Due to change in the technology thrives, there are constantly increasing number of internet users. Therefore, the information system security is becoming a raising concern. The quick addition in connectivity and accessibility of computer systems are becoming ever more susceptible to intrusions, misuses, and attacks. Developing flexible and adaptive security oriented approaches are cruel challenge causes of with novel types of attacks appearing continually. Organizations grow more vulnerable to be extra susceptible to a broad range of threats that aspire to rupture confidentiality, integrity and privileges of network resources. There are a lot of sources of threat including software bugs. Important and confidential information belonging to network users is abstracted by the illegal user (Intruder). Even though the recent security solutions have their significant roles in protecting organizations, they do not offer the precise protection against the sophisticated threats of today’s cyber-criminals. To stop the committed attacks, by isolating these networks by firewalls put in between two or more computer networks. But these firewalls are not sufficient to protect a network totally because the attacks committed from inside the network could not be stopped. Intrusions detection systems IDSs are designed to resolve this problem. The general approach pursued in network intrusion detection system is an examination of patterns of user’s activities within log and usage files.

The numbers of intrusion detection systems have been built by manipulating the recognized attack and misuse patterns. The intrusion detection systems make use of diverse techniques both anomaly and misuse intrusion detection. There are diverse techniques to recognize anomalies. Several are based on methods of forecasting future patterns of behaviour using patterns, and others exercise statistical approaches to establish anomalous behaviour. Whatever happens the behaviour that does not communicate with expected behaviour would be an intrusion. In intrusion detection, the computer attacks are identified by inspecting data records monitored by processes on the same network. The Network attacks are spitted into three categories, host-based attacks,
network-based attacks and specification-based attacks. Host based attack detection approach uses system call data from an audit process that tracks all system calls made on behalf of every user on a specific computer. These audit processes typically run on every monitored machine. Network-based attack detection approach employs network traffic data from a network packet sniffer. Specification-based attacks, this type of detection systems are accountable for supervising the processes and matching the real data with the program. Any abnormal behavior will be issued an alert at any instance must be maintained and updated where a modification was made on the observation programs.

The conventional signature-based intrusion detection systems (e.g., antivirus, firewalls etc.) that detect known attack vectors in any contrast to the anomaly-based intrusion detection system detects deviation from normal behavior, thus having the desirable property of detecting novel or zero-day attacks. In this thesis, hybrid network intrusion detection system anomaly detection system and misuse detection system are a valuable technology it is helping to guard target systems and networks against malicious activities and attacks by using multi-agents via Jade. On the other hand, in spite of the variety of such methods illustrated in the literature in recent years, but incorporating security tools anomaly detection functionalities with misuse detection are initiating to emerge , and numerous significant problems remain to be solved. The primary objective of this thesis is to evaluate the hybrid network intrusion detection with multi-agents. The first step is to make an analysis and an assessment of the environment in which the system is going to deployed; in this case the (NIDS) will be aimed at analyzing traffic generated by multi-agents and Java expert system shell Jess and snort rules. We review in this thesis the most NIDS techniques and types of multi-agents and roles of Java, snort rules, Jess, adaptive threshold algorithm and decision support system DSS. Then, available platforms systems under development and research projects in the area are presented. Chosen techniques are implemented in the testing environment.

And then determine the outline the main challenges to be dealt with for the wide scale deployment of hybrid NIDS based network intrusion detectors, with special emphasis on analysis and assessment of results finally, for providing more flexible and real-time protection. A network intrusion detection system NIDS is gaining ever increasing importance in security of information from network attacks. For better system
performance and reduce response time an improved NIDS system is proposed design hybrid NIDS anomaly detection system and misuse detection system with distinct agents in a multi-agents-based intrusion detection system. This system is being implemented in Jade, a well-known multi-agents platform based in Java. In this system, the misuse detection system is achieved by using misuse detection includes various agents like detection agent, central agent and analysis agent who include (conversion agent, response agent, alarm agent, user interface agent, and registration agent). In this design, we using Java expert system Jess and snort rules, the purpose of this software to pattern matching by Rete algorithm to detect attacks and completed the cycle of multi-agents to send the message to alert the user interface agent to take some actions about this alert. The detection agent analyses the packets in the network connections using a packet sniffer and then creates knowledge base based on the information obtained. This knowledge base is the facts to convert into a rule Jess-based inference rule engine with snort rules after convert into Jess rules, which uses the Rete algorithm for pattern matching.

In this project, anomaly detection system is achieved by using anomaly detection includes various agents like (information agent, sensor agent, statistic agent, decision agent) to interacted between them and with adaptive threshold algorithm to detected unknown attacks and determine normal and abnormal behavior. In this system, we using decision support system DSS for provide a final report to estimate the results each of the misuse detection agents and anomaly detection agents. And send the report to the user about events that occur within the system. The proposed system is simple and light weight with flexibility and effectiveness when thus utilizing multi-agents into the improved hybrid network intrusion detection system, enhances the performance and reduce response time yet achieves higher accuracy and broader spectrum of protection from different types of intrusion attacks with an attempt to detect false alarm rate for both misuse detection and anomaly detection. Additionally, the knowledge base and updating of rules library maintains the system at highest possible security from known as well as unknown network intrusion attacks.