CHAPTER 3

SYSTEM ARCHITECTURE

The overall system architecture for Intelligent Intrusion Detection and prevention system for Cloud databases proposed in this research work is shown in Figure 3.1.

Figure 3.1 Framework for Intelligent IDS
3.1 CLOUD ENVIRONMENT

Cloud environment is as top of all subsystems and provide the information for all other modules. It contains the cloud data set and cloud server with in this environment. The cloud server has two components cloud database and cloud database manager.

3.1.1 Cloud Dataset

The CIDD (Hisham 2012) is the cloud data set used here to train the database in cloud server. It contains all columns of the normal user’s data and intruder’s data. This data set has been prepared and used for intrusion detection in the literature as a benchmark data set. By using this dataset we train the cloud database available in the cloud server.

The some other data sets such SEA, Greenberg, etc., are available for detecting network IDS but they are deal with normal attack of windows users. Cloud Intrusion Detection Dataset (CIDD) that is the first one for cloud systems and that consists of both knowledge and behavior based audit data collected from both UNIX and Windows users. With respect to current datasets, CIDD has real instances of host and network based attacks and masquerades, and provides complete diverse audit parameters to build efficient detection techniques. The final statistic tables for each user are built by Log Analyzer and Correlator System (LACS) that parses and analyzes user’s binary log files, and correlates audits data according to user IP address(es) and audit time.

3.1.2 Cloud Database

This is the one built from the users data like log files which contains users ip address, usage time in system, kind of usage (data usage,
internet users, etc.,) and their signatures. Database also includes the previous decision taken on this user by the cloud server when they access the data from the public cloud databases.

3.1.3 Cloud Database Manager

The database manager is the module taken the decision on the user to access the cloud environment with the help of intelligent decision manager. The database manager gets the intruders features from the cloud dataset available in the cloud server. It also gives the features of the user to the user interface module to avoid the intruders to enter into the public cloud environment. There is any new intruders are identified from the database then it will be updated in the cloud dataset.

3.2 DATA COLLECTION AND USER INTERFACE MODULE

The user enters into the cloud through this module and the details of user will be updated in both cloud dataset and cloud server. Once the user given their details in to the user interface module, the details is given to the cloud server and to check whether there is any details already for the user in the database otherwise the new id is created and make that user as cloud user. The feature of the user is also extracted form the CIDD dataset and passes it to the IDS to taken the decision on the user.

3.3 INTRUSION DETECTION SUBSYSTEM

This subsystem consists of two modules, one is data pre-processing module and other one is classification module.

3.3.1 Data Pre-processing Module

Pre-processing includes the selection and deduction of features from the set of features. This module uses Genetic algorithm (GA) and
Discrete Particle Swarm Optimization (DPSO) algorithm in combined way to select the feature which is want to detect the intruders. Genetic algorithm is used to calculate the fitness value of the feature and to generate the new feature by apply cross over among the available feature. PSO is used to form a group of feature which is really I need to detect the intruders.

3.3.2 Classification Module

The classification module used as a hybrid multiclass classifier with the combination of Naïve Bayes and Intelligent Agent based Support Vector Machine (IASVM). In this module, Naïve Bayes classifier uses the conditional probability for effective decision making algorithm relaxes the conditional probability. The classifier also used to form intelligent rules which are used for classification of intruder’s types and its threat levels. IASVM is act as classifier which used intelligent agent for achieve better detection accuracy. Euclidean distance is used to measure the intruders features and it also helps to reduce the execution time for classify the intruder. It also achieves the better detection accuracy through binary decision tree using the intelligent agents.

3.4 PREVENTION SUBSYSTEM

This subsystem again includes two modules within that called encryption/ decryption module and key management module.

3.4.1 Encryption / Decryption Module

In this work, a new encryption / decryption algorithm has been proposed by extending the Vigenere cipher to include numbers after alphabets. This algorithm is used to encrypt the sensitive data before it is stored in the database. When a user with a valid key is providing a query, this
encrypted data are displayed after decryption. The main advantage of this proposed work is that the intruders cannot copy the sensitive data and use it for malicious activities.

### 3.4.2 Key Management Module

In order to enhance the security of cloud, it is necessary for data owners to verify the data stored in public cloud. Moreover, to verify the integrity of the data stored in a public cloud, a public verification method is proposed here that verifies the data stored in the public cloud is needed. In order to achieve this goal, an authentication scheme is proposed in this work. This ensures security and at the same time reduces the computation complexity of the data owner or a client who needs to verify the data. This work supports efficient and dynamic data operations namely block modification, insertion and deletion of the data stored in the public cloud along with multiple data verification operations. So, a new Computation efficient batch Digital Signature generation and verification Algorithm called as Computation Efficient DSA (CDSA) is proposed in this work in which the computation time for signing and verification operations are reduced when compared with the existing algorithms. The proposed scheme achieves efficiency in terms of computation time both in client sides and data base side. This method has been implemented in the cloud environment and the efficiency of the proposed scheme is compared with the existing schemes and it is found that computation complexity has been decreased significantly.

### 3.5 INTELLIGENT DECISION MANAGER

The Intelligent Decision Manager (IDM) is act as a brain for overall system framework. The decision manager with the help of intelligent decision tree classify the given user data into intruders and masquerade attackers or normal users. The decision tree proposed here uses a general naïve bayes
classifier for initial classification of data set. Later it acts as an intelligent agent who classifies the data. The classification is done by an intelligent agent for making decision on data. Once the agent examines the data of users, decision is taken on users by verifying the signature of the user. Once the signature is verified the decision should be whether the user should allow inside the public cloud or not.

3.6 KNOWLEDGE BASE

This is the module where the previous information of the users usage in the cloud environment is maintained. Decision manager is make a directly contact with the knowledge base to retrieve the information about the users. It also contains the signature information about the users and used when the intelligent decision manager sends the request.

3.7 CONCLUSION

In this chapter, the architecture of the system proposed in this research work is depicted and explained. This architecture is helpful to understand the various modules of the proposed system. The major components of this system include the proposal of the decision manager, database manager, IDS module, key management module and the encryption/decryption subsystem. The major advantages of the proposed architecture over other architectures is the provision of multilevel security using IDS and key management.