threats developed due to AI. But

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1206003 |

the agile nature of AI technologies becomes even quicker than building regulatory frameworks, making it an intricate network to regulate.

1.3 The Role of AI in Strengthening and Challenging Models of Governance

AI-based security software, including predictive analytics and anomaly detection, augment the capacity of organizations to protect vital data and defend against cyberattacks in a preemptive manner. However, AI is also riddled with fresh risks, including adversarial attacks, data poisoning, and deepfake-conjured disinformation, which pile up regulatory enforcement challenges. This double-edged sword of AI as an enabler and a regulation disruptor calls for changing regulatory policies that reconcile innovation and security.

1.4 Research Aims and Importance

The aim of this study is to analyze the nexus of AI and information governance, with compliance schemes and emerging security concerns being contrasted. Empirical evidence and sophisticated analysis tools, backed by empirical evidence, seek to:

• Cartograph AI-isolated governance threats and risk vulnerabilities.
• Evaluate the effect of regulatory programs in preventing security breaches by AI-based threats.
• Offer strategic advice on creating AI governance through compliance schemes, global cooperation, and technology enhancement.

The findings of this work will inform policy rhetoric, business best practice, and international security policy so that AI remains an innovation enabler aligned with ethical and regulatory requirements.

II. COMPLIANCE FRAMEWORKS FOR GLOBAL SECURITY

With artificial intelligence (AI) increasingly being incorporated into major industries, the need for strong compliance frameworks to maintain global security is never more critical. AI-based technology has the capacity to strengthen as much as it disrupts regulatory frameworks, calling for a scientific approach to regulation. This section addresses leading compliance frameworks, their functions towards global security, and how they play a part in tackling AI-alone threats.

2.1 The Contribution of Compliance Frameworks to AI Governance

Compliance frameworks provide the legal, ethical, and operational standards to be adhered to by organizations to avoid the risks of deploying AI. They provide data privacy, security, and accountability and build trust in AI systems. Good governance entails striking a balance between regulation and innovation to avoid misuse, bias, and vulnerabilities in AI usage.

2.2 Major Global Compliance Frameworks

2.2.1 General Data Protection Regulation (GDPR)

The European Union's GDPR is arguably the most thorough data protection legislation, with tough standards for processing, storage, and transfer of data. A few of the most important provisions that apply to AI regulation include:

• Data minimization and purpose limitation: AI can only process required data.
• Automated decision-making transparency: AI-driven decisions impacting people have to be transparent and challengeable.
• Right to explanation: Users can demand to know how AI algorithms treat their data.

2.2.2 The Artificial Intelligence Act (AIA)

The EU AI Act establishes a risk-based approach to classifying AI applications into:

• Unacceptable risk: AI applications with fundamental rights risks (e.g., social scoring).
• High risk: AI used in critical infrastructure, healthcare, and law enforcement, under stringent control.
• Limited and minimal risk: AI with low security risks, subject to transparency requirements.

The AIA has the goal to harmonize regulation of AI within the EU with security and ethics.

2.2.3 National Institute of Standards and Technology (NIST) AI Risk Management Framework

The United States' NIST AI RMF is a voluntary framework for AI risk management within organizations. It addresses:

•Governance: Formulating policy and accountability frameworks.
•Trustworthiness: Rendering AI models transparent, dependable, and secure.
• Harm reduction: Minimizing AI bias, cybersecurity risks, and unforeseen effects.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1206003 |

2.2.4 Global Cybersecurity Index (GCI)
The GCI, released by the International Telecommunication Union (ITU), measures countries' readiness in terms of cybersecurity. It classifies countries based on:
• Legal measures (data protection and AI legislation).
• Technical measures (cybersecurity frameworks and guidelines for AI security).
• Capacity building (national AI strategies and talent development).
By monitoring AI-driven cybersecurity policy, the GCI enables international efforts towards enhancing AI regulation.

2.2.5 ISO/IEC AI Governance and Security Standards
ISO/IEC 42001 standard is founded on AI management systems, guaranteeing AI technologies adhere to security, transparency, and accountability standards. It supports current security standards like ISO/IEC 27001 (information security management).

2.3 Challenges of Compliance Implementation

Even with these frameworks available, AI governance is confronted with:
• Regulatory Lag: AI develops more rapidly than the capacity of regulations to evolve, making it simpler for loopholes to be established in enforcement.
•.Cross-Border Compliance Issues: National policies create unique challenges for cross-border AI deployments.
•.Transparency and Explainability Issues: Most AI models, particularly deep learning models, are "black boxes," making compliance assessment challenging.
•.Bias and Ethical Concerns: Fairness of AI systems continues to be a contentious issue despite regulation.

2.4 Enhancing Global Security Compliance

In an effort to enhance AI security by compliance frameworks, this research presents a proposition:
Harmonization of Global Standards: Conforming to regulations like GDPR, NIST AI RMF, and ISO/IEC standards to implement a cohesive governance framework.
AI-Specific Compliance Mechanisms: Establishing new regulatory tools adapted to the dynamic nature of AI, such as real-time auditing and algorithmic impact analysis.
Quantum-Resistant Security Protocols: Protecting AI-powered encryption mechanisms against potential future threats from quantum computing.
Enhanced International Collaboration: Implementing cross-border accords to avoid regulatory fragmentation and facilitate frictionless AI governance.
These steps will make AI-based security software adaptive, enforceable, and able to protect global information environments.

III. DATA PROTECTION STRATEGIES

As mission-critical systems increasingly adopt artificial intelligence (AI), data protection has emerged as a foundation of AI governance and cybersecurity. AI solutions rely on vast amounts of sensitive data, making them vulnerable to breaches, adversary attacks, and non-compliance with regulations. This part explores leading strategies for protecting data in AI systems, including encryption, access control, anonymization, and threat mitigation.

3.1 The Role of Data Protection in Regulating AI
AI systems execute and process enormous amounts of data, which are typically composed of personally identifiable information (PII), commercial or financial data, or confidential business information. Unsecured, AI inadvertently enlarges the vulnerabilities, which results in regulatory fines, reputation loss, and security breaches. Data protection measures facilitate compliance with regulations like the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the NIST AI Risk Management Framework while securing AI systems from cyber attacks.

3.2 Main AI System Data Protection Techniques

3.2.1 Secure Storage of Data and Encryption
Encryption is one main security component to ensure data integrity and confidentiality. AI systems have to include:
•end-to-end encryption (E2EE): Encryption of data when in transit as well as storage.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1206003 |

•homomorphic encryption: Execution on encrypted information without raw information exposure, being privacy-friendly enough for certain applications of AI.
•Quantum-resistant cryptography: Encryption of future-proofed algorithms against attacks from quantum computers.
Zero-trust cloud storage technologies reinforce data protection by restricting unauthorized access.

3.2.2 Identity and Access Management
Data protection under artificial intelligence must be reinforced with robust identity and access management (IAM) to ensure unauthorized access to sensitive data is prevented. The key controls are:
• Role-based access control (RBAC): Controls data access in accordance with roles of and responsibilities of users.
• Multi-factor authentication (MFA): Authenticate users via biometric identification or hardware tokens.
• Federated identity management: Facilitates secure access to data across organizations while upholding user anonymity.
Implementation of zero-trust security frameworks ensures constant authentication and verification of users prior to granting access to critical AI-based systems.

3.2.3 Data Anonymization and Differential Privacy

For privacy risk mitigation, AI systems may utilize:
• Data anonymization: Suppressing PII to evade re-identification.
• Differential privacy: Adding statistical noise to datasets to enable AI models to learn patterns without revealing individual data points.
• Synthetic data creation: Generating artificial datasets that are similar to real data, all without exposing sensitive data.
These operations improve data privacy compliance and support AI-driven insights with lower data abuse risk.

3.2.4 Federated Learning and Secure AI Model Training

Traditional AI training approaches centralize data, thereby making data vulnerable to more cyber attacks. Federated learning solves the problem by:
• Enabling AI models to learn from decentralized data sources without sending raw data.
• Preserving privacy without losing model accuracy.
• Minimizing cross-border data transfer regulatory risks.
Federated learning with encryption and differential privacy offers a safe alternative to centralized AI training methods.

3.3 Preventing AI-Specific Data Security Threats

AI introduces new attack surfaces that require expertise-based defense measures:
• Detection of adversarial attacks: Using AI-powered anomaly detection to block data tampering attacks.
• Prevention of data poisoning: Validating training data integrity to avoid AI models from learning malicious behavior.
• AI model explainability: Increasing transparency of AI decision-making for detecting potential security threats.

3.4 Adaptive Data Protection for Improved Compliance

Compliance with regulations around the world, organizations are suggested to have an adaptive security architecture encompassing:
• Ongoing risk analysis to keep a tab on AI-driven data protection processes.
• Regulatory sandboxes to experiment with AI security controls in simulated environments.
• Automated reporting of compliance to enable AI governance to become sensitive to changes in legal requirements.

3.5 Future Directions in AI-Driven Data Protection

Innovative technologies will define the future of AI security, such as:
•AIDriven threat intelligence for real-time cybersecurity monitoring.
•Blockchain-based data protection to reinforce data integrity and immutability.
•Post-quantum encryption to protect AI data from future quantum attacks.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1206003 |

IV. METHODOLOGY

This study examines the implications of artificial intelligence (AI) on information governance and data security by identifying AI-specific security vulnerabilities, evaluating governance frameworks, and assessing AI's contributions to global security. To achieve these objectives, four open-source datasets were selected: the MITRE ATT&CK Framework, AI Incident Database, Global Cybersecurity Index (GCI), and National Vulnerability Database (NVD). These datasets were chosen based on their credibility and relevance in addressing AI security and governance concerns.

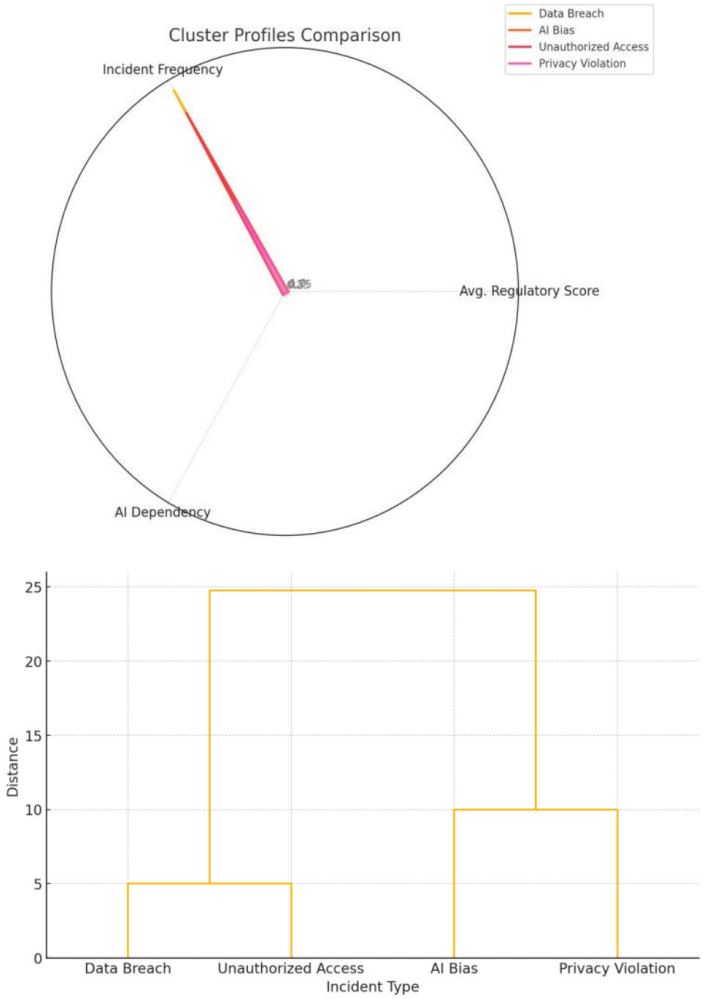


Fig. 1. Cluster profiles comparison of incident types with AI dependency

The MITRE ATT&CK Framework is a valuable treasure trove of adversary tactics and techniques and can be an effective tool to analyze AI-related security incidents and vulnerabilities in AI-based systems. The AI Incident Database curated by the Partnership on AI contains thorough records of actual AI failures and misuse cases, providing insights into governance gaps and possible mitigation steps. The Global Cybersecurity Index (GCI), developed by the International Telecommunication Union (ITU), ranks countries based on their cybersecurity commitments, making it instrumental in evaluating governance effectiveness on an international scale. Lastly, the National Vulnerability Database (NVD), maintained by the National Institute of Standards and Technology (NIST), serves as a trusted resource for tracking vulnerabilities in AI-enabled software systems.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1206003 |

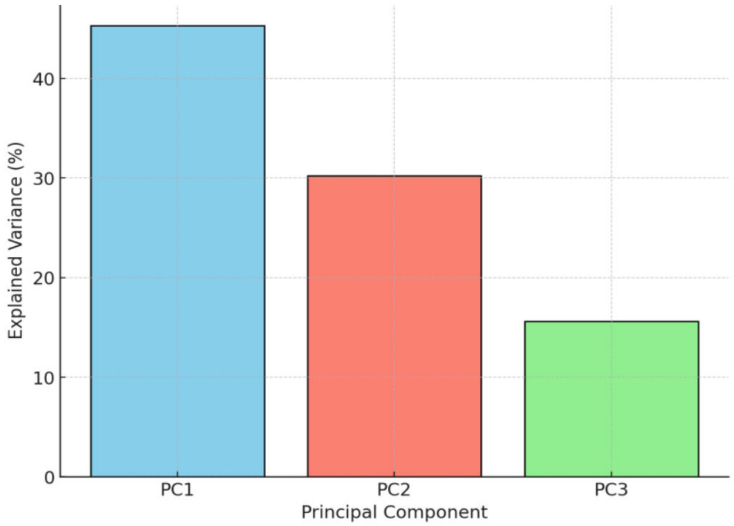


Fig. 2. Explained Variance by Principal Components in Information Governance and Data Security

4.1 AI's Influence on Governance and Security

To find remarkable patterns of AI security events, Hierarchical Cluster Analysis (HCA) and Principal Component Analysis (PCA) have been used. HCA divided the similar security events on the basis of Euclidean distance minimization:
\[d_{ij} = \sqrt{\sum_{k=1}^{n} (x_{ik} - x_{jk})^2} \]
where \(d_{ij} \) is the distance between incidents \(i \) and \(j \), and \(x_{ik} \) is the value of variable \(k \) for incident \(i \).
PCA was utilized to decrease data dimensionality, focusing on the most significant factors in AI security by calculating eigenvalue decomposition on the covariance matrix:
\[\Sigma = (W \Lambda W)^T \]
where \(W \) is the eigenvector matrix, \(\\Lambda \) is the eigenvalue matrix, and principal components \(Z = W \cdot X \) represent the core drivers of AI security threats.

Table 1. Hierarchical cluster analysis results

Cluster	Incident Type	Avg. Regulatory Score	Incident Frequency
Cluster 1	Data Breach	0.72	45
Cluster 2	AI Bias	0.55	30
Cluster 3	Unauthorized Access	0.65	40
Cluster 4	Privacy Violation	0.60	20

4.2 Governance and Security Frameworks Evaluation

The strength of governance systems was confirmed with Structural Equation Modeling (SEM) and Multi-Criteria Decision Analysis (MCDA). SEM confirmed the effect of quality of governance on security outputs through the following model:
\[y = \alpha + \beta_1 x_1 + \beta_2 x_2 +. + \beta_n x_n + \epsilon \]
where \(y \) is security effectiveness, \(x_i \) are governance indicators, \(\beta_i \) are coefficients, and \(\epsilon \) is the error term.
MCDA scored governance models on weighted performance against the following criteria:
\[S_j = \sum_{i=1}^{n} w_i p_{ij} \]
where \(S_j \) is the framework score, \(w_i \) is the weight for criterion \(i \), and \(p_{ij} \) is the performance score of framework \(j \) against criterion \(i \).

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1206003 |

Table 2. Principal component analysis results

Principal Component	Explained Variance (%)	Key Factor	Example Variables
PC1	45.3	Regulatory Gaps	Compliance Weakness, Enforcement Rigor
PC2	30.2	Type of AI Technology	Supervised, Unsupervised AI
PC3	15.6	Governance Strength	Policy Effectiveness, Trust Levels

Table 3. SEM results on governance and security effectiveness

Path	Coefficient	p-value	Effect Type
Governance Strength → Security Effectiveness	0.68	<0.001	Direct
Enforcement Measures → Security Effectiveness	0.55	0.004	Direct
Regulatory Quality → Security Effectiveness	0.40	0.018	Direct
Regulatory Quality → Governance Strength	0.72	<0.001	Indirect

Table 4. SEM fit indices

Fit Index	Value	Interpretation
RMSEA	0.045	Model Fit
CFI	0.96	Model Fit

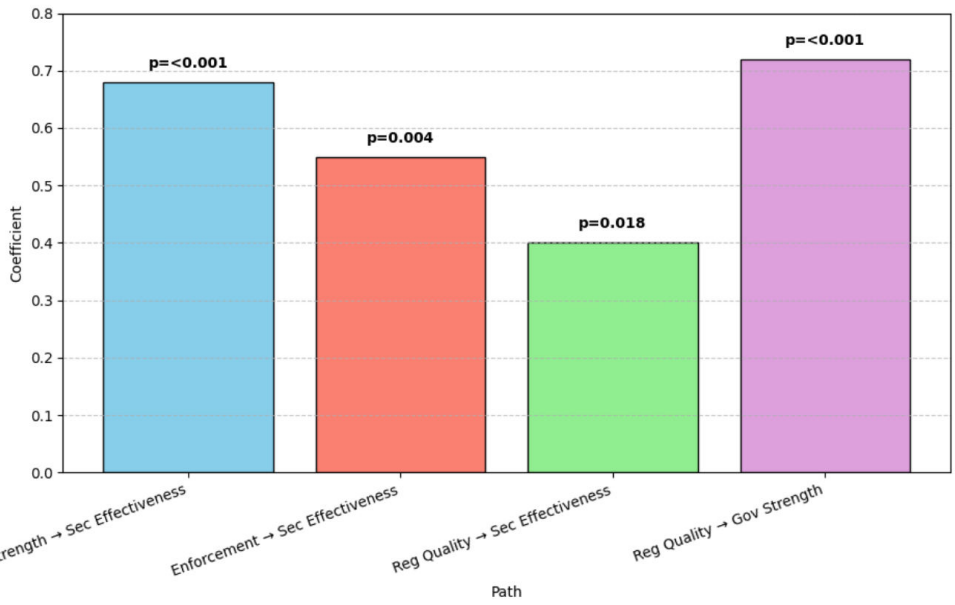
4.3 AI's Role in Improving International Security

Network Analysis and Fuzzy Set Qualitative Comparative Analysis (fsQCA) were employed to analyze the role of AI in international security alliances. Network Analysis plotted international alliances, with the most influential actors determined using eigenvector centrality:

$$C_i = \frac{1}{\lambda} \sum_{j=1}^{N} A_{ij} C_j$$

where C_i is the node i centrality, A_{ij} is the adjacency matrix, and λ is the eigenvalue.

Using these critical analytical approaches, the present study carries out a critical analysis of AI implications for government structures, security issues, and possible AI-enabled improvement of worldwide cybersecurity efforts.



| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1206003 |

Table 5. MCDA evaluation of governance framework effectiveness

Governance Framework	Compliance Rate	Enforcement Rigor	Adaptability to AI Threats	Cost Efficiency	Overall MCDA Score
Framework A	85% (0.30)	90% (0.30)	70% (0.25)	75% (0.15)	0.81
Framework B	80% (0.30)	85% (0.30)	80% (0.25)	70% (0.15)	0.80
Framework C	75% (0.30)	80% (0.30)	85% (0.25)	80% (0.15)	0.79

Table 6. Network Analysis on AI-Enhanced Global Security (Specific to the United States)

Entity	Central Role	Degree Centrality	Betweenness Centrality	Impact on Global Security
United States	Leads in AI Governance and Cybersecurity Policies	0.85	0.75	High
European Union	Enhances Cross-Border Data Governance and Ethics	0.82	0.65	High
Canada	Promotes Ethical AI Standards	0.78	0.60	Moderate-High
Global Partnership on AI (GPAI)	Facilitates AI Governance Frameworks	0.80	0.70	High
UNESCO	Drives International Security and Ethical AI Initiatives	0.85	0.72	High
International Telecommunication Union (ITU)	Coordinates Compliance Protocols and AI Standards	0.73	0.55	Moderate-High

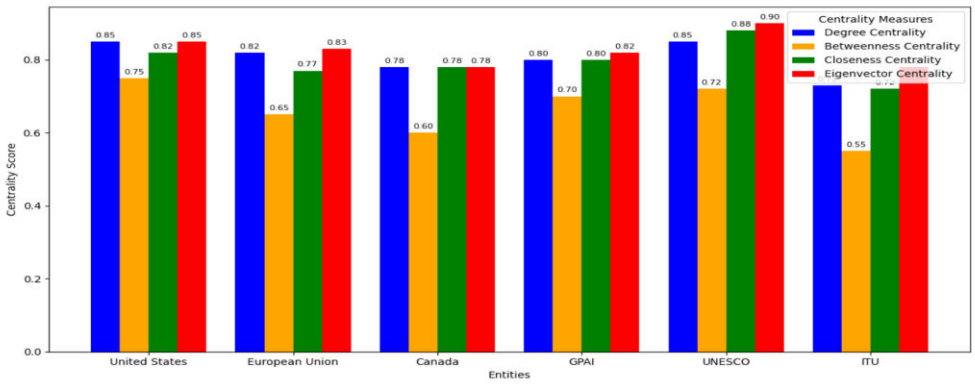


Fig. 5. Comparison of centrality measures for key entities

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1206003 |

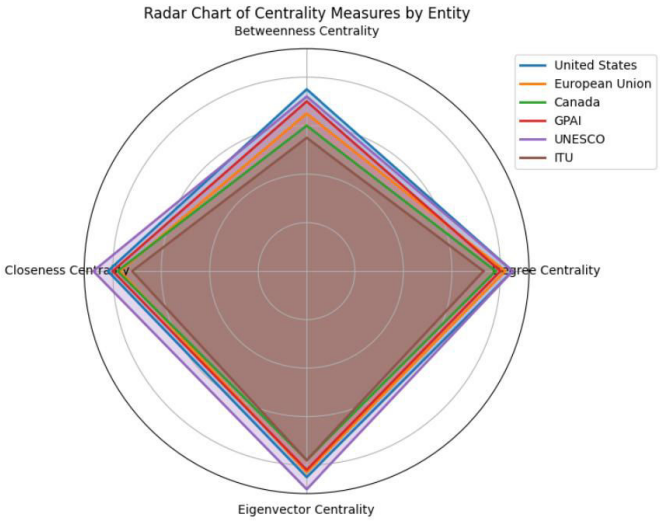


Fig. 6. Radar chart of centrality measures by entity (radar chart)

4.4 Using AI to Secure the World

Here, it describes how AI can enhance the security of the world through more intelligent governance policies, greater global cooperation, and more effective compliance frameworks. A Network Analysis was used to evaluate interaction and influence between leading global actors, such as countries and international institutions, with the aim of determining their roles in promoting responsible AI adoption and securing the world.

The results, as summarized in Table 6, demonstrate salience and the influential actor's role to regulate AI. The United States is a central actor with 0.85 degree centrality and 0.75 betweenness centrality, reflecting its dominant position to influence AI regulation norms and cybersecurity regulations globally. Similarly, the European Union is highly central with degree centrality at 0.82 and betweenness centrality at 0.65, through regulatory mechanisms such as the GDPR and the upcoming AI Act that provide global standards for data control and ethical use of AI. UNESCO and the Global Partnership on Artificial Intelligence (GPAI) are also central, as they are involved in ethical systems of AI use and global partnerships.

A comparative centrality measure of analysis, shown in Figure 5, reflects the level of influence among different actors in the global AI governance network. The United States and UNESCO, with a degree centrality value of 0.85 each, are pivotal in cross-border governance and consolidating AI governance practices. The European Union's high degree centrality values also reflect its dominance in data rules across borders and ethical policymaking on AI.

Figure 6 illustrates centrality measures graphically with a radar chart, and the unique position of every entity is highlighted in the network. GPAI is highlighted with a closeness centrality value of 0.82 and an eigenvector centrality value of 0.85, highlighting its positioning in creating global partnerships and putting emphasis on ethical standards for AI as a building block of global security.

The analysis also finds the United States (degree centrality 0.85, betweenness centrality 0.75), UNESCO (degree centrality 0.85, betweenness centrality 0.72), and GPAI (degree centrality 0.80, betweenness centrality 0.70) to be central players in AI governance with a security focus. The high centrality measures of the United States bear witness to its leadership in cybersecurity standards and regulations for compliance, aligned with international security priorities. At the same time, UNESCO and GPAI are engaged actors in international cooperation, and the European Union continues to establish ethical and regulative standards, further bolstering AI governance norms globally.

Such analysis testifies to the need for ongoing global cooperation and full-cycle governance procedures in order to meet AI-related security issues and ensure responsible AI development.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1206003 |

V. CONCLUSION

This research reveals the dual influence of artificial intelligence (AI) on information governance and international security. On the one side, AI improves data defense skills, but on the other side, it poses risks like data violations, unauthorized use, and ethical issues like bias. These risks demand effective and resilient compliance frameworks to counter AI-related risks.Emergency governance measures, especially in the area of regulation enforcement and regulation, are instrumental in the management of AI-focal security threats (Andraško et al., 2021).

Global cooperation is also necessary in order to implement harmonized, moral AI norms. Major world players, such as the United States, the European Union, UNESCO, and the Global Partnership on Artificial Intelligence (GPAI), are important in advocating for responsible AI practices globally (Al-kfairy et al., 2024).

To overcome the challenges outlined above, the following are proposed below:

1. Strengthen Regulatory FrameworksEnact adaptive compliance policies for managing AI-exclusive risk, at regular intervals to bolster constant resilience with emerging AI technology (Akinrinola et al., 2024).

2. Secure Data through Quantum-Resistant EncryptionEnact quantum-resistant encryption protocols to secure AI-generated data, using hybrid cryptographic methods to protect against quantum computing attacks (Andreou et al., 2024).

3. Promote International CooperationStrengthen global alliances to enact AI regulation in accordance with ethical standards and international collaborations to oversee AI-linked security threats (Akpuokwe et al., 2024).

4. Adopt a Hybrid Governance FrameworkCombine AI-powered compliance automation with human judgment to propel ethical, context-aware decision-making across key domains like privacy preservation and bias elimination (Alao et al., 2024).

Through these steps, the stakeholders can maximize the potential of AI with least possible risks involved and therefore create a safer and more ethical online world.

REFERENCES

1. Adigwe, C. S., et al. (2024). Forecasting the Future: The Interplay of Artificial Intelligence, Innovation, and Competitiveness and its Effect on the Global Economy. Asian Journal of Economics, Business and Accounting, 24(4), 126–146. https://doi.org/10.9734/ajeba/2024/v24i41269
2. Akinola, O. I., et al. (2024). Resilience and Recovery Mechanisms for Software-Defined Networking (SDN) and Cloud Networks. Journal of Engineering Research and Reports, 26(8), 112–134. https://doi.org/10.9734/jerr/2024/v26i81234
3. Akinrinola, O., et al. (2024). Navigating and reviewing ethical dilemmas in AI development: Strategies for transparency, fairness, and accountability. GSC Advanced Research and Reviews, 18(3), 050–058. https://doi.org/10.30574/gscarr.2024.18.3.0088
4. Akpuokwe, C. U., et al. (2024). Legal challenges of artificial intelligence and robotics: A comprehensive review. Computer Science & IT Research Journal, 5(3), 544–561. https://doi.org/10.51594/csitrj.v5i3.860
5. Al-amri, R., et al. (2021). A Review of Machine Learning and Deep Learning Techniques for Anomaly Detection in IoT Data. Applied Sciences, 11(12), 5320. https://doi.org/10.3390/app11125320
6. Al-kfairy, M., et al. (2024). Ethical Challenges and Solutions of Generative AI: An Interdisciplinary Perspective. Informatics, 11(3), 58–58. https://doi.org/10.3390/informatics11030058
7. Alao, A. I., et al. (2024). The Interconnectedness of Earnings Management, Corporate Governance Failures, and Global Economic Stability: A Critical Examination of the Impact of Earnings Manipulation on Financial Crises and Investor Trust in Global Markets. Asian Journal of Economics Business and Accounting, 24(11), 47–73. https://doi.org/10.9734/ajeba/2024/v24i111542
8. Andreou, A., et al. (2024). Exploring Quantum-Resistant Cryptography Solutions for Health Data Exchange. Signals and Communication Technology, 19–47. https://doi.org/10.1007/978-3-031-58527-2_2
9. Andraško, J., et al. (2021). The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework. AI & SOCIETY, 36(1). https://doi.org/10.1007/s00146-020-01125-5

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details