iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** XI **Month of publication:** November 2026

DOI: https://doi.org/10.22214/ijraset.2026.85695

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue XI Nov 2026- Available at www.ijraset.com

A Federated Interoperability Framework for Unified Government Digital Services

Ashwini Tekale[1], Abhijit Tikone[2], Shivprasad Suryawanshi[3]
[1, 2, 3]*Master of Computer Applications, JSPM's Narhe Technical Campus, Savitribai Phule Pune University, Pune, India*

Abstract: ***Government digital services are increasingly being presented on multiple different departmental platforms causing data silos, multiple databases, heterogeneous systems, multiple authentications and multiple submissions of citizen data. The research proposes a Federated Interoperability Framework for Unified Government Digital Services. This allows different departments to communicate despite being independently managed. The framework encompasses federated digital identities, standardised APIs and data models, secure data transfer, consent, authentication and authorisation. The Design Science Research methodology was used. This allowed us to identify the problem, gather requirements from the literature, design our framework and create a prototype based logic. Finally, the framework was evaluated to assess if it met the expected interoperability requirements. The evaluation of this framework was intentionally at framework level. This meant we could assess if our architecture had covered interoperability, digital identities, controlled data sharing, privacy, security, legacy integration, scalability and governance. There was no claim that the framework would improve anything within a live government department. However, it was found that a Federated Interoperability Framework can provide the layer of service access but not fully centralise the data. This can allow for a gradual integration process of heterogeneous systems.***

Keywords: Digital Government, Interoperability, Federated, Unified Identities, API Integration, Consent, E-Governance, Data Governance, Service Orchestration, Cyber Security.

I. INTRODUCTION

With the ever increasing rate of digital government, there are many aspects of government services that are now available digitally. This ranges from applications, certificates, welfare schemes, identification, tax, licencing, education, health care and more. By providing these services digitally there are many benefits such as reducing visits to the department, giving information to citizens whenever they want it, traceable information and consistent administration across the board. However, due to the rise of individual departmental platforms there are many issues with having a fragmented digital environment.

This can cause the citizen to struggle with finding multiple portals to navigate, creating multiple accounts, entering their personal information multiple times and understanding differing processes for services that are linked together administratively. From the departmental side, there will be multiple systems containing the same citizen data causing duplication, inconsistency, extra administration and difficulty with coordination.

It cannot always be assumed that all departmental systems will be changed to a centralised database. There may be valid reasons why the government organisation wants to keep ownership and control of their applications and data. A more realistic approach to this problem would be to create an interoperability layer. This would allow the existing systems to communicate with common interfaces and policies. This is the basis of a Federated Interoperability Framework.

The Federated Interoperability Framework allows the departments to act as independent members within a trusted environment. Each department will have their own database and internal logic. They will expose certain services through standardised APIs or adapters. A shared identity and policy can be applied to ensure trusted authentication. Consent and authorisation will help determine which information can be accessed for a specific service.

The main focus of the research was to address the integration problem. An interoperability layer can be used to provide a unified citizen experience whilst allowing the integration of heterogeneous departmental systems. This can include API Gateways, service orchestration, identity federation, policy enforcement, consent, standardised data models, monitoring and auditing.

The concept of federation is an important factor to consider. This is because government systems will vary in technology, database structure, security, development and ownership. Some services will have modern REST APIs whereas others will have legacy systems that will need to be adapted through an adapter or intermediary service. The aim of the framework is to allow for this.

©IJRASET: All Rights are Reserved

A unified identity is an important aspect to consider. The citizen should not need to prove the same identity multiple times. Instead a trusted federated system can be used to ensure they are authenticated once and given an assertion/token to authorised services. However, authorisation and consent will be needed to determine what information can be accessed by the requesting service.

Interoperability can also be a semantic issue. Whilst systems can communicate in a technically correct way the meaning of the fields can be misunderstood. This means that the data needs to be standardised. This can include common identifiers, metadata, validation and service contracts. A clear ownership of the systems can also be important. This will determine what data can be accessed, what services are available, security and how disputes are resolved.

The framework includes the technical integration but also the governance aspect to create a controlled interoperability. The overall architecture is shown in Fig. 1.

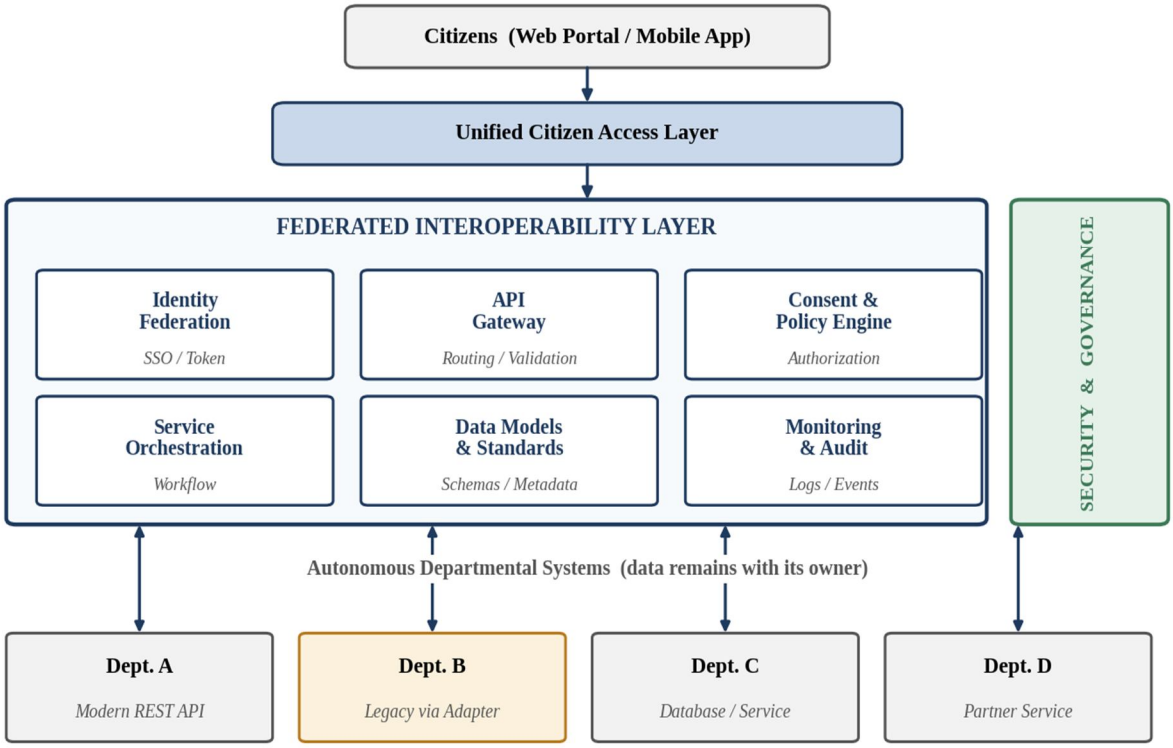


Fig. 1 High-level federated interoperability architecture

A. *Problem Statement*

The main problem to solve was that government digital services were fragmented. Whilst there may be useful services provided on individual portals, this can cause the citizen to have a disjointed process.

There are multiple reasons for this issue:

- Heterogeneous systems within each department.
- Multiple authentication methods which causes multiple accounts and logins.
- Duplication of citizen data within departmental databases.
- Difficulties in connecting legacy systems through modern integration methods.
- Privacy and security requirements so uncontrolled data sharing is not acceptable.
- Departments cannot be treated as one technical unit due to ownership.

Therefore the problem statement became how can we create an interoperability framework that will connect heterogeneous government digital services in a secure, seamless manner, whilst ensuring departmental independence, data ownership, security, privacy and governance?

We cannot simply create a centralised database. This will create a single high value target, increase the migration requirements and reduce the independence within the departments. This research looked into a federated approach to ensure data stays with the original source and only authorised information/services are shared.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

B. Research Objectives

To design a Federated Interoperability Framework that allows secure, seamless and unified access to heterogeneous government digital services. Whilst ensuring the independence and data ownership of individual government departments.

1) Analyse current issues with interoperability of government digital services. Including fragmented systems, heterogeneous systems, data silos, duplication of data and lack of standardised communication.
2) Research current interoperability frameworks and architectures used within national and international digital government environments. Understanding the key components, strengths and limitations.
3) Design an interoperability framework that will allow independent government departments and service providers to communicate. Without completely centralising the databases.
4) Create a unified digital identity and authentication that will allow citizens to access multiple government services using one authentication.
5) Create standardised and secure data sharing. This can include the use of APIs, standardised data models, interoperability and controlled services.
6) Include privacy, consent, authentication, authorisation and cyber security.
7) Allow integration of heterogeneous and legacy government systems. Minimising any changes to existing systems.
8) Include governance and accountability. This will ensure clear ownership, policies on data access, data ownership and interoperability.
9) Create a prototype or proof of concept to show how multiple government services can be connected using the interoperability framework.
10) Evaluate the framework for interoperability, security, scalability, usability, integration of services and minimising redundant citizen interaction.

C. Research Questions

RQ1: What technical and organisational barriers exist preventing seamless interoperability between heterogeneous government digital services?
RQ2: How can federation be used to provide a unified identity and access to services without centralising the data?
RQ3: What API, standardised data, consent, security and governance requirements are needed to ensure controlled information sharing?
RQ4: Can a prototype based approach be used to show how a representative set of departmental services can be integrated whilst maintaining data ownership?

D. Hypothesis

H1 (Working Hypothesis): A Federated Interoperability Framework can be created using a unified identity, standardised API, controlled data sharing, consent, security and governance. This will provide a more unified method of accessing government services whilst ensuring the independence of departmental data compared to fragmented portals.
H0 (Null Hypothesis): The proposed Federated Interoperability Framework will not provide a meaningful advantage in the architectural design compared to fragmenting departmental integration to provide unified government services.
As this research was focused on the architecture and prototype, the hypothesis became a design hypothesis. This means that instead of claiming there is a statistically significant improvement in a population, the hypothesis will be validated through scenarios.

E. Significance of Study

This study is significant to the citizen as it will reduce the complexity of accessing services. Citizens can use a common identity to access multiple eligible services. For government departments the study will show how systems can be integrated gradually. This means that there is no immediate changes to the databases and applications.
For technology and architecture researchers, the framework combines many areas that are often researched individually. This includes Enterprise Architecture, Service Oriented Interoperability, Federated Identity, Secure Data Sharing, Consent, Data Governance and Institutional Coordination. This will provide an integrated architecture that can be further implemented and analysed.
For policymakers and administrators the framework highlights that the interoperability is not just a technical issue. There needs to be clear ownership of the data, policies for accessing, auditing, common standards, accountability and governance.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

The overall significance of the research was to provide a realistic progression from fragmented digital services to a federated citizen focused service.

II. LITERATURE REVIEW

The literature review looked at research into government interoperability, digital government architecture, federated services, identity, cyber security, data governance, enterprise architecture and integration. Overall, it was identified that interoperability can be a multi-faceted problem.

The World Bank [1] looked at interoperability as a basis for a data driven public sector. This shows the importance of connecting the data and digital services from government. This relates to the framework as it shows interoperability is an enabler.

Guijarro [2] looked at interoperability frameworks and enterprise architecture for e-government. This is important as it links interoperability with architecture. This supports the use of an integration layer and common architecture principles.

Klischewski [3] looked at e-government integration as a research problem. This shows how the framework will include governance and coordination.

Gottschalk [4] introduced maturity levels for interoperability in digital government. This is relevant as government interoperability can be improved gradually. Starting with simple data sharing and working towards more integration with services, identity, orchestration and governance.

Kubicek et al. [5] looked at organisational interoperability using examples of good practice from Europe. This supported the fact that successful interoperability can only be achieved through coordination. This supports the governance aspect.

Pardo et al. [6] looked at e-government interoperability from a wider perspective. This supports the argument that technical interfaces alone cannot solve the differences in policy, coordination and ownership.

Rao [7] proposed a framework for unified digital government for India. This is directly relevant as it shows the need for integration of government services.

Al-Husban and Adams [8] proposed a connected service delivery framework to deliver an interoperable government. This supports the main research premise that a framework can be used to connect services.

Mecca et al. [9] looked at federated single sign-on within e-government interoperability frameworks. This is directly relevant to the unified identity aspect.

Krimmer et al. [10] looked at cross border e-governance and interoperability of systems with independent governance. Whilst this is not the same as government integration within the country, it highlights the importance of trust, interoperability rules and controlled sharing.

Nadhamuni et al. [11] looked at how enterprise architecture can be used to support large scale digital transformation within the public health system of India. This shows the usefulness of using architecture based approaches within complex environments in India. This supports the use of a structured architecture.

Oumkaltoum et al. [12] proposed a hybrid e-government framework using data warehousing and multi-agent systems to achieve interoperability. This shows an alternative approach to the architecture. This shows the variety of methods that can be used to connect heterogeneous information.

Kalogirou et al. [13], [14] looked at the evolution and evaluation of national interoperability frameworks. This included an example of Greece. This highlighted the need for interoperability frameworks to be adaptable to changing requirements and should constantly be evaluated.

Campmas et al. [15] looked at if interoperability can encourage the use of digital public services. This was done by analysing national interoperability frameworks within the European Union. This relates to the citizen focused framework.

Schmitz et al. [16] looked at interoperable public services architectures using service oriented approaches and PEPPOL. This supports the use of modular integration and reusable interfaces.

Alvarez-Rodriguez et al. [17] looked at national and sub-national interoperability within Spain. This is relevant as it shows how multiple levels of government can work together within a federated architecture.

Malik et al. [18] proposed mechanisms for secure digital government interoperability and data sharing using blockchain and deep learning based techniques. This supports the need for security and trust when sharing information between systems.

Xisto et al. [19] proposed a reference architecture for digital government interoperability, connectivity, management and re-use in Brazil. This supports the use of a reference based architecture to encourage re-usable integration.

Kibira et al. [20] looked at service integration for e-government in Tanzania. This provided a practical view of the problems faced when trying to share services and information between heterogeneous government systems.

Sixpence and Vasconcelos [21] provided a systematic literature review looking at enterprise architecture approaches for e-government interoperability. This supports the use of an architecture based approach and layered design.
Torab-Miandoab et al. [22] proposed a unified data driven component based framework for interoperability in healthcare. Whilst this is specific to the healthcare industry, it shows how component based systems can be used within government. This will reduce the amount of repeated integration. Figueroa et al. [23] provided a systematic analysis of cyber security approaches for e-government. This supports the need to integrate cyber security into interoperability.
Dudoit and Labillois [24] looked at digital sovereignty, federalism, data interoperability and AI governance. This is relevant to the federation as it shows how important interoperability is to institutional independence.
Gupta [25] combined data stewardship, interoperable infrastructure and public value accountability to create a data driven digital government framework. This supports our use of combining technical integration with data governance and accountability.
Jia et al. [26] proposed a federated service with federated security to provide aligned data supply with scenario focused demand. This is one of the most similar concepts to our research. This uses federated service delivery with security.
Maharjan and Maharjan [27] proposed an interoperability service delivery architecture for ministries within Nepal. This is useful as it compares the integration of independently managed government organisations.
Thela et al. [28] developed and evaluated a service oriented interoperability framework for the e-government system in Botswana. This shows how service oriented integration can be practically applied and supports the use of APIs for government interoperability.
Figueroa et al. [29] integrated risk management, secure interoperability and governance through the GAUCHO framework. This supports the principle of including security, risk and governance within the architecture.
Dudoit [30] looked at public sector data interoperability in Canada. This considered intergovernmental capability and sovereign action. This is relevant to keeping institutional ownership whilst allowing controlled data sharing.
Yazdinejad and Kong [31] explored federated learning to overcome data silos within public health. Whilst this is not the same as federated service interoperability it shows the importance of collaboration without unnecessary centralisation.
Tomlinson et al. [32] discussed coherent interoperability in healthcare data ecosystems. This highlighted the need for standardisation and coherence. This provides useful lessons that can be transferred to government.
Zheng [33] looked at digital empowerment and collaborative governance for grassroots public services. This reinforced the use of digital technologies for coordinated public services. Thirasakthana and Kiattisin [34] proposed a sustainable government enterprise architecture framework. This supports scalability, governance and sustainability.
Wimmer et al. [35] defined interoperability governance and looked at examples from Europe. This is an important contribution as it will help define policies, ownership and coordination. Ronoh et al. [36] proposed an interoperability framework for heterogeneous e-government information systems, and Schmitz and Wimmer [37] proposed a framework for developing interoperable service architectures.

A. Thematic Analysis

The following 6 themes were identified from the literature.
Architecture: Enterprise architecture, service oriented architecture and reference architecture can be used to provide structure for connecting heterogeneous systems.
Federated Identity and Services: Federated single sign-on and federated service ecosystems can be used to provide unified access whilst not forcing all departments to use one internal system.
Security / Privacy: Cyber security, authentication, authorisation, consent, encryption and auditing are required as more connections will be made.
Data / Semantic: Standardised data models, metadata, identifiers, validation and service contracts will reduce confusion.
Organisational / Governance: Technical interfaces alone provide limited capability when departments are separate and independently governed. Incremental modernisation: Adapters, gateways and services can be used to connect to legacy systems. The key part of this framework is using these components together as a federated service delivery solution.

B. Research Gap

Throughout the literature review it was found that there are many ways to look at interoperability within government, including enterprise architecture, national interoperability frameworks, service-oriented architecture, organisational interoperability, federated identity, cyber security, data ownership and federated services. However, they are often looked at in isolation or are very context specific.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

The research gap for this study is to create an architectural solution that integrates the following into one solution:

- Unified digital identity and federated identity;
- API service integration and standardised data exchange;
- Consent, security, authorisation, encryption and audit;
- Departmental data ownership and governance;
- Unified citizen access.

This aligns with the research problem of creating a federated solution that takes into account the technical, organisational, security and governance aspects.

III. RESEARCH METHODOLOGY AND DESIGN

The research will follow a Design Science Research methodology with an architectural prototype and scenario based approach. This is because we want to design and evaluate an artifact to solve the problem. The workflow is shown in Fig. 2.

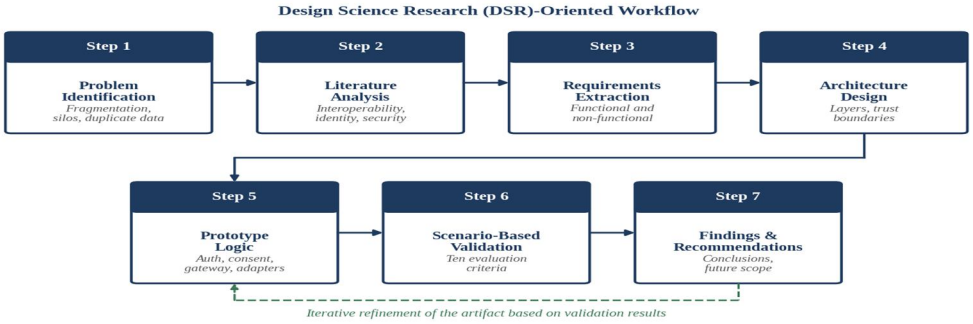


Fig. 2 Research methodology (Design Science Research-oriented workflow)

Start with identifying the problem, perform a literature review, extract requirements, design the architecture, design the Prototype Logic, perform scenario based validation, and find results and recommendations. This is not claiming to be performance based in a live government setting. It is simply confirming that the artifact contains the mechanisms to meet our objectives.

A. Methods, Requirements and Evaluation

1) Functional Requirements: The framework must support the following: Register Citizen / Trust Identity; One off authentication process and generate token/verifiable session; Discover services; Capture consent and evaluate policy to gain access to protected data; Standardised API request/response; Adapter for each department for legacy systems; Authorisation; Audit; Error / Status; Expandable to add new departments.

2) Non-Functional Requirements: The framework must satisfy the following: Security; Privacy; Scalability; Availability; Interoperability; Maintainability; Audit; Usability; Governance; Data ownership.

3) System Modelling: The federated data exchange principle is shown in Fig. 3.

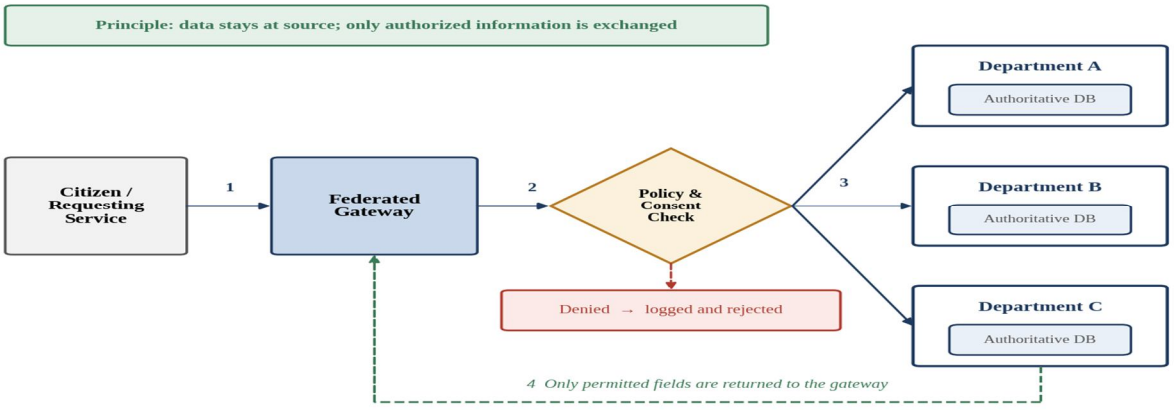


Fig. 3 Federated data exchange principle

B. Data and Trust Model

The model will ensure each aspect is owned by the correct party. The interoperability layer will not own the data of each department. Only the minimum amount of data will be stored to allow routing, evaluate policy, audit, or to have a unified citizen view. This will depend upon the governance policy.

C. Evaluation Criteria

The following criteria are used to evaluate the framework:

- Interoperability
- Unified identity
- Data exchange
- Security
- Privacy and consent
- Legacy integration
- Service integration
- Scalability
- Governance
- Citizen access

Each of these criteria will be checked. This is done by stating how the framework should behave and by providing a scenario. We will not make any claims about performance.

D. Ethics and Security

A Government Interoperability framework will handle data about citizens. The prototype will use synthetic or example data. This should not be seen as authorisation to access real government data. In a production environment there needs to be a formal process in place for legal, privacy, security, identity, data ownership, incident management, and audit.

IV. PROPOSED WORK

A. Layered Architecture

The proposed solution will have five logical layers to it. This will ensure that any changes made to one department will not require re-designing of the other departments. The architecture is shown in Fig. 4.

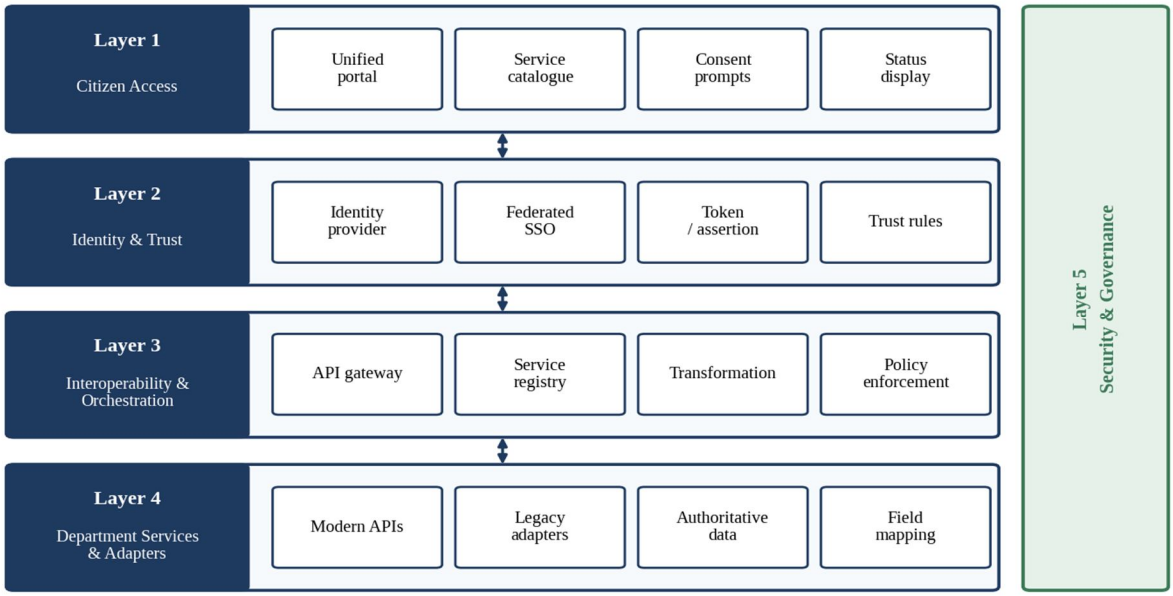


Fig. 4 Proposed federated interoperability architecture

1) *Layer 1 – Citizen Access:* This layer will provide a unified access point. It can show available services, authenticate the citizen, show consent, show service status, and responses from departments.
2) *Layer 2 – Identity and Trust:* This layer will manage the federated digital identity and trust. It can register citizens, authenticate them once through the trusted identity provider, issue and validate signed tokens or assertions, and manage the trust relationships between the departments and the identity provider.
3) *Layer 3 – Interoperability and Orchestration:* This layer will contain the API gateway, routing, service registry, transformation, validation, consent & policy, and orchestration. This layer will translate the request into a service specific request.
4) *Layer 4 – Department Services and Adapters:* Each department will still own their service and data. If a department has a modern service they can provide a standardised API. If a department has a legacy service then an adapter will be used to connect.
5) *Layer 5 – Security and Governance:* There will be aspects of security and governance throughout the architecture. The system will have authentication, authorisation, encryption, auditing, data minimisation, policy management, service ownership and data ownership. This will create a trusted federation.

B. Algorithms and Logic

Algorithm 1: Federated Service Access (inputs: citizen C and service S; output: response R or denied).

1. Receive service request from C.
2. If C has no valid federated session,
   authenticate C via the trusted identity provider.
3. Validate the identity assertion/token.
4. Determine the department/service owner.
5. Determine what data is needed and for what purpose.
6. If policy requires consent, ask for consent.
7. Evaluate authorisation and consent.
8. If denied by policy, log and return an error.
9. Create a standardised API request.
10. Send the request through the gateway to the
    department adapter/service.
11. Department validates the request and applies
    its business logic.
12. Return only the allowed parts of the response.
13. Log the event.
14. Return the response/status to C.

Algorithm 2: Consent and Authorisation.

```
def authorize(request):
    identity = validate_token(request.token)
    if identity is invalid:
        return DENY
    policy = load_policy(request.service,
                         request.data_fields)
    consent = load_consent(identity.subject,
                           request.service)
    if not policy.allows(identity, request.purpose):
        return DENY
    if policy.requires_consent and not consent.is_valid:
        return CONSENT_REQUIRED
    return ALLOW
```

C. Core Logic and Prototype

1) Core Logic: The core logic follows the principle of data minimisation. If a service is requesting data it shouldn't receive the full data of the citizen. The gateway will determine what data is needed for the service request and only request data that the department can release.

Example Code 1: Standard service request.

```
POST /federation/service-request
Authorization: Bearer <token>
Content-Type: application/json
{
  "service": "certificate-service",
  "purpose": "eligibility-verification",
  "citizen_id": "synthetic-user-001",
  "required_fields": ["name", "date_of_birth",
                      "address"]
}
```

2) Prototype / Proof of Concept: The proof of concept can be created using a light weight API service, example identity service, gateway/orchestrator, two or more example department services, consent service, and audit. The prototype should use synthetic data to prove the architecture works without using any real government data.

The prototype components are:

- Citizen Service - Request service and returns unified response.
- Identity Service - Validate example citizen and provide signed token.
- Gateway - Validate token, policy, route request, and log events.
- Consent Service - Store consent.
- Department A - Modern department service.
- Department B - Legacy service via adapter.
- Audit Service - Log authentication, consent, request, response, and deny.

Example Code 2: Prototype gateway logic.

```
from flask import Flask, request, jsonify
app = Flask(__name__)

@app.route("/service", methods=["POST"])
def service_request():
    token = request.headers.get("Authorization")
    if not validate_token(token):
        return jsonify({"error": "unauthorized"}), 401
    body = request.get_json()
    if not consent_allows(body["citizen_id"],
                          body["service"],
                          body["purpose"]):
        return jsonify({"error": "consent_required"}), 403
    result = route_to_department(body)
    audit(body, result)
    return jsonify(result)
```

[validate_token(), consent_allows(), route_to_department(), audit()] are functions to be used within the prototype.

D. Service Flow and Legacy Integration

1) Service Flow: The citizen requests a service, this will be authenticated. The framework will then evaluate policy and consent. The gateway will orchestrate the correct department services and will only request the allowed data. The result will be returned through the unified access layer. This flow is shown in Fig. 5.

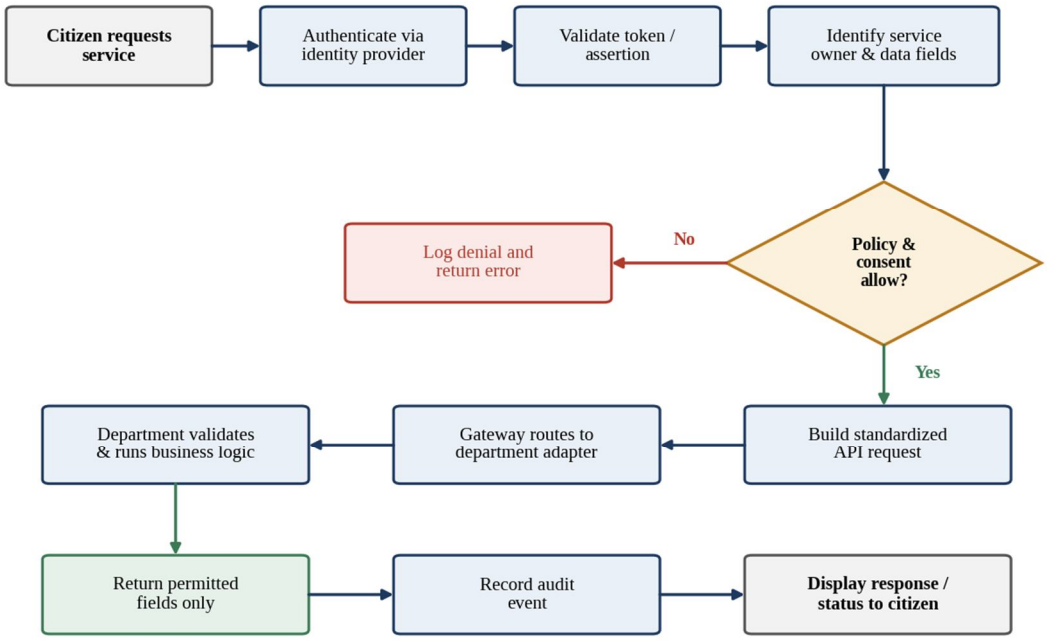


Fig. 5 Unified government service delivery

2) Authentication and Consent: This shows the necessity of having separate authentication, authorisation, and consent. It shows who is requesting, what they can do, and if they have given consent for any relevant data exchange. The sequence is shown in Fig. 6.

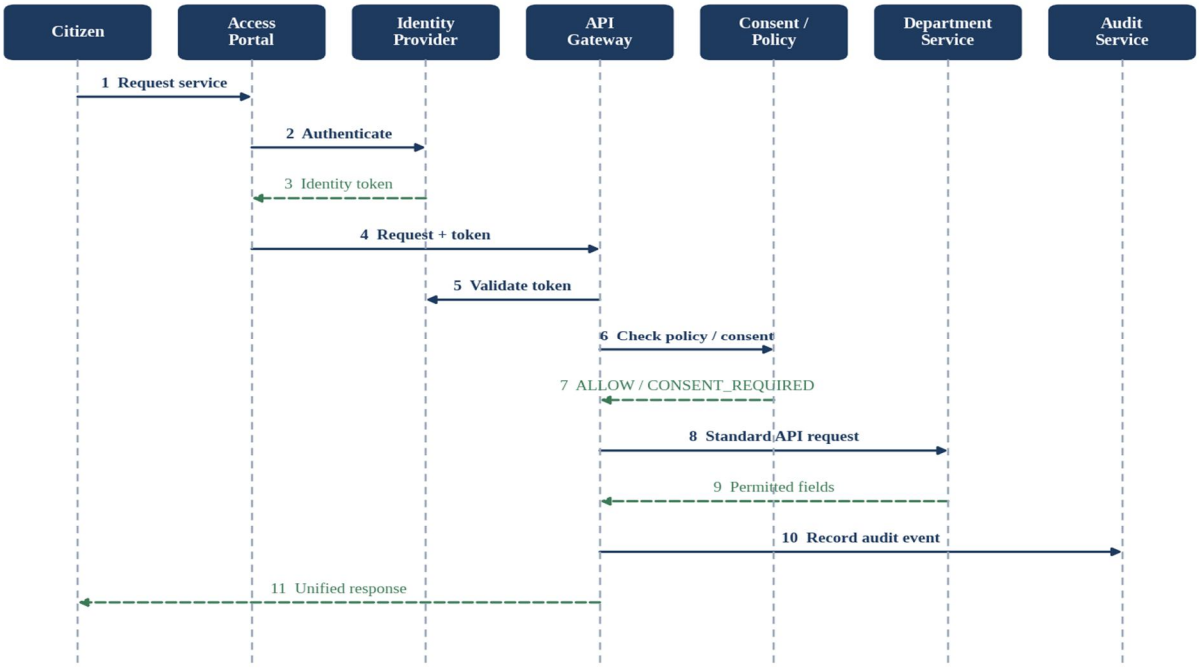


Fig. 6 Authentication, authorisation and consent sequence

3) Legacy Adapter Pattern: This will allow incremental modernisation. The department can start using the service via a wrapper. They can then update their internal service. Legacy details are encapsulated in the adapter. The pattern is shown in Fig. 7.

```
Standard Request
      |
      v
API Gateway
      |
      v
Legacy Adapter
      |
      +--> Field Mapping
      +--> Protocol Translation
      +--> Validation
      |
      v
Legacy Department Service
      |
      v
Normalized Response
      |
      v
Gateway --> Citizen

Key rule: the adapter isolates legacy-specific details
from the common interoperability contract.
```

Fig. 7 Legacy adapter pattern

V. RESULTS AND DISCUSSION

A. Evaluation Results

The proposed framework has been evaluated conceptually based on the main requirements identified during the literature review and our objectives. The framework has been evaluated to confirm that there is a clear method to meet each requirement. No live government system was deployed so we are providing results from the framework/prototype. The results are summarised in Table I.

TABLE I
EVALUATION SUMMARY OF THE PROPOSED FRAMEWORK

Sr.	Evaluation Parameter	Result / Observation	Outcome
1	Interoperability	Applications communicate using standardised APIs and protocols	Heterogeneous systems can be integrated
2	Unified digital identity	Multiple services accessed via a common authentication layer	Reduces re-registration and re-authentication
3	Data exchange	Standardised formats and controlled APIs	Minimises unnecessary duplication
4	Federated architecture	Departments keep their own databases and services	Provides autonomy
5	Security	Authentication, authorisation, encryption, access control and audit included	Provides secure exchange
6	Privacy and consent	Data accessed only for the service and policy	Provides controlled sharing
7	Legacy systems	Integrated via adapters/API gateway	Provides incremental modernisation
8	Service integration	Multiple services via one access point	Creates a more unified experience
9	Scalability	New departments added as independent nodes	Can be expanded incrementally
10	Governance	Policies, responsibilities and ownership can be defined	Improves coordination
11	Accessibility	Citizens use a common access point	Provides a consistent journey
12	Data ownership	Data owned by the origin department	Balances integration with ownership

B. Discussion

The results suggest that a federated approach can be used to provide an alternative to fully centralised government service integration. The main benefit of this architecture is that the service is being integrated but the data isn't being centralised. This means that departments can keep their own internal systems but expose some capabilities via a common interface.

Unified identity will help with the common problem of having to re-authenticate. However, federation will need a clear trust relationship, token validation, authorisation policy, and audit. Without a strong policy in place the common login will just move the vulnerability. The framework will help with reducing duplication by encouraging controlled reuse. Not every service will have access to every attribute of the citizen. The gateway and policy will determine what data is required and allowed for the service.

Security is a key aspect of the architecture. There are more potential communication pathways so authentication, authorisation, encryption, data minimisation, consent, logging, and policy will need to be considered. Scalability can be achieved conceptually by having modular integration. Any new department should be able to register their services, define their data, establish trust, and integrate via an adapter or standard API without needing to re-design all existing participants.

C. Overall Findings

This study suggests that the framework can conceptually overcome the main limitations identified in the literature. By using a federated architecture, unified identity, standardised API, secure data exchange, consent, and governance. This supports our working hypothesis at an architectural level. However, it does not show that the framework is statistically superior in a live government environment.

VI. FINDINGS AND SUGGESTIONS

A. Findings

- Government Interoperability is a socio technical issue.
- Federated architecture can provide autonomy for departments whilst allowing controlled integration between systems.
- Unified identity can help simplify access for citizens with trusted federation and policy.
- Standardised API & data need to be used to ensure predictable data exchange.
- Consent & authorisation should be considered before releasing protected data.
- Legacy systems can be integrated using adapters, allowing incremental modernisation.
- Governance should be in place to provide ownership, responsibilities, access, standards, audit, and accountability.
- Security should be considered in the interoperability architecture.
- Scalability can be better achieved via modular integration.
- This study is purely providing architectural/prototype based evidence.

B. Suggestions

- Use common API standards & data dictionary.
- Ensure that there is a government wide trust & identity federation policy in place prior to production.
- Use data minimisation & purpose limitation on all cross department requests.
- Create a formal onboarding process for services. This should include security, ownership, API contracts, testing & audit.
- Ensure there is an interoperability catalogue. This should provide details about available services, schemas, owners, and access conditions.
- Implement continuous security processes. This should include assessment, monitoring, incident management, and policy review.
- Pilot the framework using a small number of example services.
- In future empirical studies measure actual performance metrics. This should include response times, failure rates, duplicate submissions, user satisfaction, costs, and security events.

VII. CONCLUSION

Interoperability is an essential requirement for unified citizen focused digital government service delivery. Having individual departmental platforms can provide valuable digital services, however, will cause fragmented journeys, repeat authentication, duplicate data submission, and information silos. Throughout the literature review it has been shown that to be successful, there needs to be an architectural, semantic, organisational, security, and governance approach.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

The Federated Interoperability Framework will overcome this issue by having a common interoperability layer between citizens and independently managed government services. It includes federated identity, standardised API, service orchestration, controlled data exchange, consent, authorisation, security, legacy adapters, audit, and governance. The framework is based upon the principle that the integration doesn't require complete centralisation of the department's databases. This means that departments can keep ownership of authoritative data.

The prototype based evaluation suggests that the framework can provide the main requirements identified within the research objectives. It can provide unified access, controlled data exchange, incremental integration, and autonomy for departments. However, these are based upon concepts and are not showing any measurable reductions in processing time, cost, latency or effort for citizens.

The main contribution of this research is providing a coherent architecture. This can be tested in future by implementing with example government services. It can be tested for real performance, security, and citizen usability.

VIII. FUTURE SCOPE AND LIMITATIONS

A. *Future Scope*

The proposed framework can provide a basis for future implementation and empirical research. Firstly, a fully functioning prototype can be developed. This should include multiple example government services. This can include a real identity federation, API gateway, service registry, consent engine, policy engine, audit, and department adapters. Secure development practices should be followed.

Secondly, real or officially simulated government data standards can be integrated. Future work can include defining canonical data models, metadata, identifiers, schema validation, versioning, and semantic mapping. This will allow systems developed independently to exchange information.

Thirdly, the framework can be evaluated for security. Future studies can include threat modelling, penetration testing, token security analysis, API abuse testing, privacy risk assessment, and audit validation. Zero trust can also be investigated along with stronger policy based access.

Fourthly, the framework can be evaluated for performance. Researchers can measure API latency, throughput, service availability, recovery from failure, effort to onboard, reduce duplicate data, and infrastructure requirements. Controlled usability studies can also be performed to measure task completion, complexity, and citizen satisfaction.

Fifthly, intelligent service orchestration can be implemented. Future versions can include policy aware workflow engines to automatically determine what services & information are needed to complete a citizen process. This should be transparent & auditable.

Lastly, the framework can be expanded to include cross jurisdiction interoperability. This can include departments from multiple administrations. This will require trust, identity, policy, and data sharing agreements.

The framework can also be studied with emerging technologies. This should include privacy enhancing computation, federated learning, verifiable credentials, decentralised identifiers, and confidential computing. These should be evaluated based upon real governance & privacy requirements.

B. *Limitations*

There are a number of limitations to this study. Firstly, the framework is mainly architectural/prototype based and is not a production deployment.

Secondly, the evaluation is scenario based and qualitative. No statistically powered user study or controlled experiment was performed. Therefore, no claims can be made that there is a measurable improvement in citizen satisfaction, processing time, cost, latency, or admin effort.

Thirdly, service examples were used to demonstrate the concept of proof of concept. Real world government systems can have unknown limitations and bespoke systems which would require further engineering.

Fourthly, the security was described at an architectural and prototype level. In relation to production environments, a threat model would need to be formalised, testing would need to be done by a third party and key management processes, security processes, incident management, compliance checks and ongoing monitoring would need to be implemented.

Fifthly, interoperability requires legal and organisational agreements which cannot be fully verified with a technical prototype. Data ownership, consent, storage, accountability and responsibilities between departments would need to be set by the relevant authorities.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Finally, the framework does not specify any particular technology. This makes it easier to apply the concept to different systems however, there are still decisions to be made around what technologies will be used. This could include cloud architecture, messaging brokers, API management platforms, identity standards and database technologies.

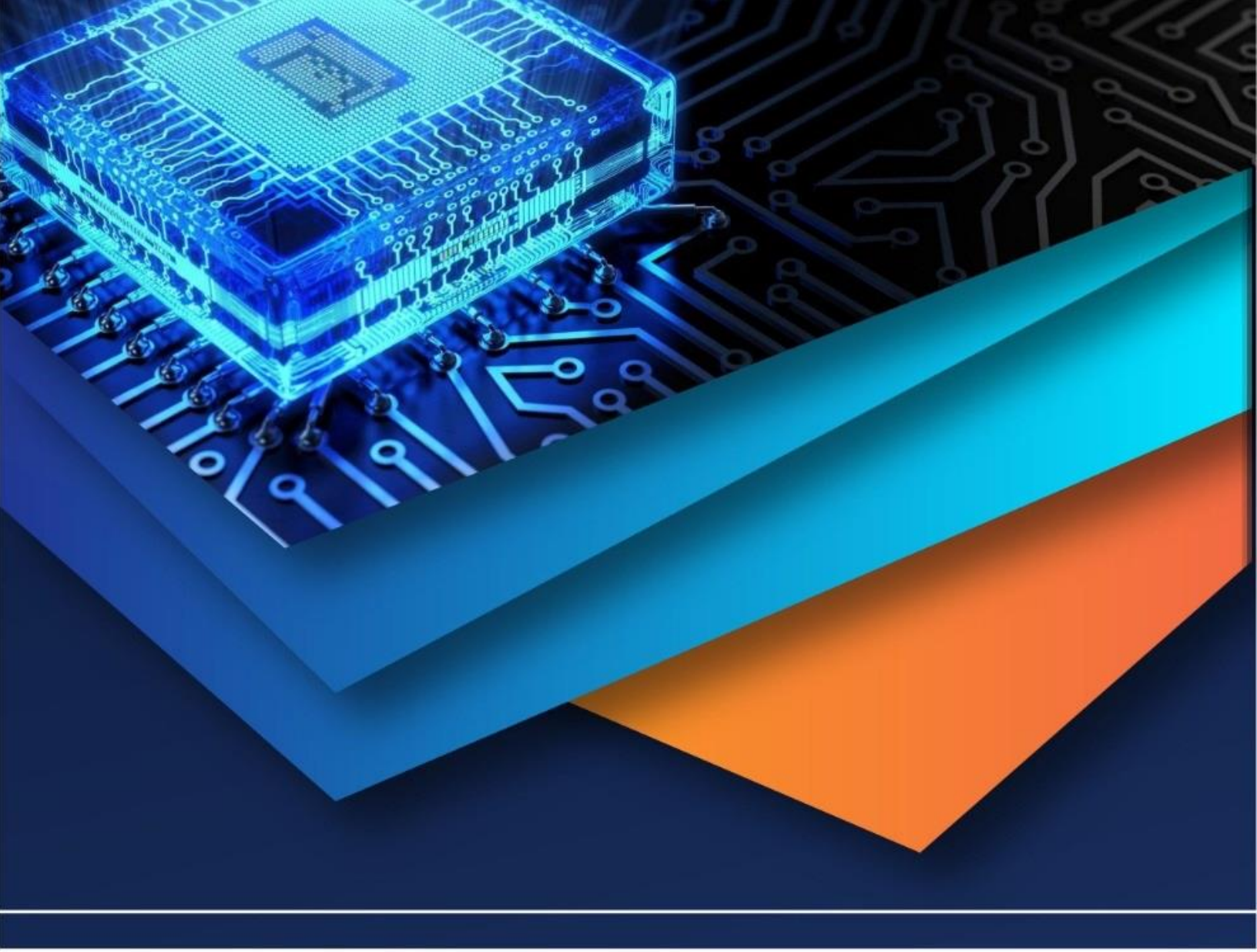
REFERENCES

[1] World Bank, "Interoperability: Towards a data-driven public sector," 2023, doi: 10.1596/38520.
[2] L. Guijarro, "Interoperability frameworks and enterprise architectures in e-government initiatives in Europe and the United States," Government Information Quarterly, vol. 24, pp. 89–101, 2006, doi: 10.1016/j.giq.2006.05.003.
[3] R. Klischewski, "E-government integration and interoperability: Framing the research agenda," International Journal of Public Administration, vol. 30, pp. 889–920, 2007, doi: 10.1080/01900690701402668.
[4] P. Gottschalk, "Maturity levels for interoperability in digital government," Government Information Quarterly, vol. 26, pp. 75–81, 2008, doi: 10.1016/j.giq.2008.03.003.
[5] H. Kubicek, R. Cimander, and H. Scholl, Organizational Interoperability in E-Government: Lessons from 77 European Good-Practice Cases. Springer, 2011, doi: 10.1007/978-3-642-22502-4.
[6] T. A. Pardo, T. Nam, and G. Burke, "E-government interoperability: Interaction of policy, management, and technology dimensions," Social Science Computer Review, vol. 30, pp. 7–23, 2012, doi: 10.1177/0894439310392184.
[7] V. Rao, "A framework for unified digital government: A case of India," Journal of E-Governance, vol. 36, pp. 35–55, 2013, doi: 10.3233/GOV-120329.
[8] M. Al-Husban and C. Adams, "Connected service delivery framework: Towards interoperable government," in Emerging Mobile and Web 2.0 Technologies for Connected E-Government, Z. Mahmood, Ed. Hershey, PA, USA: IGI Global, 2014, pp. 50–75, doi: 10.4018/978-1-4666-6082-3.ch003.
[9] G. Mecca, M. Santomauro, D. Santoro, and E. Veltri, "On federated single sign-on in e-government interoperability frameworks," International Journal of Electronic Governance, vol. 8, pp. 6–21, 2016, doi: 10.1504/ijeg.2016.076684.
[10] R. Krimmer, S. Dedović, C. Schmidt, and A.-A. Corici, "Developing cross-border e-governance: Exploring interoperability and cross-border integration," in Electronic Participation (ePart 2021), Lecture Notes in Computer Science, vol. 12849. Cham, Switzerland: Springer, 2021, pp. 107–124, doi: 10.1007/978-3-030-82824-0_9.
[11] S. Nadhamuni et al., "Driving digital transformation of comprehensive primary health services at scale in India: An enterprise architecture framework," BMJ Global Health, vol. 6, 2021, doi: 10.1136/bmjgh-2021-005242.
[12] B. Oumkaltoum, E. B. Omar, O. Aris, and C. Loqman, "Hybrid e-government framework based on data warehousing and MAS for data interoperability," International Journal of Advanced Computer Science and Applications, 2021, doi: 10.14569/ijacsa.2021.0121008.
[13] V. Kalogirou, A. Stasis, and Y. Charalabidis, "Adapting national interoperability frameworks beyond EIF 3.0: The case of Greece," in Proc. 13th Int. Conf. Theory and Practice of Electronic Governance, 2020, doi: 10.1145/3428502.3428536.
[14] V. Kalogirou, A. Stasis, and Y. Charalabidis, "Assessing and improving the national interoperability frameworks of European Union member states: The case of Greece," Government Information Quarterly, vol. 39, Art. no. 101716, 2022, doi: 10.1016/j.giq.2022.101716.
[15] A. Campmas, N. Iacob, and F. Simonelli, "How can interoperability stimulate the use of digital public services? An analysis of national interoperability frameworks and e-government in the European Union," Data & Policy, vol. 4, 2022, doi: 10.1017/dap.2022.11.
[16] A. Schmitz, A. Mondorf, and M. Wimmer, "Framework for designing interoperable public service architectures with exemplification along small-scale procurement and PEPPOL," in Proc. 23rd Annu. Int. Conf. Digital Government Research, 2022, doi: 10.1145/3543434.3543473.
[17] M. Alvarez-Rodriguez, V. Kalogirou, F. Chiarelli, A. Crahay, N. Custers, and E. Miscenà, "National and sub-national approaches towards the creation of an interoperability framework: The case of Spain," in Proc. 24th Annu. Int. Conf. Digital Government Research, 2023, doi: 10.1145/3598469.3598513.
[18] V. Malik et al., "Building a secure platform for digital governance interoperability and data exchange using blockchain and deep learning-based frameworks," IEEE Access, vol. 11, pp. 70110–70131, 2023, doi: 10.1109/access.2023.3293529.
[19] A. Xisto, F. Sommer, M. Costa, J. L. C. Da Silva, C. Cappelli, and V. Nunes, "Interoperability of digital government services: A Brazilian reference architecture model to promote communication, management, and reuse of solutions," in Electronic Government (EGOV 2022), Lecture Notes in Computer Science. Cham, Switzerland: Springer, 2022, pp. 91–107, doi: 10.1007/978-3-031-17604-3_6.
[20] Y. Y. Kibira, M. Mohsin, and D. Shao, "Services integration in Tanzania e-government systems," International Journal of Innovative Science and Research Technology, 2024, doi: 10.38124/ijisrt/ijisrt24mar1155.
[21] E. Sixpence and A. Vasconcelos, "E-government interoperability enterprise architecture: Systematic literature review," in Int. Conf. Information Systems Development, 2024, doi: 10.62036/isd.2024.46.
[22] A. Torab-Miandoab, T. Samad-Soltani, A. Jodati, F. Akbarzadeh, and P. Rezaei-Hachesu, "A unified component-based data-driven framework to support interoperability in the healthcare systems," Heliyon, vol. 10, 2024, doi: 10.1016/j.heliyon.2024.e35036.
[23] V. Figueroa, A. Santos-Olmo, D. Rosado, and E. Fernández-Medina, "Building a holistic cybersecurity framework for e-government based on a systematic analysis of proposals," International Journal of Information Security, vol. 24, 2025, doi: 10.1007/s10207-025-01024-0.
[24] A. Dudoit and T. Labillois, "Digital sovereignty and federalism: Data interoperability and AI governance," CIRANO, Montréal, QC, Canada, Rep. 2025PR-12, 2025, doi: 10.54932/dnan8237.
[25] M. Gupta, "A socio-technical big data analytics framework for digital government: Integrating data stewardship, interoperable infrastructure, and public value accountability in data-driven public administration," International Journal of Transformations in Business Management, 2025, doi: 10.37648/ijtbm.v15i01.009.
[26] X. Jia et al., "Federated services: A smart service ecology with federated security for aligned data supply and scenario-oriented demands," IEEE/CAA Journal of Automatica Sinica, vol. 12, pp. 925–936, 2025, doi: 10.1109/jas.2024.124860.
[27] M. Maharjan and S. Maharjan, "Interoperability service delivery architecture among ministries of Nepal," MVIC Journal of Management and Information Technology, 2025, doi: 10.3126/mvicjmit.v1i1.77312.
[28] B. Thela, I. Zlotnikova, M. Galani, and T. Sigwele, "Development of a service-oriented interoperability framework: The Botswana e-government system case study," Digital Government: Research and Practice, vol. 6, pp. 1–32, 2025, doi: 10.1145/3712706.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

[29] V. Figueroa, A. Santos-Olmo, D. G. Rosado, and E. Fernández-Medina, "Strengthening digital government: Integrating risk management, secure interoperability, and governance with the GAUCHO framework," IT Professional, vol. 28, pp. 99–105, 2026, doi: 10.1109/mitp.2026.3685436.
[30] A. Dudoit, "Interoperability of public sector data in Canada: Structuring intergovernmental capacity for sovereign action in service of citizens," 2026, doi: 10.54932/lqey7039.
[31] A. Yazdinejad and J. Kong, "Breaking interprovincial data silos: How federated learning can unlock Canada's public health potential," Royal Society Open Science, 2026, doi: 10.1098/rsos.250959.
[32] H. Tomlinson et al., "The FAIR case for a coherent interoperability to support NHS 10 year health plan," Scientific Data, vol. 13, 2026, doi: 10.1038/s41597-026-07858-0.
[33] Z. Zheng, "Optimization and effectiveness evaluation of digital empowerment for collaborative governance of grassroots public services," Advanced Electromagnetics, 2026, doi: 10.7716/aem.v15i3.3882.
[34] M. Thirasakthana and S. Kiattisin, "Sustainable government enterprise architecture framework," Sustainability, 2021, doi: 10.3390/su13020879.
[35] M. Wimmer, R. Boneva, and D. Di Giacomo, "Interoperability governance: A definition and insights from case studies in Europe," in Proc. 19th Annu. Int. Conf. Digital Government Research, 2018, doi: 10.1145/3209281.3209306.
[36] H. K. Ronoh, K. Omieno, and S. Mutua, "An interoperability framework for e-government heterogeneous information systems," IJARCCE, 2018, doi: 10.17148/ijarcce.2018.71025.
[37] A. Schmitz and M. A. Wimmer, "Framework for interoperable service architecture development," Government Information Quarterly, Art. no. 101869, 2023, doi: 10.1016/j.giq.2023.101869.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)