6.1 INTRODUCTION

Interoperability in enterprise application integration among various business processes is an essential quality for all seamless integration between them and architectural model based system is observed as the most predominant way for achieving interoperable solutions. (Alberti, A.M. et al, 2013; Rezaei, R. et al 2014). The effectiveness of the proposed architectural model is analyzed by various parameters qualitatively and quantitatively. Evaluation parameter is one kind of calculating efficiency measure obtained in the proposed architecture model implementation. One of the techniques which best suites is applying the architectural model on the case study to get quantitative measures of the system. The case study selected is certificate verification system among various heterogeneous systems which possess their own structure and language. An experiment is designed for obtaining interoperability service measure among various heterogeneous sources by requesting the interoperability request in the form of data, service and process levels. It is computed by using the impact of interoperability ratio in various levels and the request should be tested under four different aspects such as no interoperability, min interoperability, average interoperability and maximum interoperability. Based on the case study approach, the execution of various categories of interoperability is evaluated and results are presented.
6.2 APPLYING THE AMSI – CASE STUDY APPROACH

Various approaches are available (Zhiying, T. et al, 2016; Autili, M. et al, 2014; Badr, Y. et al, 2011) in which they help to integrate various business process in the system and achieves interoperability for the intended request. Various interoperability approaches exists in the researches such as unified, integrated, federated and model driven are carried out in the various scenarios and dependent requirements (MacLennan, E. et al, 2013; Woo, J. et al, 2012). Integrated approach uses static and standardized format for connecting business process. Unified approach uses mapping of enterprise systems using Meta model. Whereas model driven approach is based on the translation model that suits only for the specific applications. Federated approach is mainly done based on dynamic and on the fly specific requirements between the business processes. (Tauber, A. et al, 2012, Zhiying, T. et al, 2016). Based on the above approaches it is observed that in all the above approaches the interoperability levels is carried out depending on their specific requirements levels such as data, service, process and business between the heterogeneous sources. No approaches can combine all those levels of interoperability requirements in a single model or approach that suits different kind of requirements.

Case study based approach is an efficient way of implementing interoperability among heterogeneous domains are found to be executed. It brings the interoperability process among the domain in abstract using the four categories. So the proposed architectural model for service interoperability is proved by using a case study and the results were discussed. The proposed architectural model has been verified for the functional aspects by using the CPN (Barker, A. et al, 2009; Bi, J. et al, 2016) for the effectiveness of interoperability between heterogeneous domains by
using AMSI to deliver the best outcome on certificate verification case study. The remaining of this chapter gives the abstraction of case study, object oriented modelling of proposed case by using architectural model for service interoperability (AMSI) followed by conducting experiments.

6.3 CASE STUDY - OVERVIEW

Interoperability acts as one of the important factors in enterprise application integration in which sharing of information among various business processes is more advantages than other methodologies. Issues occur in many ways when sharing of resources among business processes but the motives on this are ease of use, seamless, shared understanding and error free services. Various aspects present in communication between heterogeneous domains lead to data, service and process perspectives that will lead to have high potential over business processes and promotes interoperable integration. Certificate verification is the integration of various heterogeneous sources which provides different business processes to communicate with each other seamlessly and effectively which leads to new improvements and innovations in businesses.

6.3.1 Overview of Certificate Verification System

Recent developments in the business processes in EAI indicate that there is always demand for information integration among the systems. (Garcia, E. G. et al, 2015; Issarny, V. et al, 2011). One of the scenarios is certificate verification system in which the credentials details from one system are verified with two or more systems automatically by invoking request-response services. The verification system shows the significance due to number of heterogeneous organization growing nowadays with various standards and specification. Currently in certificate
verification system, two kinds of methodologies adopted for verifying the particulars. One is Manual verification invoked by the organization itself and other one is rendering to the thirty party verification in which it also done manually by contacting person, communicating through mail etc.

The demand for certificate verification increased nowadays because, for example: one in ten candidates in India provides false data about their education to the employer. (Jennings, B. et al 2015; Ismail, B.I. et al, 2016). To speed up this process and increase efficiency in this type of system, establishing communication and information sharing among the various heterogeneous systems is needed. For Example an employee providing his details to the employer, Let us take academic credentials in which the candidate pursued his high school, higher secondary and graduation in different education system need to be verified automatically by invoking a request from the employer domain. Consider each education system having different structure, language, database schema, standards, specifications and security policies. To establish communication between various heterogeneous data sources there needs interoperability model to integrate the business processes in smooth manner without any manual intervention.

Decisions should be taken based on the required verification process and resolves interoperability in the required levels such as data, service and process levels in enterprise application integration and ensures the usability and integrability of the heterogeneous data sources. By integrating this system, the certificate verification process offered to third party system was done on individual enterprise system automatically by invoking an architectural model among various heterogeneous systems. In terms of organization, their experience should be
Seamless - Get connected without any third party system anywhere, anytime and in any format.

Scalable - More number of requests can be invoked at a time to different entities.

Performance - Automated system by invoking simultaneous request instead of manual system.

Interchange ability - Ability to interchange the required format.

Various studies that has been carried out on certificate verification system are analysed and the major principles have been classified as

- Data sources integration among heterogeneous databases
- Ease of use and Personalization
- Efficiency of results
- Handling interoperability in the perspective of data, service and process levels.
- Being anywhere and everywhere.

Integration and Interoperability are the core aspects of connecting the heterogeneous data sources without any incompatibilities. To achieve the complete interoperability among information systems, it is essential to categorize the interoperability levels into data, service and process perspective. Interoperability plays a major role in connecting heterogeneous information systems because too many sources interact to request and response and meet the expected result. Changing needs of business requirements in information sources defined the need for a generic solution that leads to an architectural model for interoperability in the form of service. The change in
business requirements that has to be concentrated dynamically is (Iyanov, C. et al, 2016)

- Dynamic change in integration platform
- Request Response Analysis
- Categorization of interoperability levels
- Optimization of results

Enterprises experience the various data and information sources are integrated and interoperated on changing requirements in business processes. These requirements lead to complete structuring of the business requirement with respect to the organization and are needed for a developing a model for interoperable using service that gives seamless experience and improve the efficiency of the system.

6.3.2 Verification System for Enterprise systems

On analyzing the importance of certificate verification in a domain (For example: Joining a company, Joining new course) it has been found that its reach is yet to be experienced by the domain. The Proposed architecture model for interoperability implemented is a verification system for certificate by integrating various domain preferences and dynamic service needed. The Request given by the Domain (A) to match credentials [Say Format A] will send a request to corresponding domains (B and C) having credentials in [Say Format B and C Respectively]. This data incompatibility creates issues even though data provided are accurate. Other than the data request, the service and process request also invoked for interoperability and executed based on requirements. Using the architectural model the certificate verification systems, requirements are implemented and evaluated using parameters such as openness, autonomy, serviceability, availability, scalability, generality and

6.4 DESIGN OF CERTIFICATE VERIFICATION SYSTEM USING OBJECT ORIENTED MODELLING

To design a software system in an efficient way object oriented modelling concepts are the most preferred way to implement it. (Reed, L. et al, 2011; Venkatesan, V.P., et al, 2008; Arul doss, M., et al, 2015; Madhusudanan, J., et al, 2014; Punithadevi, C., et al, 2015). Object oriented modelling analyzes the system based on the requirements from the developer’s perspective. When comparing to other methods such as procedural and structural methods, the design using object oriented modelling has more benefits. It provides improved software development and ease of maintenance.

6.4.1 Use Case Modelling for the Certificate Verification System

The essential users of the certificate verification systems are user candidate, employer, AMSI administrator and domain administrator in which verification should be done. Figure 6.1 represents the use case diagram of the certificate verification system.
When the user candidate submits the credential details of a particular degree, the verification information details are framed as request for interoperable service by the employer and are given to AMSI administrator which in turn communicates with the particular domain.

The requested domain responds to the query generated in the perspective of data, service and process levels and resolves interoperability issues based on generic specification provided by the mediator and choreographed to give the response as interoperable service. Hence AMSI is applied among the various heterogeneous domains.

Figure 6.1: Use Case diagram of the Certificate Verification System
systems which in turn help the domain to integrate and interoperate the business processes among them to deliver better and error free communication in the form of services.

6.4.2 Object oriented design for Certificate Verification System using AMSI

The use case diagram represented above indicates the requirements of the system with respect to the user and domain involved in it. The associated representation of certificate verification system on applying the architectural model for service interoperability is shown by using a class diagram. The design of architectural model for certificate verification system is depicted in the class diagram as shown in the Figure 6.2. The objective and characteristics of the individual components of the system are discussed below.

User Information

Carryout Information: Entity which is used to enter the credential details of a user in the system invoked by the employer domain.

- Carryout function() - To initialize the Certificate Verification Process
- To format () – Returns the service specification format mentioned in ontology knowledge for the given data.

Functional Activity: It is defined as the work flow mechanism involved in the user interface.

- AddData (Credential information) – Adds the individual information provided by the user to the database.
- SaveData ( ) - Saves the information credential of the user with respect to specification of the domain.
- Request Invoke (Saved format state) – It provides the reference format for the handling object and the user interface mechanism.

- OnCreateOptions Category (Level) – It specifies the level of interoperability to be achieved to the action bar if it is present.

- OnEnter (view, code of verification, event) – Performs various operation depends upon the event on submitting the key.

- OnClick(process) - Performs desired functions on mouse click

**Response Activity:** It is responsible for providing interoperable service by resolving incompatibilities over heterogeneous business processes.

- Request Invoke (Saved format state) – It provides the reference format for the handling object and the user interface mechanism.

- OnCreateOptions Category (Level) – It specifies the level of interoperability to be achieved to the action bar if it is present.

- OnEnter (view, code of verification, event) – Performs various operation depends upon the event on submitting the key.

- OnClick (view) - Performs necessary operation on mouse click.

**Certificate Verification Service:** It is a request response service used to communicate with the corresponding server in which where it is located.

- CertificateVerificationService () – It is a constructor and invoker for the desired certificate request to be obtained from the heterogeneous domain.

- OnComplete () – Used to perform action when the service request process ends.
- `isNetworkStatus()` – Check whether the network connectivity between the various domain sources is established.

- `SendData()` – sends the verification list with respect to domain knowledge to the corresponding server and gets the response.

- `ResponseNotification()` – Used to notify the response when returned.

- `OnCompose()` – Compose the service with the required intent.

- `OnResponseEvent(Intent)` – Used to perform by calling `SendData()` method and provides response.

- `ConvertDataStream to Service (input data)` – Used to convert the given input data into service.
Figure 6.2 Class diagram of Certificate Verification System on applying AMSI
Request for Interoperable Service

Certificate Verification Request Handler: It is responsible for understanding the request by obtaining the required credential information and is analyzed with what kind of interoperability to be verified with relevance to the certificate by communicating a particular domain using the following methods.

- Get request details() method is used to retrieve the credential details of the particular user for verification.
- Decompose request () method is used to splitting request into set of associated business processes for communicating heterogeneous domains for verification.
- Align request () method is used to collect and organize the certificate verification details that to be retrieved and verified with the request domain sources.

Certificate Verification Data Request Handler: The request is processed as data level interoperable request between the various domain sources.

- Get data interoperability service request () method is used to align data formats with respect to the requested and response domains.
- Decompose data request () methods is used to split data with respect to the requesting domain as data interoperability services.

Certificate Verification Service Request Handler: The verification request depends on the service to match the credentials of the user as interoperable service request.

- Get service interoperability request context () method is used to align the requested service with respect to match with the credentials.
- Decompose service request () method is used to split the required request as input/output services such as name conversion, data conversion, etc.

**Certificate Verification Process Request Handler:** The verification request is analyzed and identified as it needs appropriate process in the form of service to meet interoperability between the domains.

- Get process interoperability request service () method is used to align the several requirements with appropriate information with needed process.
- Decompose process request () method is used to split the process if required.
- Collect request () method is used to align the process with respect to the requirements by satisfying access policies.

**Certificate Verification Domain Analyzer**

The input request for interoperable service for verifying the credential details given by the user is to be analyzed by the appropriate information such as context, physical structure, operating platform, language, syntax and semantics etc.

- getDomain request service () method is used to analyze the request in which the requested service is present in which domain and kind of policies adopted.
- decomposeDomain request () method is responsible for analyzing the request service having solutions from various domain and invoke to obtain the solution.
- composeDomain request () method is used to align and structure the services from heterogeneous domains matching with the mediator policies.
**Acquisition of Interoperable Service**

**Certificate Verification Interoperability Service Request Handler**: The required interoperability request service received from the request handler with the data pertaining to the verification of certificate is identified and the corresponding request handler is invoked associated with various data sources.

- Get information request () method is used to retrieve the certificate verification details from the request builder and associated information.
- Identify the request () method is responsible to check the type of interoperable request for a particular certificate which falls under data, service or process.

**Certificate Verification Interoperability Service Manager**: The interoperability service manager is responsible for facilitating and managing the data retrieval from invoking certificate verification request domain and invoking corresponding request.

- Get required service request () method is responsible for retrieving the certificate credentials from the domain analyzer as service and given to interoperability service request handler.
- Set access rights() method is responsible for aligning and structuring the certificate request service policies with the matching domain business policies.

**Certificate Verification Interoperability Service Selection Policy Manager**: The verification request invoked from the certificate credential submitted domain has to be communicated to various heterogeneous domains, the policy associated with each domain service is to be structured to match other service policies.

- Formulate policy service () method to formulate the various service policies with respect to the request invoking domain and sources.
• Update service () method to add upgraded business policies of an enterprise system time to time.

Modelling for Interoperability Service

Certificate Verification Mediator Modeller: It is a component to understand the structure and organize the certificate verification request data into information services according to the mediator specification.

• Transform interoperability service() method to add mediator specification and business policies to convert the service from different data sources into interoperable service.

• Organize interoperability service() method to structure the certificate verification request whether it should be needed, what kind of interoperability along with business policies.

Certificate Verification Mediator Builder: To organize the various requested domain information pertaining to service policies and wrapped according to mediator specification.

• Build wrapper service () method used to create the wrapper interface for meeting the requirements of certificate verification.

• Set access () method is used to assign the access policies according to various domain verification system.

• Wrapper service operation() method is responsible for making reachable operation/services among the certificate verification domain and invoking enterprise with respect to incompatibility over interoperability request.
**Certificate Verification Mediator Selection Policy Manager:** To incorporate service policies among the services selected.

- Certificate Verification Mediator Ownership () method that assign the service policy and ownership details.
- Verify access rights () method is used to check the verification service obtained from the corresponding domain to match with the mediator rights.
- Get service scope () method is used to get the scope of the mediator information service.

**Choreography of interoperability services**

**Certificate Verification interoperability Choreography Manager:** These are the composition engines which compose all the wrapper services which have the credentials details of the user from different heterogeneous domains.

- ComposeServices () is used to compose two or more interoperable services.
- Check services () method is used to verify all the levels of interoperability aspects is used for enterprise application integration.

**Certificate Verification Strategy Selector:** To uphold the context of the requested and response domains.

- Identify context request () method to obtain the context of the certificate verification information.
- Generate strategy () method to formulate the integrated information to achieve interoperability between the desired strategy.

**Certificate Verification Context Manager:** To create a context with respect to the request initiated between the heterogeneous sources.
• Create context request () method is responsible for obtaining the context happening among the request response services.

• Get Access Policy () method is used to assign the access policy with respect to the context.

**Build response**

*Certificate Verification Response Builder:* It is a method responsible for organizing the received response from the various sources with respect to the certificate verification domain and to produce interoperability services as per requirements in the form of service.

• Collect response () method is used to collect the response with adherence to request.

• Produce response () method is used to produce the response as generic interoperability service to the non interoperable domains.

**6.4.3 Sequence diagram for the Certificate Verification System using AMSI**

The sequence diagram as shown below is used to represent the process flows between the various layers of AMSI. It is divided and shown in three levels due to clear presentation and working of the diagrams.

Level 1 defines the handling of request from the invoking domain as request for interoperable service and the choreography part of the various services requested from the heterogeneous domains. The starting part of the level is handling of request, the choreography of services received with respect to the context are brought out in the Figure 6.3.
Level 2 is the continuation process of Level 1. It is a mediator process which acts between the service request and service selection layer to formulate the request and are confined to the requirements are shown in the Figure 6.4. It identifies the particular domain in which the request for interoperability process sequences and wrapping of acquired information according to the generic specification are exhibited here.

Level 3 provides interactions between the layer related to the retrieval of required interoperable request handler and corresponding mediator management for the integration for providing efficient interoperability. The request is then passed to the service manager in order to continue the corresponding request handler by the component interoperability service request handler. It categorizes the query formulation with respect to domain into three perspectives such as data, service and process and is retrieved from the corresponding domain, required ontology, policies and service registry.
Figure 6.3: Representation of Sequence diagram for Certificate Verification - Level 1
Figure 6.4: Representation of Sequence diagram for Certificate Verification - Level 2
Figure 6.5: Representation of Sequence diagram for Certificate Verification - Level 3
6.5 EXPERIMENTATION

Demonstrating the impact of interoperability in business processes in enterprise application integration, experimental analysis is done on certificate verification system in which the interoperation among the heterogeneous organization is handled in three perspectives such as data, service and process levels. The mechanism should be based on adopting the importance of interoperability in various levels which resolves the incompatibilities. By analysing these perspectives in the existing systems (Section 2.4), the interoperability among systems using service based was also examined. To bring out the extent of interoperability satisfied in various levels, should achieved in the existing frameworks and models, their processes and mechanisms are examined. Existing models and frameworks considered here discussed about the process involved, levels in which interoperability is achieved with respect to the requirements are shown in the table 2.3.

The DSIS framework proposed by (Pang, L.Y. et al, 2015) corresponds to solving interoperability in data level aspects. It acts as a middleware between data requestors and domain sources. It is mainly used for managing data, extracting information from different data sources and standardization by ensuring data consistency and accuracy in single enterprise information systems. Likewise the Athena interoperability framework (AIF) proposed by (Woo, J. et al, 2012) was mainly used to provide mapping function for data interoperability between sources based on data description, syntax, semantics and standardization based on web service. The other frameworks such as SIF, CMS (Rezaei, R et al., 2014; Tauber, A et al., 2012) mainly concentrates on modelling of process with respect to the individual requirements and are aligned. Hence it is resolved by adopting semantic web services and ontology based systems are used to resolve the heterogeneity issues.
TAHI, GWISC, WSMF (Wu Li et al, 2011; Polzonetti, A. et al, 2011; Ali Khan, W. et al, 2013) is a reference model which involves interoperability by concerning identification, registering, composition and execution of various applications which are developed independently.

From the existing works, interoperability among business processes for achieving integration should satisfy the incompatibilities in various perspectives such as data, service and process levels. The existing models operate on this levels individually based on the needs which suits to the specific application. The interoperability strategies adopted in those frameworks and models are based on their own requirements and it was specific to the application as mentioned earlier. At the earliest stage it was established between the data sources within an enterprise and later established over heterogeneous organizations. From the various interoperability models and frameworks it was identified that the service level and process level interoperable communication over the enterprise information system was also done between the request response entities but not in generic approach.

The advent of various business process sources like database structure, data sources, knowledge sources, internetwork, etc initiated various business enterprises to involve them to gain better insight towards interoperability in enterprise application integration. Hence the process towards next step involves a generic model for interoperability using services to communicate to external heterogeneous sources with the sources specified in invoking enterprise domain. Hence to experiment, the various categories of interoperability in EAI could be classified in four categories namely:

- **Category 1**: No Interoperability i.e., Integration of information not needed from external sources.
• **Category 2**: Minimum Interoperability i.e., Integration of information between heterogeneous sources in data level.

• **Category 3**: Average Interoperability i.e., Category 2 along with standard format conversion sources.

• **Category 4**: Maximum Interoperability i.e., Inter enterprise integration of information with dynamic invoking of any required process along with category 2 and category 3.

Hence the service based architectural model for interoperability works well when compared with existing frameworks and models reviewed and represented in Table 2.2 and Table 2.3 in chapter two helps to categorize interoperability in EAI under the above mentioned logic.

**Table 6.1: Interoperability categories achieved in Existing frameworks and models**

<table>
<thead>
<tr>
<th>Existing Interoperability Models and Frameworks</th>
<th>No Interoperability</th>
<th>Data</th>
<th>Data, Service</th>
<th>Data, Service &amp; Process</th>
<th>Category Identified</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCA (Lewis, M.J, et al., 2005)</td>
<td>√</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>Category 1</td>
</tr>
<tr>
<td>ATF(Khan, W.A et al., 2012)</td>
<td>√</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>XML-DIUE(Asanka, W et al, 2015)</td>
<td>√</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>STARLINK(Bromberg, Y.D et al., 2011)</td>
<td>√</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>IDEAS (Chen, J et al., 2008)</td>
<td>√</td>
<td>√</td>
<td>--</td>
<td>--</td>
<td>CATEGORY 2</td>
</tr>
<tr>
<td>Model Driven(Paul, G et al, 2014)</td>
<td>√</td>
<td>√</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>Service Based</td>
<td>√</td>
<td>√</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------</td>
<td>-------------------------------------</td>
<td>-------------------------------</td>
<td>---------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>3</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>4</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
</tbody>
</table>

-- Not Handed  √ INDICATES Handling of Interoperability Level  √- Specific- Applied to specific requirements
6.5.1 Experimental Discussion

Conducting experiments in research is an efficient way of implementation in which the researcher operates the proposed objective in multiple perspectives and controls if any changes happen. Usually to prove the fact, experiments are conducted. When implementing the experiment there are various perspectives and aspects to be identified and utilized in the environment. To carry out the experiment in proper manner planning and design according to that in well advance make the system proper and the outputs are utilized in the real time environment in a useful way. The main purpose of implementing the experiment towards certificate verification demonstrates the various interoperability levels in the proposed architectural model. By using the sample data sets, the experiment has been demonstrated and the results are obtained.

Interoperability Categories in Enterprise application integration

As discussed earlier, the interoperability among various business processes has been done in four categories: Category 1, Category 2, Category 3 and Category 4.

The experimentation has been carried out to the effect of the interoperability done by the proposed architectural model. In the following case study, the categories of interoperability carried out are

- CATEGORY 1 : No Interoperability
- CATEGORY 2 : Minimum Interoperability with Data interoperation
- CATEGORY 3 : Average Interoperability with Data and Service interoperation
- CATEGORY 4 : Maximum Interoperability with Data, Service and Process interoperation
These types of interoperation among various business processes in enterprise application integration provide us the effect of efficient and error free communication between the various enterprise information systems.

**Query Statement Types**

In order to evaluate the experiment, based on the request invoked by the user, the appropriate query statements were generated. Effectiveness and seamlessness of interoperability should be carried out by bringing the various categories of interoperability. Based on the categories the candidate user request invoked from one heterogeneous domain has been formulated in the below four types: Query Type 1, Query Type 2, Query Type 3 and Query Type 4.

- Query Type 1 query is responsible for invoking a request to get the user credential verification details.
- Query Type 2 query is responsible for invoking a request to get specified user credential verification details along with data interoperation involved in it.
- Query Type 3 query is responsible for invoking a request to get specified user credential verification details along with data and service (Eg: Format change) interoperation wherever required.
- Query Type 4 query is responsible for invoking a request to get specified user credential verification details along with data, service and required process (Eg: Translation of request) interoperation.

For example, the queries designed for execution of satisfying the categories of interoperability from various heterogeneous sources mentioned here as
**Query Type 1:** SELECT * FROM Table WHERE Entity1 =?

**Query Type 2:** SELECT * FROM Table WHERE Entity 1 =? AND Entity 2 =?

**Query Type 3:** SELECT * FROM Table WHERE Entity 1 =? AND Entity 2 =? AND Entity 3=?

**Query Type 4:** SELECT * FROM Table WHERE Entity 1 =? AND Entity 2 =? AND Entity 3 =? AND Entity 4 =?

The above query types represent the various service request invoked for different categories of interoperability by using certificate verification system among heterogeneous database sources. To discuss the above queries in the perspective of how many of user request and number of queries are generated, minimized approach is needed to ensure the various categories of interoperability as stated by the authors (Rezaei, R. et al, 2013; Spalazzese, R. et al, 2017). The structure of the experimentation setup is designed with twenty users mark credentials obtained by them in High school level and Pre-University level from four different states and one University level in which each having their own database structure, data format, database language, request response protocol etc. Usually the request for obtaining information from heterogeneous domains, the users has to pose four query statement types such as Query Type 1, Query Type 2, Query Type 3 and Query Type 4 and implemented with four interoperability categories of interoperability levels such as Category A, Category B, Category C and Category D.

The candidate details are stored in their corresponding boards such as High school level, Pre-University level, University level and other related domain sources are formulated with data sets and enable the query types to implement the interoperability in the categories represented above. To execute the above presented
four query types, consider 50 candidate user requests invoked as request for interoperable service, based on the four query types 200 cases are obtained. Next the 200 query cases are applied with respect to the categories of interoperability results in 800 case scenarios. By using the data sources collected from various domains, the certificate verification process is experimented with sample inputs.

The data elements present in the various heterogeneous domain sources presented with explanation of each fields specifying sample data, results and discussions are presented in Annexure A and B respectively.

### 6.6 IMPLEMENTATION AND DISCUSSION

Applying AMSI (Architectural model for service interoperability) on the verification system for a particular user certificate data should be retrieved, modelled, choreographed and implemented as response by using the experimental mechanism as mentioned above. For example: In this case study, three education related domains are taken such as High school level, Pre-University level from four different states (TamilNadu, Kerala, Gujarat and Delhi) in which each state having different kind of structure and policies in storing and retrieving the profile credentials of the user and UG domain with respect to particular university system. The certificate verification process request is invoked with the following particulars such as, register number, name, certificate number, marks obtained and year of passing etc. The request initiated by the candidate user is generated as four query types with the category levels of interoperability. The model query type and the related results are presented in Table 6.2 and Table 6.3. The detailed results and their calculations are shown in Appendix B.
Table 6.2: Model Queries for Query Statement types

<table>
<thead>
<tr>
<th>Query Type</th>
<th>Query</th>
</tr>
</thead>
<tbody>
<tr>
<td>QUERY TYPE 1</td>
<td>SELECT * FROM Table WHERE Entity1 = ?</td>
</tr>
<tr>
<td>QUERY TYPE 2</td>
<td>SELECT * FROM Table WHERE Entity 1 =? AND Entity 2 =?</td>
</tr>
<tr>
<td>QUERY TYPE 3</td>
<td>SELECT * FROM Table WHERE Entity 1 =? AND Entity 2 =?</td>
</tr>
<tr>
<td>QUERY TYPE 4</td>
<td>SELECT * FROM Table WHERE Entity 1 =? AND Entity 2 =? AND Entity 3 =?</td>
</tr>
<tr>
<td></td>
<td>AND Entity 4 =?</td>
</tr>
</tbody>
</table>

Table 6.3: Sample Results for four categories of Interoperability Service

<table>
<thead>
<tr>
<th>Query Type</th>
<th>CATEGORY A</th>
<th>CATEGORY B</th>
<th>CATEGORY C</th>
<th>CATEGORY D</th>
</tr>
</thead>
<tbody>
<tr>
<td>QUERY TYPE 1</td>
<td>{Reg No=445871, Name=Shafana, Category=BCM, Service=Yes}</td>
<td>{Reg No=445871, Name=Shafana, Category=BCM, Service=No}</td>
<td>{Reg No=445871, Name=Shafana, Category=BCM, Service=No}</td>
<td>{Reg No=445871, Name=Shafana, Category=BCM, Service=No}</td>
</tr>
<tr>
<td>QUERY TYPE 2</td>
<td>{Reg No=445871, Name=Shafana, Category=BCM, Service=Yes}</td>
<td>{Reg No=445871, Name=Shafana, Category=BCM, Service=Yes}</td>
<td>{Reg No=445871, Name=Shafana, Category=BCM, Service=Yes}</td>
<td>{Reg No=445871, Name=Shafana, Category=BCM, Service=No}</td>
</tr>
<tr>
<td>QUERY TYPE 3</td>
<td>{Reg No=445871, Name=Shafana, Category=BCM, Service=Yes}</td>
<td>{Reg No=445871, Name=Shafana, Category=BCM, Service=Yes}</td>
<td>{Reg No=445871, Name=Shafana, Category=BCM, Service=Yes}</td>
<td>{Reg No=445871, Name=Shafana, Category=BCM, Service=No}</td>
</tr>
<tr>
<td>QUERY TYPE 4</td>
<td>{Reg No=445871, Name=Shafana, Category=BCM, Service=Yes}</td>
<td>{Reg No=445871, Name=Shafana, Category=BCM, Service=Yes}</td>
<td>{Reg No=445871, Name=Shafana, Category=BCM, Service=Yes}</td>
<td>{Reg No=445871, Name=Shafana, Category=BCM, Service=Yes}</td>
</tr>
</tbody>
</table>
To find the effectiveness of the interoperability among the heterogeneous domain sources, the number of services which are responded after all inputs from the users have been noted and calculated based on service response. The certificate credential validations of the invoked candidate user by using the sample query type evaluated in various categories of interoperability are represented in Table 6.4. Table 6.5 specifies the values which give the number of services got along with the interoperable category. The various outputs of the queries with the four different categories of interoperability with respect to the service have been shown in Appendix B.

**Table 6.4: Interoperable services for different categories for one user**

<table>
<thead>
<tr>
<th>Query Type</th>
<th>Category A</th>
<th>Category B</th>
<th>Category C</th>
<th>Category D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query Type 1</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Query Type 2</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Query Type 3</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Query Type 4</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The different query type responses obtained from the various interoperable categories evaluated and measured by taking number of services got from each query type as shown in Table 6.5. By calculating the number of interoperable services we got (“Yes”) as shown in the Table 6.4 in which different service variations can be found. The performance and efficiency of the AMSI model is obtained by interoperability service measure (I) which is defined as impact ratio between the number of interoperable services we got and total number of services available. Thus the formula for calculating Interoperability service measure (I) could be framed as
Where

\[ I = \frac{(N_I) \times (F_I)}{N} \]

\( N_I \) indicates Number of Interoperable Services Response

\( F_I \) indicates Interoperability Factor

\( N \) Total Number of Service

\( F_I \) is represented as interoperability factor which is calculated by

\[ [(\text{Number of Interoperability level achieved}) / \text{Maximum Level of Interoperability}] \]

This efficiency measure is framed with four query types with respect to interoperability categories represented as I₁, I₂, I₃ and I₄.

**Table 6.5. Interoperability Service Measure among Various Categories calculated for one user**

<table>
<thead>
<tr>
<th>Query Type</th>
<th>I₁</th>
<th>I₂</th>
<th>I₃</th>
<th>I₄</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query Type 1</td>
<td>0.14</td>
<td>0.21</td>
<td>0.28</td>
<td>0.78</td>
</tr>
<tr>
<td>Query Type 2</td>
<td>0</td>
<td>0.22</td>
<td>0.30</td>
<td>0.70</td>
</tr>
<tr>
<td>Query Type 3</td>
<td>0</td>
<td>0</td>
<td>0.30</td>
<td>0.70</td>
</tr>
<tr>
<td>Query Type 4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.80</td>
</tr>
</tbody>
</table>

The above results demonstrate the purpose of the interoperable services in the following ways:

1. Effectiveness and Seamlessness of converting non interoperable services into interoperable services among heterogeneous sources is quantified by calculating the interoperability impact ratio.
2. Interoperating various services and process level operations from heterogeneous business processes in enterprise application integration and with derived sources shows better impact.

The query types involved in the certificate verification case study which is invoked by the candidate user evaluates and operated in four categories for interoperability using service calculation measure is shown in figure 6.6.

![Interoperability service ratio of users using Query Type 1](image)

**Figure 6.6. Interoperability service ratio of users using Query Type 1**

The interoperability effect is demonstrated as shown in the above Figure 6.6 in the aspects of no interoperability, minimum interoperability, average interoperability and maximum interoperability. Candidate User 1 is taken to display the interoperability effect for Query type 1 as shown in the figure 6.6. It is derived from the diagram, that in query type 1 the calculation of Category D interoperability displays minimal deviation and therefore lies to the maximum interoperability which possesses data, service and process level interoperability. Consider the candidate user 1 which has the
service calculation measure \( I_1 \) has the value of 0.14, \( I_2 \) has 0.21, \( I_3 \) has 0.28 and \( I_4 \) has 0.78. It represents that \( I_4 \) has the closest to obtain the effect of maximum interoperability variation which shows the effect of Category D interoperable service which accommodates data, service and process level interoperability. \( I_3 \) and \( I_2 \) displays considerable variation like 0.21, 0.28 mentions the interoperability at various levels with the data sources derived from it. \( I_1 \) which reflects no interoperability displays strong difference in accessing the particular service.

**Figure 6.7. Interoperability service ratio of users using Query Type 2**

Candidate User 1 is taken to display the interoperability effect for Query type 2 as shown in the figure 6.7. It represents that \( I_4 \) has closer to obtain the effect of minimum interoperability variation of 0.7. The Service calculation measure entity \( I_3 \) and \( I_2 \) displays considerable variation. \( I_1 \) which shows interoperability services that displays strong difference of 0.35 in accessing the particular service while comparing
with non available services. This shows the interoperability effect obtained at Category D performs well when compared with other interoperability services. The interoperability categories C and D displays the positive impact on various services which are interoperable but Category A exposes that without any data, services and process interoperability.

![Figure 6.8. Interoperability service ratio of users using Query Type 3](image)

The result of various interoperable services with respect to the query type represented in figure 6.6 and 6.7, Figure 6.8 too brings out the effect towards interoperability by involving Query type 3. Considering the candidate user 1, the calculated available services measures are 0.16, 0.25, 0.31, and 0.72, is related to the outputs identified in query type 2. Hence it also specifies that the result of interoperable services is strong in Category D interoperability when compared with better output obtained from
Category B and Category C, while Category A should not display any measure value near as it does not perform any interoperability.

Figure 6.9. Interoperability service ratio of users using Query Type 4

As like the above query types Figure 6.9 shows the effect of interoperability by involving Query type 4 and the results are extracted. The effect of interoperability services with respect to the candidate user perspective by calculating the number of available services is represented in the figure 6.6, 6.7, 6.8 and 6.9. Now to bring out the effect of available services for process interoperability category by taking the combined results of all query type, the number of average services obtained from different categories is identified and shown in Table 6.6. The illustration of interoperability impact ratio is presented in graph by using the values in the Table 6.6.
Table 6.6. Interoperability Impact Ratio

<table>
<thead>
<tr>
<th>Type</th>
<th>No Interoperability</th>
<th>Minimum Interoperability</th>
<th>Average Interoperability</th>
<th>Maximum Interoperability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type 1</td>
<td>28</td>
<td>38</td>
<td>37</td>
<td>40</td>
</tr>
<tr>
<td>Type 2</td>
<td>0</td>
<td>36</td>
<td>35</td>
<td>43</td>
</tr>
<tr>
<td>Type 3</td>
<td>0</td>
<td>0</td>
<td>36</td>
<td>46</td>
</tr>
<tr>
<td>Type 4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>47</td>
</tr>
</tbody>
</table>

Figure 6.10. Comparison of Different Interoperable Services

The figure 6.10 displays that interoperable service in Category D is considered as very near to obtain many services when comparing to other categories. It is identified that the other categories B and C follows the interoperable category D using the optimal result between B and C due to the impact of services received from other process interoperability. Other than this the Category A interoperability which possesses low
interoperability insists the need for interoperability in service perspective among heterogeneous business processes.

From the experimental analysis the implementation of interoperability between domains using service is considered and shown in 6.6, 6.7, 6.8 and 6.9. It represents that the interoperability service measure is minimum in category D interoperability for every query type in which the AMSI follows the above.

The result of service interoperability has defined comprehensively and achieved more service interoperability measures based on the number of service requested and received from the total number of services to solve the different aspects of interoperability. The architectural model is better analysed by using extensive analysis and leads to future enhancements.

6.7 SUMMARY

The architectural model for service interoperability (AMSI) was evaluated quantitatively and represented its characteristics towards interoperable solution among heterogeneous enterprises. For evaluating the proposed model a certificate verification case study has been taken and modelled according to the different domain requirements. Experimental analysis is done to show the impact of the service interoperability measure. The interoperability service measure I is evaluated based on the interoperability categories and query types executed. With respect to the requirements of the candidate user the various interoperable request for certificate verification is invoked. The interoperable services are consumed and the outputs are analysed quantitatively and compared with other services effectively.