CHAPTER 3
SYSTEM ARCHITECTURE

3.1 INTRODUCTION

The overall system architecture of the Hybrid Intrusion Detection System proposed in this research work is shown in Figure 3.1. The proposed hybrid IDS with collaboration is effective in terms of detection accuracy and detection time. This proposed hybrid system consists of two major subsystems namely the Data Preparation and Collaborative Hybrid Intrusion Detection System. The subsystems in this hybrid system consist of subcomponents such as Feature Extractor, Misuse Detection System (MDS), Anomaly Detection System and Collaborative Intrusion Detection Network.

![Figure 3.1 Overall System Architecture](image-url)
3.2 DATA PREPARATION

This subsystem is used for effective data selection to enhance the performance of the intrusion detection system. It contains the feature extractor component to extract the required features from KDD CUP 1999 Dataset for the process of intrusion detection. The dataset has been formed out of the selected features and the reduced instances of the KDD CUP 1999 Dataset for classification. This dataset is divided into two sub-datasets. In one sub-dataset, class labels have been removed and are given as input to unsupervised anomaly intrusion detection. The second sub-dataset is supplied as input to the trainer in the supervised misuse intrusion detection, which has the class label. Audit Trails Dataset is taken as an input to the host-based hybrid intrusion detection system. In this, user profile has been considered and set of user behavior (behavior-set) is given to this detection system.

3.2.1 Feature Extractor

The Feature Extractor subcomponent extracts the relevant features (feature selection) from the database using efficient data pre-processing techniques namely Genetic Algorithm, Incremental Support Vector Machine and Discriminant Analysis according to the type of intrusion detection used in the system. If the features extracted are carefully chosen, it is expected that the feature set extracts the relevant information from the input data in order to perform the desired task using this reduced representation instead of the full size input. Then, the refined dataset is classified into training dataset and test dataset. Training dataset is used to train the system by using effective classifiers and test dataset is given to the classifiers for classifying them as normal and abnormal patterns.
3.3 COLLABORATIVE HYBRID INTRUSION DETECTION SYSTEM

This subsystem is employed for detecting the unseen intrusive patterns from the network traffic data or audit trail data. It contains the subcomponents namely Misuse Detection System, Anomaly Detection System, Collaborative Intrusion Detection Network and Administrator. The misused detection system and anomaly detection system constitutes a hybrid intrusion detection system. The identified known and novel attacks are directed to the Administrator who raises the alarm as well as takes the appropriate actions for preventing the system.

3.3.1 Misuse or Signature-based Detection System

Misuse Detection System or Signature-based IDS employs a priori knowledge of attack signatures. The signatures are manually constructed by security experts analyzing previous attacks. The collected signatures in the attack signature database are used to match with incoming traffic to detect intrusions. Whenever incoming traffic goes out of the normal profile, anomalous system behavior is identified. In this research work, the effective classifiers are used to classify the data as normal or unseen attacks. Such classifiers used in this misuse detection system of the hybrid intrusion system are Reserved Set-Incremental Support Vector Machine with Genetic Network Programming, Fuzzy Class-Association Rule Mining and Pattern Matching for the source data of network or host.

3.3.2 Anomaly Detection System

Anomaly Detection System treats any network connection violating the normal profile as an anomaly. A network anomaly is revealed if the incoming traffic pattern deviates from the normal profiles significantly.
Through a data mining approach, anomaly detection discovers temporal characteristics of network traffic. This system can detect unknown attacks and handles multi-connection attacks well. In this research work, the supervised and unsupervised algorithms are used to detect unseen or novel attacks. The signatures of such detected attacks are generated and stored in the attack signature database for future detection which will act as misuse detection. The data mining algorithms for anomaly detection such as an Enhanced Self-Organizing Map, Minimum Spanning Tree-based Genetic Clustering and Canopy and K-Means Clustering have been implemented to detect unseen attacks.

3.3.3 Collaborative Intrusion Detection Network

The collaboration framework is built around the IDS component. Collaborative Intrusion Detection Network framework connects Hybrid IDSs to form a collaborative network, in which each Hybrid IDS is free to choose the node or network with which to collaborate. When a Hybrid IDS detects suspicious behavior but lacks expertise to make a decision whether it should raise an alarm, it may send requests to its acquainted Hybrid IDSs for consultation. Feedback from the acquaintances is aggregated and a final decision can be made based on the aggregated results. The alert information provided to acquaintances depends on the trust level of each acquaintance. In this research work, a Dirichlet-based trust management algorithm is implemented to achieve Collaborative Intrusion Detection Network which actively detects the anomalies and confirmed attacks are reported to the administrator.

3.3.4 Administrator

The Administrator receives outputs from the above detection systems and reports them to the user through different means like Graphical
User Interface (GUI), log files or email. The significant role of the administrator is to react to the detected intrusions in order to prevent future damage. The active responses like dropping the connectivity of the potential attacker or even counter-attacks. A response may be triggered automatically or manually via the user interface. This kind of response will be taken care by Intrusion Prevention System.

3.4 THESIS CONTRIBUTIONS ON SYSTEM ARCHITECTURE

The key contributions of this research work with respect to the system architecture are the proposal of a hybrid intrusion detection system which comprises a misuse detection system and anomaly detection system with effective collaboration. In this work, the effective data mining techniques have been employed in extracting relevant features as well as in classifying known and unknown attacks from normal patterns. Finally, this proposed system achieves a high detection rate and low false alarm rate in comparison with the existing individual and hybrid IDSs.