CHAPTER 9
CONCLUDING REMARKS

The thesis covers research work on a framework for cryptographically secure web service composition with the help of business processes over the network. The proposed framework provides security interfaces, introduces broker’s layer to reduce the load of UDDI, applies multithreading based secure algorithm with the concept of key matrices and establishes two phase authentication mechanism. The conclusion of the presented research is summarized in the following paragraphs.

Various literatures on web services and service composition mechanisms along with their merit and demerit have been discussed in Chapter 2. There are several composition techniques such as, iterative, sequential, parallel and choice composition. Web service composition mechanism is discussed with its types such as, static composition and dynamic composition. The comparative study of various methods for static composition such as, orchestration and choreography has been also explained. There are various composition languages unveiled and compared such as, business process execution language, ontology web language, web service choreography interface, business process management language and web service choreography description language on technical parameters. Each composition language discussed has its own setting, architecture and scenario. The design goals of composition languages and different composition tools are also discussed and evaluated in this Chapter 2.

The proposed secure framework constructs environmental surroundings secure for business processes over the network and prevents intended audiences from unauthorized access as presented in Chapter 3. The secure generalized framework for web service composition is proposed and evaluated. The literature study has
provided information to create the security interfaces around the business processes. This kind of protection through security interfaces provide secured data transfer over the network. The diverse components of proposed secure framework possess on important parameters such as, roles, responsibilities and their coordination with each other. The proposed secure framework secures the business processes in numerous application domains on the internet as well as constructs secure interaction such as, entertainment, banking sectors, e-commerce etc. The working example illustrates proposed secure framework throughout real time frame scenario. The end user finds set of involved pictorial representation supported inside working example that assist audience to be able to better understand the system. The framework builds the environment secure for business processes, so that the business processes easily fulfill business demands and prevent end users from attacks.

Chapter 4 focuses on the expansion of security interfaces as ENC module (encryption module) and DEC module (decryption module). The ENC and DEC modules are formulated through the Caesar Cipher technique. The description of business processes with algorithmic approach has explained in this chapter. The proposed algorithmic representation on service consumer and service provider ends have been tested and discussed.

The broker based secure web service composition has been illustrated and examined in Chapter 5. This chapter targets on introducing broker’s layer, which is accountable for managing the group of brokers and minimizing the UDDI load by load managing activity. The brokers are classified in a manner that each broker is liable for responding the varieties of application domain requests. The algorithmic outline of complete process has also demonstrated in the current chapter. The algorithmic rendering illustrates the step-by-step procedure of recommended broker based mechanism for secure web service composition. The experimental evaluation has been performed
using the example of business processes. The comparative analysis is also performed for broker based and broker less environment and their effects. It is observed that broker based mechanisms are faster in response as compared with this broker less mechanism. The graphical representation associated with research has discussed for broker based versus broker less architectures with different key parameters such as, volume of web services, response time and type of composition mechanisms.

The multithreading based secure algorithm for business processes has developed and tested in Chapter 6. This chapter targets on providing high security to business processes within the network by bringing out an algorithm, which has rapid encryption along with decryption time period because of multiple thread support. In addition, the algorithm has support of key matrices, which produces the key pairs randomly for different data blocks. The algorithmic representation on sender along with receiver side is also described in the current chapter. The experimental evaluation on encryption time period with regard to triple DES along with MBSA algorithms possess studied on several important parameters such as, file size and file type. The graphical representation represents that MBSA algorithm is much faster and secure as compared to the triple DES algorithm.

The pattern based authentication mechanisms for secure business processes has been designed and illustrated in Chapter 7. The chapter presents pattern based phase II of authentication mechanism, where pattern generation process generates the pattern randomly and the end user has to select the right pattern. The comparative study associated with existing authentication mechanisms has explained based on important parameters such as, authentication time, authentication type and memory storage requirements. There are various authentication types for different authentication mechanisms, exists such as, text based, graphic based, matrices based and color based but the proposed system has pattern based authentication type. The pattern
based authentication mechanism is usually fast and hard to break. The memory storage can be high pertaining to several authentication mechanisms but proposed system requires very less memory storage. There are various authentication mechanisms exists in current scenario, which doesn’t have robustness, accuracy, easiness but reliable in addition to confidentiality. The proposed phase II of authentication mechanism as compared with existing mechanisms has good accuracy, easiness, reliability and confidentiality.

The integrated secure framework for business processes has been evaluated using the working application of file uploader and downloader inside the Chapter 8. The file uploader along with downloader application assists the end users to add their critical, private, and important data or contents including, text files, audio tracks, video files in the server in secure manner. The insecurity prevails in current scenario due to hackers, crackers, trojans, worms and so forth. The developed secure integrated framework protects end users from all kinds of thefts mentioned above. The users’ contents can be secured over the network in the uploading and the downloading processes because of introducing the security layer and multithreading based secure algorithm. The multithreading based secure algorithm builds the device secure by using key matrices, exactly where key pairs is actually generated randomly. The proposed load sharing layer and broker’s layer are supportive to business processes in order to avoid heavy load in UDDI. The central broker categorized the incoming requests much like the different application domains. The authorized users at other end must successfully processed the phase II of authentication. The phase II of authentication mechanism requests for choosing the right pattern generated from the system depends on the user’s fundamental and personal facts.

Finally, security requirements are the essential activity for design, development and deployment of business processes over the network to fulfill the business needs. In this research, different
security requirements around the business processes have been discussed, evaluated and tested. The proposed secure framework for business processes helps intended audience to be secure in web service composition. These business processes can be constructed using web service composition operation.

Further, the business processes have support of load sharing layer, multithreading based secure algorithm and new proposed authentication mechanism. They can collectively build the complete business processing fast in execution and secure in fashion. Our contribution unlocks further possible research in the field of business processes and it can be explored in the following areas.

- The business processes have limited native support for authorization mechanism, which is one of basic fundamental of security.
- The business processes have partial support for digital signature mechanism. The digital signature is a mechanism for validating the end users in terms of security aspects.
- The business process requires automatic security method selection approach to improve the existing performance overhead.
- The business process based workflow designs require automatic security configuration mechanism to protect end users from unauthorized access.
- The business processes are also lacking into query processing to expose the state of execution processes in secure manner.