ABSTRACT

Cloud computing systems enable the customers in using a lot of resources and computing facilities through Internet. Cloud systems attract many users with their desirable features. With the uninterrupted improvement of cloud technology, cloud computing attracts many intruders in and around cloud environment. This issue necessitates in developing a malware detection component to protect cloud from any unwanted activities that can harm cloud resources and services.

Therefore, to suit the dynamic nature of cloud environment, a hypervisor based malware detection component is developed by using different soft computing techniques. This thesis encompasses two different modules that are used to detect Service Level Agreement (SLA) violations and anomalous activities in cloud systems. The first module named SLA violation detection concentrates on detecting a malicious insider attack and Denial of Service attack (DoS) by applying the detection systems named Hypervisor Scanner and Hypervisor Controller respectively. The second module named anomaly detection focuses on two different systems called Hypervisor Detector-I and Hypervisor Detector-II at hypervisor layer to detect the anomalous activities in cloud systems.

For smooth sharing of services and resources, the cloud service provider enters into Service Level Agreements with every authorized user. Service Level Agreements play an important role in cloud computing. The cloud system with a deceitful management domain suffers from lack of transparency in offering provider experiences to malicious insiders violating SLA. Violation of SLAs is considered as a severe threat. Hence, it is proposed to design a detection

element named Hypervisor Scanner to identify malicious insiders who contravene SLA in untrustworthy systems. The SLA attributes such as Bandwidth requirement, Memory utilization and Storage capacity are considered for the experiments. This proposal develops a Hypervisor Scanner by using Artificial Neural Network (ANN) modeling and Levenberg- Marquardt (LM) back propagation training. The Hypervisor Scanner is simulated and the results show that this model is effective and efficient against malicious insiders' threats. The extensive analysis on the performance shows that the proposed component can determine the malicious insiders with high detection rate and lower false negatives.

One of the major security issues in cloud is Denial of service attack. DoS attack may harm or deny the legitimate users access and affect cloud resources and services deserved for cloud users. The proposed Hypervisor Controller is designed with the mixture of Fuzzy Time Series (FTS) model and Expectation Maximization (EM) algorithm. The Hypervisor controller can progress the performance by iteratively identifying the clusters with maximum probability of EM and analyzing the time interval by using FTS analysis. The Hypervisor Controller is simulated and the performance analysis shows that the Hypervisor Controller can greatly improve the performance by detecting the malware activities in cloud environment with high detection rate and low false negatives.

Besides, the unknown malicious behavior of users may lead to severe threat in cloud environment. Thus, it is essential to build up an anomaly detection system to detect the attacks with high detection accuracy in cloud environment. However, the existing Intrusion Detection Systems (IDS) show low detection accuracy and high false negative values for low frequent attacks such as User-to-Root (U2R) and Remote-to-Local (R2L) attacks. Further, most of the IDS designed in the past are suitable for medium range of datasets.

Therefore it is significant to develop an anomaly detection system suitable for tackling the mentioned problems.

Accordingly, the Hypervisor Detector-I is developed for detecting even low frequent attacks by employing a hybrid approach which is a combination of fuzzy clustering and ANN. To enhance the learning ability of ANN, the fuzzy clustering method is integrated to obtain the integrated technique named FCANN. The proposed Hypervisor Detector-I system is simulated and also compared with the Naïve Bayes classifier, Naïve Bayes and Random Forest (NBRF) and ANN algorithm. The DARPA's KDD cup dataset 1999 is used for experiments. The extensive theoretical and performance analysis carriedout confirms that the proposed system is able to detect the anomalies with high detection accuracy and low false negative rate for low frequent attacks also. The performance comparison results show that the Hypervisor Detector-I outperforms the Naïve Bayes classifier, NBRF and ANN.

Despite its continuous improvement, cloud computing system is still vulnerable to malicious activities due to vast amount of communication that takes place between users and cloud servers. This has necessitated in constructing an anomaly detection component that is suitable to work with very large data values so as to discover the anomalies in cloud environment. Hence, an Anomaly Detection System (ADS) at hypervisor layer named Hypervisor Detector-II suitable for very large datasets is developed and evaluated to detect the malicious activities in cloud environment. Deployment of fuzzy systems in Intrusion Detection Systems (IDS) creates the ability to detect the presence of uncertain and imprecise nature of anomalies in cloud environment. But they fail in constructing models based on target data. One of the successful approaches based on target data is integration of Fuzzy Systems with adaptation and learning proficiencies of Neural Network called Adaptive Neuro Fuzzy Inference System (ANFIS) model. The Hypervisor Detector is designed and

developed with ANFIS and is practiced with a hybrid algorithm which is a combination of back propagation gradient descent technique with least square method. For Hypervisor Detector-II experiments also the DARPA's KDD cup data set is used. The performance analysis and results show that the proposed Hypervisor Detector-II based on ANFIS is well designed to detect the anomalies in cloud environment with minimum false negative rate and high detection accuracy for very large datasets. Based on the results obtained, it is evident that the hypervisor based malware detection component detects the SLA violations and anomalous activities with high detection accuracy and low false negative values.