IJETST- Vol.||02||Issue||05||Pages 2383-2395||May||ISSN 2348-9480 2015

Open access Journal International Journal of Emerging Trends in Science and Technology

Security Model to Secure legacy OPC Server and Client Communication

Author

Aakanksha Dhidhi

Master of Technology (Electronics Design)

National Institute of Electronics and IT, Aurangabad, India

Email: *aakankshadhidhi@gmail.com*

Abstract

Steel Authority Of India Limited (SAIL) is the leading steel making company in India. SAIL has its own private network connecting different production units located at Durgapur, Bokaro, Bhilai, Rourkela steel plants etc and corporate offices at Delhi, Kolkata etc. Some of the links in private network are also connected to open and larger network such as internet to communicate with suppliers and customers. Therefore the internal network of SAIL is private as well as public network. So security for this network is most important. Everyday a number of attacks are launched. Among them service attacks are growing exponentially. Since private network of SAIL is indirectly connected to public network through internet. Therefore OPC connected to PLC in steel plants are also indirectly connected to internet. Since it is not possible to route data from OPC through firewall and switching off the firewall makes the plant network insecure and prone to viruses like STUXNET. In this paper, I will propose a security model to secure OPC client and server communication

Keywords: *OPC Service Provider, OPC Data Client, OPC Service Broker, Service Oriented Architecture*

1. Introduction

1.1 General Introduction

Since the private network of SAIL is private as well as public network it is necessary to protect or secure OPC server and client communication. Since OPC ver-2 is based on COM/DCOM technology it is not possible for OPC Data client/OPC service consumer to access data from OPC server through firewall.

1.2 OPC SERVER

OLE for process control (OPC) is a software interface technology used to facilitate the transfer of data between industrial control systems, Human Machine Interfaces (HMI), supervisory systems and enterprise systems such as historical databases. The primary use of OPC is that it provides a common interface for communicating with diverse industrial control products, regardless of the software and hardware used in the process. OPC is an industrial standard based on Microsoft Distributed Component Object Model (DCOM) interface of the Remote Procedure Call (RPC) service. OPC is being increasingly used to

interconnect. Human Machine Interface (HMI) workstation, data historians and other servers on the control network with enterprise databases.

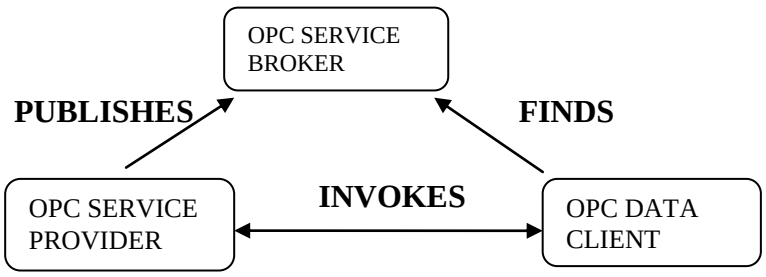
1.3 Service Oriented Architecture (SOA)

A Service Oriented Architecture (SOA) is an architectural pattern in which application components provide services to other components via a communication protocol typical over a network. The principles of service orientation are independent of any vendor, product or technology. SOA is based on the concept of service. SOA contains three software's:- Service provider, Service consumer, Service broker. Each **Service** is built as a discrete piece of code. Service is well defined function that does not depend on the state of other services. **Service Provider Software** helps to register OPC wcf services with the Service Broker. Service Broker stores service metadata information in a repository connected to Service Broker service. **Service Consumer Software** is the one who want to access data of OPC server. Service Consumer Software helps to select the relevant service from the set of services retrieved from the Service Broker repository..**Data Dictionary (OPC Web Service Repository)** contains Domain specific information related to E-Learning Data Dictionary is also called as metadata repository. The content of it are automatically updated as changes occur in the database.

1.3.5 OPC Service Broker

The important in this Broker based OPC web services are played by OPC Web Service Broker. The Broker communicates with the service provider who wants to register and provide its OPC Web Services. The Broker also interacts with OPC data client when he wants to search for particular OPC web services. It also searches the OPC web service Repository when the service provider and OPC Data Client perform publishes and search operations.

1.4 Working Principle Of Service Oriented Architecture (SOA)



1. OPC Web Service Provider publishes its web services to OPC Web Services Broker.
2. OPC Web Service Broker registers OPC Providers Web Service and stores it in repository.
3. When OPC Data Client connects to OPC Web Service Broker, Broker searches its registry and provides the OPC Data Client required OPC Web Services metadata information.

1.5 OPC Client and OPC Server Current Communication Scenario

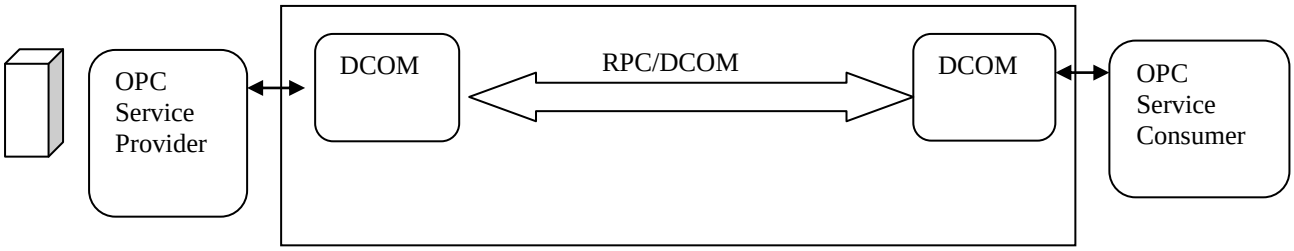


Figure 1.1 OPC Client and OPC Server Current Communication Scenario

In the current OPC Client and OPC server communication scenario communication is through DCOM based technology because OPC ver-2 server is based on COM/DCOM technology. Thus the use of OPC connectivity in control systems and servers leads to DCOM based control protocol attacks (Such as STUXNET). STUXNET is a computer worm discovered in June 2010. It was designed to attack Industrial Programming Logic Controllers. It functions by targeting machines using Microsoft windows operating system and networks, then seeking out Siemens step 7 software.

1.6 Proposed Model To Secure OPC Data Client And OPC Server Communication

In the proposed security model 9 will migrate OPC Data Client and OPC Server communication from DCOM based architecture to potentially more secure. NET based architecture or service oriented architecture in which communication will be through firewalls

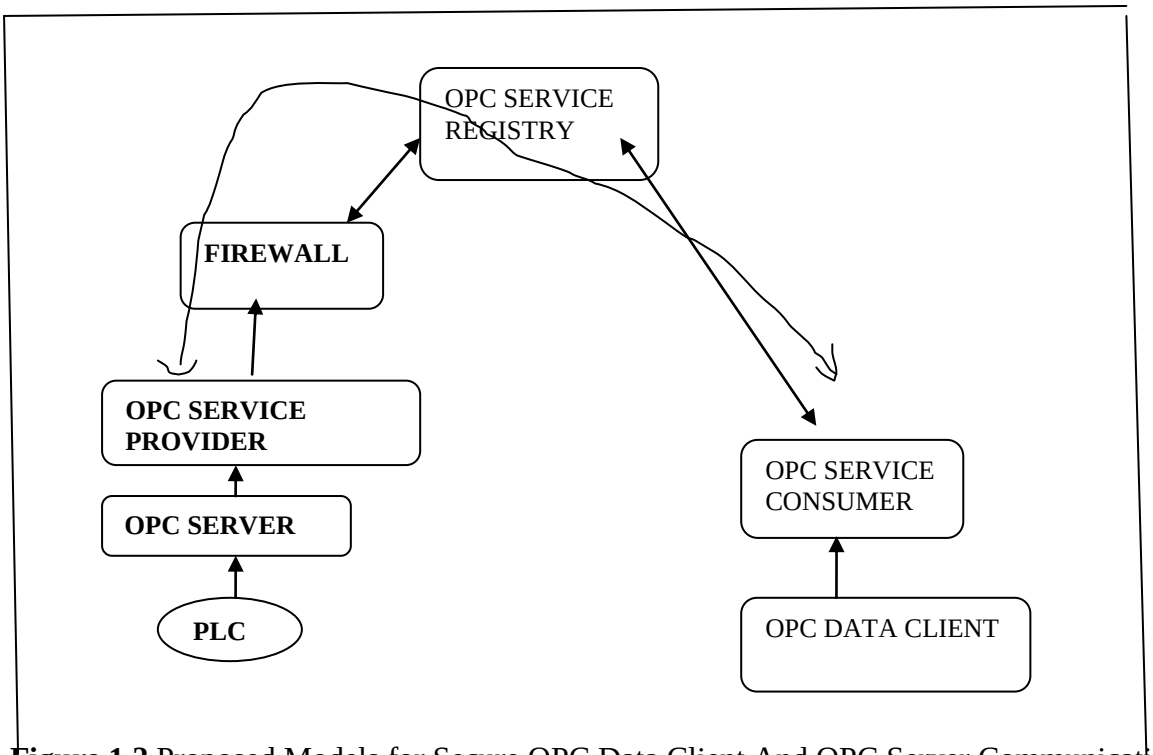


Figure 1.2 Proposed Models for Secure OPC Data Client And OPC Server Communication

2. PROBLEM DEFINITION

2.1 Problems with COM/DCOM Communication

The Microsoft Component Object Model (COM) is a platform independent, distributed, object oriented system for creating binary software components that can interact..COM is not an object oriented programming language but a standard, nor does COM specify how an application should be structured, language, structure and implementation details are left to the application developer. A COM object is one in which access to objects data is achieved exclusively through one or more sets of related functions. These functions sets are called Interface, and the functions of an interface are called methods.COM object are exposed through a set of interface that represent the only point of contact between client and object.COM defines a binary structure for the interface between the client and the object. Distributed Component Object Model (DCOM) is a proprietary Microsoft technology for communication among software components distributed across networked computers MSRPC.This exposed interfaces of COM/DCOM Object can communicate only with Networked computers working on Windows. Therefore communication between Networked computers is not platform independent and insecure due misconfigured firewalls

Figure 2.1 Object in General

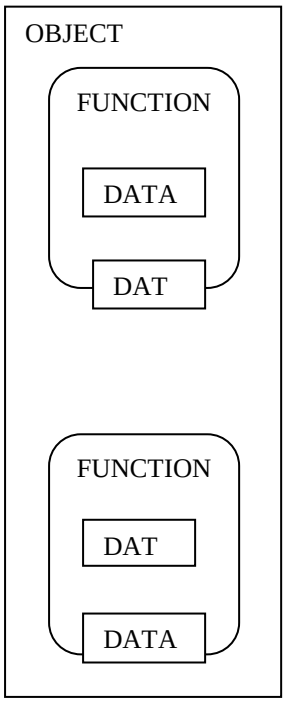
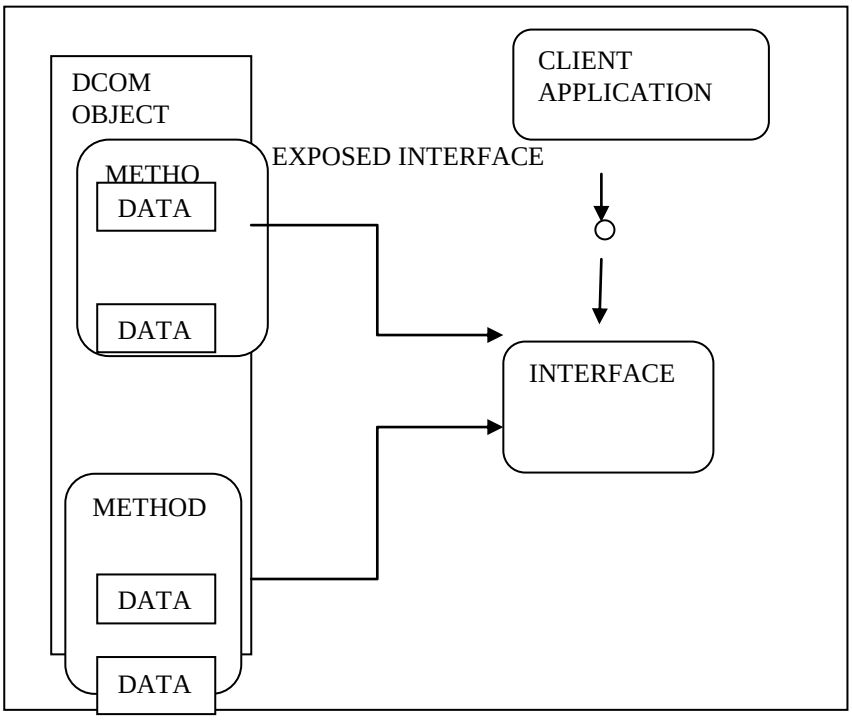


Figure 2.2 COM/DCOM OBJECT



Problems Solved By DCOM

DCOM had solved the problems of:-

- Marshalling – Serialising and deserialising the arguments and return values of method calls “Over the Wire”.
- Distributed garbage collection – Ensuring that references held by clients of interfaces are released when for example, the client process crashed, or the network connection was lost.

The difficulties involved in getting either of COM/DCOM technology is to work over internet firewall, and on unknown and insecure machines, meant that normal HTTP request in combination with web browsers won out over both COM/DCOM.

2.4 Problem Faced with Current OPC Server and Client Communication using COM/DCOM Technology

OPC data client located on remote location when try to access data from OPC server through firewall, it is not able to read or log data from OPC server because of COM/DCOM technology and RPC/DCE network communication. Since communication is not possible through firewall in COM/DCOM technology. Internet network of SAIL become insecure and prone to viruses like STUXNET.

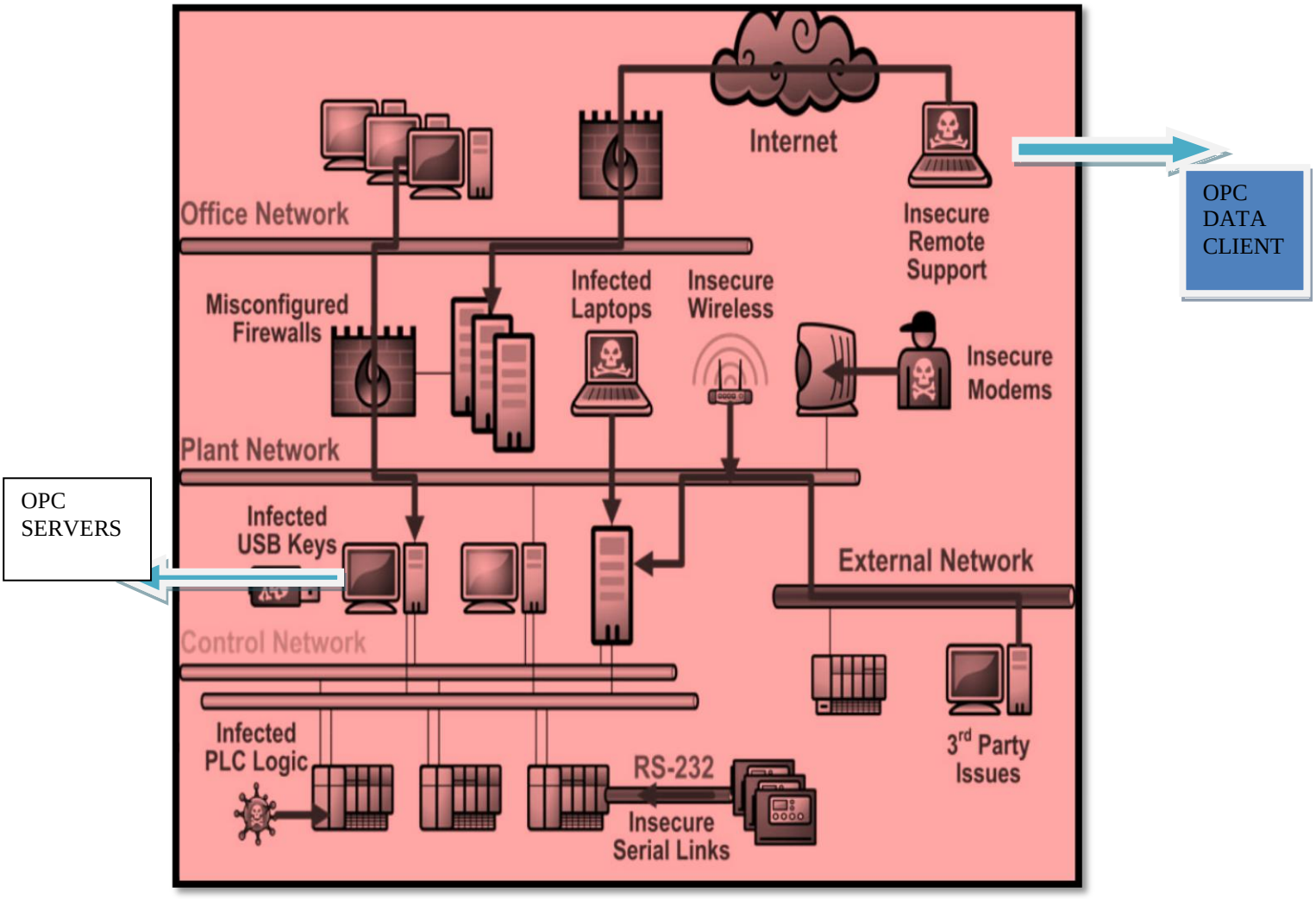
2.4.1 What is STUXNET?

STUXNET is a computer worm that was discovered in June 2010. It was designed to attack Industrial programmable logic controllers (PLCs). It is the 1st discovered malware to include the programmable logic controller (PLC). STUXNET virus on targeted Iranian nuclear including Busnehr nuclear power plant or the natanz nuclear facility. It may have shut down 100 centrifuges or gas pipelines.

2.4.1.1 How STUXNET Operates?

- STUXNET functions by targeting machines using Microsoft windows operating system and networks, then seeking out Siemens step7 software.
- The worm then propagates across the network scanning for Siemens step7 software on computers controlling PLC.
- In the absence of PLC and SCADA software, STUXNET becomes dormant inside the computer.
- If the PLC or SCADA software is found STUXNET introduces the infected commands to the PLC and step7 software, modifying the codes and giving unexpected commands to the PLC.
- It returns a loop of normal operation values to the system operations operating it while introducing unexpected commands to the PLC.
- After the malware installs in the PLC software it periodically modifies the frequency from high to low or vice versa thus effect the normal operation of connected motors, centrifuges and causing them to shutdown or damage the machine.

2.5 Why Current OPC Client Server Communication in SAIL is prone to viruses like Stuxnet.



OPC Data Client at corporate office has insecure remote support through internet and due to which there is a possibility of Office Network of SAIL's been attacked by STUXNET type of viruses . Misconfigured Firewalls , Insecure Modems and External Network of SAIL'S office Network also makes the plant and office Network insecure and prone to viruses like STUXNET .And Because of STUXNET infected PLC'S and LAPTOP working over plants and office Network of SAIL.PLC'S attached

3. Solution

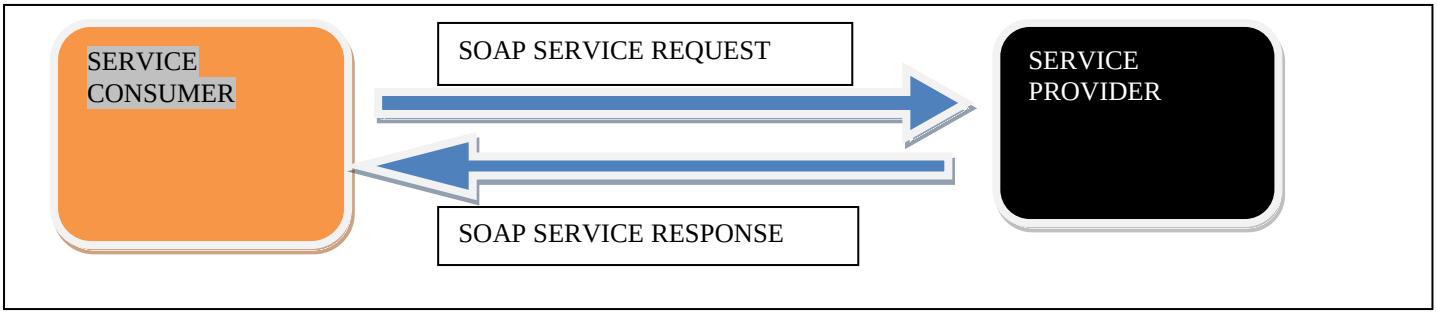
Introducing Broker based Registry Architecture to consume services through firewall. Broker based Registry Architecture Service will be having 3-softwares which communicates with each other. Broker based Registry Architecture will be based on WCF (Windows Communication Foundation).It uses SOAP based on XML to talk to Service Description stored in Registry and WSDL(also based on XML) is used for describing services which provides a machine and human readable description of how the service operates and what parameter it expects.

3.1 Basic Infrastructure of WCF services.

The term WCF Services describes a standardized way of integrating service based applications using XML, SOAP (Simple Object Access Protocol),WSDL(web service description language) and UDDI open standard over an internet protocol backbone. These facilities allow the integration of system written in different languages and running on different computers in different platforms. A WCF service is a standalone software component that has a unique URI (Uniform Resource Identifier is a unique address) and that operates over networked computers. The basic premise is WCF service has 2 major software's

A. Service Provider

B.Service Consumer or users

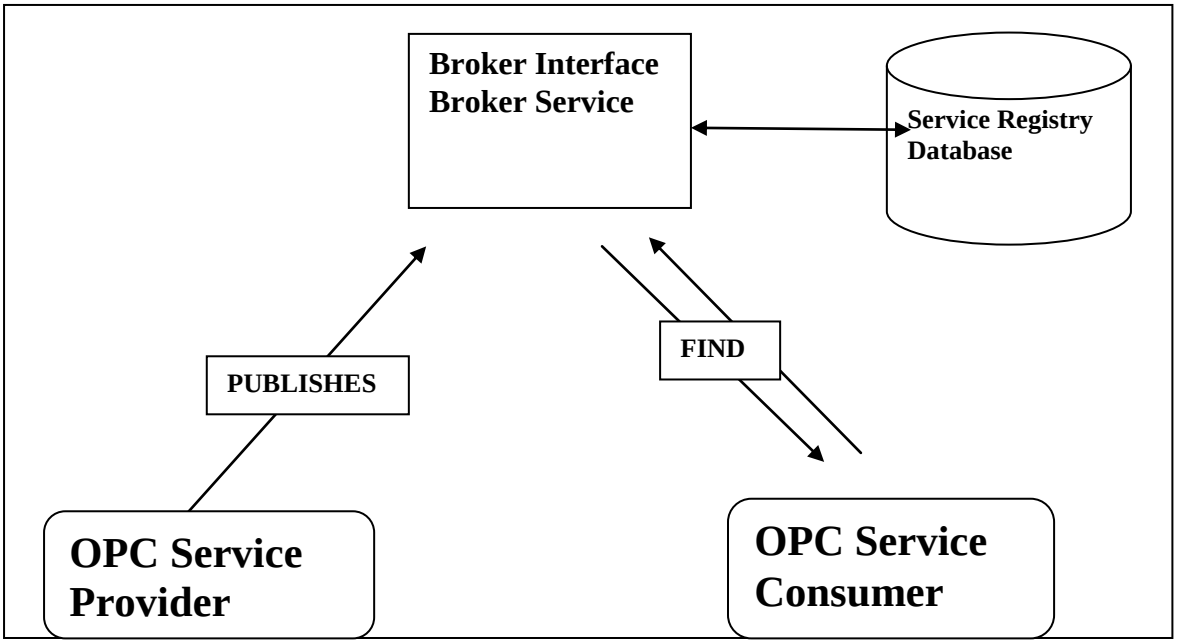


1.2 WCF IMPLEMENTATION ON CURRENT OPC SERVER AND CLIENT

1.3 COMMUNICATION

1. OPC Service Provider publishes its Service Description to OPC Service Broker .OPC Service Broker with the help of its Interface and OPC broker Service accepts service descriptions from the provider and stores it in Service registry. All OPC Service Providers publishes their service description and registers themselves with service broker.
2. OPC Service providers communicate to the directory using SOAP protocol in order to send its service description written in WSDL (an XML based language for information exchange in Distributed Environments). WSDL definitions describe how to access a web service and what operations it will perform.WSDL is a language for describing how to interface with XML-based services
3. OPC Service Consumers make queries against this directory to know what services are available and how to communicate with those services using industry standard SOAP protocol.

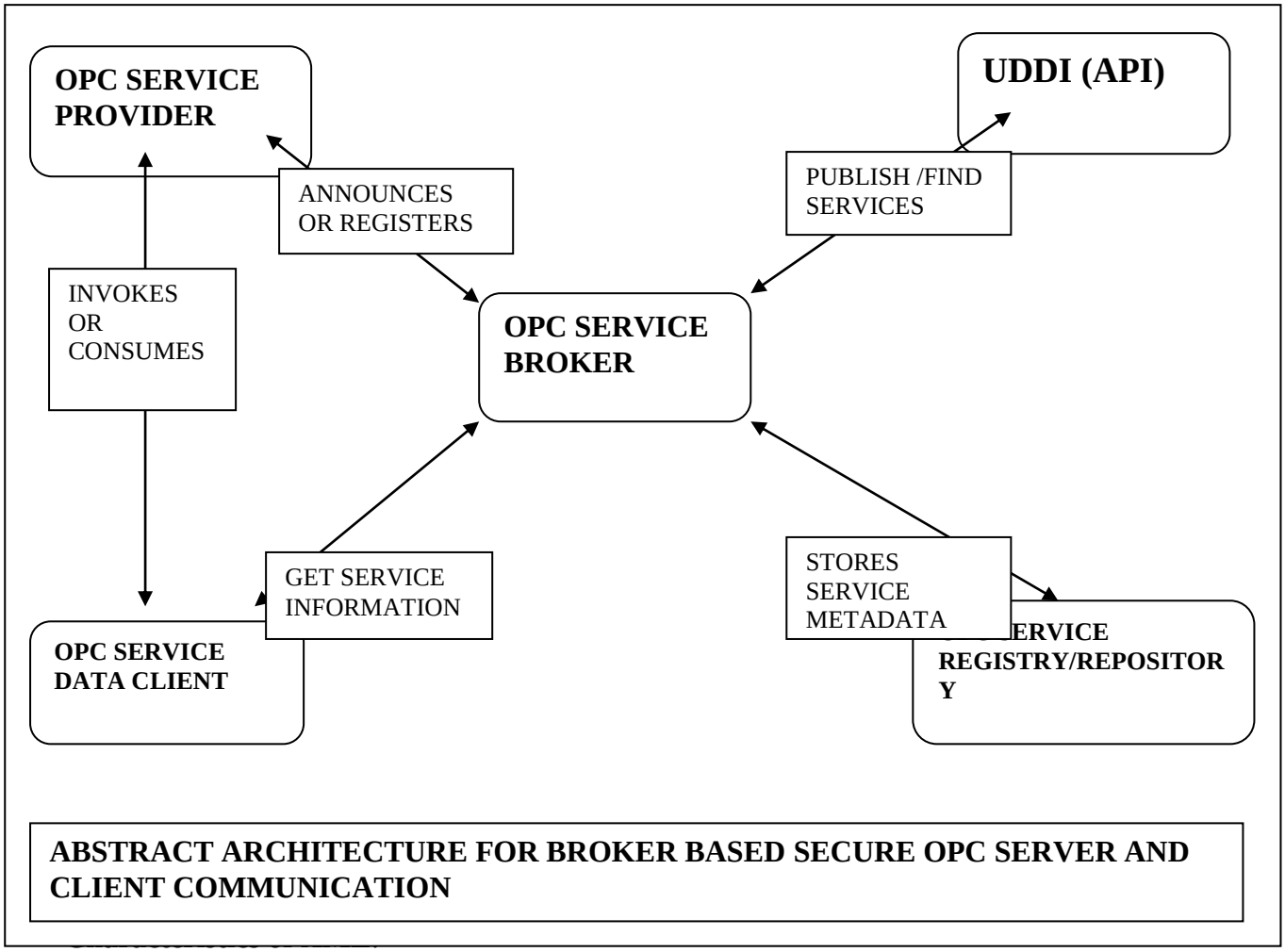
4. OPC Service Providers and consumers use industry standard SOAP(XML tag based language) protocol because **it is language independent ,platform independent and helps to get around firewalls** which is a major problem is OPC Server and Client Communication.
5. The Response generated by the Service Provider is also a SOAP (format to send message between application via internet) message based on specification defined in service description using WSDL. SOAP carried over HTTP helps to get around firewalls. It is good to easily integrate remote applications with security concern.
6. OPC Service Provider publishes its Service Description to OPC Service Broker .OPC Service Broker with the help of its Interface and OPC broker Service accepts service descriptions from the provider and stores it in Service registry. All OPC Service Providers publishes their service description and registers themselves with service broker
7. OPC Service Provider publishes its Service Description to OPC Service Broker .OPC Service Broker with the help of its Interface and OPC broker Service accepts service descriptions from the provider and stores it in Service registry. All OPC Service Providers publishes their service description and registers themselves with service broker.
8. OPC Service providers communicate to the directory using SOAP protocol in order to send its service description written in WSDL (an XML based language).
9. OPC Service Consumers make queries against this directory to know what services are available and how to communicate with those services using industry standard SOAP protocol
10. OPC Service Providers and consumers use industry standard SOAP(XML tag based language) protocol because **it is language independent ,platform independent 3.3 Augmenting above service Publication and Announcement using Broker based registry Architecture for secure OPC Server and Client Communication**



3.3 Augmenting above service Publication and Announcement using Broker based registry Architecture for secure OPC Server and Client Communication.

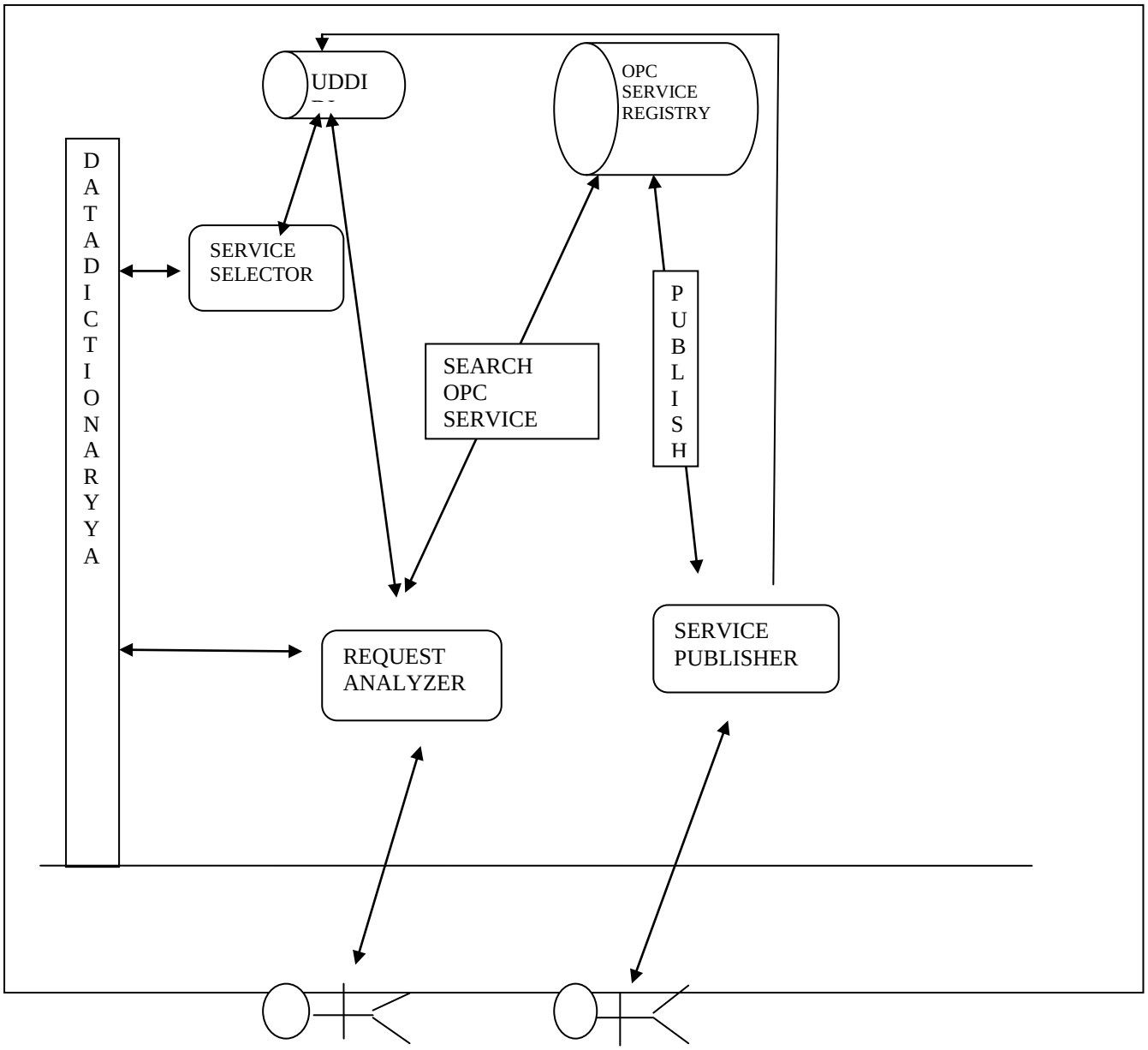
1. Design of OPC Service Broker for OPC Service Discovery and Announcement.
2. Design of OPC Service Registry /Repository to save Service Descriptions written in WSDL (Web service Description Language).
3. Creating sockets for Discovery and Announcement Service. Sockets will be continuing listening for announcement from OPC Providers and discovery from OPC Data Client.
4. When announcement message is received by OPC Service Broker, announcement service at announcement endpoint is invoked which accepts service description from OPC Service Providers and stores it in OPC Service Repository connected to it.
5. When Discovery message or find message is by OPC Service Broker, Discovery Proxy Service at discovery endpoint is invoked which accepts the query message and after searching the queried service in a Repository displays appropriate results.

3.4 **ABSTRACT ARCHITECTURE FOR BROKER BASED SECURE OPC SERVER AND CLIENT COMMUNICATION**



ABSTRACT ARCHITECTURE FOR BROKER BASED SECURE OPC SERVER AND CLIENT COMMUNICATION

3.4 INTERNAL ARCHITECTURE OF OPC SERVICE BROKER



4. OPC SERVICE DISCOVERY MECHANISM

In a minimalistic scenario, there exists at least one WCF OPC Service provider that publishes some service such as a OPC data logger service and a OPC Data Client that uses this service. The WCF Service discovery is the process of finding a suitable Web Service for given task of a requester or a composition mechanism. The OPC Service Provider registers its services at the OPC Service broker and the OPC Service broker publishes the provider's information into the UDDI. When the OPC Data Client searches for the service at the broker, the broker will search for the exact keywords in the database and returns the Object_id for further processing.

4. Mechanism and Implementation

4.1. The Announce OPC Service Mechanism

• First the OPC Service provider should register the service with the broker which is listening at announcement socket for announcements, by enabling Metadata exchange of application configuration file of the service

• The broker then stores its description and metadata Information using UDDI APIS to the OPC Service registry/Repository connected.

• The broker also sends an acknowledgement to the OPC service provider that it has been registered and available for OPC Data Client for consuming.

4.2. The OPC Service Discovery Mechanism

The sequence of activities involved in OPC service(discovery) is described below.

- The OPC Data Client sends the query using UDDI API, enriched with functional semantics to the broker for the Discovery of relevant OPC services.
- The Discovery Proxy Service running at Discovery Endpoint resolves the query and finds the specific keywords to search the OPC Services in the OPC Service registry/Repository.
- The Discovery Proxy Service using Data Dictionary finds the perfect match for the query using Word Net and obtains the Keywords in XML form.
- Using these matched keywords the Discovery Proxy Service searches the relevant information about the OPC Service from OPC registry/Repository.
- Once the contents are found, the URIs, object name, object type are encapsulated in an Object and returned to the Discovery Proxy Service which in turn return it to the OPC Data Client

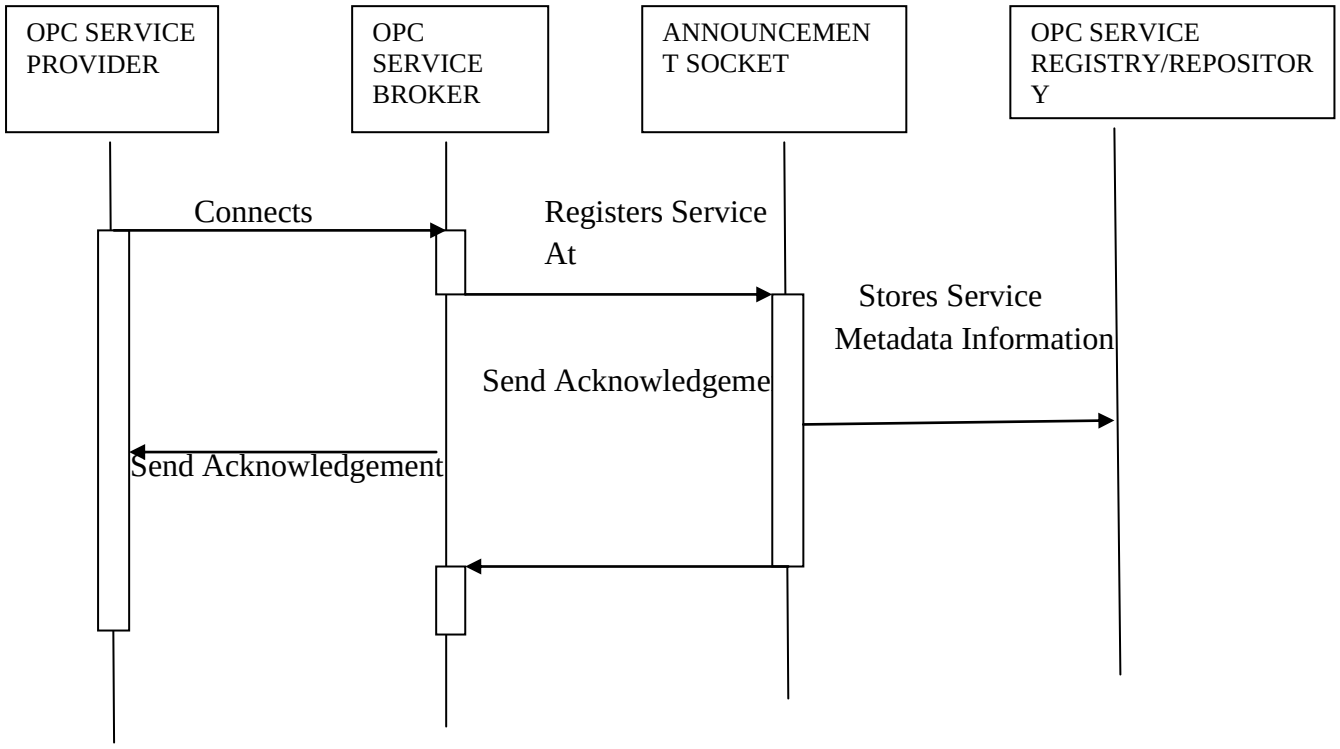


Figure: Sequence Diagram for Announcing OPC Service Operation

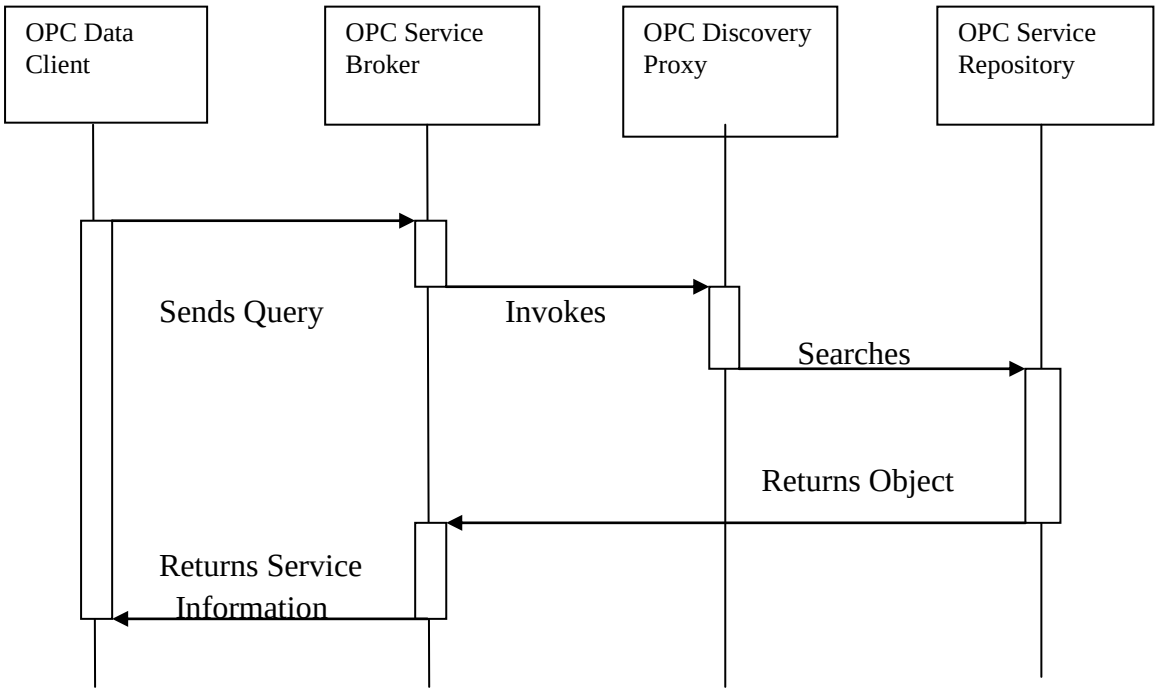


Figure 4.Sequence Diagram for Select E-Learning Service Operation

5. Implementations

The OPC service discovery architecture is implemented on Intel Core i5-2430M machine with Microsoft Windows 7 as computing environment. The OPC service Announcement and discovery mechanism is developed using Microsoft Visual Studio 2010 with .NET Framework 4.0. To find the similar words (synonyms) of query the WordNet.Net 2.1 (2005) API is used.

5.1. Implementation of Announcement and Discovery (OPC SERVICE BROKER)

The service provider registers its service through the user interface which calls register_provider_details () function. Figure 5 depicts the user interface created to announce the OPC services. Figure 6 presents the user interface designed to search relevant OPC Services. When the OPC Data Client requests the broker by sending a query, the query is given as a Parameter to the readxml () function used by the Data Dictionary. This makes use of Word Net 2.1 to differentiate the exact keywords. The readxml ( ) function implicitly calls the Word Net 2.1 Using words match ( ) function to find the synonyms and displays the result in an XML format. Using these synonyms the appropriate information about the service content is then retrieved and encapsulated in an object. This object is returned by the function display object ( ). The search result will contain the type of the content (Address, Binding and Contract or Metadata Information of the service), brief information about the searched content and it's URI. This Object is used by the Discovery proxy service the contents of this object based on the object type and stores it. The service selector also responsible for finding the perfect Address, binding and contract from the OPC Service registry to retrieve suitable URI based on the order of precedence.

6. Conclusion

WCF Services provide an attractive alternative for businesses to reach out to their potential customers. This paper addresses the issues related to Secure OPC Server and Client Communication. The quest of OPC Data Client to find the appropriate OPC Services can be fulfilled by using this architecture. This research work comprises of the discovery mechanism used to search for the appropriate OPC Services. In order to minimize the search only the appropriate synonyms of the service requester's query are obtained from the WorldNet which gives better search results. The paper implements broker based architecture which helps in overcoming the disadvantages of legacy OPC Server Client Communication. It simplifies the work of Discovering and Announcing of OPC Data Client and OPC Server respectively. It also makes it simple for the OPC Data Client to find services and its metadata Information.

Acknowledgement

This research work is sponsored by "SAIL (STEEL AUTHORITY OF INDIA LIMITED), INDIA" and guided by Mr.Ravishankar (AGM), SAIL, India dated: 14/05/2015.

References

1. The Expert's voice in .NET by Nishinth Pathak Pro WCF 4 Practical Microsoft Implementation (2nd Edition)
2. C# Network Programming by Richard Blum (2nd Edition)/
3. OPC Security White Paper -1(Understanding OPC and How it is Deployed) prepared by Digital Bond, British Columbia Institute of Technology ,Byres Research, July 27,2007
4. OPC Security White Paper -2(OPC Exposed) prepared by Digital Bond, British Columbia Institute of Technology, Byres Research, November 13, 2007.
5. OPC Security White Paper -3(Hardening Guidelines For OPC Hosts) prepared by Digital Bond, British Columbia Institute of Technology, Byres Research, November 13,2007
6. Programming WCF Services by OReilly in Net.4 Framework (3rd Edition).
7. A Registry Based Discovery Mechanism For E-Learning Web Services by Demian Antony D'Mello1, Pramod Prabhu2, Naveen Baliga3, NikhilMisquith4 and Flexon Fernandes5 (Department of Computer Science and Engineering, St. Joseph Engineering College, Mangalore, INDIA – 575 028) published in International Journal of Computer Science and Technology.

.