CHAPTER VII

CONCLUSION

In this chapter, conclusion of the presented thesis based on the SuVa Security Framework is discussed and presented. In the end, the future scope of this project is described.

7.1 OVERALL CONCLUSION

After cloud computing has emerged, security threat has been increasing every year. Lot of techniques are emerging to address the security challenges found in cloud environment. Nevertheless, several approaches towards security in conventional IT environment were not efficient and successful in the cloud environment. Hundreds of tools are already available in the market for vulnerability assessment. Though these tools are effective in finding the vulnerabilities in the traditional environment, it is not fully successful in the cloud environment due to the cloud characteristics like virtualization besides more on reactive mode. Security has been challenging with the complicated dynamic approach of cloud architecture.

In the present scenario, cloud has introduced a SaaS (Security as a Service) which has lot of functionality to provide security to its customers. The cloud infrastructure uses virtualization technology, it is possible that, it is shared by multiple users, multiple organizations invariably not depending on the location. The customer’s data which exists in cloud infrastructure (depending on the service they use) is scanned for the vulnerabilities and/or security threats in the cloud environment in a post migration scenario. This is a major challenge, because the vulnerability or threat which exists in customer data can be easily transferred among customers who exists in cloud environment, thereby it infects the whole cloud infrastructure. This issue is mitigated by the SuVa Security Framework which is deployed in the cloud computing infrastructure as a gateway and thus all the data which are migrated to cloud while on-premise to cloud migration is safely transferred.

7.2 RESEARCH CONTRIBUTION BY SUVA SECURITY FRAMEWORK FOR CLOUD MIGRATION

In the chapter 3, the SuVa Security Framework’s core design is explained in detail. SuVa Security Framework to be deployed in cloud framework as a gateway through which the
data, web applications, storage, etc., are been transferred to cloud. SuVa Security Framework makes sure that the secured data are moved to cloud during on-premise to cloud migration. Objective of SuVa Security Framework is explained clearly with the overview of where the framework exists in cloud computing architecture.

SuVa Security Framework’s introduction session presents the core design of the framework under security module platform with explanation of layers namely; IT management layer and security management layer. Under both layers six core modules exists, three modules under each layer in higher level. In IT management layer, there exists modules namely; business logic, workflow and scheduler. Under security management, three modules presented namely; scan engine (network scan, host scan and web application scan), validation and report engine. Further, an execution work flow is presented explaining how this framework can be executed.

Functional layers of SuVa Security Framework are described namely; presentation layer, Business Layer, Programming Layer, Data Layer and Network Layer. System architecture of SuVa Security Framework, back end components are presented and inter relation is explained in detail and how does it is connected to the front end is presented. Detailed description of business logic module is explained with the factors to be considered while defining the business logic. In work-flow and scheduler module Choudhary et al. [2016], Shishira et al. [2017], a work flow of execution is presented explaining how the business logic initiates the flow to the work engine and scheduling Panwar and Rauthan [2017], Rani and Babu [2016] and Tawfeek et al. [2013] and Vashishth et al. [2017] takes place. Scan engine module is presented with its simple scan engine architecture with the vulnerability assessment process of SuVa Security Framework.

In chapter 4, SuVa Security Framework’s assessment is carried out by four different scenarios to discover the vulnerabilities exists in the organization’s data which is being migrated to cloud computing infrastructure. These four scenarios are conducted on the basis of (a) Operation Systems based (b) Web application based (c) Network based and (d) Network and Web application based. For all these scenarios vulnerability assessment is executed and various types of reports are presented. In chapter 5, SuVa Security Framework is validated by executing the penetration testing. Two scenarios have been taken in this validation process. For the both the scenarios first the vulnerability assessment is carried out. From the results derived from the vulnerability reports, certain vulnerabilities are selected to execute the penetration testing. Thus, selected vulnerability where been performed for exploitation.
In the end, penetration test reports are presented with remediation reports. Thus, the SuVa Security Framework is validated.

7.3 MERITS OF SUVA SECURITY FRAMEWORK

SuVa Security Framework pro-actively initiates the scan process for vulnerability assessment and penetration testing of on-premise data before migrating the data on to the cloud. By implementing SuVa framework, pro-actively it excludes the vulnerabilities and threats moving on to the cloud environment. In other words, the organization is presented with the vulnerability and the threats found in their infrastructure. The SuVa Security Framework is reliable, as it verifies the data before the commencement of data outsourcing. The architectural framework of SuVa includes various scan tools for performing the vulnerability assessment and penetration test. Options can be provided to run the penetration testing automatically once the vulnerabilities are found. Results, thus delivered validates with the list of vulnerabilities found in the on-premise’s data. Reports are tailor made and the output of reports can be delivered in various file formats such as .txt, .csv, .html, .xml, .pdf. Moreover, the report can be filtered with respect to severity and priority.

The proposed security framework detects the vulnerabilities being present in the premise data in a proactive fashion. This idea is beneficial to the cloud computing environment, as the data is scanned before the start of data outsourcing. The proposed SuVa framework detects different vulnerabilities and the report is shared with the data owner and the cloud provider as well. This in turn increases the Quality of Service (QoS) and reliability of the security framework.

7.4 LIMITATIONS OF SUVA SECURITY FRAMEWORK

SuVa Security Framework is a complicated architecture which integrates various tools and technologies to achieve its purpose. Due to its complexity, full implementation of SuVa Security Framework costs in millions, considering combining the vulnerability assessment tools penetration tool and it is business intelligence areas in the cloud architecture. Results parsing and reporting also takes considerable amount of cost and technologies knowhow.
7.5 FUTURE ENHANCEMENTS

There is lot of challenging in coding and deployment of SuVa Security Framework in cloud infrastructure. This will be taken as the continuation of the future enhancement and further exploratory study of SuVa Security Framework. Since the complexity of architecture of SuVa Security Framework and Cloud Computing Architecture it is challenging to combine all the three types of scan under one tool. This is challenging and taken for the future study enhancement. Parsing the results which are output from the scan tool can be more tailor made and leave this to the further research studies. In the end, need to find out good solution with less cost involved.