CHAPTER 3

SYSTEM ARCHITECTURE

3.1 OVERALL SYSTEM ARCHITECTURE

The overall architecture of the proposed security system with major subsystems namely Intelligent Access Control Subsystem and Intrusion Detection Subsystem for securing the web databases proposed in this thesis is shown in Figure 3.1.

Figure 3.1 Overall System Architecture
It consists of seven different major components namely User Interface, Web Server, Security Manager, Access Control Subsystem, Intrusion Detection Subsystem, Web Database Manager and Web Database.

The Access control subsystem consists of seven sub components namely, Access control management agent, STRBAC manager, Role Base, Spatio-temporal information management agent, Spatio-temporal constraints base, Rule management agent and rule base. These sub components include an access control module to assign user to roles and to assign privileges to the roles based on constraints and to limit the access. The Intrusion Detection subsystem consists of five sub components namely Input Data Set, Preprocessing, outlier detection module, classification module, decision making and action agent. These components are responsible for detecting intrusions that attempt to intrude the system in order to access the web database.

3.2 USER INTERFACE

The User Interface component of the proposed system is responsible for sending data requests and to receive the responses from the web database. It accepts queries in the form of key words. In addition, it provides special menus and forms through XML based and SQL based queries can be submitted.

3.3 WEB SERVER

Web server is an important component of the proposed system. It acts as a mediator between the user interface and the rest of the system. Its main duty is to receive the request from the user interface, process it and send it to the security manager. It is also responsible for sending the responses coming from the web database manager through the security manager to the
interface. It maintains web logs to store the browsing pattern of users. Therefore, the web server module takes care of maintaining cookies at the clients and also performs session monitoring.

### 3.4 SECURITY MANAGER

The security manager plays an important role in the proposed system. It acts as a mediator agent between the web server and the web database manager. It has a set of intelligent agents which are useful for decision making. One of the major responsibilities of the security manager is its functionality in providing effective security by interacting with the Intrusion Detection Subsystem and the Access Control Subsystem. Whenever a response is received by the security manager from the Intrusion Detection Subsystem, it decides whether the request has to be sent to the Access Control Subsystem or not. If the Status of the response is not an intruder, then it passes the request to the Access control Module for further process.

### 3.5 INTRUSION DETECTION SUBSYSTEM

This Intrusion Detection subsystem uses a Hybrid Intelligent Agent Based Approach to classify a pattern as normal or intrusive. This subsystem uses a rough set and fuzzy rough set based algorithms for feature selection. In addition it uses new classifiers developed by enhancing the C4.5 algorithm with fuzzy rough sets and SVM to improve the detection accuracy. Moreover, it uses a fuzzy rough set based outlier factor to minimize the false alarm rate. This subsystem consists of many sub components including input data set, preprocessing module, outlier detection module, classification module with agents and decision module.
3.5.1 Input Data Set

In this work, two types of input data sets have been used for the implementation of the Intrusion Detection system. First, the KDD cup data set is used as the input data set while the intrusion detection algorithms have been developed and tested. Later, the web log data were used as the input data set to the same algorithm in order to detect the intrusions which attempt to tamper the web database.

3.5.2 Preprocessing Module

In this module, preprocessing is used to select features from the KDD cup data set and the web log data. This enables to build effective classification models. Moreover, the selection process is helpful to determine a minimal feature subset by eliminating useless features. This is necessary to enhance the accuracy of intrusion detection and to increase the computational speed. This module uses a feature validation and ranking agent that utilizes a fuzzy rough set approach to perform effective selection of minimal subset.

3.5.3 Outlier Detection Module

The outlier detection module uses classification techniques in order to classify the attacks effectively. Therefore, a rough set based outlier detection algorithm that uses a fuzzy rough membership based outlier factor to improve the detection accuracy.

3.5.4 Classification Module

This module is used to classify the web log data using fuzzy rough set based C4.5 and SVM classifiers to identify the intruders. It receives the data set from feature selection agent after reduction. It uses only reduced data set for classification in order to reduce the classification time and to improve
the detection accuracy. Further to improve the detection accuracy, this module also uses the hybrid classifiers to classify the reduced dataset.

### 3.5.5 Decision Module

This is an important subcomponent of the IDS Subsystem. This decision making module uses a decision agent which performs effective monitoring to decide on the type of incoming traffic pattern and to classify them as normal or intruder. The proposed technique allows the system to adapt to web environment. These sub components cooperate and coordinate together to detect an intrusion in a loosely coupled way. This module uses a set of intelligent agents namely the intrusion detection agent, decision making agents and action agents to make a final decision.

### 3.6 THESIS CONTRIBUTIONS

The Intrusion Detection Subsystem proposed in this work uses new intelligent decision making techniques using intelligent agents to classify a pattern as normal or intrusive and to take suitable preventive actions on intrusions.

In this work, the Intrusion Detection subsystem utilizes anomaly detection techniques for classifying a pattern as normal or intruder. This subsystem utilizes fuzzy rough sets for feature selection and to compute outlier factor. Moreover, fuzzy rough set is used to perform decision making in the decision tree algorithm. When outlier detection is combined with classification algorithm it improves the detection accuracy and reduces the false alarm rate.

In this work, two classification algorithms have been used for effective classification namely, Fuzzy rough set based decision tree algorithm
and Support Vector Machine (SVM). Moreover fuzzy rough set based outlier
detection algorithm is proposed as first level detection technique and then the
result is passed on to the classification algorithms for effective classification.

3.7 ACCESS CONTROL SUBSYSTEM

3.7.1 Access Control Management Agent

The Access control management agent, a component of the access
control subsystem receives the request from the security manager and
validates the request using the subcomponents namely the rule management
agent, spatio-temporal role based access control manager and spatio-temporal
information management agent. These three components use three storages
namely rule base, role base and spatio-temporal constraints base. The main
aim of this component to achieve is assigning privileges based on spatial,
temporal, constraints to limit and manage the access to the web database.

3.7.2 Spatio-Temporal Role Based Access Control Manager

The spatio-temporal role based access control (STRBAC) manager
is widely used for access control management through the validation of roles
with respect to location and time for users since authorizations are specified
with respect to individual users. The main notion of this module is that
permissions are associated with spatio-temporal roles and users are assigned
to appropriate spatio-temporal roles by this component. This greatly enhances
the security of the system.

3.7.3 Spatio-Temporal Information Management Agent

The main duty of spatial temporal information management agent is
to receive the spatio temporal constraints from the spatial temporal constraints
base and provide to the RBAC module for assigning user to role and
permission to role so that it is possible to limit user access to the web database.

### 3.7.4 Rule Management Agent

The rule management agent is capable of providing rule matching and rule firing techniques, so that accuracy level is increased. The rules can be obtained from rule base, which consist of set of rules.

### 3.8 WEB DATABASE MANAGER

In this work, Web Database Manager Component receives the decision of the Access Control Subsystem and permits only authorized users who have been assigned with assigned permissions to access the web database.

### 3.9 CONTRIBUTIONS IN ACCESS CONTROL

The Access Control Subsystem utilizes Intelligent agent based Techniques by allowing separate agents for managing spatio-temporal rules. Moreover, it uses separate rule matching and rule firing algorithms for managing spatio temporal constraints.

This System also utilizes a modified conflicts detection algorithm to identify conflicts that might occur between multiple permission assignment in order to ensure the privacy issue.

Using all these constraints, access has been restricted to the unauthorized users and only authorized users are allowed to access the web database with limited privileges.