CHAPTER 3

THE FRAME WORK

3.1 INTRODUCTION

This chapter explains the framework for preserving privacy with dynamic trust management policies for enhancing security in a pervasive environment. By executing this framework, communication of data through the network will be done in a secured manner. Due to high rates of technical challenges in pervasive environment, development of new model that faces the issues related to security, privacy and trust is needed. To provide a secure and reliable communication between the user and system environment we have developed an enhanced privacy model with dynamic trust engine in a pervasive environment.

3.2 SYSTEM DESIGN

The overview of the research is shown in Figure 3.1. It is an abstract view of this research work. It is also called Trust Security Privacy (TSP) Model in pervasive computing environment. It covers the various challenges and technical advances in the subject of the relationship among trust, security and privacy. So, users can access any services or resources at anytime from anywhere. This architecture provides security which dynamically manages the trust for information privacy in pervasive environment with policies for all system components and their trust values. It offers protection against security threats and privacy threats existing in
pervasive computing environments. It is targeted to ubiquitous healthcare systems. Although it is suitable for small set of components, it can be extended to other ubiquitous applications.

Figure 3.1 Overview of Proposed Work

It includes two models. They are, Security Model and Privacy Model.
In the security model, the focus is on development of security mechanism for providing reliability via single and multi path communication with DDOS attacks. Those mechanisms will address the issues during communication and provide the solution in pervasive environment at different layers like network layer, transport layer and application layer. Thus, a model for improving security with single path and multipath routing technique is developed.

In privacy model, to achieve privacy preservation, proposal of privacy mechanisms can be solved by two approaches. They are, Qualitative Approach and Quantitative Approach.

The qualitative approach will statically or dynamically protect the sensitive data so that it is not being accessed or modified by any unauthorized user. Privacy of such sophisticated data (sensitive data) encompasses the method of g- anonymity which is based on the following three methods.

1. **Data Globalization**

   Data globalization is the substitution method, to replace the values of sensible information with more common values. This technique promotes the privacy of information. It can be replaced by less precious value, that reduces the risk involved in protecting such an information from unauthorized user.

2. **Data Virtualization**

   Data virtualization is the technology that offers the data to consumers a unified, abstracted and encapsulated view for data stored in a heterogeneous set of data stores. In Figure 3.2 shows the services of the
virtualized applications that can be achieved through both the virtualized entities like Internal and External.

![Data Virtualization Server Diagram]

**Figure 3.2 Data Virtualization Server**

The architecture of the data virtualization, the server takes the following steps for selected import of tables to the consumer.

- The process of import tables
- Creation of wrapper table
- Query execution
- Accessing the virtual table

Before selection of the source tables, which act as a virtual table and those tables have to import first. Only then it will be known as the data virtualization server. This is a simple process if the table is already available in the required database. The developer, after logging in to the virtualization server, has to select imported tables from the catalog of the virtualization server. Then virtualization server extracts all the data available on the table and store it in own directory for their further process.
When a source table has been selected for import, the virtualization server determines whether some values of Meta data are in standard format or not. Each table has its own data format to define the contents. So, necessarily it has to be determined and to be converted to the standard form. After this process has been carried out, the virtualization server has to create wrapper table. The virtual content of the wrapper table is 100% identical to its source table. The wrapper table is not like source table which contain the source data along with Meta data of the following:

- The Network location of the source table where it resides
- Information on how it can be accessed
- The owner, date of creation of the source table
- The structure of the source table
- Data types for columns specified in the source table
- Primary and foreign keys of the source table
- The number of rows in the original table

The wrapper table behaves like any table in the data base. It can be queried, added, deleted and updated if the virtual server will allow it into the context. The virtual server developer can study the contents of wrapper table. Because, he can verify that the contents are available to the level of expectation.

The process of query execution is a mapping, which defines the structure of the virtual table and tells about how do the contents transfer from the source table to the virtual table through the wrapper table. This is called virtual table definition.
Without mapping, virtual table cannot be queried or viewed. This process of mapping usually consist of operations such as

- Row selection
- Column selection
- Column concatenation
- Name change of column
- Groupings

The Figure 3.3 shows the relationship among source table, wrapper table and virtual table. A virtual table of the virtual server also has a name, a structure, query definition and contents of a table is also virtual and is derived from source table though the following steps

- Wrapper Table Creation= Source Table +Wrapper Table
- Accessing Virtual Table= Query Execution+ Virtual Table

Once virtual table has been created, its contents can be viewed and cannot be altered. Virtual Table is like SQL database server. Different language can be used to define virtual mapping in virtual server. Languages in use are

- SQL
- ETL
- Extended SQL
- XSLT and XQuery
• Procedural programming languages

• Combination of above

After creation of virtual table, it has to be published, which is called virtual exposing. That means it should be available to the consumers through one of the languages or programmatic interfaces. Most data virtualization server support the following range of interfaces:

• SQL with ODBC

• SQL with JDBC

• SQL with ADO.NET

• SOAP/XML via HTTP

• ReST (Representational State Transfer) with JSON (Java Script Object Notation)

• ReST with XML

• ReST with HTML

• JCA(Java Connector Architecture)

• JMS(Java Message Service)

• Java(POJO)

• RSS (RDF Site Summary or Really Simple Syndication)

• SPARQL

For each virtual table, one or more different interfaces enable and allow the consumers via their respective interfaces.
Data virtualization server supports transaction management. That means it will consider many transactions as one logical unit of work. Hence, it leads to automatic transaction of business intelligence.

Also it supports distributed transaction management. In a distributed transaction, all transactions are considered as one atomic unit of work for multiple stores.

Most virtual server offers a concept of caching mechanism. The contents of the source table are retrieved from the underlying source table and the running the mapping and storing the contents on disk with help of cache.

This is also called materialized virtual table. It improves the query performance and minimizes the interfaces on source systems. If virtual tables are nested, at each level caches can be defined. The benefit of caching is, to speed up process up to 100% for executing query. Query optimization also improves the performance of data virtual server. This is the process which helps to provide the best processing strategy for a query.

3. Data Embellishment

Data embellishment is the action of adding decorative details of the sensitive data or hiding the values of information as many times as possible. The goal of this technique is to present the information in the form of different perspective as user cannot be expected. So, attackers will not be accessed their expectation in the form of information stored in original storage.
3.3 SUMMARY

In this chapter, a system design and its components are discussed. Two models of this work TSP model have been divided into sub models as security model and privacy model. The security model has been further carried out into different communication paths like single and multi path communication in a pervasive environment. Same way the privacy model has been further carried out by two approaches. One is qualitative method with data globalization, data virtualization and data embellishment. Another approach is quantitative methods, which helps the environment to determine privacy with their metrics by trust, security and privacy models.