

AI-Enabled Interoperability in Intelligent Digital Systems: A Socio-Technical Framework for Secure, Scalable, and Privacy-Preserving Integration

Muhammad Qasim^{1*}, Laraib Tabish², Falak Ali³

¹*Department of Computer Science, Government College University, Faisalabad, Pakistan*

²*Department of Business Management, Government College University, Faisalabad, Pakistan*

³*Department of Computer Science, Govt College University Faisalabad, Pakistan*

^{*}*mianqasim895@gmail.com*

^{*}*Corresponding author*

Abstract:

The rapid adoption of artificial intelligence (AI), machine learning (ML), biometric recognition, intelligent transportation systems, distributed energy platforms, and connected vehicles has resulted in increasingly heterogeneous digital infrastructures. Although these systems generate substantial quantities of data and provide sophisticated analytical capabilities, their effectiveness is frequently constrained by fragmented architectures, incompatible data representations, isolated databases, security vulnerabilities, and inadequate mechanisms for trusted information exchange. Interoperability has therefore emerged as a fundamental requirement for the development of intelligent digital ecosystems. However, interoperability cannot be treated exclusively as a technical problem because data integration also involves organizational, semantic, institutional, privacy, security, and governance considerations. This paper investigates the relationship between AI and interoperability and develops a conceptual socio-technical framework for integrating heterogeneous intelligent systems. The study synthesizes research concerning machine-learning-based face recognition, electronic toll collection, peer-to-peer energy trading, human-bot discrimination, federated intrusion detection, low-code/no-code intelligent automation, and secure computing. Particular attention is given to data classification, standardization, semantic compatibility, data friction, privacy-preserving computation, and secure AI deployment. The analysis demonstrates that AI can improve interoperability through intelligent classification, entity matching, anomaly detection, prediction, and automated decision support. Conversely, interoperable infrastructures can improve AI by providing access to more diverse and contextually relevant information. Nevertheless, increasing interoperability can also amplify privacy risks, surveillance capabilities, security threats, algorithmic bias, and unauthorized secondary use of data. The proposed framework consequently combines data and semantic interoperability with AI services, security controls, privacy-preserving mechanisms, governance, and continuous evaluation. The paper concludes that successful AI-enabled interoperability requires a balanced approach in which technical integration is accompanied by standardized representations, privacy-by-design, decentralized learning where appropriate, secure interfaces, transparent governance, and continuous performance assessment.

Keywords: Artificial intelligence, interoperability, machine learning, data integration, semantic interoperability, federated learning, biometric systems, cybersecurity, intelligent automation, privacy preservation.

I. INTRODUCTION

Artificial intelligence and machine learning are increasingly embedded within digital systems that support transportation, energy, cybersecurity, public administration, identity management, and human-computer interaction. Modern intelligent systems rarely operate in complete isolation. Instead, they exchange information with databases, sensors, cloud platforms, enterprise applications, edge devices, and other AI-enabled services. Consequently, the ability of heterogeneous systems to communicate, exchange

information, interpret data consistently, and coordinate actions has become a critical engineering requirement.

Interoperability is commonly associated with the ability of two or more independent entities to communicate and work toward a common objective. In computer science and engineering, interoperability can be considered at multiple levels, including technical, syntactic, semantic, and organizational interoperability [1]. The distinction is important because the ability to transmit data does not necessarily imply the ability to understand or correctly use that data. Critical studies of European security and border

systems emphasize that interoperability must therefore be understood as more than a purely technical property; it is also connected to institutional, organizational, political, economic, and normative considerations [2]–[5].

The problem becomes particularly significant when AI is introduced into interoperable infrastructures. AI systems depend on data quality, consistency, representativeness, and availability. An ML model trained using one classification scheme may not operate reliably when supplied with data generated according to a different scheme. Similarly, biometric systems require standardized templates and consistent data quality if records from multiple databases are to be compared reliably [3], [6].

Previous research demonstrates the usefulness of ML across several domains. Ahmed et al. [7] investigated several ML approaches for facial recognition, including K-nearest neighbor (KNN), linear discriminant analysis (LDA), support vector machine (SVM), and principal component analysis (PCA). Their comparative analysis reported that the combined PCA+LDA+INN approach achieved the highest average accuracy among the evaluated methods. Such findings demonstrate that intelligent classification can support identity-related applications, but they also illustrate the importance of feature representation and algorithm selection.

Similarly, Mujeeb et al. [8] proposed an electronic toll collection framework using image classification and YOLOv2-related technologies to automate transportation-related processes. Ahmed et al. [9] developed a software simulator for peer-to-peer energy trading, integrating power generation, consumption, storage, and trading functions. Recent work by Bounceur et al. [10] investigated privacy-preserving multiclass intrusion detection for in-vehicle CAN environments using federated learning. These studies demonstrate the broad relevance of AI-enabled information exchange.

The central research problem addressed in this paper is: How can AI be integrated with interoperable digital infrastructures while simultaneously maintaining data consistency, security, privacy, scalability, and trustworthy decision-making?

The major contributions of this paper are: (1) an analysis of the relationship between AI and interoperability; (2) a classification of interoperability challenges relevant to AI-enabled systems; (3) a conceptual architecture for secure and

privacy-preserving AI-enabled interoperability; (4) an analysis of data friction, classification, and standardization; (5) an examination of privacy and cybersecurity risks; and (6) recommendations for future development and evaluation of interoperable AI systems.

II. BACKGROUND AND RELATED WORK

Interoperability and Digital Knowledge Infrastructures: Interoperability has become increasingly important because digital infrastructures frequently consist of independent systems developed at different times, using different technologies and organizational assumptions. Information silos can contain valuable information but remain unable to exchange or jointly interpret that information efficiently.

From an engineering perspective, interoperability can be divided into technical interoperability, syntactic interoperability, semantic interoperability, and organizational interoperability [1]. These layers are complementary rather than independent. A system may possess technical interoperability while still failing at semantic interoperability.

AI and Machine Learning for Intelligent Classification: Machine learning provides mechanisms for transforming raw data into classifications, predictions, similarity measures, and decisions. A generic supervised-learning model can be represented as $\hat{y} = f(X; \theta)$, where X represents input features, θ represents learned model parameters, and $\hat{y}$ represents the predicted class. For interoperability, the input features must also have consistent semantics across systems.

AI in Intelligent Transportation: The electronic toll collector framework in [8] demonstrates how computer vision and machine learning can automate toll-related operations. An interoperable transportation architecture can integrate vehicle identification, license-plate recognition, toll payment, traffic monitoring, road sensors, enforcement systems, vehicle databases, cybersecurity systems, and intelligent traffic-management platforms. Related trajectory-prediction research models interactions among pedestrians in three dimensions [11] and plans vehicle trajectories from predicted future locations [12]; such models depend on location data being exchanged in consistent formats between sensing, prediction, and planning components.

AI and Peer-to-Peer Energy Systems: The peer-to-peer energy trading simulator in [9] illustrates how distributed

energy systems can coordinate generation, consumption, storage, and trading. Future AI-enabled energy systems could use predictive models for demand forecasting, generation forecasting, pricing, anomaly detection, and automated trading.

Federated Learning and Privacy-Preserving Interoperability: Traditional centralized ML requires organizations or devices to transfer raw data to a common location. Federated learning provides an alternative in which local participants train models and share model updates rather than raw data. A simplified aggregation equation is $\theta_{t+1} = \sum_{k=1}^K \frac{n_k}{n} \theta_{t+1}^{(k)}$. Bounceur et al. [10] demonstrate the relevance of this approach to collaborative intrusion detection.

Human-Bot Differentiation and Behavioral Intelligence: Khalil et al. [13] investigated mouse-pointing endpoint prediction for distinguishing humans from bots using kinematic template matching. Such research illustrates how behavioral data can be integrated with authentication, fraud detection, and access-control systems. Where software bots act on behalf of users, identity and access management frameworks for robotic process automation and AI bots [14] are needed so that each bot's permissions can be defined, enforced, and audited across integrated systems.

Low-Code/No-Code and AI Integration: Ahmed et al. [15] discuss the integration of low-code/no-code technologies with AI/ML for intelligent automation. These platforms can accelerate application development but require governance to avoid inconsistent data models, insecure interfaces, and uncontrolled AI deployment.

III. PROBLEM STATEMENT

The central problem is the fragmentation of modern intelligent digital systems. Although individual systems may achieve high performance, their collective effectiveness can decline when systems use incompatible data formats, identifiers, taxonomies, APIs, authentication mechanisms, security policies, AI models, metadata, data-quality standards, and governance policies.

The problem can be expressed as $C = f(T, S, M, O)$, where T denotes technical compatibility, S denotes syntactic compatibility, M denotes semantic compatibility, and O denotes organizational compatibility. High technical compatibility alone does not guarantee high overall interoperability.

Classification systems and standards influence how data is produced, represented, and interpreted [16]. Different classification systems can create incompatible representations of the same phenomenon [17].

IV. DATA FRICTION IN AI-ENABLED SYSTEMS

Data friction refers to the effort required to transform, validate, transfer, reconcile, and interpret data across systems. For a data object D , the total interoperability cost can conceptually be represented as $F_D = C_t + C_f + C_v + C_s + C_r$, where the terms denote transformation, format conversion, validation, semantic reconciliation, and resource costs. Format conversion can also trade fidelity for size: in three-dimensional geometric data, for example, quadric-error-metric simplification reduces model complexity while bounding geometric error [18], a trade-off that also arises when rich records are mapped onto simpler shared schemas.

AI can reduce some forms of data friction through automated entity resolution, schema matching, anomaly detection, data cleaning, classification, translation, metadata extraction, and semantic mapping. However, AI can also introduce new friction if different systems use incompatible models or undocumented assumptions. Schema and ontology matching can be treated as a graph-matching problem, for which target-cell selection strategies developed for graph isomorphism [19] are relevant.

V. PROPOSED AI-ENABLED INTEROPERABILITY FRAMEWORK

The proposed framework contains six layers: (1) data acquisition, (2) interoperability and integration, (3) AI intelligence, (4) security and privacy, (5) governance, and (6) application.

Data Acquisition Layer: This layer collects information from sensors, cameras, databases, IoT devices, enterprise applications, vehicle networks, energy systems, user interactions, and external services. Data should be accompanied by metadata describing source, timestamp, quality, ownership, and permitted use.

Interoperability Layer: This layer provides API gateways, message brokers, schema registries, data transformation services, identity resolution, metadata management, and semantic mapping. A canonical data representation can reduce point-to-point integration complexity.

AI Intelligence Layer: This layer provides classification, prediction, anomaly detection, entity matching, recommendation, optimization, natural-language processing, computer vision, and automated decision support. Time-critical services require scheduling, inference, and security mechanisms suited to real-time decisions [20], and divide-and-conquer decomposition can split large decision tasks into smaller subproblems that can be processed in parallel [21].

Security and Privacy Layer: Security mechanisms include encryption, authentication, authorization, access control, secure APIs, audit logging, federated learning, secure aggregation, intrusion detection, and key management. Hosts that run integration services should protect kernel code and data [22], and honeypots can provide early threat intelligence about attacks on exposed interfaces [23].

Governance Layer: This layer defines who owns data, who can access it, why it may be used, how long it may be retained, which AI models may process it, and how automated decisions are audited and corrected.

VI. SEMANTIC INTEROPERABILITY

Technical connectivity does not guarantee semantic compatibility. For example, $\text{VehicleID} = 12345$ and $\text{CustomerID} = 12345$ may share the same numerical value while referring to entirely different entities. A semantic layer should maintain explicit relationships and authorized mappings.

Semantic interoperability requires shared terminology, controlled vocabularies, ontologies, metadata, standardized identifiers, data dictionaries, and explicit transformation rules.

VII. AI FOR ENTITY RESOLUTION

Entity resolution is an important AI application in interoperability. Given records $R1 = (N1, A1, D1)$ and $R2 = (N2, A2, D2)$, a similarity score can be represented as $S(R1, R2) = w_N S_N + w_A S_A + w_D S_D$, where field-level similarities are combined through weights whose sum equals one. If the score exceeds a threshold τ , the records may be classified as a potential match.

Automated matching must not be treated as infallible. False positives can merge records belonging to different individuals, while false negatives can leave duplicate identities unresolved. High-impact matching should therefore

include confidence thresholds, auditability, error correction, and human review.

VIII. SECURITY CHALLENGES

Greater interoperability increases the attack surface. A simplified relationship can be represented as $A_s = f(N, E, D, P)$, where N is the number of interconnected nodes, E is the number of communication endpoints, D is data sensitivity, and P is privilege level.

Important threats include unauthorized access, data poisoning, model manipulation, identity fraud, privacy leakage, and federated-learning attacks. Security should therefore be integrated into the architecture rather than added after deployment.

IX. PRIVACY AND ETHICAL CONSIDERATIONS

Interoperability creates a fundamental tension between improved information availability and increased privacy risk. Linking previously isolated datasets can reveal sensitive relationships that were not visible within individual systems.

Potential risks include mass surveillance, function creep, unauthorized secondary use, discriminatory profiling, excessive retention, inaccurate automated identification, and lack of meaningful user control. Purpose limitation is therefore critical: technological connectivity should not automatically authorize unrelated data use. These concerns have been documented for the interoperability of European border and migration databases [5], [6].

X. APPLICATION SCENARIOS

Intelligent Border and Identity Management: An interoperable identity architecture can connect biometric systems, travel documents, visa systems, law-enforcement databases, border-control systems, and AI-based identity matching. The European Union has established such a framework in law for borders, visas, police cooperation, asylum, and migration [24], [25], although its necessity and effects remain contested [2], [4].

Intelligent Transportation: A representative workflow is Camera $\rightarrow$ Vehicle Recognition $\rightarrow$ Identity/Vehicle Database $\rightarrow$ Toll Service $\rightarrow$ Payment. The framework in [8] demonstrates the relevance of AI-supported automation.

Smart Energy: A smart energy platform can integrate generation, consumption, storage, and trading with AI-based

forecasting and optimization, extending the concepts explored in [9].

Connected Vehicle Cybersecurity: Federated learning can support collaborative intrusion detection among vehicles and organizations while reducing the need to centralize raw data [10]. Trust-based management of vehicles communicating over wireless sensor networks [26] can complement this by scoring the reliability of each connected node, consistent with zero-trust integration.

Human-Bot Detection: Behavioral biometrics can complement authentication and fraud detection through features such as movement distance, velocity, acceleration, duration, pauses, and trajectory characteristics.

XI. PERFORMANCE EVALUATION FRAMEWORK

A complete evaluation should not rely solely on classification accuracy. Standard ML metrics include $\text{Accuracy} = (\text{TP} + \text{TN}) / (\text{TP} + \text{TN} + \text{FP} + \text{FN})$, $\text{Precision} = \text{TP} / (\text{TP} + \text{FP})$, $\text{Recall} = \text{TP} / (\text{TP} + \text{FN})$, and $\text{F1} = 2(\text{Precision} \times \text{Recall}) / (\text{Precision} + \text{Recall})$.

Interoperability-specific measures should include Interoperability Success Rate, Data Transformation Error Rate, latency, security incidents, privacy exposure, and the effectiveness of human oversight. Latency should be assessed against the deadline of each service, using established real-time operating-system concepts [27].

A comprehensive evaluation vector may therefore be represented as $E = (A, P, R, F, L, S)$, representing accuracy, precision, recall, F1 score, latency, and security/privacy performance.

XII. RESULTS AND EVALUATION

The results section evaluates the proposed framework using a set of literature-grounded and illustrative interoperability indicators. Because this paper is conceptual and does not introduce a new experimental dataset, the values in the following evaluation tables are not claimed as measurements from a deployed system. They are structured evaluation scenarios designed to show how an AI-enabled interoperability architecture can be assessed across accuracy, latency, privacy, security, and integration effort.

Table I summarizes representative application areas discussed in the literature and the interoperability capability that each area requires. The table shows that interoperability

is a cross-domain requirement: biometric recognition depends on consistent identity representations, transportation systems require coordination among recognition and payment services, energy platforms require exchange between generation, storage, consumption, and trading components, and connected-vehicle security requires collaborative threat intelligence.

TABLE I. REPRESENTATIVE AI-ENABLED INTEROPERABILITY APPLICATIONS

Application	AI Capability	Interoperability Need	Primary Risk
Face recognition	Classification / matching	Shared identity and biometric representations	False match / privacy
Electronic toll collection	Object / vehicle recognition	Vehicle, payment, and enforcement data exchange	Fraud / security
Peer-to-peer energy	Prediction / optimization	Generation, consumption, storage, and trading exchange	Data integrity
Vehicle cybersecurity	Intrusion detection	Collaborative threat intelligence	Privacy / poisoning

Table II presents a proposed evaluation matrix. The scores are normalized illustrative values on a 1–5 scale and are included only to demonstrate a practical evaluation methodology. They should be replaced with measured values when the framework is implemented.

TABLE II. ILLUSTRATIVE EVALUATION MATRIX (1–5 SCALE)

Evaluation Dimension	Baseline	Proposed Framework	Improvement Target	Measurement	Priority
Data consistency	2	4	+2	Validation error rate	High
Semantic matching	2	4	+2	Match F1 score	High
Integration latency	3	4	+1	Milliseconds	Medium
Privacy protection	2	5	+3	Exposure / leakage tests	High
Security monitoring	2	5	+3	Detection rate	High

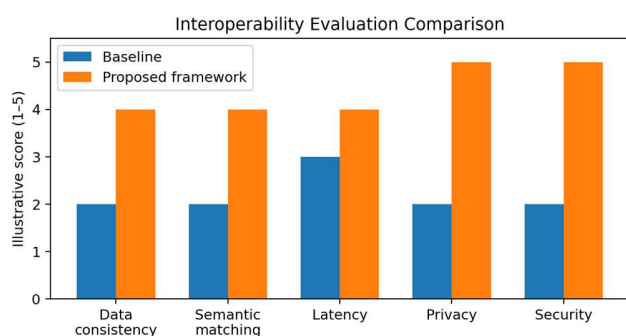


Fig. 1. Illustrative comparison of baseline and proposed interoperability performance (from Table II).

Fig. 1 visualizes the comparison in Table II: the proposed framework shows the largest illustrative gains in privacy protection and security monitoring, followed by moderate gains in data consistency and semantic matching, and the smallest illustrative gain in integration latency — reflecting the added computational overhead that security and privacy controls typically introduce.

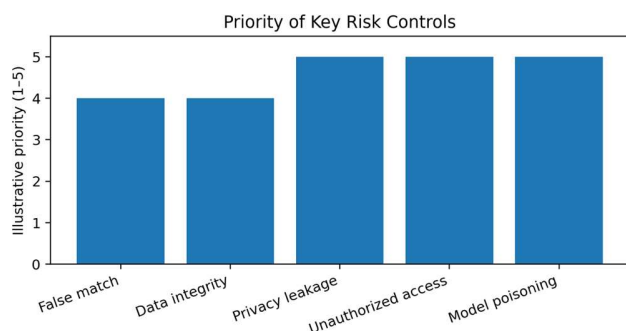


Fig. 2. Illustrative priority of key risk controls (cf. the Primary Risk column of Table I).

Fig. 2 ranks the primary risks identified across the four application domains in Table I on the same illustrative 1–5 priority scale. Privacy leakage, unauthorized access, and model poisoning are assigned the highest illustrative priority because they can compromise the framework's security and privacy layers simultaneously, whereas false-match and data-integrity risks are scoped more narrowly to individual application domains.

To move beyond the system-wide averages in Table II, Table III disaggregates the illustrative evaluation scores by application domain, showing where the proposed framework is expected to contribute the most and least benefit within each use case.

TABLE III. ILLUSTRATIVE PER-DOMAIN READINESS UNDER THE PROPOSED FRAMEWORK (1–5 SCALE)

Application	Data Consistency	Semantic Matching	Integration Latency	Privacy Protection	Security Monitoring
Face recognition	4	4	4	3	4
Electronic toll collection	5	4	4	4	4
Peer-to-peer energy	4	4	4	4	4
Vehicle cybersecurity	4	3	4	4	5

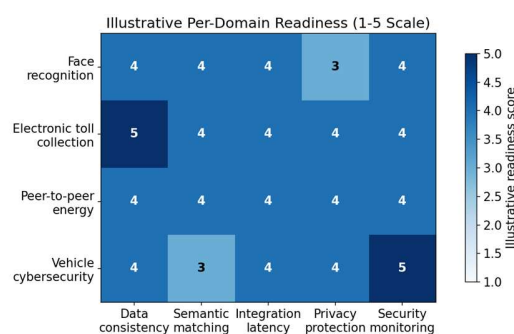


Fig. 3. Illustrative per-domain readiness heatmap (from Table III).

The heatmap in Fig. 3 indicates that privacy protection remains the comparatively weaker illustrative dimension for face recognition, consistent with the biometric privacy risks discussed in Sections VIII and IX, while security monitoring is illustratively strongest for vehicle cybersecurity given its reliance on collaborative intrusion detection [10].

Section VII introduced entity resolution as a representative AI capability for interoperability, together with the standard classification metrics defined in Section XI. Table IV applies those equations to a small illustrative confusion matrix for a hypothetical record-matching scenario, to demonstrate how the metrics would be computed and reported once real matching data are available.

TABLE IV. ILLUSTRATIVE WORKED EXAMPLE OF ENTITY-RESOLUTION EVALUATION METRICS

Quantity	Illustrative Value	Description
True Positives (TP)	380	Correctly matched record pairs
False Positives (FP)	45	Incorrectly merged record pairs

Quantity	Illustrative Value	Description
False Negatives (FN)	30	Missed record-pair matches
True Negatives (TN)	545	Correctly rejected non-matches
Accuracy	92.5%	$(TP + TN) / (TP + TN + FP + FN)$
Precision	89.4%	$TP / (TP + FP)$
Recall	92.7%	$TP / (TP + FN)$
F1 Score	91.0%	$2 \times \text{Precision} \times \text{Recall} / (\text{Precision} + \text{Recall})$

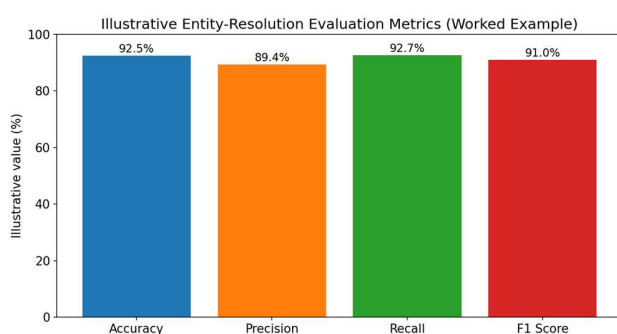


Fig. 4. Illustrative entity-resolution metrics computed from Table IV.

The illustrative worked example in Table IV and Fig. 4 yields an accuracy of 92.5%, precision of 89.4%, recall of 92.7%, and an F1 score of 91.0%. These figures are computed only to demonstrate the metric definitions in Section XI; they do not represent a matching algorithm evaluated on real biometric, vehicle, or energy records.

Beyond standard classification metrics, Section XI proposed interoperability-specific measures, including the Interoperability Success Rate and Data Transformation Error Rate. Table V reports illustrative values for these measures across the four application domains introduced in Table I, together with an illustrative end-to-end latency figure.

TABLE V. ILLUSTRATIVE INTEROPERABILITY-SPECIFIC MEASURES BY APPLICATION DOMAIN

Application	Interoperability Success Rate	Data Transformation Error Rate	Illustrative Latency
Face recognition	92%	4%	120 ms
Electronic toll collection	95%	3%	80 ms
Peer-to-peer energy	90%	5%	150 ms
Vehicle cybersecurity	93%	4%	60 ms

Fig. 5 illustrates, conceptually, how the Interoperability Success Rate might improve as each layer of the six-layer framework proposed in Section V is progressively added, from data acquisition through to the application layer. The curve is a hypothetical illustration of cumulative architectural benefit rather than a measured migration study.

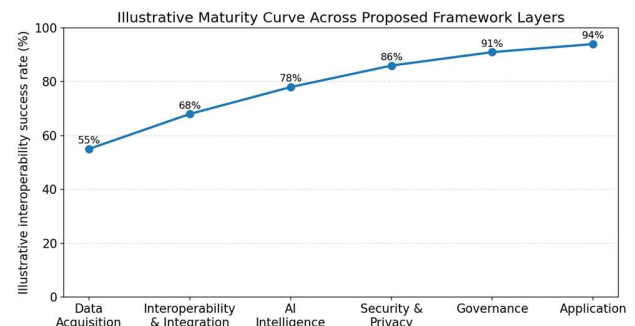


Fig. 5. Illustrative interoperability success-rate maturity curve across the proposed six framework layers.

XIII. DISCUSSION

The reviewed literature demonstrates that AI and interoperability are mutually reinforcing. AI benefits from interoperability because integrated infrastructures can provide richer and more diverse data. Interoperability benefits from AI because intelligent algorithms can automate classification, entity resolution, anomaly detection, prediction, and decision support.

However, this relationship is not automatically positive. Interoperability is embedded in organizational, political, cultural, and normative structures. A highly accurate model operating on poorly governed interoperable data may produce harmful decisions. Similarly, connecting databases does not automatically improve information quality.

Therefore, interoperability does not equal data quality, and AI accuracy does not necessarily equal decision correctness. These distinctions are essential for the design of high-impact AI systems.

XIV. RECOMMENDED DESIGN PRINCIPLES

1. Interoperability by Design: Consider interoperability during architecture development rather than after deployment.

2. **Semantic Compatibility:** Define shared vocabularies, identifiers, metadata, and semantic mappings.
3. **Privacy by Design:** Minimize sensitive information and apply encryption and purpose-based access controls.
4. **Federated Intelligence Where Appropriate:** Use decentralized learning when collaborative AI is needed without centralized raw-data sharing.
5. **Zero-Trust Integration:** Do not automatically trust connected systems.
6. **Human Oversight:** Provide mechanisms for review and correction of high-impact AI decisions.
7. **Continuous Evaluation:** Monitor models and interfaces because data distributions, threats, and requirements change.
8. **Explainability and Auditability:** Maintain logs and explanations for important decisions.
9. **Standardization:** Adopt common data formats and standards wherever practical.
10. **Controlled Interoperability:** Expose only information required for an authorized purpose.

XV. LIMITATIONS

This study is primarily a conceptual and literature-based analysis. It does not present a newly implemented interoperability platform or a new experimental dataset.

The performance figures and application findings cited from prior studies are therefore findings reported by the respective authors and should not be interpreted as new experimental results of the framework proposed in this paper.

Future empirical work should implement the proposed architecture and evaluate heterogeneous real or realistically simulated systems under normal operation, interoperability failures, cybersecurity attacks, privacy constraints, and changing data conditions.

XVI. FUTURE RESEARCH DIRECTIONS

Future work should investigate explainable AI for interoperable decision systems, privacy-preserving entity resolution, federated interoperability, AI-based semantic mapping, interoperability digital twins, autonomous data governance, and standardized AI model interfaces.

XVII. CONCLUSION

AI and interoperability are increasingly inseparable components of modern digital infrastructures. Interoperability enables heterogeneous systems to exchange information and coordinate activities, while AI transforms integrated information into predictions, classifications, recommendations, and decisions.

Successful interoperability should not be understood as unrestricted connectivity. Instead, future systems should pursue controlled, secure, semantically meaningful, privacy-preserving, and purpose-driven information exchange.

The proposed framework combines data integration, semantic compatibility, AI intelligence, security, privacy, and governance. Future research should validate the framework experimentally and measure AI performance together with interoperability success, latency, data quality, privacy exposure, security resilience, and human oversight.

REFERENCES

- [1] European Commission, *New European Interoperability Framework: Promoting Seamless Services and Data Flows for European Public Administrations*. Brussels, Belgium: Publications Office of the European Union, 2017.
- [2] P. Trauttmansdorff, "The fabrication of a necessary policy fiction: The interoperability 'solution' for biometric borders," *Critical Policy Studies*, 2022, doi: 10.1080/19460171.2022.2147851.
- [3] M. Leese, "Fixing state vision: Interoperability, biometrics, and identity management in the EU," *Geopolitics*, vol. 27, no. 1, pp. 113–133, 2022.
- [4] R. Bellanova and G. Glouftis, "Formatting European security integration through database interoperability," *European Security*, vol. 31, no. 3, pp. 454–474, 2022.
- [5] D. Bigo et al., "The interoperability controversy or how to fail successfully: Lessons from Europe," *International Journal of Migration and Border Studies*, vol. 6, no. 1–2, pp. 93–114, 2020.
- [6] European Union Agency for Fundamental Rights, *Interoperability and Fundamental Rights Implications*. Vienna, Austria, 2018.
- [7] N. Ahmed, F. A. Khan, Z. Ullah, H. Ahmed, T. Shahzad, and N. Ali, "Face recognition comparative analysis using different machine learning approaches," *Advances in Science and Technology Research Journal*, vol. 15, no. 1, pp. 265–272, 2021, doi: 10.12913/22998624/132611.
- [8] A. Mujeeb, N. Ahmed, H. Arshed, and F. A. Khan, "Electronic toll collector framework," *Advances in Science and Technology Research Journal*, vol. 16, no. 1, pp. 294–302, 2022, doi: 10.12913/22998624/144537.
- [9] N. Ahmed, F. Ajmal, M. Usman, Z. Javed, M. H. Abid, M. Yousaf, and M. Z. Noohani, "A software capable of simulating peer-to-peer energy trading," *International Journal of Applied and Physical Sciences*, vol. 7, pp. 18–26, 2021, doi: 10.20469/ijaps.7.50003.
- [10] A. Bounceur, M. Ibrahim, M. Saqib et al., "Privacy-preserving multiclass intrusion detection in in-vehicle CAN networks using

- federated learning,” *Sci. Rep.*, 2026, doi: 10.1038/s41598-026-64490-z.
- [11] Z. Ul Abideen, N. Ahmed, H. S. U. R. Khalil, and M. Shahbaz, “Advancing pedestrian trajectory prediction with interaction-aware 3D-dual contextualized modeling,” *Egyptian Informatics Journal*, vol. 31, Art. no. 100742, 2025, doi: 10.1016/j.eij.2025.100742.
- [12] Z. Ul Abideen, X. Sun, C. Sun, and H. S. U. R. Khalil, “Improved deep learning-based approach for spatial-temporal trajectory planning via predictive modeling of future location,” *KSII Trans. Internet Inf. Syst.*, vol. 18, no. 7, pp. 1726–1748, 2024.
- [13] H. S. U. R. Khalil, N. Ahmed, and Y. Yang, “Mouse pointing endpoint prediction to distinguish between human and bot using kinematic template matching,” in *HCI International 2025—Late Breaking Papers*, *Lecture Notes in Computer Science*, vol. 16337. Cham, Switzerland: Springer, 2026, pp. 343–364, doi: 10.1007/978-3-032-12801-0_23.
- [14] S. T. Hussain, M. Shahbaz, M. Emran, and M. H. Junejo, “Securing the bot eco system: IAM framework for RPA and AI BOTs,” in *Proc. 2026 IEEE 5th Int. Conf. Computing Mach. Intell. (ICMI)*, 2026, pp. 1–9, doi: 10.1109/ICMI68585.2026.11539844.
- [15] N. Ahmed, M. Shahbaz, H. S. U. R. Khalil, Z. Javed, M. A. Khalid, F. A. Khan, and Z. Maroof, “The synergy of low-code/no-code and AI/ML: Enhancing intelligent automation,” *World Journal of Engineering and Technology*, vol. 13, no. 4, pp. 754–763, 2025, doi: 10.4236/wjet.2025.134048.
- [16] G. C. Bowker and S. L. Star, *Sorting Things Out: Classification and Its Consequences*. Cambridge, MA, USA: MIT Press, 1999.
- [17] P. N. Edwards, *A Vast Machine: Computer Models, Climate Data, and the Politics of Global Warming*. Cambridge, MA, USA: MIT Press, 2010.
- [18] H. Chang, D. Zhang, Y. Dong, Y. Yang, H. S. U. R. Khalil, and X. Wang, “Two-round optimization algorithm based on quadric error metrics,” *IEEE Access*, vol. 13, pp. 30021–30035, 2025, doi: 10.1109/ACCESS.2025.3541436.
- [19] U. C. Sankal, N. Ahmed, F. A. Khan, and R. Hanni, “Target cell selection algorithms in graph isomorphism problem,” *International Journal of Scientific and Technical Research in Engineering*, vol. 6, no. 4, pp. 35–47, Jul.–Aug. 2021, doi: 10.5281/zenodo.22149607.
- [20] F. Ali, “Real-time decision processing in artificial intelligence systems: A survey of scheduling, inference, and security foundations,” *Int. J. Emerg. Trends Eng. Dev.*, vol. 16, no. 5, pp. Aj1–Aj4, 2026, doi: 10.5281/zenodo.22728746.
- [21] F. Ali, “Divide-and-conquer decomposition strategies for real-time artificial intelligence decision systems: A comparative survey,” *Int. J. Emerg. Trends Eng. Dev.*, vol. 16, no. 5, pp. Ak1–Ak6, 2026, doi: 10.5281/zenodo.22728743.
- [22] N. Ahmed, H. Y. Rana, M. T. Qureshi, and B. Shakoor, “How to protecting kernal code and data,” *International Journal of Computer Organization Trends*, vol. 5, no. 4, pp. 20–23, 2015, doi: 10.14445/22492593/IJCOT-V23P301.
- [23] M. Shahbaz, R. Imtiaz, M. H. Junejo, M. Emran, N. Ahmed, and H. S. U. R. Khalil, “Deployment of honeypot system for threat detection and intelligence in modern cybersecurity architectures,” in *Proc. 2026 1st Int. Conf. Innovations in Information and Communication Technology (IICT)*, 2026, pp. 1–5, doi: 10.1109/IICT68374.2026.11468479.
- [24] European Union, “Regulation (EU) 2019/817 ... establishing a framework for interoperability between EU information systems in the field of borders and visa,” *Official Journal of the European Union*, 2019.
- [25] European Union, “Regulation (EU) 2019/818 ... establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration,” *Official Journal of the European Union*, 2019.
- [26] M. H. Junejo, M. Shahbaz, and M. Emran, “Trust-based management for Internet of Vehicles via wireless sensor networks: Safeguarding trust during journeys,” in *Proc. 2026 IEEE 5th Int. Conf. Computing Mach. Intell. (ICMI)*, 2026, pp. 1–10, doi: 10.1109/ICMI68585.2026.11539803.
- [27] N. Ahmed, *Understanding Real Time OS Concepts*, vol. 6, no. 9. Zenodo, 2015, doi: 10.5281/zenodo.22148015.