CHAPTER 7

CONCLUSION AND FUTURE DIRECTIONS

7.1 CONCLUSION

It is proven that cloud computing is growing as a destiny of future enterprise business computing due to its catchy technical and financial benefits. Considering cloud’s exposed public nature, it equally attracts the attention of hackers and attackers, which intersects more severe security challenges and risks to it. On the other hand, the investments made by these Cloud Service Providers are also significantly high. At this point of time, unless CSP’s takes some action, by removing these present security issues/vulnerabilities in reaching more customers using cloud services, they will be in serious trouble. Considering all these facts, this work presents eCloudIDS, a state-of-the-art generic cloud security framework for cloud computing environment which is designed with a next-generation hybrid two-tier expert engine-based intrusion detection system.

As the eCloudIDS experimentation was targeted to be a prototype proof-of-concept (POC), few limitations were enforced into the investigation. Only four crucially commended logs were subjected for implementation on Instance-M. Subjecting more logs can bring a better approach to the system. A big challenge in machine learning theory which was adopted to eCloudIDS is that the unsupervised algorithm technique used takes numerical data for its functioning. All the log files consisted of many non-numeric fields, which may or may not be relevant to identify an anomalous behavior while designing a security system.
Optimal fields may be identified for further exploration in this area. In uX-Engine, SOM algorithm was able to maintain topology of data while clustering and also works on non-linear data-set with excellent capability to visualize high dimensional data. Though SOM was time consuming and had computational complexity, SOM was easy to understand and its outstanding ability to visualize high-dimensional data onto 1 or 2 dimensional space makes it unique especially for dimensionality reduction. On the other hand, for sX-Engine, though SVM consumed training time, the sound mathematical foundation embedded in SVM process provided a very fast evaluation on the targeted function. The prediction was high as the SVM technique worked even when the training sample had some negligible errors. Thus an accuracy of 85% for uX-Engine and 90.3% for sX-Engine which are pretty decent, was achieved.

These results thus effectively proves that the eCloudIDS Generic Cloud Security Framework answers the top three state-of-the-art cloud computing security taxonomies such as logical storage segregation & multi-tenancy security issues (taxonomy #1), identity management issues (taxonomy #2), and insider attacks (taxonomy #3). This architecture can help build greater confidence in small, medium and large businesses in migrating their applications and databases into public cloud environment. For businesses that value security of information, this system will give adequate reassurance that their data is safe and they can rely on CSPs with greater transparency. The eCloudIDS can utilize a variety of advanced machine learning algorithms for uX-Engine and sX-Engine, due to its generic nature. The greater the learning capacity, the greater will be the security.
7.2 FUTURE DIRECTIONS

eCloudIDS Generic Cloud Security Framework can however be improved by integrating host-based firewall technology, as well as other technologies, such as virus scanners and integrity checkers as currently the system is only concerned with providing security on the basis of logs which are maintained by the OS and other applications. The current POC doesn’t provide complete support for protection from all signature-based threats and vulnerabilities, which can be taken for further research.

As per the core nature of eCloudIDS (i.e. Generic), another impending direction is to generalize this prototype to work for other VM operating systems as well. There is a tradeoff between the application’s accuracy and performance. For the intelligent systems of eCloudIDS, i.e. the uX-Engine and sX-Engine, increasing the training data leads to decrease in performance, but at the same time, it will lead to increase in accuracy, leading to better classification of new patterns as attacks. Some more research work is proposed to be done and that will lead to even better generalization.

To populate the training data from the original file, an algorithm of numerical conversion was employed. In future a textual pattern recognizing algorithm can be directly implemented and the results may be analyzed for a better recognition rate.

Currently, the logs for Standard Audit Repository and Acute Audit Repository are stored in a native text format and persisted into a MySQL Database. But, for the application of eCloudIDS in real time, these audit repositories must be capable of handling large scale datasets. Hence concept of Big Data can be brought in to handle large volume of logs.
Along with all these, the other state-of-the-art cloud computing security taxonomies can be experimented with possible permutations of technology and innovation. Thus the eCloudIDS system can be built to be a master cloud security package for CSPs and can be taken forward to emerge as a product that would in turn make Cloud Computing more reliable than what it is today.