CHAPTER 8
INTEGRATED FRAMEWORK FOR SECURE BUSINESS PROCESS

8.1 INTRODUCTION

The integrated framework for secure business processes has several modules, which are responsible for different kind of activities. These modules are majorly focusing on the development of different web services, central broker, broker’s layer, business processes, security interfaces, multithreading based proposed algorithm, and phase II of authentication mechanism etc. These all modules are developed together to provide the secure integrated framework to end users. The development of security interfaces around business processes, registration of those business processes with UDDI, creation of application client etc., are significant activities handled in the framework. The development of phase II of authentication mechanism in integration with application client is critical activity for end user.

The conceptual model of integrated framework with its components is demonstrated in Section 8.2. The layered architecture of integrated framework is illustrated in Section 8.3. The implementation of proposed framework using an example of file uploader and downloader application is carried out in Section 8.4. The observation and summary of the chapter are organized in Section 8.5 and Section 8.6, respectively.

8.2 CONCEPTUAL MODEL OF INTEGRATED FRAMEWORK

The conceptual model for the integrated secure framework for business processes or web service composition is shown in Figure 8.1. The proposed framework protects end users from malicious attacks.
Figure 8.1: Integrated Secure Framework for Business Processes
The integrated framework consists of various layers such as, security layer, business process layer, broker layer, web service layer and database layer, which are collectively responsible for building the secure integrated framework over the network. The secure integrated framework for business processes have various components such as, service consumer, phase II of authentication mechanism, pattern generator, multithreading based system, key matrices, ENC and DEC modules, business processes, business process manager, brokers, broker’s layer, web services, service provider and databases. Each component has its own responsibilities and behavior in the integrated framework, which are discussed in subsequent paragraphs. The implementation of the proposed framework is performed for an application of file uploader and downloader.

**Service Consumer**

Service consumer is an end user, which is intended to use integrated secure framework around business processes. In this secure framework, the service consumer interacts with phase II of authentication mechanism. User has to select the right pattern generated by pattern generator. Once the right pattern is selected, service consumer is eligible for accessing the business processes for the fulfillment of business requirements.

**Phase II of Authentication**

The phase II of authentication mechanism is an important component, which has the support of pattern generator. The pattern generator is responsible for generation of patterns and phase II of authentication mechanism is responsible for the selection of right patterns. The phase I of authentication mechanism requests for valid username and password for login process, which was allocated to end user during registration process from the system. Once the end user logged in successfully during phase I, he/she can proceed for phase II of authentication mechanism. If the end user logs in successfully in
phase II, he/she can access the credentials. The complete process of phase II of authentication mechanism is discussed in Chapter 7.

**Pattern Generator**

The pattern generator is responsible for generating the patterns randomly based on the end user’s basic details, family details, blood group, date of birth, height of family members etc., which are known to end users only and it is difficult for any other person to remember. The end user has to provide their details during the registration process. The end user can use the integrated framework once the registration process is completed. The pattern generation mechanism is also discussed in Chapter 7.

**Multithreading based System**

Once the right pattern is selected by the end user in phase II of authentication mechanism, user can use the file uploader and downloader application for data transfer in the secure manner. The data transfer over the network is secured due to multithreading based system, which is discussed in Chapter 6. The multithreading based system has the support of multiple threads and the concept of key matrices. The data transfer between the application client and server is divided into N number of plaintext blocks. Each plaintext block is encrypted using the proposed multithreading based secure algorithm. Each block is encrypted using ENC module and decrypted using DEC module associated with the multithreading based system. The key matrices are responsible for generating the key pairs for each block.

**Key Matrices**

The key matrices have set of key pairs, where each key pair is triplet of three unique keys. The key matrices have a support of two different key matrix, one is for sender and another is for receiver. At sender’s side, the key matrices are developed in a way that if sender knows the first key pair for encrypting first plaintext block then user
can generate other key pairs by rotating the first key pair into the anti clockwise direction. At receiver’s side, if the receiver knows the first key pair for decrypting the first ciphertext block then user can rotate the first key pair into clockwise direction to produce the other key pairs. Each block requires different key pairs for encryption and decryption processes. The concept of key matrices is discussed in Chapter 6, which is used in multithreading based system.

**Table 8.1: Abbreviations and Their Details**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Details</th>
<th>Abbreviation</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>First Thread</td>
<td>K1, K2, K3</td>
<td>First Key Pair</td>
</tr>
<tr>
<td>T2</td>
<td>Second Thread</td>
<td>K2, K3, K1</td>
<td>Second Key Pair</td>
</tr>
<tr>
<td>T3</td>
<td>Third Thread</td>
<td>K3, K1, K2</td>
<td>Third Key Pair</td>
</tr>
<tr>
<td>B1,B2</td>
<td>Brokers</td>
<td>B5,B6,B7</td>
<td>Brokers</td>
</tr>
<tr>
<td>B3,B4</td>
<td>Brokers</td>
<td>S2</td>
<td>Authentication Service</td>
</tr>
<tr>
<td>S1</td>
<td>Login Service</td>
<td>S4</td>
<td>Basic Details Service</td>
</tr>
<tr>
<td>S3</td>
<td>Pattern Service</td>
<td>S6</td>
<td>Pattern Generator Service</td>
</tr>
<tr>
<td>S5</td>
<td>Family Details Service</td>
<td>S8</td>
<td>Authentication Checks Service</td>
</tr>
<tr>
<td>S7</td>
<td>Login Checks Service</td>
<td>S10</td>
<td>Change Password Service</td>
</tr>
<tr>
<td>S9</td>
<td>Registration Service</td>
<td>S12</td>
<td>Upload Service</td>
</tr>
<tr>
<td>S11</td>
<td>Change Pattern Service</td>
<td>S13</td>
<td>Download Service</td>
</tr>
</tbody>
</table>
ENC and DEC Modules

The ENC and DEC modules discussed in Chapter 4 are responsible for encryption and decryption processes, respectively in association with multithreading based system in integrated secure framework. Each plaintext block will move through three different levels called, ENC, DEC and ENC again before converting it into the ciphertext block. These all ciphertext blocks are appended together as single ciphertext block. Business processes in a secure manner will process the encrypted request from service consumer in the form of ciphertext block. At receiver side, the ciphertext block will be processed through DEC, ENC and DEC again for converting ciphertext block into the plaintext block. The plaintext block as a service consumer’s request is send to different web services for fulfilling the incoming requests. The web service is responsible for collecting the appropriate response send back to business processes. The business processes further send the response back to the service consumer.

Business Process

The business processes are major concern in integrated secure framework because of security aspects. Business process is an industry oriented approach of service composition through BPEL language. The secure integrated framework is proposed and developed with the purpose of securing the business processes over the network. The business processes need to be secure and responsible for fulfilling the business needs in various application domains such as, banking services, online transactions, e-commerce activities, education systems and entertainments etc. The business processes can be constructed with the help of web services and their description language.

Business Processes Manager

Business process manager is responsible for managing the business processes in terms of compilation, error checks, workflow designing, connectivity of individual activities, execution of workflow,
execution of business processes, connectivity of parnerLinks etc. The business process manager keeps the track of overall execution of business processes to fulfill the business needs.

**Central Broker**

The central broker is responsible for reducing the load of UDDI by categorizing the incoming requests and forwarding them to the desired brokers. When the end user requests file uploader application to upload data over the server, then the central broker categorizes requests and sends them to the corresponding broker. The main responsibility of central broker is the categorization and management of incoming requests at the time of heavy load over UDDI.

**Broker Layer**

The broker layer has a set of brokers responsible for different kind of work associated with them such as, authentication, patterns check, password change request, pattern change request, end user registration, file uploading process, and file downloading process etc. Each broker can deal with different connected web services to process the incoming requests and generate the relative responses. These all brokers are used together to handles all incoming requests and reduce the load of central repository.

**Web Service**

Web services are responsible for uploading the data over the server in case of file uploader activity and send the data back to client location in case of file downloader activity. Each web service has its own description defined inside WSDL language such as, number of functions supported by web services, function parameters, service location etc. The WSDL language is used as an intermediate interface between the service consumer and service provider. The service consumer interacts with web services with the help of WSDL description language.
**Service Provider**

Service provider is an end developer, which develops different web services as per the requirements, and registers those web services into central repository. Once the web services are registered, service consumer can search the appropriate web service according to their needs.

**Database Layer**

The database is a software application, which stores the details of different files uploaded and downloaded from different client locations by different end users. The actual file will be stored on the server, when end user uploads it through file uploader application. The file details stored into databases are login ID, file name, file size, type of file, time of file upload, time of file download, folder path etc. The database has seven database tables in file uploader and downloader application containing different information.

**8.3 LAYERED ARCHITECTURE OF INTEGRATED FRAMEWORK**

The layered architecture for proposed conceptual model of integrated framework is shown in Figure 8.2. As per the layered architecture, the end user interacts with security layer before accessing the business processes at business process layer. The load sharing layer is responsible for reducing the load of central repository from the perspective of business processes. The broker’s layer handles the categorization of different incoming requests and calls the appropriate web services.

The end users use layered architecture for securing communication at business process layer, reducing load activity, handling the brokers on broker’s layer for incoming requests and outgoing responses. The web service layer deals with the database
layer for data storage and fulfill all kind of incoming requests by generating desired responses.

Figure 8.2: Layered Architecture of Integrated Secure Framework

8.4 IMPLEMENTATION

The end user will be registered to the proposed system by filling the registration form with their basic and personal details as shown in Figure 8.3. Once the registration process is over, system will assign username, password and pattern to the end user for further communication. The pattern assigned to the end user will be generated by pattern generator based on basic and personal details such as, number of family members, date of birth, height in centimeters, age, gender, blood group of each family member etc. Once the registration process is completed, the user has to pass phase I of authentication by entering the valid user name and password.
Figure 8.3: Registration Process

The integrated secure framework has a support for changing the passwords and patterns, if required for an end user. The password changing facility requests end user to enter username, current password and new password for change. Whereas, the pattern changing facility requests end user to enter username, current password, current pattern and new pattern for change. Once the end user passes phase I of authentication successfully, the user has to pass the phase II of authentication process by selecting right pattern from set of random patterns generated by the system as shown in Figure 8.4. Otherwise, the end user has to restart the process.

Once the user passes phase II of authentication, the end user is eligible for uploading the files on the server as part of file uploader and downloader application. The end user has to select the file to upload from file system as shown in Figure 8.5.
Phase II of Authentication

Please Select Right Pattern

User Name: [Field]

- [ ] DABR2-09/01-28/08-009/05-12/08
- [ ] 09/01-17/05-15/08-13/08-28/08
- [ ] DABR2-09/01-17/05-12/08-15/08-28/08
- [ ] DABR2-28/08-12/08-09/01-17/05

Authenticate

Figure 8.4: Phase II of Authentication

Please Choose the File for Upload

User Name: Alex

File for Upload: [Field]

File Type: [Field]

Submit

Figure 8.5: File Uploading Process
Once the file is selected for uploading, data of the file will be encrypted with multithreading based algorithm. The plaintext data and its corresponding ciphertext are shown in Figure 8.6.

**Figure 8.6: Encrypted Data for Uploaded File**

The encrypted data is send to business processes over the network in secure manner. The decryption of ciphertext into plaintext with same algorithm and key is performed at service end. Once the decryption is performed successfully, the file in plaintext form will be stored on server with the help of web services. The end user can also use the developed application to download a file from the server to his preferred location in a file system in secure manner as shown in Figure 8.7. The user has to select the file to download and provide the location on which the download operation has to be performed. The end user will be authenticated by phase II of authentication mechanism to download the file from server. Once the user has selected file and its location to download, the data of the file again encrypted with
multithreading algorithm at server side. The encrypted data of the file is transferred from server to business process and business process to end user as shown in Figure 8.8.

The intended user can use file uploader application to store critical data over the server. User can also use downloader application for downloading the file from the server on preferred location.
Figure 8.8: Encrypted Data for Downloading File

```sql
SELECT * FROM upload;
```

```
SELECT * FROM download;
```

Figure 8.9: Database Details
8.5 OBSERVATIONS

The proposed integrated secure framework for business processes has been evaluated and tested with the developed file uploader and downloader application. File uploader and downloader application assists end users to upload their critical, personal, and important data or contents such as, text files, audio files, video files over the server in a secure manner. In general, insecurity exists in current scenario because of hackers, intruders and crackers. The developed secure integrated framework protects end users from all kind of thefts. The contents of end user’s will be secured over the network during uploading and downloading processes by introducing security layer and multithreading based secure algorithm. The multithreading based secure algorithm builds the system secure with the help of key matrices, where key pairs are generated randomly.

The integrated secure framework has been evaluated on several key parameters such as, number of service consumers using the system, number of patterns generated for individual, number of threads in multithreading based system, number of key pairs generated from key matrices, number of business processes and web services used in the system, number of brokers on broker’s layer, number of databases and its tabular structures, number of requests and responses etc. The analysis of service consumers and their patterns are described in Table 8.2. In this table, first family member is abbreviated with FFM, second family member is abbreviated with SFM and third family member is abbreviated with TFM and so on. The date of birth and blood group are abbreviated as DOB and BG, respectively. The height in centimeters is abbreviated with HC.

The patterns generated for different families listed in table 8.2 are based on the details listed in table as well as the pattern order selected by end user. The pattern order can be developed from personal information of end users such as, DOB-BG-MOB, MOB-BG-DOB,
DOB-FN-HC, HC-BG-YOB etc. The MOB is month of birth, FN is first name of family members, HC is height in centimeters etc. Once the end user has selected the right pattern, he/she can access multithreading based system to upload/download personal and critical data in a secure manner on/from the server.

**Table 8.2: Family Details and Pattern Generation**

<table>
<thead>
<tr>
<th>End User Name</th>
<th>First Family</th>
<th>Second Family</th>
<th>Third Family</th>
<th>Fourth Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>FFM Name</td>
<td>Fabia</td>
<td>Nadia</td>
<td>Kaley</td>
<td>Octavia</td>
</tr>
<tr>
<td>SFM Name</td>
<td>Packer</td>
<td>Easter</td>
<td>Nadir</td>
<td>Radley</td>
</tr>
<tr>
<td>TFM Name</td>
<td>Tadashi</td>
<td>Halle</td>
<td>Ogechi</td>
<td>Kalisha</td>
</tr>
<tr>
<td>End User DOB</td>
<td>20/01/1983</td>
<td>25/02/1996</td>
<td>08/04/2001</td>
<td>12/07/1956</td>
</tr>
<tr>
<td>SFM DOB</td>
<td>09/11/1957</td>
<td>14/02/1992</td>
<td>19/01/1977</td>
<td>13/01/1999</td>
</tr>
<tr>
<td>TFM DOB</td>
<td>17/05/1983</td>
<td>22/02/1983</td>
<td>18/08/2010</td>
<td>20/02/1984</td>
</tr>
<tr>
<td>End User BG</td>
<td>O+</td>
<td>AB-</td>
<td>A+</td>
<td>O-</td>
</tr>
<tr>
<td>FFM BG</td>
<td>A+</td>
<td>O-</td>
<td>O+</td>
<td>B+</td>
</tr>
<tr>
<td>SFM BG</td>
<td>A-</td>
<td>B-</td>
<td>O-</td>
<td>A+</td>
</tr>
<tr>
<td>TFM BG</td>
<td>B+</td>
<td>A+</td>
<td>AB-</td>
<td>A+</td>
</tr>
<tr>
<td>End User HC</td>
<td>150</td>
<td>160</td>
<td>90</td>
<td>180</td>
</tr>
</tbody>
</table>
The multithreading based system has the support of number of threads. When end users want to upload some data over the server then the data is divided into number of blocks and individual block will be processed by individual threads in parallel. Each thread requires different key pairs generated from key matrices to secure the data over the network. The encryption time analysis, file type, file size, and key pairs are listed in Table 8.3. The encryption time analysis based on multithreading based system is performed in the Table 8.3 with different keys for individual files and have different encryption time in seconds.

**Table 8.3: Number of Data Blocks and Encryption Time Analysis**

<table>
<thead>
<tr>
<th>File Type</th>
<th>File Size (in MB)</th>
<th>Key Pairs K1,K2,K3</th>
<th>Encryption Time (in Sec.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text/Image File</td>
<td>1</td>
<td>K1:bombay_isa_beautiful_city K2:davvis_topgradeuniversity K3:he_loves_to_eat_ice_cream</td>
<td>21</td>
</tr>
<tr>
<td>Text/Image File</td>
<td>5</td>
<td>K1:narendra_modi_will_be_pm. K2:phd_requires_researchwork K3:every_body_must_be_honest</td>
<td>125</td>
</tr>
</tbody>
</table>
8.6 SUMMARY

The integrated secure framework for business processes has been developed and tested in this chapter. The integrated framework secures data communication over the network from unauthorized users. The layered architecture of integrated framework is also illustrated. The layer architecture consists of various layers such as, load sharing layer, broker’s layer, security layer and business process layer. The load sharing layer and broker layer assists business processes to avoid heavy load on UDDI. The central broker categorizes incoming requests according to different application domains.

In proposed integrated secure framework, end users have to pass the phase II of authentication before accessing their credentials. The phase II of authentication mechanism requests for selecting the right pattern generated by the system. The business processes route the incoming requests and responses between the service consumers and service providers. The end users can use the integrated framework to upload and download their important data on/from the server in a secure manner with the help of multithreading system. Each file uploaded or downloaded from and to the server is encrypted with different key pairs in three different stages of ENC, DEC, and ENC. Similarly the data block is decrypted with different key pairs in three different stages of DEC, ENC and DEC.