Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 200 - 211
Received 05 March 2021; Accepted 01 April 2021.

Discovery of Malicious Intruders in Cloud Environment Violating Service Level Agreements

N Pandeeswari[1]Department of Information Technology, PSNA College of Engineering &Technology.Dindigul.pandeeswari@psnacet.edu.in

K.Sridar[2] Department of Computer Science and Engineering, Veerammal Engineering College, Dindigul.

Sivakami Raja[3]Department of Information Technology, PSNA College of Engineering &Technology.Dindigul.

R.Revathi[4]Department of Computer Science and Engineering, Theni Kammavar Sangam College of Technology,Theni.

P.Rajalakshmi[5]Department of Electrical and Electronics Engineering, Dr.Mahalingam College of Engineering and Technology, Pollachi.

T.Anand Kumar[6]Department of Electrical and Electronics Engineering,Dr.Mahalingam College of Engineering and Technology, Pollachi.

Abstract: Many researchers have carried out lots of analysis for intrusion detection and finding the defense techniques for malicious insiders in cloud systems. Most of the existing works have discussed malicious insiders of cloud systems theoretically. In this proposed work, an Intrusion detection system named Malicious Insider detector (MID) is designed and implemented with artificial neural network (ANN) to detect malicious insiders. This work describes the malicious insiders as who are disobeying the Service Level Agreements (SLA)in cloud IaaS to distress and reject the cloud resources. This system uses bandwidth utilization (BU), memory utilization (MU) and storage utilization (SU) as SLA attributes. In this work, Malicious Insider detector system is simulated and performance is measured.The performance analysis shows that this system efficient, capableto detect the malicious insiders' intimidations. The feasibleinvestigation on the concertdemonstrates that malicious insider detectormoduleis being capable to determine and detect the malicious insiders with high detection rate.

Keywords: ANN**,** Artificial neural network**, c**loud computing, Intrusion detection malicious insiders,

1. Introduction

Cloud computing is the on demand emerging storage and processing innovation that promotes redesigned data innovation through adaptable configuration of assets.Methods for designing an effective resource management technique[12] have also shown that effective resource allocating between multiple customers takes into account power saving, service-level agreements, and network traffic simulation.

A Malicious Insider detector (MID) that can use ANN is suggested in this paper. Each algorithm's concert is evaluated individually to get the algorithm grouping that ensures a resource-effective cloud data center structure. This Malicious Insider detector approach yields

optimized concertbuilt on somecrucialconcert indicators, such as Bandwidth Utilization, Memory utilization and storage utilization for also the entirestructure or the termination-user.

The objective of the proposed method is to detect the malicious insiders [1, 3] abuse the SLA.This paper utilizes three attributes of SLA which uses 1.Bandwidth utilization, 2. Memory utilization and 3. Storage utilization. In cloud systems, the hypervisor layer [15,23] can be designed as a monitoring and control layer that examines multiple operating systems that are running on a hardware platform. The cloud system provides storage resources through the IaaS that make use of cloud virtualization technology. The proposed system aims to design a detection system called as Malicious Insider detector at hypervisor layer, to determine the malicious insiders affecting the cloud resources. This proposed system is developed with artificial neural network (ANN) modeling. The Levenberg-Marquardt (LM) back propagation
supervised learning algorithm) algorithm for ANN is used to train and test the malicious insider detector.

2. Related works

Besides the researches about malicious insider treats, many researchers have established the way to prevent information leakage and reducedamages caused by MIs.But still, the cloud system compliances with security threats. Subsequently, the security threats and risks introduced by the cloud computing system should be clearly identified and understood. Cloud security alliance [11, 21] prepared document for top threats on cloud computing and their implications. The cloud security threats described are datafissures, dataforfeiture, account or service traffic hijacking, Insecure interfaces and APIs, abuse of cloud servicesdenial of service attack, malicious insiders, insufficient due to diligence,shared expertise vulnerabilities.

Many of the existing malware detection system usespacket sniffers,access control [28],key loggers, backdoor analysis [6] to detect privacy breaching malware activities.And also, many researchers have used network profilebased technique for malware detection [26], behavior based malware detection [8, 24], and dynamic analysis system [2, 4] for detecting malware actions in cloud environment.

The authors William et al, [20] discussed insider's threat in three different perspectives and analyses the structure of cloud system. They have described the nature of malicious insider as. 1. Malevolent insider owing to dishonest cloud administrator, 2. The worker in the organization who reveals the private information to others 3.Insider who uses cloud resources to annoy the infrastructures. However, there is no exact solution to detect the attackers.

To protect the cloud environment, most ofthe researchers proposednumerous methods including, a secure virtualized architecture [15], architecture for insider threat security reference (ITSRA) [18] and architecture named as CSAViD (Cloud Application SLA Violation Detection Architecture) [16]where the organizations have to pose the adequate security controls**.**

The authors, Hai Jin et al [30]developed a component called VMFence to detect malicious activity in cloud using Virtual machine monitor (VMM) which isadditional computationally complex. This model orders for occurrence patternsapproaching through all VMs linked to the honored VM.Muqtyar et al [22] have utilized fog computing technique to put off malicious insiders byperplexing the masquerader. Perceptibly, decoying IT to confuse the attacker is more complex.

The researchers, Xuxian Jiang et al [5] developed VMWatcher component toidentify the malware activities that aims at supporting especially anti-malware software for outsider attacks. To work with the dynamic nature of cloud, the IDS should be developed at the cloud

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 200 - 211
Received 05 March 2021; Accepted 01 April 2021.

virtualization layer to monitor and managethe dynamic environment.The authorAmjadHussainBhat [27] et al designed VMM based IDS to perceive the cloud attacks. Two distinct machine learning algorithms are used by the virtual machine monitor based intrusion detection system. There are two approaches: 1. Navie Bayes classifier. 2. A mix of Naïve Bayes and Random Forest hybrid approach.

An anomaly detection system at the hypervisor layer was developed by the authors Pandeeswari N and Ganeshkumar P [31]. A hybrid algorithm was developed to improve the accuracy of the detection method by combining the Fuzzy C-Means clustering algorithm and the Artificial Neural Network (FCM-ANN). This model is trained and validated with the KDD cup dataset from DARPA, specifically developed for the IDS dataset.By using the fuzzy systems with neural network adaptation and learning skills called the adaptive neuro-fuzzy inference system (ANFIS) model, the authors Ganeshkumar P and Pandeeswari N [32] have developed a cloud anomaly detection system at hypervisor. A hybrid algorithm is used to train this framework, where the technique of back propagation gradient descent is combined with the least square method.

Though there are lot of cloud attack detection systems have been designed, still the system suffers with security breaches. Hence, the proposed scheme aims to provide a better solution for cloud insider attack. Here, the detection system,MID is designed by using ANN modeling and LM algorithm to detect the malicious insiders privilege the virtual cloud and this proposed work is compared ANN [27].

3. Malicious Insider Detection

Cloud virtualization expertiseencourages large amount of users to utilize the cloud infrastructure for low cost.Virtualization defines [13] as the virtual version of hardware, application, operating system, and etc. Cloud system delivering online services encounters vulnerabilities in and around the virtual environment. Cloud service provider (CSP) is responsible for providing services. Service Level Agreements play a significant role in service providers. These agreements helps in selection of different cloud service providers [25]based on their necessities. Cloud service providers [19] wish to provide resource efficiently according to the service level agreements (SLA) guaranteeing to minimize the SLA violations and maximizing resource consumptions. In some conditions, users can violate the SLAs by sending large resource request, while accessing the cloud services.

This paper discusses the malicious insiders as the authorized users who are contravening the SLAs. The features of SLA's [19] are 1.Bandwidthutilization, 2. Memory utilization and 3. Storage utilization. The deceiving cloud administrator,who is beinglacking in control over cloud service provider,wasnot capable to identify the behavior of users. The virtual machine monitor (VMM), called hypervisor provides abstraction layer between the real and virtual machines that can be able to monitor and manage the activities of virtual clients. The proposed system uses the abilities of hypervisor to monitor the virtual clients requesting for resources in virtual environment. The proposed system is designed with artificial neural network modeling technique to have a better categorization [9]of user's activity.The training algorithm, Levenberg-Marquardt (LM) back propagation (supervised learning algorithm) is used to train the MID component. Each factor is assigned with some adaptive threshold values dynamically such that BT_{thres} ,MT_{thres} and SCT_{thres} for bandwidth utilization, memory utilization and storage utilization respectively. The Levenberg – Marquradt algorithm [17], developed by Kenneth Levenberg and Donald Marquardt provides better solution to the problem of reducing a nonlinear problem. The author TummalaPradeep[16] describes the importance of LM training algorithm for ANN. The following algorithm.1 explains how this procedure works.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 200 - 211
Received 05 March 2021; Accepted 01 April 2021.

Algorithm 1

{Algorithm for detecting malicious insiders}

Input: {BT, MT, SCT}

Let $BT - bandwidthutilization$

$MT - memoryutilization$

$SCT - storageutilization$

(BT, MT, SCT) attributes of SLA

Assume BT_{thres} , MT_{thres} and SCT_{thres} be adaptive threshold value for bandwidth utilization, memory utilization and storage utilization respectively.

Output: {malicious insider, allowable users}

For i = 1 to n

$n: users$

$beginfor$

$ifBT > BT_{thres} then$

return %malicious insider %

$elseifMT > MT_{thres} then$

return %malicious insider%

$elseifSCT > SCT_{thres}$ then

return%malicious insider %

$else$

return %allow the resource allocation%

$endif$

end for

Hypervisor [15]is the cloud software, acting as the supervisory control to examine and manage the virtual machines running on the same hardware platform. For the flexible and fine grained access control for efficient resource sharing, thereby avoiding the problems with direct user-resource mapping, domain based decentralized approach [14] can be used. The virtual machines execute the guest operating systems. Virtual operating systems share the resources of virtualized hardware on host machines where the hypervisor controls the virtual operating platform. The hypervisor manages the amount of access, based on the requirements of guest OSes.The different hypervisors[30] are XEN, Virtual PC and VMware.

The cloud hypervisor based Malicious Insider Detector component is illustrated in Fig .1

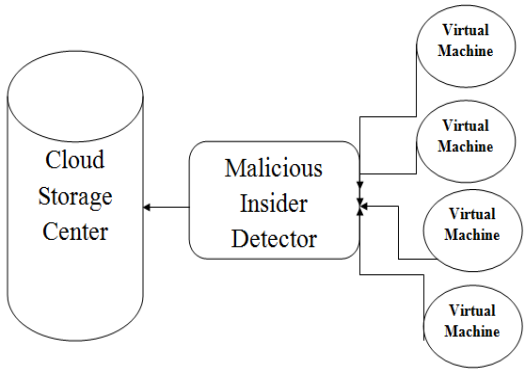

Fig. 1 Malicious Insider Detector component

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 200 - 211
Received 05 March 2021; Accepted 01 April 2021.

4. Malicious Insider Detector modeled with ANN

The Malicious Insider Detectoris designed using artificial neural network modeling that utilizesLM back propagation algorithm [10]. The conventionalorganizationtechniques necessitate lot of computational power, memory and CPU resources for the larger data sets. ANN is the most predictable learning technique [7] for machine learning methodsto advance the intelligent system concert. ANN[9]is the very significant modeling tool to make classification precisely [29] where the conventional categorization is difficult. ANN is an effective tool to replicate the capability of human brain mathematically. Neural network contains of a group of neurons which is the essential processing unit. Withnumerous neuronsworking simultaneously, the brain can stimulate quick and improved result. According to the same methodANN works with various neurons simultaneously to improve theperformance. The artificial neural network amplifies the knowledge to predict the knowledge either by supervised or unsupervised learning techniques. The supervised back propagation learning method uses the input and output condition, where the training takes place iteratively by using a set of training samples. Theconcert of the learning technique is restrained in terms of false alarm rate, which is difference between predicted result and actual result. Thefalse alarm rate has to be minimized by adjusting weights. Thefeed forward neural network (multilayer perceptron network) is used to design the malicious insider detector.

Artificial Neural Network can be defined by the following:

1. The interconnection along with the neurons in different layers.
2. The training process for adjust the weights of interconnections.
3. The activation purpose: The outcome of the layers is forwarded to the next layers where the outputs are produced using the sigmoid function.

This system has three layers

1. Input layer with three input neurons
2. Hidden layer with 30 hidden computational neurons

3.Output layer with one output neuron. The feed forward network works in forward direction layer by layer.

The Fig .2illustrates artificial neural network modeling for Malicious Insider Detector.

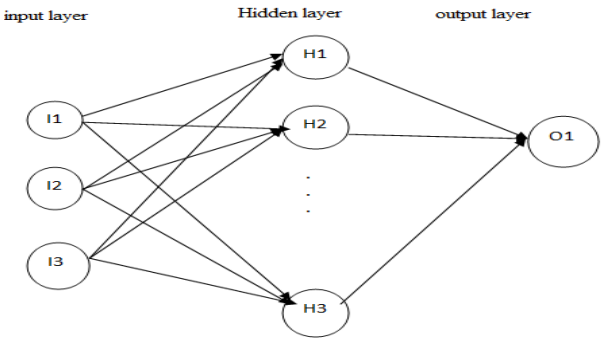

Fig.2 ANN modeling for Malicious Insider Detector

The net input $\bar{x}$ of a neuron is calculated as

$$\bar{x_j} = \sum_i w_{ij}\, x_i + w_j \qquad (1)$$

The output of a neuron is defined as,

$$x_j = f(\bar{x}_j) = \frac{1}{1+\exp(-\bar{x}_j)} \qquad (2)$$

Where,

$x_j - outputofneuronj$

$w_{ij} - weightassociatedwithconnectionbetween neuronsiandj$

$w_j - biasofnodej$

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 200 - 211
Received 05 March 2021; Accepted 01 April 2021.

$f - logisticsigmoidfunction\ (activationfunction)$

The performance of the malicious insider detector component model is validated in terms of false alarm rate and linear correlation coefficient (R). The objective of LM algorithm is to minimize the MSE and to obtain the value nearest to zero.

The false error value is determined as,

$$E = \frac{1}{p}\sum_{k=1}^{p} E_m \quad (3)$$

$E_m - canbecalculatedas,$

$$E_m = \frac{1}{2}\sum_{i=1}^{n}(d_k - x_k)^2 \quad (4)$$

Where,

$p - numberoftrainingpatterns$

$E_m - errorvaluefortrainingpatternm$

The intend of LM algorithm is to offer second order working speed without calculating Hessian matrix.

The Hessian matrix can be approximated as,

$$H = J^T J \quad (5)$$

and gradient value can be calculated as

$$g = J^T \varepsilon \quad (6)$$

Where,

$J - Jacobianmatrix$

$\varepsilon - errorvalue$

To get the gradient value, the error term ε_j for neuron j is described as,

$$\varepsilon_j = \frac{\partial E_m}{\partial \bar{x}_j} = \frac{\partial \sum_{(d_k - x_k)^2}}{\partial \overline{x_j}} \quad (7)$$

The recursive equations for ε_j can be described using chain rule

$$\varepsilon_j = \begin{cases} -2\left(d_j - x_j\right)\dfrac{\partial x_j}{\partial \bar{x}_j} = -2\left(d_j - x_j\right)x_j\left(1 - x_j\right), & if\,j\,is\,output\ neuron \\ \dfrac{\partial x_j}{\partial \bar{x}_j}\sum_{k,j<k}\dfrac{\partial E_m}{\partial \bar{x}_k}\dfrac{\partial x_j}{\partial \bar{x}_j} = x_j\left(1 - x_j\right)\sum_{k,j\leq k}\varepsilon_k w_{jk}\ , & otherwise \end{cases}$$

(8)

Where,

$w_{jk} - connectionweightfromjtok$

ifw_{jk} is zero , then no direct connection between $jandk$,then

$$\Delta w_{jk} = -\eta\frac{\partial E}{\partial w_{jk}} = -\eta\sum_p \frac{\partial E}{\partial w_{jk}} \quad (9)$$

Where,

$\eta - learningrate$

Learning rate influences the convergence speed and stability of the weights during learning. So,

$$\Delta w = -\eta\Delta_{\mathrm{w}}\mathrm{E} \quad (10)$$

Here,

$$E = \sum_m E_m \quad (11)$$

To increase the speed of the training process, momentum term can be used as follows,

$$\Delta w = -\eta\Delta_w E + \alpha\Delta w_{prev} \quad (12)$$

Where,

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 200 - 211
Received 05 March 2021; Accepted 01 April 2021.

$w_{prev} - momentumterm; previousupdatedconstant$

The linear correlation coefficient (R) can be computed as,

$$R = \frac{N\sum_{m=1}^{N} d_m x_m - (\sum_{m=1}^{N} d_p)(\sum_{m=1}^{N} x_m)}{\sqrt{\left[N\sum_{m=1}^{N} d_m^2 - (\sum_{m=1}^{N} d_p)^2\right] \mathrm{X} \left[N\sum_{m=1}^{N} x_m^2 - (\sum_{m=1}^{N} x_m)^2\right]}}$$

(13)

Where,

$d_m - desiredvalue(target)$

$x_m - outputvalueform^{th}pattern$

$N - numberofpatterns$

The performance analysis is made against the three different factors, 1.bandwidthutilization.2.memory utilization.3.storage utilization and the performance graphs are shown in figures 2, 3, 4 respectively.

5. Experimental results

The Malicious Insider Detector is designed with ANN modeling that uses Levenberg-Marquardt (LM) training algorithm. For the implementation of malicious insider detector component, VMware cloud is installed on ubuntu OS. The malicious insider detector was installed in VMware ESX. The licentious form of VM was enabled. The virtual network was formed. The malicious insider detector is used to observe and examine the virtual traffic between VMs and cloud server. The malicious insider detector analyses activities of virtual machines and captures packets intended for cloud services. The concert of the malicious insider detector is leisurely in terms of training performance. The training performance shows how well system is modeled. Besides testing and validation performances are analyzed. The percentage of data used for training, validation and testing are 90%, 25% and 25% respectively.

5.1 Performance analysis

In this work, the proposed system Malicious Insider Detectoris tested with three service level agreement parameters such as bandwidth utilization, memory utilization and storage utilization.Each parameter is assigned with adaptive threshold value. The performance of this system is measured in terms of false alarm rate.

5.1.1Bandwidthutilization

The bandwidth requirement is considered as the parameter for Service Level Agreements [19]. The Malicious Insider Detectorcomponent supervises the activities of cloud VMs. This can detect the maximum bandwidth requirement requested by the virtual client based on the adaptive threshold value. The Fig 3. shows the training, validation and testing performance of Malicious Insider Detectorfor bandwidth requirement.

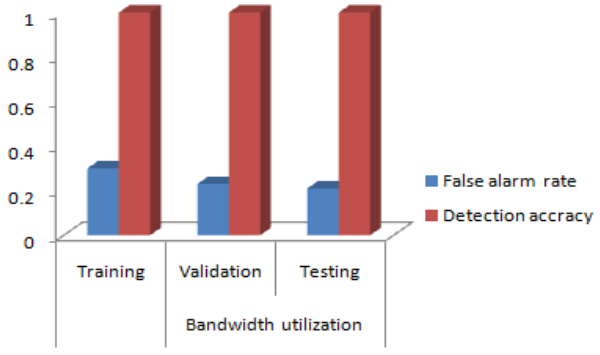

Fig 3.Performance analysis against bandwidth requirement

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 200 - 211
Received 05 March 2021; Accepted 01 April 2021.

The Fig.3 shows the false alarm value nearer to zero and detection accuracy value nearer to one. From this it is observed that how well the component has been trained to detect the malicious insiders with minimum error.

5.1.2 Memory Utilization

The memory utilization is one of the factors of Service Level Agreements [19].The cloud virtual machines which is requesting for large memory utilization (greater than memory utilization threshold) is recognized as malicious activity inside the cloud. The Fig.4 shows MSE and regression value for training, validation and testing performance of Malicious Insider Detectoragainst memory utilization requirement. From Fig. 4, it is experiential that how well the Malicious Insider Detectorcomponent has been skilled to discover the malicious insider with low false alarm rate. The false alarm rate and detection accuracy (R) values of training, validation and testing are nearer to zero and one respectively.

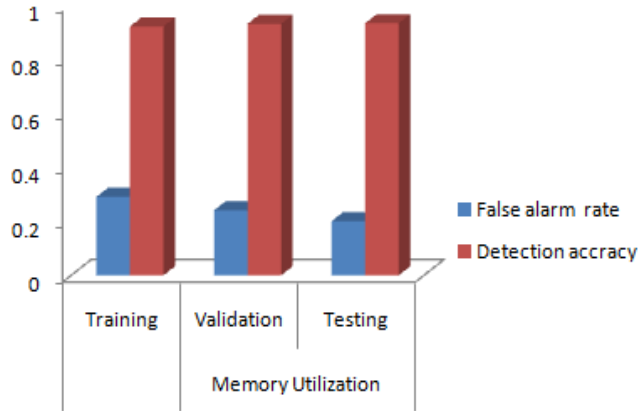

Fig 4.Performance analysis against memory utilization

5.1.3 Storage Utilization

The cloud users are enabled to use the storage as a service provided by cloud computing. However the users acquiring the agreement for resource usage should follow that one. The storage capacity requirement is also one of the factors of Service Level Agreements [19].The cloud virtual machines request for maximum storage capacity (greater than maximum threshold for storage capacity) is determined as malware within cloud. The Fig.5 shows that how well the Malicious Insider Detectorcomponent has been skilled to determine the malicious insider with little error overhead.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 200 - 211
Received 05 March 2021; Accepted 01 April 2021.

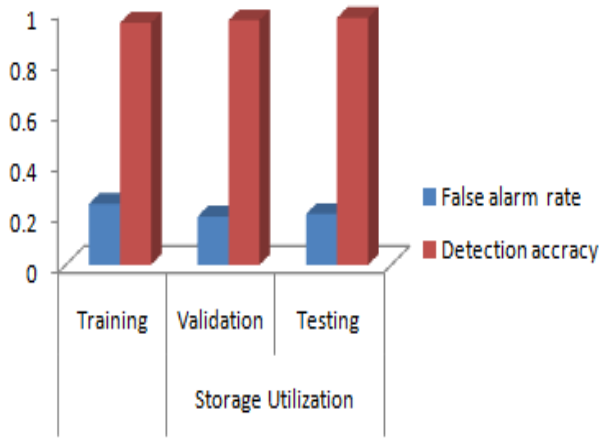

Fig 5.Performance analysis against storage utilization

Fig. 5 values show that the training, validation and testing performance of Malicious Insider Detectorfor storage utilization. The mean squared error and Regression (R) values of training, validation and testing are nearer to zero and one respectively.

The result performance analysis shows that the proposed component is designed with minimal false alarm rateand also shows that the detection accuracy nearest to one. The Figures (3-5) shows that mean squared values for each of the SLA parameters for training, validation, and testing values. From the obtained results, it is observed that the Malicious Insider Detectoris designed well and it can be able to detect malicious insiders attacking cloud resources efficiently.

However for the performance analysis of IDS, the factors detection accuracy and false alarm rate are considered as the significant factors. Theperformance of Malicious Insider Detectoris compared with IDS proposed by Naïve Bayes and hybrid approach (Naïve Bayes with Random Forest) [NBRF] [27].The Figures 6and 7 show that performance comparison of Malicious Insider Detector with the methods developed by Amjad Hussain, B et al [27] in which they have used Naïve Bayes classifier and a hybrid approach (NBRF).

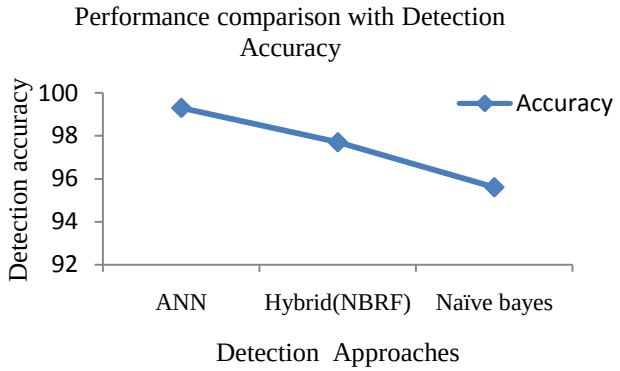

Fig. 6Output comparison of proposed Naïve Bayes work and hybrid approach (Naïve Bayes with Random Forest) using detection accuracy

In Fig.6, the Malicious Insider Detectoris compared with an IDS which is developed with Naïve Bayes and the hybrid approach against detection accuracy. The Fig.6 shows that when compared to the intrusion detection systems built using Naïve bayes and Hybrid NBRF

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 200 - 211
Received 05 March 2021; Accepted 01 April 2021.

method, the detection precision of Malicious Insider Detector is relatively high.

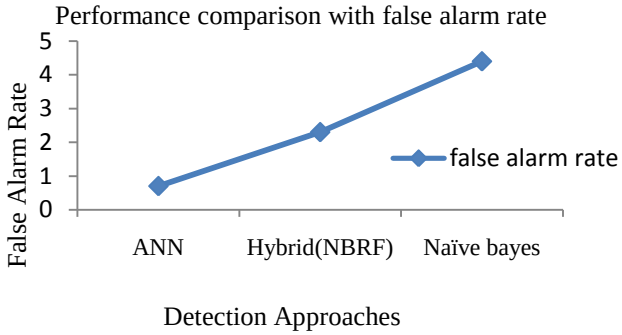

Fig. 7Output comparison of proposed Naïve Bayes work and hybrid approach (Naïve Bayes with Random Forest) in terms of False Alarm Rate.

The Fig.7 shows the comparison of the Malicious Insider Detectorwith IDS which is developed with Naïve Bayes and the hybrid approach against false alarm rate. Fromthe Fig.7, it is experimentalshows that false alarm rate of Malicious Insider Detectoris very low when compared with the intrusion detection systems established by using Naïve bayes and Hybrid NBRF approach.

From Fig.6 and 7, the Malicious Insider Detectorestablished with ANN produces high detection accuracy and low false alarm rate when linked with the approaches 1. Naïve Bayes and 2. Hybrid NBRF approach respectively.

6. Conclusion

This proposed malicious insider detector offers a best governing system called Malicious Insider Detectorto perceive the malicious insiders in virtual cloud setting where the cloud is managed by a single cloud managing domain shared with absence of control over the cloud service provider (CSP).Here, the best classification technique ANN modeling is used to design the malicious insider detector. The proposed method uses threshold values for SLA parameters to detect the malicious insiders. From, the performance comparison it can be observed that the Malicious Insider Detectorcan be the best one to detect malware actions. TheMalicious Insider Detectordesigned with ANN has high detection accuracy and low false alarm rate. Hence, this could be the efficient, robust and immediate to practical system to identify malicious insiders in the cloud environment.

References

[1] Ahmed, A., Latif, R., Latif, S. et al. Malicious insiders attack in IoT based Multi-Cloud e-Healthcare environment: A Systematic Literature Review. Multimed Tools Appl 77, 21947–21965 (2018). https://doi.org/10.1007/s11042-017-5540-x

[2]Bayer, U, Christopher, K, and Engin, K,“TTAnalyze: A Tool for Analyzing Malware,”In Proceedings of the Annual Conference of the European Institute for Computer Antivirus Research (EICAR 2006) Annual Conference, Austria. 2006. doi=10.1.1.60.7584.

[3]Rakotondravony, N., Taubmann, B., Mandarawi, W. et al. Classifying malware attacks in IaaS cloud environments. Journal of Cloud Comp 6, 26 (2017). https://doi.org/10.1186/s13677-017-0098-8

[4]Andreas, M, Christopher, K, and Engin, K, “Exploring Multiple Execution Paths for Malware Analysis,” In proceedings of IEEE Symposium on Security and Privacy, SP’07.Berkeley, CA.pp.231-245, 2007.

[5]Xuxian, J, Xinyuan Wang DongyanXu,“Stealthy Malware Detection through VMM- Based “Out-of-the-Box” Semantic View Reconstruction,” In Proceedings of 14th ACM

Conference on Computer and communications security, CCS'07,ACM New York, NY, USA, 2007, pp.128-138.

[6]Yin,H,Dawn, S, "Panorama: Capturing System-wide Information Flow for Malware Detection and Analysis," In Proceedings of the 14th ACM conference on Computer and communications security (CCS'07), ACM, NewYork, USA. pp. 116-127, 2007. doi:10.1145/1315245.1315261.

[7]PanJuinYang,J, Chun Che,F,"Artificial Intelligence in Malware -Cop or Culprit?,"In proceedings of 9th Postgraduate Electrical Engineering and Computing Symposium, (PEECS2008), Perth, W.A,pp. 181-184, 2008.

[8]Lorenzo M, Roberto P, Danilo B, "A framework for behavior Based malware analysis in the cloud," In Proceedings of 5th International Conference, (ICISS 2009), pp. 178-192, 2009. DOI: 10.1007/978-3-642-10772-6_14.

[9]Abdel-AzimM,Abdel-Fatah A.I, Mohamed A, "Performance Analysis of Artificial Neural Network Intrusion Detection Systems," In proceedings of International Conference on Electrical and Electronics Engineering, Bursa,pp.385-389, 2009.

[10] LindaO,Vollmer T, Milos M, "Neural Network Based Intrusion Detection System for Critical Infrastructures," In proceedings of International Joint Conference on Neural Networks (IJCNN 2009),pp.1827–1834, 2009.

[11]Cloud Security Alliance (CSA). Top Threats to Cloud Computing.http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf. 2010.

[12]Hassan, H.A., Maiyza, A.I. &Sheta, W.M. Integrated resource management pipeline for dynamic resource-effective cloud data center. J Cloud Comp 9, 63 (2020).
https://doi.org/10.1186/s13677-020-00212-8

[13]Mishra M, SudevalayamS,"Introduction to Cloud computing and virtualization,"http://www.cse.iitb.ac.in/convergence/workshops/Intro_to_Virtualization.pdf.2011.

[14]Shin D, Akkan H, ClaycombW,Kim K, "Toward role based provisioning and access control for infrastructure as a service (IaaS)," Internet Services and Applications, Vol.2, issue.3, pp.243–255, 2011.

[15]FarzadS, "Secure Virtualization for Cloud Environment Using Hypervisor-based Technology,"International Journal of Machine Learning and Computing,vol. 2, issue.1,pp.39-45, 2012.

[16]Emeakaroha VC, FerretoT.C,NettoM.A.S, BrandicI, De Rose C.A.F, "Casvid: Application level monitoring, for SLA violation detection in clouds," In proceedings of IEEE 36th Annual conference on Computer Software and Applications Conference (COMPSAC),IEEE, Izmir. pp: 499-508, 2012. DOI:10.1109/COMPSAC.2012.68.

[17]Hao Y, BogdanM,"Levenberg–Marquardt Training"Intelligentsystems,pp. 1-16, 2012.K10149_C012.inddpp.

[18]Montelibano J, MooreA,"Insider threat security reference architecture,"In proceedings of Hawaii International Conference on System Sciences, Hawaii.pp.2412–2421, 2012.

[19]Maurer M, Brandic I, SakellariouR,"Self-adaptive and resource-efficient SLA Enactment for cloud computing infrastructures,"In proceedings of IEEE 5th International Conference on Cloud Computing (CLOUD), Honolulu, HI. pp.368-375, 2012.

[20]Claycomb WR, Nicoll A, " Insider Threats to Cloud Computing: Directions for New Research Challenges," In proceedings of IEEE 36th Annual Conference in Computer Software and Applications Conference (COMPSAC), Izmir,pp.387–394, 2012.

[21]Cloud Security Alliance, "The Notorious Nine Cloud Computing Top Threats in 2013". http://www.cloudsecurityalliance.org/topthreats, 2013.

[22]Muqtyar Ahmed S, NamrathaP, Nagesh C, ”Prevention of Malicious Insider in the Cloud Using Decoy Documents”,International Journal of Engineering Research and Technology (IJERT), Vol. 2, issue. 4,pp.1651-1654, 2013.

[23]Apolinar G, Walter M, Alfons C, Miguel M, José F, Alvaro A, “A hypervisor based platform to support real-time safety critical embedded java applications,” Computer systems science and engineering, Vol.28, issue. 3,pp.157-168, 2013.

[24]LorenzoM, Elizabeth S, FredriksonM,Somesh J, Mitchell J, C, ”A Layered Architecture for Detecting Malicious Behaviors,” In Proceedings of the 11th international symposium on Recent Advances in Intrusion Detection, Springer- Verlag Berlin, Heidelberg. pp.78-97, 2013. doi: 10.1007/978-3-540-87403-4_5.

[25]PreetiG,Sumedha S, ”Dynamic Ranking and Selection of Cloud Providers Using Service Level Agreements,” International Journal of Advanced Research in Computer Science and Software Engineering,vol. 3, issue. 6, pp.93-101, 2013.

[26]Sanchika G, Padam K, Abraham A, ”A Profile Based Network Intrusion Detection and Prevention System for Securing Cloud Environment,” International Journal of Distributed Sensor Networks,vol.2013, pp.1-12, 2013.

[27]AmjadHussainB, Sabyasachi P, Debasish J, ” Machine Learning Approach for Intrusion Detection on Cloud Virtual Machines,” International Journal of Application or Innovation in Engineering & Management, Vol. 2, issue.6, pp. 57-66, 2013.

[28]MassimoF, Salvatore V,BeniaminoDi,M,”An advanced intrusion detection framework for cloud computing,” Computer systems Science and Engineering,Vol.8, issue.6, 2013.

[29]Donghai,Weiwei Y,”A Survey of Mislabeled Training Data Detection Techniques for Pattern Classification,” IETE Technical Review (MedknowPublications & Media Pvt. Ltd.), vol. 30, issue 6, pp.524-530, 2013.

[30]Hai J, Guofu, X,“A VMM-based intrusion prevention system in cloud computing Environment,”The Journal of Supercomputing,Springer US, Vol. 66, issue. 3, pp.1133-1151, 2013.

[31]NPandeeswari, PGaneshkumar,“Anomaly Detection System in Cloud Environment Using Fuzzy Clustering Based ANN,” Mobile Networks and Applications,vol. 21, no. 3, pp. 494 - 505, 2016.

[32] P Ganeshkumar,NPandeeswari,” Adaptive Neuro-Fuzzy-Based Anomaly Detection System in Cloud,” International journal of fuzzy systems,vol. 18, no. 3, pp. 367 - 378, 2016.